ELLIPTIC CURVES WITH RATIONAL 2-TORSION AND RELATED TERNARY DIOPHANTINE EQUATIONS

by

JAMIE THOMAS MULHOLLAND

B.Sc. Simon Fraser University, 2000
M.Sc. The University of British Columbia, 2002

A THESIS SUBMITTED IN PARTIAL FULLFILLMENT OF THE REQUIREMENTS FOR THE DEGREE OF

DOCTOR OF PHILOSOPHY

in

THE FACULTY OF GRADUATE STUDIES

Mathematics

THE UNIVERSITY OF BRITISH COLUMBIA

July 2006

Abstract

Our main result is a classification of elliptic curves with rational 2-torsion and good reduction outside 2, 3 and a prime p. This extends the work of Hadano and, more recently, Ivorra. A key factor in doing this is to have a method for efficiently computing the conductor of an elliptic curve with 2-torsion. We specialize the work of Papadopolous to provide such a method.

Next, we determine all the rational points on the hyper-elliptic curves $y^2 = x^5 \pm 2^a 3^b$. This information is required in providing the classification mentioned above. We show how the commercial mathematical software package MAGMA can be used in solving this problem.

As an application, we turn our attention to the ternary Diophantine equations $x^n + y^n = 2^a p z^2$ and $x^3 + y^3 = \pm p^m z^n$, where p denotes a fixed prime. In the first equation, we show that for $p = 5$ or $p > 7$ the equation is unsolvable in integers (x, y, z) for all suitably large primes n. In the second equation, we show the same conclusion holds for an infinite collection of primes p. To do this, we use the connections between Galois representations, modular forms, and elliptic curves which were discovered by Frey, Hellegouarch, Serre, and Wiles.

Table of Contents

List of Tables

Acknowledgement

It gives me great pleasure to thank the many people and organizations who have helped me to get where I am today.

I am very grateful for financial support from the University of British Columbia and from NSERC.

To the many teachers who have guided me to where I am today – thanks for your knowledge, wisdom, and inspiration.

I owe an enormous debt to my supervisor, Dr. Michael Bennett, for having guided me through my PhD, sharing his knowledge, wisdom and experience of mathematics with me along the way.

My fiancée, Heather, who has offered love and support through thick and thin – my deepest thanks.

And my family, whose love and support, encouragement and guidance, have always been complete, and whose belief in me has enabled me to get to this point, the warmest thanks of all.

To Heather – my love, my life

Chapter 1
Introduction

1.1 Introduction to Diophantine Equations

The study of Diophantine equations has a long and rich history, dating to the "Arithmetica" of Diophantus, written in the middle of the 3rd century, and dealing with the solution of algebraic equations and the theory of numbers. Much of modern number theory, as we know it, stems from tools developed to solve Diophantine equations.

By a Diophantine equation, we mean, intuitively, an equation where we are interested only in integer and/or rational solutions. For example the equation

$$x^2 + y^2 = z^2$$

has the following solutions in positive integers (x, y, z):

$$(3, 4, 5), (5, 12, 13), (8, 15, 17), (7, 24, 25).$$

In fact, there are infinitely many solutions in positive integers to this equation, and they can be parametrized: any solution (with y even, say) is of the form

$$(d(u^2 - v^2), 2uvd, d(u^2 + v^2))$$

where $u, v, d \in \mathbb{Z}$ and $gcd(u, v) = 1$. On the other hand, the equations

$$x^3 + y^3 = z^3, \;\; x^4 + y^4 = z^4, \;\; \text{and } x^5 + y^5 = z^5$$

have only the trivial solutions; solutions where one of the values is 0. Fermat[1]

[1] 1601 - 1665.

wrote in the margin of his copy of Arithmetica that, in fact, the equation

$$x^n + y^n = z^n$$

has no nontrivial solutions for any $n \geq 3$, and commented that he had a marvelous proof of this fact but the margin was too small to contain it. This became known as Fermat's "Last Theorem" [2]. The quest to prove (or disprove, for that matter) Fermat's Last Theorem became the driving force for modern number theory over the last three hundred years. Amateurs and professionals alike all had their crack at a proof. Their attempts gave birth to many new beautiful ideas and tools that are used in number theory today, though, for more than three centuries, none were enough to resolve Fermat's enigma. After the work of Godel on "undecidability" in formal systems, many wondered whether the truth of Fermat's Last Theorem was even decidable. Ten years ago, Andrew Wiles announced a proof verifying Fermat's Last Theorem and finally putting to rest Fermat's challenge. Wiles attacked the problem by treating a more general question regarding the connection between elliptic curves and modular forms. We'll say more on this in our final two chapters.

Consider the Diophantine equation

$$y^2 = x^3 + 1.$$

The only integer solutions are

$$(-1, 0), (0, \pm 1), (2, \pm 3).$$

These are, in fact, the only rational solutions. On the other hand, the Diophantine equation

$$y^2 = x^3 + 17$$

has 16 integer solutions

$$(-2, \pm 3), (-1, \pm 4), (2, \pm 5), (4, \pm 9), (8, \pm 23),$$

$$(43, \pm 282), (52, \pm 375), (5234, \pm 378661),$$

[2] "Last" because it was the remaining conjecture of his that needed resolving.

and infinitely many rational solutions. Both of these curves are examples of elliptic curves. A curve of the form

$$E: \ y^2 + a_1xy + a_3y = x^3 + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

with $a_i \in \mathbb{Z}$ is called an *elliptic curve* (provided it is nonsingular). For curves in *Weierstrass form*

$$y^2 = x^3 + a_2x^2 + a_4x + a_6$$

the condition of being nonsingular is equivalent to the cubic on the right-hand side having distinct roots (i.e. nonzero discriminant). For elliptic curves it is known that the number of integral points is finite (Siegel's theorem, see [69]), but the number of rational points could possibly be infinite. Though the proof of Siegel's theorem was not effective (i.e. did not give a method to find all the integral points) de Weger [30], using Baker's work on bounding linear forms in logarithms, was able to give an algorithm for finding all the integral points on an elliptic curve.

The set of rational points $E(\mathbb{Q})$ on an elliptic curve carry an abelian group structure, the identity being the point at infinity which we denote by O (or sometimes ∞). That is, there is a natural way to add two rational points $P_1, P_2 \in E(\mathbb{Q})$ to obtain a third rational point $P_3 = P_1 + P_2$. Geometrically, this is done by taking the (rational) line through P_1 and P_2 and letting P_4 be the third point of intersection of the line with E. Next, take the vertical line through P_4 (i.e. the line through P_4 and O) and let P_3 be the other point of intersection with E, and set $P_1 + P_2 = P_3$. Mordell showed that $E(\mathbb{Q})$ is finitely generated and abelian so it is of the form

$$E(\mathbb{Q}) \simeq E(\mathbb{Q})_{tors} \times \mathbb{Z}^r$$

where $E(\mathbb{Q})_{tors}$ is a finite group consisting of the torsion elements and r is an integer called the *rank* of E. $E(\mathbb{Q})_{tors}$ is straightforward to compute; a theorem of Nagell and Lutz gives a method for computing its points. Moreover, a general result of Mazur ([50], [51]) states that it can only be one of 15 possible groups (see for example [69], p. 223). However, there is no known algorithm for computing the rank of an elliptic curve. There are methods (i.e. a 2-descent) that work on bounding the rank. One can then hope to find enough

independent points to meet this bound to obtain the rank exactly. In practice this works quite well. For our two examples above we have

$$E_1 : y^2 = x^3 + 1,\ E_1(\mathbb{Q}) \simeq \mathbb{Z}/6\mathbb{Z}$$
$$E_2 : y^2 = x^3 + 17,\ E_2(\mathbb{Q}) \simeq \mathbb{Z}^2.$$

A *hyperelliptic curve* is a curve of the form

$$y^2 = f(x)$$

where, for our purpose, $f \in \mathbb{Z}[x]$ of degree $2g + 1$. The integer g is called the *genus* of the curve. For example, an elliptic curve is a genus 1 hyperelliptic curve. However, unlike the situation for elliptic curves, a celebrated theorem of Faltings states that $C(\mathbb{Q})$ is finite when $g \geq 2$. Unfortunately, Faltings theorem is not effective, but older work of Chabauty has recently been revived and in practice often works very well in determining $C(\mathbb{Q})$. For a hyperelliptic curve C the set of rational points do not form a group, but $C(\mathbb{Q})$ does embed into a finitely generated abelian group called the *Jacobian* of C, denoted $J(\mathbb{Q})$. The work of Chabauty requires calculation in the Jacobian. In Chapter 5 we occupy ourselves with determining the rational points on curves of the form $y^2 = x^5 \pm 2^a 3^b$. Chapter 5 can be read independently of all other chapters. It provides an introduction to the theory and practice of computing all rational points on genus 2 curves, with a heavy emphasis on using MAGMA as a computational tool, something the current literature is somewhat lacking. The results of this chapter are used in proofs of the Diophantine lemmata of Chapter 4.

1.2 Generalized Fermat Equations

In relation with Fermat's last theorem the equation

$$x^p + y^q = z^r \tag{1.1}$$

has a long history. For a very fine survey on this topic see [45]. Here, we will provide a very brief outline of what is known.

The *characteristic* of equation (1.1) is defined to be $\chi(p,q,r) = \frac{1}{p} + \frac{1}{q} + \frac{1}{r} - 1$, and the study of these equations has been broken up into three cases: $\chi(p,q,r) > 0$ (spherical case), $\chi(p,q,r) = 0$ (euclidean case), and $\chi(p,q,r) < 0$ (hyperbolic case). Let $S(p,q,r)$ be the set of nontrivial proper solutions to equation (1.1).

In the spherical case, $S(p,q,r)$ is infinite and there are in fact parametized solutions. In this case the possible sets of $\{p,q,r\}$ are $\{2,2,r\}$ with $r \geq 2$, $\{2,3,3\}$, $\{2,3,4\}$, and $\{2,3,5\}$, and the proper solutions correspond to rational points on genus 0 curves.

In the euclidean case, possible sets of $\{p,q,r\}$ are $\{3,3,3\}$, $\{2,4,4\}$, and $\{2,3,6\}$, and the points in $S(p,q,r)$ corresponds to rational points on genus 1 curves. It is known that the only proper nontrivial solution corresponds to the equality $1+2^3 = 3^2$. We have already mentioned that $S(3,3,3)$ was empty and the fact that $S(2,4,4)$ is empty was first proven by Fermat using an argument of infinite descent.

In the hyperbolic case there are only ten known solutions to date:

$$1^p + 2^4 = 3^2, \;\; 2^5 + 7^2 = 3^4, \;\; 7^3 + 13^2 = 2^9, \;\; 2^7 + 17^3 = 71^2,$$

$$3^5 + 11^4 = 122^2, \;\; 17^7 + 76271^3 = 21063928^2, \;\; 1414^3 + 2213459^2 = 65^7,$$

$$9262^3 + 15312283^2 = 113^7, \;\; 43^8 + 96222^3 = 30042907^2,$$

$$33^8 + 1549034^2 = 15613^3.$$

Notice that an exponent of 2 appears in each solution. This leads to the following conjecture.

Conjecture 1.1 *If* $min\{p,q,r\} \geq 2$ *and* $S(p,q,r) \neq \emptyset$ *then* $min\{p,q,r\} = 2$.

A number of names can be associated with this conjecture, including Beukers, Zagier (who incidently found the five larger solutions above in 1993), Tijdeman, Granville and Beal.

The first known result in the hyperbolic case is due to Darmon and Granville [27]. They used Faltings' theorem to show that $S(p,q,r)$ is finite. Next was Wiles' proof of Fermat's last theorem; $S(n,n,n) = \emptyset$. Since then a number of specific cases have been tackled using the modularity of elliptic curves (Wiles, et al), and Chabauty techniques. Some cases are as follows.

(p, q, r)	
$(n, n, 2)$	Darmon, Merel (Poonen for $n \in \{5, 6, 9\}$)
$(n, n, 3)$	Darmon, Merel (Lucas $n = 4$, Poonen for $n = 5$)
$(3, 3, n)$	Kraus for $17 \leq n \leq 10000$, Bruin for $n = 4, 5$
$(2, 4, n)$	Ellenberg for $n \geq 211$, Bruin for $n = 5, 6$,
	Bennett, Ellenberg, Ng for $n \geq 7$
$(2, n, 4)$	Bennett, Skinner
$(2, 3, 7)$	Poonen, Schaefer, Stoll
$(2, 3, 8)$	Bruin
$(2, 3, 9)$	Bruin
$(2, 2n, 3)$	Chen for $7 \leq n \leq 1000, n \neq 31$
$(5, 5, n), (7, 7, n)$	Darmon and Kraus (partial results)
$(2n, 2n, 5)$	Bennett
$(4, 2n, 3)$	Bennett, Chen

1.3 Statement of Principal Results

Modularity techniques have since been applied to generalized Fermat equations with coefficients:

$$Ax^p + By^q = Cz^r.$$

Here, A, B, C, p, q, and r are fixed integers and we are interested in integral solutions for x, y and z. If $p = q = r$, then results have been obtained by Serre [64] for $A = B = 1$ and $C = N^\alpha$, $\alpha \geq 1$, with

$$N \in \{3, 5, 7, 11, 13, 17, 19, 23, 29, 53, 59\}, \quad N \neq p, \quad p \geq 11,$$

Kraus [41] for $ABC = 15$, Darmon and Merel [28] for $ABC = 2$, and Ribet [61] for $ABC = 2^\alpha$, $\alpha \geq 2$. If $(p, q, r) = (p, p, 2)$ then results have been obtained by Bennett and Skinner [5] for various A, B, C, Ivorra [36] for $ABC = 2^\beta$, and Ivorra and Kraus [38] for various A, B, and C. If $(p, q, r) = (p, p, 3)$ then Bennett, Vatsal and Yazdani [6] have shown

Theorem 1.2 (Bennett, Vatsal, Yazdani) *If p and n are prime, and α is a nonnegative integer, then the Diophantine equation*

$$x^n + y^n = p^\alpha z^3$$

has no solutions in coprime integers x, y and z with $|xy| > 1$ and $n > p^{4p^2}$.

Their proof of this proceeds as follows. Attach to a supposed solution (a, b, c) an elliptic curve $E = E_{a,b,c}$ with a 3-torsion point, and to this a Galois representation $\rho_{E,n}$ on the n-torsion points. To $\rho_{E,n}$ there corresponds a cuspidal newform $f_{E,n}$ of weight 2 and level $N_n(E)$, where $N_n(E)$ can be explicitly determined. It then remains to show that such a newform f cannot exist. In doing this, it is shown that the existence of f implies either n is bounded by p^{4p^2} or that there exists an elliptic curve over $\mathbb{Q}$ with rational 3-torsion and conductor $3^\tau p^\omega$. Hence a classification of such curves is needed to finish the argument.

In Chapter 8, we apply a similar argument to the equation

$$x^n + y^n = 2^\alpha p z^2$$

and prove the following

Theorem 1.3 (Bennett, Mulholland) *Let $p \neq 7$ be prime. Then the equation*

$$x^n + y^n = 2^\alpha p z^2$$

has no solutions in coprime nonzero integers x and y, positive integers z and α, and prime n satisfying $n > p^{27p^2}$.

A key ingredient in the proof is a classification of the elliptic curves with conductor $2^M p^2$ and possessing a rational 2-torsion point. In Chapter 6, we provide such a classification.

In Chapter 9, we study the equation

$$x^3 + y^3 = \pm p^m z^n,$$

where p is prime and prove the following,

Theorem 1.4 (Mulholland) *Let $p \in T$ and $m \geq 1$ an integer. Then the equation*

$$x^3 + y^3 = \pm p^m z^n$$

has no solutions in coprime nonzero integers x, y and z, and prime n satisfying $n \geq p^{8p}$ and $n \nmid m$.

Here T denotes the set of primes p for which there does not exist an elliptic curve with rational 2-torsion and conductor $2^M 3^2 p$, $1 \leq M \leq 3$. Thus, in this case we need a classification of the elliptic curves with conductor $2^M 3^2 p$, $1 \leq M \leq 3$, and possessing a rational 2-torsion point. In Chapter 7, we provide such a classification.

Since we are interested in elliptic curves of conductor $2^M p^2$ or $2^M 3^L p$ and possessing a rational point of order 2 we start by considering the following more general question.

Problem 1 *Determine all the $\mathbb{Q}$-isomorphism classes for elliptic curves over $\mathbb{Q}$ of conductor $2^M 3^L p^N$ and having at least one rational point of order 2.*

As is well-known, there do not exist any elliptic curves defined over $\mathbb{Q}$ with conductor divisible by 2^9, 3^6, or q^3 for $q \geq 5$ prime (see e.g. Papadopoulos [57]). Furthermore, as we show in Chapter 2, the existence of rational 2-torsion implies the conductor is not divisible by 3^3. Therefore, we can suppose in the statement of problem 1 that

$$0 \leq M \leq 8 \text{ and } 0 \leq L, N \leq 2.$$

In addition, a theorem of Shafarevich states that there are only finitely many isomorphism classes, for fixed p (see [69] p. 263).

The first work on Problem 1 appears to have be done by Ogg in 1966, [55], [56]. He determined the elliptic curves defined over $\mathbb{Q}$ with conductor of the form $2^M 3^L$ or $2^M 3$. Coghlan in his dissertation [17] also studied the curves of conductor $2^M 3^L$ independently of Ogg. Vélu [78] classified curves of conductor 11, and in general Setzer [66] answers Problem 1 for any prime conductor. He shows that there are two distinct isomorphism classes when $p - 64$ is a square, and four when $p = 17$. Hadano [34] begins treatment of conductors p^N and $2^M p^N$, and Ivorra, in his dissertion [37], classifies those of conductor $2^M p$.

There has been other work in classifying elliptic curves with conductors of a particular form and specified torsion structure. Most notable are the works of Hadano [35] and Miyawaki [53].

In Chapter 3, we take up Problem 1 in general. In Section 3.1, we obtain results analogous to those of Ivorra for conductor $2^N p^2$. In Sections 3.2 and 3.3

we obtain results for conductor $2^N 3^L p$ and $2^N 3^L p^2$, respectively, thus completing the remaining cases of Problem 1. As seen from glancing at the table of contents, the tables presented account for 120+ pages of this work (not to mention the 30+ pages of refined tables in Chapter 6, and the 40+ pages of technical case by case analysis in Appendix A). We have tried to tidy this work up as best we can and make it readable but, unfortunately, there is no way to fully condense it; the tables are what they are – long and technical. But we believe the determination of these tables provides a useful public service.

As seen from glancing at the tables in Chapter 3, one is mainly confronted, as in [66] and [37], with the problem of determining the integer solutions of certain ternary Diophantine equations. In Chapter 4, we take up the problem of resolving these Diophantine equations. We then come back the tables of Chapter 3 with these solutions at hand. This allows us to simplify the tables, these results appear in Chapters 6 and 7.

Some of the works mentioned above regarding Problem 1 treat the following more general problem, which we do not know how to attack in general.

Problem 2 *Determine all the $\mathbb{Q}$-isomorphism classes for elliptic curves over $\mathbb{Q}$ of conductor $2^M 3^L p^N$.*

Let us note that Brumer and McGuinness have determined the elliptic curves of conductor $p < 10^8$. The definitive web source for tables of all the elliptic curves of conductor < 130000 is John Cremona's home page [3]. These tables are constantly being expanded so the reader should check the web page to determine their extent at this time. The techniques Cremona uses for constructing his tables (and, indeed, a fine introduction to the arithmetic of elliptic curves) can be found in his excellent book [26] which is available for download from his web page. In addition, Cremona has prepared tables for conductor $2^k m^2$ with $m \leq 23$ prime and also $m = 15$ and 21.

1.4 Overview of chapters

A brief outline of the contents of each chapter is as follows.

In Chapter 2, we specialize the results of Papadopolous [57] to the problem of computing the conductor of an elliptic curve with a rational 2 torsion point,

[3] www.maths.nottingham.ac.uk/personal/jec/

i.e. curves of the form

$$y^2 = x^3 + ax^2 + bx.$$

There we present an easy criterion for computing the conductor. The results of this section are used throughout the rest of this work.

Chapter 3 is the first step toward our classifying problem. Here we present twenty-seven theorems, one for each value of $2^M 3^L p^N$, listing the $\mathbb{Q}$-isomorphism classes of the elliptic curves with that conductor. The proof is long and tedious but not that technical, it depends on two main lemmata which are proven in Appendix A. It is in these tables that we are confronted with the problem of determining the integer solutions to certain ternary Diophantine equations. In order to get a useful classification theorem we need to resolve these Diophantine equations. This is taken up in Chapter 4.

In order to solve some of the Diophantine equations, it is sufficient to find all $\{2, 3, \infty\}$-integral points on the genus 1 curves

$$y^2 = x^3 \pm 2^\alpha 3^\beta,$$

and the genus 2 curves

$$y^2 = x^5 \pm 2^\alpha 3^\beta.$$

We deal with the former in Appendix B and the latter in Chapter 5.

Having these Diophantine results at hand, we come back to the tables of Chapter 3. In Chapter 6, we present nine theorems classifying elliptic curves of conductor $2^M p^2$ possessing a rational 2-torsion point. These table are analogous to those of Ivorra [37]. In Chapter 7, we investigate the admissible p for which there exist curves of conductor $2^M 3^2 p$, $1 \leq M \leq 3$, with rational 2-torsion. These results will be used in Chapter 9.

In Chapters 8 and 9, we look at what can be said about the generalized Fermat equations

$$x^n + y^n = 2^\alpha p z^2 \text{ and } x^3 + y^3 = \pm p^m z^n,$$

respectively. A modified version of Chapter 8 has appeared in print [4].

Chapter 2

The Conductor of an Elliptic Curve over $\mathbb{Q}$ with 2-torsion

In this chapter, we specialize the work of Papadopolous [57] to elliptic curves over $\mathbb{Q}$ with nontrivial 2-torsion:

$$y^2 = x^3 + ax^2 + bx,$$

and show that the exponent of 2 in the conductor of the curve is determined by the values $v_2(a)$ and $v_2(b)$ and some simple congruences of a and b modulo 2, 4 and 8. Here v_p denotes the p-adic valuation on $\mathbb{Q}$.

2.1 Introduction

Let E be the elliptic curve over $\mathbb{Q}$ defined by

$$E : y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

with $a_i \in \mathbb{Z}$. Let b_2, b_4, b_6, b_8, c_4, c_6, and Δ be the standard invariants associated with E:

$$b_2 = a_1^2 + 4a_2, \;\; b_4 = a_1a_3 + 2a_2, \;\; b_6 = a_3^2 + 4a_6 \tag{2.1}$$

$$b_8 = a_1^2a_6 - a_1a_3a_4 + 4a_2a_6 + a_2a_3^2 - a_4^2 \tag{2.2}$$

$$c_4 = b_2^2 - 24b_4, \;\; c_6 = -b_2^3 + 36b_2b_4 - 216b_6 \tag{2.3}$$

$$\Delta = -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6. \tag{2.4}$$

The conductor of an elliptic curve over $\mathbb{Q}$ is defined to be

$$N = \prod_p p^{f_p}$$

where $f_p = v_p(\Delta)+1-n_p$. Here n_p is the number of irreducible components of the special fibre of the minimal Néron model at the prime p (see [69]). Essentially, N is an encoding of the primes for which E has bad reduction and the reduction types at these primes. E has *bad reduction* at a prime p if and only if $p \mid N$, and the reduction type of E at p is *multiplicative* (E has a node over $\mathbb{F}_p$) or *additive* (E has a cusp over $\mathbb{F}_p$) depending on whether $f_p = 1$ or ≥ 2, respectively. It is well known that for $p \neq 2, 3$, the value of f_p is completely determined by the values of $v_p(c_4)$, $v_p(c_6)$ and $v_p(\Delta)$. This is not always the case when $p = 2$ or 3. Papadopolous [57] has determined when the triple $(v_2(c_4), v_2(c_6), v_2(\Delta))$ (resp. $(v_3(c_4), v_3(c_6), v_3(\Delta))$) is not sufficient to determine the value of f_2 (resp. f_3) and in these cases he has given supplementary conditions involving the values of a_1, a_2, a_3, a_4, a_6, b_2, b_4, b_6 and b_8. In the case of the prime 3 these supplementary conditions involve checking a single congruence involving c_4 and c_6 modulo 9. However, for the prime 2 the supplementary conditions are a little more complicated. One usually needs to check a number of congruences in sequence for solutions. Furthermore, in the case when $(v_2(c_4), v_2(c_6), v_2(\Delta)) = (6, \geq 9, 12)$ one is unable to decide from Table IV in [57] whether f_2 is 5 or 6 (whereby one is forced to apply Tate's algorithm directly).

If E is an elliptic curve over $\mathbb{Q}$ with nontrivial 2-torsion then E is isomorphic to a curve of the form

$$y^2 = x^3 + ax^2 + bx,$$

where $a, b \in \mathbb{Z}$ are such that $v_p(a) \geq 2$ and $v_p(b) \geq 4$ do not both hold for all p. The discriminant in this case is

$$\Delta = 2^4 b^2 (a^2 - 4b).$$

In this chapter, we show that for such curves the conditions one needs to check in [57] simplify greatly. In fact, the value of f_2 is completely determined by the values of $v_2(a)$, $v_2(b)$ and the congruence classes of a and b modulo 4, with one exception. In this exceptional case, $v_2(\Delta) = 8$, one needs to check a congruence involving a and b modulo 8 (see Theorem 2.1).

2.2 Statement of Results.

Let p denote a prime ≥ 5. We will prove the following theorems.

Theorem 2.1 *If $a, b \in \mathbb{Z}$ are such that not both $v_2(a) \geq 2$ and $v_2(b) \geq 4$ hold, then the Néron type at 2 of the elliptic curve $y^2 = x^3 + ax^2 + bx$ is given by Tables 2.1 and 2.2 on pages 15 and 16. In the cases where $f_2 = 0$ or 1 the model $y^2 = x^3 + ax^2 + bx$ is non-minimal at 2, this is indicated in Table 2.1 by the appearance of "non-minimal" in the corresponding column. In the cases where $f_2 \neq 0, 1$ the model $y^2 = x^3 + ax^2 + bx$ is minimal at 2.*

During the course of the proof of Theorem 2.1 we will also deduce the following.

Corollary 2.2 *In the case that the model $E(a, b) : y^2 = x^3 + ax^2 + bx$ is non-minimal at 2 we have the following:*

1. *If $v_2(a) = 0$, $v_2(b) \geq 4$ and $a \equiv 1 \pmod 4$ then*

$$y^2 + xy = x^3 + \left(\frac{a-1}{4}\right)x^2 + \left(\frac{b}{16}\right)x$$

   is a minimal model for $E(a, b)$ at 2.

2. *If $v_2(a) = 1$, $v_2(b) = 0$, $v_2(\Delta) \geq 12$ and $\frac{a}{2} \equiv -1 \pmod 4$ then*

$$y^2 + xy = x^3 + \left(\frac{-(a+2)}{8}\right)x^2 + \left(\frac{-(a^2-4b)}{64}\right)x + \left(\frac{a(a^2-4b)}{512}\right)$$

   is a minimal model for $E(a, b)$ at 2.

Theorem 2.3 *If $a, b \in \mathbb{Z}$ are such that not both $v_3(a) \geq 2$ and $v_3(b) \geq 4$ hold, then the Néron type at 3 of the elliptic curve $y^2 = x^3 + ax^2 + bx$ is given by Table 2.3 on page 16. In all cases the model $y^2 = x^3 + ax^2 + bx$ is minimal at 3.*

Theorem 2.4 *Let p be a prime ≥ 5. If $a, b \in \mathbb{Z}$ are such that not both $v_p(a) \geq 2$ and $v_p(b) \geq 4$ hold, then the Néron type at p of the elliptic curve $y^2 = x^3 + ax^2 + bx$ is given by Table 2.4 on page 16. In all cases the model $y^2 = x^3 + ax^2 + bx$ is minimal at p.*

We have the following corollary to Theorems 2.3 and 2.4.

Corollary 2.5 *Let q be an odd prime. If $a, b \in \mathbb{Z}$ such that not both $v_q(a) \geq 2$ and $v_q(b) \geq 4$ hold and $N_{(a,b)}$ is the conductor of the elliptic curve $y^2 = x^3 + ax^2 + bx$ then:*

(i) $q \mid N_{(a,b)}$ *if and only if* $q \mid \Delta = 2^4 b^2 (a^2 - 4b)$,

(ii) if $q \parallel N_{(a,b)}$ *then* q *does not divide* a,

(iii) $q^2 \parallel N_{(a,b)}$ *if and only if* q *divides* a *and* b.

$v_2(a)$ $v_2(b)$	0 0				0 1		0 2		0 3	
$v_2(\Delta)$										
Supplementary conditions	$a \equiv 1\,(4)$ $b \equiv 1\,(4)$	$a \equiv 1\,(4)$ $b \equiv -1\,(4)$	$a \equiv -1\,(4)$ $b \equiv 1\,(4)$	$a \equiv -1\,(4)$ $b \equiv -1\,(4)$		$a \equiv 1\,(4)$	$a \equiv -1\,(4)$		$a \equiv 1\,(4)$	$a \equiv -1\,(4)$
Kodaira symbol	II	IV	III	II	III	I_1^*	I_0^*		III^*	I_2^*
Case of Tate	3	5	4	3	4	7	6		9	7
Exponent $v_2(N)$ of conductor	4	2	3	4	5	3	4		3	4

$v_2(a)$ $v_2(b)$	0 4		0 ≥ 5		1 0	
$v_2(\Delta)$	8				7	
Supplementary conditions	$a \equiv 1\,(4)$ non-minimal	$a \equiv -1\,(4)$	$a \equiv 1\,(4)$ non-minimal	$a \equiv -1\,(4)$	$a - b \equiv 13\,(16)$	$a - b \equiv 5\,(16)$
Kodaira symbol	I_0	I_4^*	$\mathrm{I}_{v_2(\Delta)-12}$	$\mathrm{I}^*_{v_2(\Delta)-8}$	II	I_0^*	I_1^*
Case of Tate	1	7	7	7	3	6	7
Exponent $v_2(N)$ of conductor	0	4	1	4	7	4	3

$v_2(a)$ $v_2(b)$	1 0		1 0		1 0		1 0	
$v_2(\Delta)$	8 (con't)		9		10		11	
Supplementary conditions	$a - b \equiv 1\,(16)$	$a - b \equiv 9\,(16)$		$\frac{a}{2} \equiv 1\,(4)$	$\frac{a}{2} \equiv -1\,(4)$	$\frac{a}{2} \equiv 1\,(4)$	$\frac{a}{2} \equiv -1\,(4)$	
Kodaira symbol	I_0^*	IV^*	I_0^*	I_2^*	III^*	I_3^*	II^*	
Case of Tate	6	8	6	7	9	7	10	
Exponent $v_2(N)$ of conductor	4	2	5	4	3	4	3	

$v_2(a)$ $v_2(b)$	1 0		1 0		1 1	1 2	1 ≥ 3	≥ 2 0		≥ 2 1
$v_2(\Delta)$	12		≥ 13							
Supplementary conditions	$\frac{a}{2} \equiv 1\,(4)$	$\frac{a}{2} \equiv -1\,(4)$ non-minimal	$\frac{a}{2} \equiv 1\,(4)$	$\frac{a}{2} \equiv -1\,(4)$ non-minimal					$b \equiv 1\,(4)$	$b \equiv -1\,(4)$
Kodaira symbol	I_4^*	I_0	$\mathrm{I}^*_{v_2(\Delta)-8}$	$\mathrm{I}_{v_2(\Delta)-12}$	III	I_0^*	$\mathrm{I}^*_{v_2(\Delta)-10}$	II	III	III
Case of Tate	7	1	7	2	4	6	7	3	4	4
Exponent $v_2(N)$ of conductor	4	0	4	1	7	6	6	6	5	8

Table 2.1: Néron type at 2 of $y^2 = x^3 + ax^2 + bx$.

$v_2(a)$	2		2	≥ 3		≥ 3
$v_2(b)$	2		3	2		3
$v_2(\Delta)$						
Supplementary conditions	$\frac{b}{4} \equiv 1\ (4)$	$\frac{b}{4} \equiv -1\ (4)$		$\frac{b}{4} \equiv 1\ (4)$	$\frac{b}{4} \equiv -1\ (4)$	
Kodaira symbol	$\mathrm{I}^*_{v_2(\Delta)-10}$	I^*_2	III^*	I^*_3	I^*_2	III^*
Case of Tate	7	7	9	7	7	9
Exponent $v_2(N)$ of conductor	6	7	7	5	6	8

Table 2.2: Néron type at 2 of $y^2 = x^3 + ax^2 + bx$ (con't).

$v_3(a)$	0		0	≥ 1	≥ 1	1	≥ 2	≥ 2
$v_3(b)$	0		≥ 1	0	1	≥ 2	2	3
Supplementary conditions	$b \equiv 1\ (3)$	$b \equiv -1\ (3)$						
Kodaira symbol	$\mathrm{I}_{v_3(\Delta)}$	I_0	$\mathrm{I}_{v_3(\Delta)}$	I_0	III	$\mathrm{I}^*_{v_3(\Delta)-6}$	I^*_0	III^*
Case of Tate								
Exponent $v_3(N)$ of conductor	1	0	1	0	2	2	2	2

Table 2.3: Néron type at 3 of $y^2 = x^3 + ax^2 + bx$.

$v_p(a)$	0		0	≥ 1	≥ 1	1		1	≥ 2	≥ 2
$v_p(b)$	0		≥ 1	0	1	2		≥ 3	2	3
Supplementary conditions	$a^2 \not\equiv 4b\ (p)$	$a^2 \equiv 4b\ (p)$				$a^2 \not\equiv 4b\ (p^3)$	$a^2 \equiv 4b\ (p^3)$			
Kodaira symbol	I_0	$\mathrm{I}_{v_p(\Delta)}$	$\mathrm{I}_{2v_p(b)}$	I_0	III	I^*_0	$\mathrm{I}^*_{v_p(\Delta)-6}$	$\mathrm{I}^*_{2v_p(b)-4}$	I^*_0	III^*
Case of Tate										
Exponent $v_p(N)$ of conductor	0	1	1	0	2	2	2	2	2	2

Table 2.4: Néron type at p of $y^2 = x^3 + ax^2 + bx$.

2.3 The Proof of Theorem 2.1.

We prove this theorem using the work of Papadopolous [57][1] except in cases (ix) $v_2(a) = 1$, $v_2(b) = 2$ and (xiv) $v_2(a) = 2$, $v_2(b) = 2$ where we will need to apply Tate's algorithm directly. The seventeen cases we consider are labeled as follows:

	(i)	(ii)	(iii)	(iv)	(v)	(vi)	(vii)	(viii)	(ix)
$v_2(a)$	0	0	0	0	0	0	1	1	1
$v_2(b)$	0	1	2	3	4	≥ 5	0	1	2

	(x)	(xi)	(xii)	(xiii)	(xiv)	(xv)	(xvi)	(xvii)
$v_2(a)$	1	1	≥ 2	≥ 2	2	2	≥ 3	≥ 3
$v_2(b)$	3	≥ 4	0	1	2	3	2	3

The standard invariants for the curve

$$y^2 = x^3 + ax^2 + bx$$

are (see (2.1))

$$a_1 = 0,\ \ a_2 = a,\ \ a_3 = 0,\ \ a_4 = b,\ \ a_6 = 0,$$

$$b_2 = 4a,\ \ b_4 = 2b,\ \ b_6 = 0,\ b_8 = -b^2,$$

$$c_4 = 2^4(a^2 - 3b),\ \ c_6 = 2^5 a(9b - 2a^2),\ \ \Delta = 2^4 b^2(a^2 - 4b).$$

Some of the cases immediately follow from Table IV of [57] so we quickly deal with these first. We have the following table.

	$v_2(a)$	$v_2(b)$	$v_2(c_4)$	$v_2(c_6)$	$v_2(\Delta)$	Case of Tate	Kodaira	f_2
(viii)	1	1	5	7	8	4	III	7
(ix)	1	2	≥ 6	8	10	6	I_0^*	6
(xi)	1	≥ 4	6	9	≥ 14	7	$\mathrm{I}^*_{v_2(\Delta)-10}$	6
(xiii)	≥ 2	1	5	≥ 8	9	4	III	8
(xv)	2	3	7	10	14	9	III*	7
(xvii)	≥ 3	3	7	≥ 11	15	9	III*	8

[1] Errata: In the column labeled *Equation non minimale* of table IV in [57] the first column should read $[4, 6, \geq 12]$ not $[4, 6, 12]$.

As for the remaining cases, we must check the supplementary conditions in [57].

(i) When $v_2(a) = 0$ and $v_2(b) = 0$ we have

$$v_2(c_4) = \begin{cases} 5 & \text{if } b \equiv 1 \pmod 4, \\ \geq 6 & \text{if } b \equiv -1 \pmod 4, \end{cases} \quad v_2(c_6) = 5, \;\; v_2(\Delta) = 4.$$

If $b \equiv 1 \pmod 4$ then from Table IV of [57] we are in case 3 or 4 of Tate. We use Proposition 1 of *loc. cit.* with $r = t = 1$. The congruence

$$a_4 + a_2 = b + a \equiv \begin{cases} 2 \pmod 4 & \text{if } a \equiv 1 \pmod 4, \\ 0 \pmod 4 & \text{if } a \equiv -1 \pmod 4, \end{cases}$$

implies that if $a \equiv 1 \pmod 4$ we are in case 3 of Tate and $f_2 = 4$. So assume $a \equiv -1 \pmod 4$, whence we are in case ≥ 4 of Tate. Using Proposition 2 of *loc. cit.* with $r = 1$ and since

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 2(1 + 2a) \not\equiv 0 \pmod 8,$$

we are in case 4 of Tate and $f_2 = 3$.

On the other hand, if $b \equiv -1 \pmod 4$ then from Table IV of [57], we are in case 3 or 5 of Tate. Take $r = t = 1$ in Proposition 1 of *loc. cit.*. It follows from the congruence

$$a_4 + a_2 = b + a \equiv \begin{cases} 0 \pmod 4 & \text{if } a \equiv 1 \pmod 4, \\ 2 \pmod 4 & \text{if } a \equiv -1 \pmod 4, \end{cases}$$

that if $a \equiv -1 \pmod 4$, we are in case 3 of Tate and $f_2 = 4$, whereas if $a \equiv 1 \pmod 4$, we are in case 5 of Tate and $f_2 = 2$.

(ii) When $v_2(a) = 0$ and $v_2(b) = 1$ we have

$$v_2(c_4) = 4, \;\; v_2(c_6) \geq 7, \;\; v_2(\Delta) = 6,$$

so, from Table IV of [57], we are in case 3 or 4 of Tate. Using $r = t = 0$ in Proposition 1 of *loc. cit.*, it follows that we are in case 4 of Tate and $f_2 = 5$.

(iii) When $v_2(a) = 0$ and $v_2(b) = 2$ we have

$$v_2(c_4) = 4, \;\; v_2(c_6) = 6, \;\; v_2(\Delta) = 8.$$

and, from Table IV of [57], we are in case 6, 7 or 8 of Tate. We use Proposition 3 of [57]. The integer $r = 2$ satisfies the congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \pmod{32}.$$

The integer $t = 2$ satisfies the congruence

$$a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \equiv 0 \pmod{8}.$$

Moreover, for $r = t = 2$ we have the congruence

$$a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \equiv 2b + 4a + 4 \equiv 0 \pmod{16}.$$

if and only if $a \equiv 1 \pmod 4$. It follows from Proposition 3 of *loc. cit.* that if $a \equiv -1 \pmod 4$ we are in case 6 of Tate and $f_2 = 4$, whereas if $a \equiv 1 \pmod 4$ then we are in case ≥ 7 of Tate. So assume $a \equiv 1 \pmod 4$ and that we are in case ≥ 7 of Tate. Take $r = 2$ in Proposition 4 of *loc. cit.*. The congruence

$$0 \equiv a_2 + 3r - ta_1 - t^2 \equiv 3 - t^2 \pmod 4$$

has no solutions for t thus it follows that we are in case 7 of Tate and $f_2 = 3$.

(iv) When $v_2(a) = 0$ and $v_2(b) = 3$ we have

$$v_2(c_4) = 4, \;\; v_2(c_6) = 6, \;\; v_2(\Delta) = 10,$$

and, from Table IV of [57], we are in case 7 or 9 of Tate. The integer $r = 0$ satisfies the congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \pmod{32}.$$

Moreover, we have the congruence

$$0 \equiv a_2 + 3r - ta_1 - t^2 \equiv \begin{cases} 1 - t^2 \pmod 4 & \text{if } a \equiv 1 \pmod 4, \\ 3 - t^2 \pmod 4 & \text{if } a \equiv -1 \pmod 4, \end{cases}$$

has a solution for t if and only if $a \equiv 1 \pmod 4$. It follows from Proposition 4 of *loc. cit.* that if $a \equiv -1 \pmod 4$, we are in case 7 of Tate and $f_2 = 4$, whereas if $a \equiv 1 \pmod 4$, we are in case 9 of Tate and $f_2 = 3$.

(v) When $v_2(a) = 0$ and $v_2(b) = 4$ we have

$$v_2(c_4) = 4, \;\; v_2(c_6) = 6, \;\; v_2(\Delta) = 12,$$

and, from Table IV of [57], we are in case 7 of Tate or the model is non-minimal. The integer $r = 0$ satisfies the congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \pmod{32}.$$

Moreover, the congruence

$$0 \equiv a_2 + 3r - ta_1 - t^2 \equiv \begin{cases} 1 - t^2 \pmod 4 & \text{if } a \equiv 1 \pmod 4, \\ 3 - t^2 \pmod 4 & \text{if } a \equiv -1 \pmod 4, \end{cases}$$

has a solution for t if and only if $a \equiv 1 \pmod 4$. It follows from Proposition 4 of *loc. cit.* that if $a \equiv -1 \pmod 4$, we are in case 7 of Tate and $f_2 = 4$, whereas if $a \equiv 1 \pmod 4$ the model is non-minimal. In the latter case, consider the change of variables

$$x = 4X, \;\; y = 8Y + 4X.$$

We obtain the new model with integer coefficients

$$(a_1', a_2', a_3', a_4', a_6') = (1, \frac{a-1}{4}, 0, \frac{b}{16}, 0),$$

and such that $v_2(c_4') = 0$, $v_2(c_6') = 0$, and $v_2(\Delta') = 0$. Hence we are in case 1 of Tate and $f_2 = 0$.

(vi) When $v_2(a) = 0$ and $v_2(b) \geq 5$ we have

$$v_2(c_4) = 4, \;\; v_2(c_6) = 6, \;\; v_2(\Delta) \geq 14,$$

and, from Table IV of [57], we are in case 7 of Tate or the model is non-minimal. The integer $r = 0$ satisfies the congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \pmod{32}.$$

Moreover, the congruence

$$0 \equiv a_2 + 3r - ta_1 - t^2 \equiv \begin{cases} 1 - t^2 \pmod 4 & \text{if } a \equiv 1 \pmod 4, \\ 3 - t^2 \pmod 4 & \text{if } a \equiv -1 \pmod 4, \end{cases}$$

has a solution for t if and only if $a \equiv 1 \pmod 4$. It follows from Proposition 4 of *loc. cit.* that if $a \equiv -1 \pmod 4$, we are in case 7 of Tate and $f_2 = 4$, whereas if $a \equiv 1 \pmod 4$ the model is non-minimal. In the latter case, take the change of variables

$$x = 4X, \;\; y = 8Y + 4X$$

to obtain the new model with integer coefficients

$$(a_1', a_2', a_3', a_4', a_6') = (1, \frac{a-1}{4}, 0, \frac{b}{16}, 0).$$

Then $v_2(c_4') = 0$, $v_2(c_6') = 0$, and $v_2(\Delta') \geq 2$, whence we are in case 2 of Tate and $f_2 = 1$.

(vii) When $v_2(a) = 1$ and $v_2(b) = 0$ we have

$$v_2(c_4) = 3, \;\; v_2(c_6) = 6, \;\; v_2(\Delta) \geq 7.$$

We consider the cases $v_2(\Delta) = 7, 8, 9, 10, 11, 12, \geq 13$ separately.

If $v_2(\Delta) = 7$ then from Table IV of [57] we are in case 3 of Tate and $f_2 = 7$.

If $v_2(\Delta) = 9$ then from Table IV of [57] we are in case 6 of Tate and $f_2 = 5$.

In the remaining cases; $v_2(\Delta) = 8, 10, 11, 12, \geq 13$, some work is required to determine f_2. We defer the proof for these cases until Section 2.4.

(x) When $v_2(a) = 1$ and $v_2(b) = 3$ we have

$$v_2(c_4) = 6, \;\; v_2(c_6) \geq 9, \;\; v_2(\Delta) = 12,$$

and from Table IV of [57] we are in case 7 of Tate. There are, however, two possibilities for f_2. We need to apply Tate's algorithm directly in this case.

We will use the pseudocode for Tate's algorithm given in [26]. It is straightforward to check that we may pass directly to line 42 in *loc. cit.* without having to make any changes to our model. Furthermore, in the notation of *loc. cit.* since $xa3 = \frac{a_3}{4} = 0$ is even, $xa6 = \frac{a_6}{16} = 0$ is even, and $xa4 = \frac{a_4}{8} = \frac{b}{8}$ is odd we exit the loop after line 54, with $m = 2$. Thus $f_2 = v_2(\Delta) - 6 = 6$ and the Kodaira symbol is I_2^*.

(xii) When $v_2(a) \geq 2$ and $v_2(b) = 0$ we have

$$v_2(c_4) = 4, \;\; v_2(c_6) \geq 7, \;\; v_2(\Delta) = 6,$$

so, from Table IV of [57], we are in case 3 or 4 of Tate. Take $r = 1$ and $t = 0$ in Proposition 1 of *loc. cit.*. It follows from the congruence

$$a_6+ra_4+r^2a_2+r^3-ta_3-t^2-rta_1 = b+a+1 \equiv \begin{cases} 2 \pmod 4 & \text{if } b \equiv 1 \pmod 4, \\ 0 \pmod 4 & \text{if } b \equiv -1 \pmod 4, \end{cases}$$

that if $b \equiv 1 \pmod 4$, we are in case 3 of Tate and $f_2 = 6$, whereas if $b \equiv -1 \pmod 4$, we are in case 4 of Tate and $f_2 = 5$.

(xiv) When $v_2(a) = 2$ and $v_2(b) = 2$ we have

$$v_2(c_4) = 6, \;\; v_2(c_6) = 9, \;\; v_2(\Delta) \geq 13,$$

so, from Table IV of [57], we are in case 7 of Tate. There are, however, two possibilities for f_2 depending on whether $v_2(\Delta) = 13$ or $v_2(\Delta) \geq 14$. We claim $v_2(\Delta) = 13$ if and only if $b/4 \equiv -1 \pmod{16}$. Indeed, since $\Delta = 16b^2(a^2 - 4b)$, the hypothesis on a and b imply

$$v_2(\Delta) = 13 \iff v_2\left(\left(\frac{a}{4}\right)^2 - \frac{b}{4}\right) = 1.$$

But $(a/4)^2 \equiv 1 \pmod 4$, from which the claim follows. Thus, $f_2 = 7$ if $b/4 \equiv -1 \pmod 4$ and $f_2 = 6$ if $b/4 \equiv 1 \pmod 4$.

(xvi) When $v_2(a) \geq 3$ and $v_2(b) = 2$ we have

$$v_2(c_4) = 6, \;\; v_2(c_6) \geq 10, \;\; v_2(\Delta) = 12,$$

and, from Table IV of [57], we are in case 7 of Tate. There are, however, two possibilities for f_2. We need to apply Tate's algorithm directly in this case.

Again, we will use the pseudocode for Tate's algorithm given in [26]. We consider the cases $b/4 \equiv -1 \pmod 4$ and $b/4 \equiv 1 \pmod 4$ separately.

Suppose $b/4 \equiv -1 \pmod 4$. Before starting the algorithm let us first make the change of variables

$$x = X + 2, \;\; y = Y$$

so our new model has coefficients

$$a_1 = 0, \;\; a_2 = a + 6, \;\; a_3 = 0, \;\; a_4 = b + 4a + 12, \;\; a_6 = 2b + 4a + 8.$$

It follows that

$$v_2(a_2) = 1, \;\; v_2(a_4) = 3, \;\; v_2(a_6) \geq 5,$$

where we've used the fact that $b/4 \equiv -1 \pmod 4$. It is straight forward to check that we may pass directly to line 42 in *loc. cit.* without having to make any changes to our model. Furthermore, in the notation of *loc. cit.* since $xa3 = \frac{a_3}{4} = 0$ is even, $xa6 = \frac{a_6}{16}$ is even, and $xa4 = \frac{a_4}{8}$ is odd, we exit the loop after line 54, with $m = 2$. Thus $f_2 = v_2(\Delta) - 6 = 6$ and the Kodaira symbol is I_2^*.

Suppose $b/4 \equiv 1 \pmod 4$. Similar to above, we first make the change of variables

$$x = X + 6, \;\; y = Y + 4$$

to obtain a new model with coefficients

$$a_1 = 0, \;\; a_2 = a + 18, \;\; a_3 = 8, \;\; a_4 = b + 12a + 108, \;\; a_6 = 6b + 36a + 200,$$

and find

$$v_2(a_2) = 1, \;\; v_2(a_3) = 3, \;\; v_2(a_4) \geq 4, \;\; v_2(a_6) \geq 5,$$

(here we've used the fact that $b/4 \equiv 1 \pmod 4$). Moreover,

$$v_2(b_2) = 3, \;\; v_2(b_4) \geq 5, \;\; v_2(b_6) = 3, \;\; v_2(b_8) \geq 7.$$

It is straightforward to check that we may pass directly to line 42 in *loc. cit.* without having to make any changes to our model. Furthermore, in the notation of *loc. cit.* since $xa3 = \frac{a_3}{4} = 0$, $xa6 = \frac{a_6}{16}$, and $xa4 = \frac{a_4}{8}$ are all even, we have from line 56 that

$$r = \begin{cases} 4 & \text{if } \frac{a_6}{32} \text{ is odd,} \\ 0 & \text{if } \frac{a_6}{32} \text{ is even.} \end{cases}$$

We then must apply the change of variables transcoord$(r, 0, 0, 1)$ at line 59. In either case the change of variables leads to a curve $(a_1', a_2', a_3', a_4', a_6')$ such that

$$a_1' = 0, \;\; v_2(a_2') = 1, \;\; v_2(a_3') = 3, \;\; v_2(a_4') \geq 4, \;\; v_2(a_6') \geq 5.$$

We have now reached the end of the loop and return back to line 45. Since $xa3 = \frac{a_3'}{8}$ is odd we exit the loop after line 47 with $m = 3$. Thus $f_2 = v_2(\Delta) - 7 = 5$ and the Kodaira symbol is I_3^*.

To finish the proof it remains to verify the cases when $v_2(a) = 1$, $v_2(b) = 0$, and $v_2(\Delta) = 8, 10, 11, 12$, and ≥ 13. We do this in the next section.

2.4 The case when $v_2(a) = 1$, $v_2(b) = 0$.

We have already determined in part (iv) of the proof of Theorem 2.1 the values of f_2 when $v_2(\Delta) = 7$ or 9. In this section we determine the value of f_2 for the remaining cases: $v_2(\Delta) = 8$, 10, 11, 12, ≥ 13. First we make two observations.

Lemma 2.6 *If $a, b \in \mathbb{Z}$ such that $v_2(a) = 1$, $v_2(b) = 0$ and $v_2(\Delta) = v_2(16b^2(a^2 - 4b)) \geq 8$ then $b \equiv 1 \pmod 4$. Furthermore, if $v_2(\Delta) = 8$ then $b \equiv 5 \pmod 8$.*

Proof. If $v_2(\Delta) = v_2(16b^2(a^2 - 4b)) \geq 8$ then $v_2((\frac{a}{2})^2 - b)) \geq 2$. It follows that $b \equiv 1 \pmod 4$ since $a/2$ is odd. Moreover, if $v_2(\Delta) = 8$ then $v_2((\frac{a}{2})^2 - b) = 2$ thus $b \neq 1 \pmod 8$. □

We will use the next lemma when applying Proposition 4 of [57].

Lemma 2.7 *For $a, b \in \mathbb{Z}$ such that $v_2(a) = 1$ and $v_2(b) = 0$ the congruence*

$$-b^2 + 6r^2b + 4r^3a + 3r^4 \equiv 0 \pmod{32}$$

has no solutions for r if $b \equiv -1 \pmod 4$, whereas for $b \equiv 1 \pmod 4$ it has solutions

$$r = \begin{cases} 3 & \text{if } a \equiv 2 \pmod 8, \\ 1 & \text{if } a \equiv 6 \pmod 8. \end{cases}$$

Proof. If $b \equiv -1 \pmod 4$ then the congruence has no solutions mod 8 (when a is even). So, it certainly can't have any solutions mod 32.

Assume $b \equiv 1 \pmod 4$ and write $b = 4k + 1$ for some $k \in \mathbb{Z}$. If $a \equiv 2 \pmod 8$ then we may write $a = 8\ell + 2$ for some $\ell \in \mathbb{Z}$. Taking $r = 3$ we have

$$-b^2 + 6r^2b + 4r^3a + 3r^4 \equiv 16k(k + 1) \equiv 0 \pmod{32}.$$

Similarly, one can easily show $r = 1$ is a solution when $a \equiv 6 \pmod 8$. □

2.4.1 Proof of Theorem 2.1 part (vii) when $v_2(\Delta) = 8$

It follows from Lemma 2.6 that $b \equiv 5 \pmod 8$. Since $v_2(c_4) = 4$, $v_2(c_6) = 6$ and $v_2(\Delta) = 8$ it follows from Table IV of [57] that we are in case 6, 7 or 8 of Tate. We use Proposition 3 of *loc. cit.*. By Lemma 2.7 the congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \pmod{32}$$

has solutions

$$r = \begin{cases} 3 & \text{if } a \equiv 2 \pmod 8, \\ 1 & \text{if } a \equiv 6 \pmod 8. \end{cases}$$

In either case the integer $t = 2$ satisfies the congruence

$$a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \equiv rb + r^2a + r^3 - t^2 \equiv 4 - t^2 \equiv 0 \pmod 8.$$

Fix $t = 2$ and r as above.

Suppose $a \equiv 2 \pmod 8$. We have the congruence

$$a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \equiv 3b + 9a + 7 \equiv 0 \pmod{16}$$

if and only if $a - b \equiv 5 \pmod{16}$. Thus, we are in case 6 of Tate (and $f_2 = 4$) if $a - b \equiv 13 \pmod{16}$, and in case ≥ 7 of Tate if $a - b \equiv 5 \pmod{16}$. So, suppose the latter holds. Taking $r = 3$ in Proposition 4 of *loc. cit.* the congruence

$$a_2 + 3r - sa_1 - s^2 \equiv 3 - s^2 \equiv 0 \pmod 4$$

has no solution for s, whereby we are in case 7 of Tate and $f_2 = 3$. In the statement of the theorem we do not need to include the condition $a \equiv 2 \pmod 8$ since this automatically follows from the congruences $b \equiv 5 \pmod 8$ and $a - b \equiv 5$ or $13 \pmod{16}$.

Now suppose $a \equiv 6 \pmod 8$. We have the congruence

$$a_6 + ra_4 + r^2a_2 + r^3 - ta_3 - t^2 - rta_1 \equiv b + a - 3 \equiv 0 \pmod{16}$$

if and only if $a - b \equiv 9 \pmod{16}$. Thus, we are in case 6 of Tate (and $f_2 = 4$) if $a - b \equiv 1 \pmod{16}$ and in case ≥ 7 of Tate if $a - b \equiv 9 \pmod{16}$. So, suppose the latter holds. Taking $r = 1$ in Proposition 4 of *loc. cit.* the congruence

$$a_2 + 3r - sa_1 - s^2 \equiv 1 - s^2 \equiv 0 \pmod 4$$

has solution $s = 1$, whereby we are in case 8 of Tate and $f_2 = 2$. Again, we do not need to include the condition $a \equiv 6 \pmod 8$ in the statement of the theorem since it follows automatically from $b \equiv 5 \pmod 8$ and $a - b \equiv 1$ or $9 \pmod{16}$.

2.4.2 Proof of Theorem 2.1 part (vii) when $v_2(\Delta) = 10$

In this case we have

$$v_2(c_4) = 4, \;\; v_2(c_6) = 6, \;\; v_2(\Delta) = 10,$$

so from Table IV of [57] we are in case 7 or 9 of Tate. We use Proposition 4 of *loc. cit.* to distinguish between these two cases. By Lemma 2.7, the congruence

$$b_8 + 3rb_6 + 3r^2b_4 + r^3b_2 + 3r^4 \equiv 0 \pmod{32}$$

has solutions

$$r = \begin{cases} 3 & \text{if } a \equiv 2 \pmod 8), \\ 1 & \text{if } a \equiv 6 \pmod 8). \end{cases}$$

Furthermore, the congruence

$$0 \equiv a_2 + 3r - t^2 \equiv \begin{cases} 3 - t^2 \pmod 4 & \text{if } a \equiv 2 \pmod 8, \\ 1 - t^2 \pmod 4 & \text{if } a \equiv 6 \pmod 8, \end{cases}$$

has solution $t = 1$ if $a \equiv 6 \pmod 8$ and no solution for t otherwise. Thus, we are in case 9 of Tate if $a \equiv 6 \pmod 8$ and in case 7 of Tate if $a \equiv 2 \pmod 8$. The assertion follows.

2.4.3 Proof of Theorem 2.1 part (vii) when $v_2(\Delta) = 11$

In this case

$$v_2(c_4) = 4, \;\; v_2(c_6) = 6, \;\; v_2(\Delta) = 11,$$

so, from Table IV of [57], we are in case 7 or 10 of Tate. By exactly the same argument as in Section 2.4.2, if $a \equiv 6 \pmod 8$, we are in case 10 of Tate and if $a \equiv 2 \pmod 8$, we are in case 7 of Tate. The assertion follows.

2.4.4 Proof of Theorem 2.1 part (vii) when $v_2(\Delta) = 12$

In this case

$$v_2(c_4) = 4, \;\; v_2(c_6) = 6, \;\; v_2(\Delta) = 12,$$

so, from Table IV of [57], we are in case 7 of Tate or the model is non-minimal. By exactly the same argument as in section 2.4.2, if $a \equiv 2 \pmod 8$, we are in case 7 of Tate and if $a \equiv 6 \pmod 8$, the model is non-minimal. In the case that the model is non-minimal, we make the change of variables

$$x = 4X - a/2, \;\; y = 8Y + 4X. \tag{2.5}$$

The new model has coefficients

$$(a_1', a_2', a_3', a_4', a_6') = \left(1, -\frac{a+2}{8}, 0, -\frac{a^2-4b}{64}, \frac{a(a^2-4b)}{512}\right), \tag{2.6}$$

which are all integers (by assumptions on a and b). Also, $v_2(c_4') = 0$, $v_2(c_6') = 0$, and $v_2(\Delta') = 0$, whence we are in case 1 of Tate and $f_2 = 0$.

2.4.5 Proof of Theorem 2.1 part (vii) when $v_2(\Delta) \geq 13$

In this case

$$v_2(c_4) = 4, \;\; v_2(c_6) = 6, \;\; v_2(\Delta) \geq 13,$$

so, from Table IV of [57], we are in case 7 of Tate or the model is non-minimal. By exactly the same argument as in section 2.4.2, if $a \equiv 2 \pmod 8$, we are in case 7 of Tate and if $a \equiv 6 \pmod 8$, the model is non-minimal. In the case that the model is non-minimal we take the change of variables (2.5) which gives us a new integral model with coefficients as in (2.6). Since $v_2(c_4') = 0$, $v_2(c_6') = 0$, and $v_2(\Delta') \geq 1$, we are in case 2 of Tate and $f_2 = 1$.

This completes the proof of Theorem 2.1.

2.5 The Proof of Theorem 2.3.

We can quickly deal with the following cases by using Table II of [57].

$v_3(a)$	$v_3(b)$	$v_3(c_4)$	$v_3(c_6)$	$v_3(\Delta)$	Case of Tate	Kodaira	f_3
0	≥ 1	0	0	≥ 2	2	$\mathrm{I}_{v_3(\Delta)}$	1
≥ 1	0	1	≥ 3	0	1	I_0	0
1	≥ 2	2	3	≥ 6	6 or 7	$\mathrm{I}^*_{v_3(\Delta)-6}$	2
≥ 2	1	2	≥ 5	3	4	III	2
≥ 2	2	3	≥ 6	6	6	I^*_0	2
≥ 3	3	4	≥ 8	9	9	III*	2

There are only three remaining cases to check: (1) $v_2(a) = 0$, $v_2(b) = 0$; (2) $v_2(a) = 1$, $v_2(b) = 1$; (3) $v_2(a) = 2$, $v_2(b) = 3$.
(1) Suppose $v_3(a) = 0$ and $v_3(b) = 0$. Then $v_2(c_4) = 0$, $v_3(c_6) = 0$, and 3 divides Δ if and only if $b \equiv 1 \pmod 3$. It follows that

$$f_3 = \begin{cases} 1 & \text{if } b \equiv 1 \pmod 3, \\ 0 & \text{if } b \equiv -1 \pmod 3, \end{cases}$$

and the Néron type at 3 is $\mathrm{I}_{v_3(\Delta)}$ if $b \equiv 1 \pmod 3$ and I_0 if $b \equiv -1 \pmod 3$.
(2) Suppose $v_3(a) = 1$ and $v_3(b) = 1$. Then $v_2(c_4) \geq 2$, $v_3(c_6) = 3$, and $v_3(\Delta) = 3$. We consider the intervening condition P_2 in Table II of [57]. P_2 is decided if we have

$$\left(2^5 \left(\frac{a}{3}\right)\left(b - 2\left(\frac{a}{3}\right)^2\right)\right)^2 + 2 \equiv 3 \cdot 2^4 \left(\left(\frac{a}{3}\right)^2 - \frac{b}{3}\right) \pmod 9,$$

or equivalently

$$\left(\frac{a}{3}\right)^4 \left(\frac{b}{3}\right) + \left(\frac{a}{3}\right)^2 + 2\left(\frac{b}{3}\right) - 1 \equiv 0 \pmod 9,$$

Since $v_3(a) = v_3(b) = 1$, this is certainly the case. Therefore $f_3 = 2$ and the Néron type at 3 is III.
(3) Suppose $v_3(a) = 2$ and $v_3(b) = 3$. Then $v_2(c_4) \geq 4$, $v_3(c_6) = 6$, and $v_3(\Delta) = 9$. We consider the intervening condition P_5 in Table II of [57]. P_5 is decided if we have

$$\left(2^5 \left(\frac{a}{9}\right)\left(\frac{b}{9} - 2\left(\frac{a}{9}\right)^2\right)\right)^2 + 2 \equiv 3 \cdot 2^4 \left(\left(\frac{a}{9}\right)^2 - \frac{b}{27}\right) \pmod 9,$$

or equivalently

$$\left(\frac{a}{9}\right)^4\left(\frac{b}{27}\right)+\left(\frac{a}{9}\right)^2+2\left(\frac{b}{27}\right)-1\equiv 0 \pmod 9,$$

Since $v_3(a)=2$ and $v_3(b)=3$, this is the case. Therefore $f_3=2$ and the Néron type at 3 is III*.

2.6 The Proof of Theorem 2.4.

We can quickly deal with the following cases by using Table I of [57].

$v_p(a)$	$v_p(b)$	$v_p(c_4)$	$v_p(c_6)$	$v_p(\Delta)$	Case of Tate	Kodaira	f_p
0	≥ 1	0	0	≥ 2	2	$\mathrm{I}_{2v_p(b)}$	1
≥ 1	0	0	≥ 1	0	1	I_0	0
≥ 1	1	1	≥ 2	3	4	III	2
1	≥ 3	2	3	≥ 8	7	$\mathrm{I}^*_{2v_p(b)-4}$	2
≥ 2	2	2	≥ 4	6	6	I^*_0	2
≥ 2	3	3	≥ 5	9	9	III*	2

There are only two remaining cases to check: (1) $v_2(a)=0$, $v_2(b)=0$; (2) $v_2(a)=1$, $v_2(b)=2$.
(1) Suppose $v_2(a)=0$, $v_2(b)=0$. In this case, p can divide at most one of c_4, c_6 and Δ. If p does not divide Δ then $f_p=0$. If $p\mid\Delta$ then p does not divide c_4 or c_6, whence $f_2=1$ and the Néron type at p is $\mathrm{I}_{v_p(\Delta)}$.
(2) Suppose $v_2(a)=1$, $v_2(b)=2$. Then $v_p(c_4)\geq 2$, $v_p(c_6)\geq 3$, and $v_p(\Delta)\geq 6$. Moreover, in this case, p^3 can divide at most one of a^2-3b, $9b-2a^2$ and a^2-4b. If $v_p(\Delta)\geq 7$, i.e. $a^2-4b\equiv 0 \pmod{p^3}$, then we are in case 7 of Tate, $f_p=2$, and the Néron type at p is $\mathrm{I}^*_{v_p(\Delta)-6}$. On the other hand, if $v_p(\Delta)=6$, i.e. $a^2-4b\not\equiv 0 \pmod{p^3}$, then we are in case 6 of Tate, $f_p=2$, and the Néron type at p is I^*_0.

This proves Theorem 2.4.

Chapter 3

Classification of Elliptic Curves over $\mathbb{Q}$ with 2-torsion and conductor $2^\alpha 3^\beta p^\delta$

Let p be a prime number and L, M and N integers satisfying the inequalities

$$p \geq 5, \;\; 0 \leq M \leq 8, \;\; \text{and} \;\; 0 \leq L, N \leq 2.$$

In what follows we announce twenty-seven theorems which describe, up to $\mathbb{Q}$-isomorphism, all the elliptic curves over $\mathbb{Q}$, of conductor $2^M 3^L p^N$, having a rational point of order 2 over $\mathbb{Q}$. The first nine theorems list curves of conductor $2^M p^2$. The next nine list curves of conductor $2^M 3^L p$, and the last nine list those of conductor $2^M 3^L p^2$. Together, with the work of Ogg on conductor 2^M, Coghlan on conductor $2^M 3^L$, Setzer on prime conductor, and Ivorra on conductor $2^M p$, this completes the classification problem of curves with bad reduction at 2, 3, and $p \geq 5$, and having rational 2-torsion.

The results which are obtained are presented in the form of tables analogous to those of [26] and [37]. Each row consists of an elliptic curve of $\mathbb{Q}$ realizing the desired conditions. The columns of the table consist of the following properties of E:

i. A minimal model of E of the form

$$y^2 + a_1 xy = x^3 + a_2 x^2 + a_4 x + a_6,$$

where the a_i are in $\mathbb{Z}$; except in the cases when $N < 2$, in these cases minimal models could be found using Corollary 2.2 but we choose not to do this here. All models listed are chosen such that $a_1 = a_3 = a_6 = 0$, so in the statements of these theorems we omit the columns corresponding to these coefficients.

ii. The factorization of the discriminant Δ of E.

Also appearing in the table are letters of identification (A,B,...) for each elliptic curve. Our usage of such letters is inspired by the tables of Cremona (and [37]) but one should not attempt to assign any meaning to our labeling other than the following. The curves which are labeled by the same letter are linked by an isogeny over $\mathbb{Q}$ of degree 2 or a composition of two such isogenies. For example if two curves are labeled A1 and A2 then they are linked by a degree 2 isogeny, whereas if four curves are labeled A1, A2, A3, and A4 then A1 is linked to each of the other three by a two isogeny and A2, A3, A4, are linked to each other by degree 4 isogenies. Moreover, they are numbered in the order of how they are to be determined.

Notations

a. For each elliptic curve E over $\mathbb{Q}$, we denote by E' the elliptic curve over $\mathbb{Q}$ obtained from E by a twist by $\sqrt{-1}$.

b. Given an integer n which is a square in $\mathbb{Z}$ we denote, in the rest of this work, by $\sqrt{n}$ the square root of n satisfying the following condition:

$$\begin{cases} \sqrt{n} \equiv 1 \bmod 4 & \text{if } n \text{ is odd} \\ \sqrt{n} \geq 0 & \text{if } n \text{ is even .} \end{cases} \tag{3.1}$$

3.1 Curves of Conductor $2^\alpha p^2$

The tables presented here are an intermediate step in the classification problem for curves of conductor $2^\alpha p^2$. In Chapter 6, we refine these tables by using the Diophantine lemmata of Chapter 4 to resolve the Diophantine equations in the tables below. If the reader is interested in a classification of curves of conductor $2^N p^2$ then it would be best to look at the results in Chapter 6 for the "polished" tables. The results here are strictly transitional.

3.1.1 Statement of Results

Theorem 3.1 *The elliptic curves E defined over $\mathbb{Q}$, of conductor p^2, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *$p = 7$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	minimal model	T_2	Δ
A1	$7 \cdot 3$	$2^4 \cdot 7$	$[1, -1, 0, -2, -1]$	2	7^3
A2	$-7^2 \cdot 3$	$2^4 \cdot 7^3$	$[1, -1, 0, -107, 552]$	2	7^9
B1	$-2 \cdot 7 \cdot 3$	-7	$[1, -1, 0, -37, -78]$	2	7^3
B2	$2 \cdot 7^2 \cdot 3$	-7^3	$[1, -1, 0, -1822, 30393]$	2	7^9

2. *$p = 17$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	minimal model	T_2	Δ
C1	$17 \cdot 33$	$2^4 \cdot 17^3$	$[1, -1, 1, -1644, -24922]$	4	17^8
C2	$-2 \cdot 17 \cdot 33$	17^2	$[1, -1, 1, -26209, -1626560]$	2	17^7
C3	$17 \cdot 9$	$2^4 \cdot 17^2$	$[1, -1, 1, -199, 510]$	4	17^7
C4	$2 \cdot 17 \cdot 15$	17^4	$[1, -1, 1, -199, -68272]$	2	17^{10}

3. *$p - 64$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_1	a_2	a_4	a_6	$\lvert T_2 \rvert$	Δ
A1	1	$\frac{p\sqrt{p-64}-1}{4}$	$-p^2$	0	2	p^7
A2	1	$\frac{p\sqrt{p-64}-1}{4}$	$4p^2$	$p^3\sqrt{p-64}$	2	$-p^8$

Theorem 3.2 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $m \geq 7$ and $n \geq 0$ such that $2^m p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon p\sqrt{2^m p^n + 1}$	$2^{m-2}p^{n+2}$	$2^{2m}p^{2n+6}$
A2	$-\epsilon 2p\sqrt{2^m p^n + 1}$	p^2	$2^{m+6}p^{n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

2. *there exist integers $m \geq 7$ and $n \geq 0$ such that $2^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon p\sqrt{2^m + p^n}$	$2^{m-2}p^2$	$2^{2m}p^{n+6}$
B2	$-\epsilon 2p\sqrt{2^m + p^n}$	p^{n+2}	$2^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

3. *there exist integers $m \geq 7$ and $n \geq 0$ such that $2^m - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon p\sqrt{2^m - p^n}$	$2^{m-2}p^2$	$2^{2m}p^{n+6}$
C2	$-\epsilon 2p\sqrt{2^m - p^n}$	$-p^{n+2}$	$2^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

4. *there exist integers $m \geq 7$ and $n \geq 0$ such that $p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon p\sqrt{p^n - 2^m}$	$-2^{m-2}p^2$	$2^{2m}p^{n+6}$
D2	$-\epsilon 2p\sqrt{p^n - 2^m}$	p^{n+2}	$-2^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

5. *there exist integers $m \geq 7$ and $t \in \{0, 1\}$ such that $\frac{2^m+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon p^{t+1}\sqrt{\frac{2^m+1}{p}}$	$2^{m-2}p^{2t+1}$	$2^{2m}p^{3+6t}$
E2	$-\epsilon 2p^{t+1}\sqrt{\frac{2^m+1}{p}}$	p^{2t+1}	$2^{m+6}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of p^{t+1} modulo 4.

6. *there exist integers $m \geq 7$ and $t \in \{0, 1\}$ such that $\frac{2^m-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon p^{t+1}\sqrt{\frac{2^m-1}{p}}$	$2^{m-2}p^{2t+1}$	$2^{2m}p^{3+6t}$
F2	$-\epsilon 2p^{t+1}\sqrt{\frac{2^m-1}{p}}$	$-p^{2t+1}$	$2^{m+6}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of p^{t+1} modulo 4.

Theorem 3.3 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $4p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exists an integer $n \geq 0$ such that $p^n - 4$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon p\sqrt{p^n - 4}$	$-p^2$	$2^4 p^{n+6}$
A2	$-\epsilon 2p\sqrt{p^n - 4}$	p^{n+2}	$2^8 p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

Theorem 3.4 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $8p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $m \in \{4, 5\}$ and $n \geq 0$ such that $2^m p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon p\sqrt{2^m p^n + 1}$	$2^{m-2} p^{n+2}$	$2^{2m} p^{2n+6}$
A2	$-\epsilon 2p\sqrt{2^m p^n + 1}$	p^2	$2^{m+6} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

2. *there exists an integer $n \geq 0$ such that $4 + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$-\epsilon p\sqrt{4 + p^n}$	p^2	$2^4 p^{n+6}$
B2	$\epsilon 2p\sqrt{4 + p^n}$	p^{n+2}	$2^8 p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

3. *there exist integers $m \in \{4, 5\}$ and $n \geq 0$ such that $2^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon p\sqrt{2^m + p^n}$	$2^{m-2}p^2$	$2^{2m}p^{n+6}$
C2	$-\epsilon 2p\sqrt{2^m + p^n}$	p^{n+2}	$2^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

4. *there exist integers $m \in \{4, 5\}$ and $n \geq 0$ such that $2^m - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon p\sqrt{2^m - p^n}$	$2^{m-2}p^2$	$-2^{2m}p^{n+6}$
D2	$-\epsilon 2p\sqrt{2^m - p^n}$	$-p^{n+2}$	$2^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

5. *there exists an integer $n \geq 1$ such that $p^n - 4$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon p\sqrt{p^n - 4}$	$-p^2$	2^4p^{n+6}
E2	$-\epsilon 2p\sqrt{p^n - 4}$	p^{n+2}	-2^8p^{2n+6}

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

6. *there exist integers $m \in \{4, 5\}$ and $n \geq 0$ such that $p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon p\sqrt{p^n - 2^m}$	$-2^{m-2}p^2$	$2^{2m}p^{n+6}$
F2	$-\epsilon 2p\sqrt{p^n - 2^m}$	p^{n+2}	$-2^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

7. *there exists an integer $t \in \{0, 1\}$ such that $\frac{4+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$-\epsilon p^{t+1}\sqrt{\frac{4+1}{p}}$	p^{2t+1}	2^4p^{3+6t}
G2	$\epsilon 2p^{t+1}\sqrt{\frac{4+1}{p}}$	p^{2t+1}	2^8p^{3+6t}

where $\epsilon \in \{\pm 1\}$ is the residue of p^{t+1} modulo 4.

8. *there exist integers $m \in \{4, 5\}$ and $t \in \{0, 1\}$ such that $\frac{2^m+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$\epsilon p^{t+1}\sqrt{\frac{2^m+1}{p}}$	$2^{m-2}p^{2t+1}$	$2^{2m}p^{3+6t}$
H2	$-\epsilon 2p^{t+1}\sqrt{\frac{2^m+1}{p}}$	p^{2t+1}	$2^{m+6}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of p^{t+1} modulo 4.

9. *there exist integers $m \in \{4, 5\}$ and $t \in \{0, 1\}$ such that $\frac{2^m-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$\epsilon p^{t+1}\sqrt{\frac{2^m-1}{p}}$	$2^{m-2}p^{2t+1}$	$-2^{2m}p^{3+6t}$
I2	$-\epsilon 2p^{t+1}\sqrt{\frac{2^m-1}{p}}$	$-p^{2t+1}$	$2^{m+6}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of p^{t+1} modulo 4.

Theorem 3.5 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $16p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $m \geq 4$ and $n \geq 0$ such that $2^m p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$-\epsilon p\sqrt{2^m p^n + 1}$	$2^{m-2}p^{n+2}$	$2^{2m}p^{2n+6}$
A2	$\epsilon 2p\sqrt{2^m p^n + 1}$	p^2	$2^{m+6}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

2. *there exists an integer $n \geq 0$ such that $4+p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon p\sqrt{4 + p^n}$	p^2	$2^4 p^{n+6}$
B2	$-\epsilon 2p\sqrt{4 + p^n}$	p^{n+2}	$2^8 p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

3. *there exist integers $m \geq 4$ and $n \geq 0$ such that $2^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$-\epsilon p\sqrt{2^m + p^n}$	$2^{m-2}p^2$	$2^{2m}p^{n+6}$
C2	$\epsilon 2p\sqrt{2^m + p^n}$	p^{n+2}	$2^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

4. *there exist integers $m \geq 4$ and $n \geq 0$ such that $2^m - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$-\epsilon p\sqrt{2^m - p^n}$	$2^{m-2}p^2$	$2^{2m}p^{n+6}$
D2	$\epsilon 2p\sqrt{2^m - p^n}$	$-p^{n+2}$	$2^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

5. *there exists an integer $n \geq 1$ such that $p^n - 4$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon p\sqrt{p^n - 4}$	$-p^2$	$2^4 p^{n+6}$
E2	$-\epsilon 2p\sqrt{p^n - 4}$	p^{n+2}	$-2^8 p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

6. *there exist integers $m \geq 4$ and $n \geq 0$ such that $p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$-\epsilon p\sqrt{p^n - 2^m}$	$-2^{m-2}p^2$	$2^{2m}p^{n+6}$
F2	$\epsilon 2p\sqrt{p^n - 2^m}$	p^{n+2}	$-2^{m+6}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of p modulo 4.

7. *there exists an integer $t \in \{0, 1\}$ such that $\frac{4+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$\epsilon p^{t+1}\sqrt{\frac{4+1}{p}}$	$2^m p^{2t+1}$	$2^4 p^{3+6t}$
G2	$-\epsilon 2p^{t+1}\sqrt{\frac{4+1}{p}}$	p^{2t+1}	$2^8 p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of p^t modulo 4.

8. *there exist integers $m \geq 4$ and $t \in \{0,1\}$ such that $\frac{2^m+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$-\epsilon p^{t+1}\sqrt{\frac{2^m+1}{p}}$	$2^m p^{2t+1}$	$2^{2m} p^{3+6t}$
H2	$\epsilon 2p^{t+1}\sqrt{\frac{2^m+1}{p}}$	p^{2t+1}	$2^{m+6} p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of p^{t+1} modulo 4.

9. *there exist integers $m \geq 4$ and $t \in \{0,1\}$ such that $\frac{2^m-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$-\epsilon p^{t+1}\sqrt{\frac{2^m-1}{p}}$	$2^m p^{2t+1}$	$-2^{2m} p^{3+6t}$
I2	$\epsilon 2p^{t+1}\sqrt{\frac{2^m-1}{p}}$	$-p^{2t+1}$	$2^{m+6} p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of p^{t+1} modulo 4.

Theorem 3.6 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $32p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exists an integer $n \geq 0$ such that $p^n - 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$2p\sqrt{p^n-1}$	$-p^2$	$2^6 p^{n+6}$
A2	$-4p\sqrt{p^n-1}$	$4p^{n+2}$	$2^{12} p^{2n+6}$
A1′	$-2p\sqrt{p^n-1}$	$-p^2$	$2^6 p^{n+6}$
A2′	$4p\sqrt{p^n-1}$	$4p^{n+2}$	$2^{12} p^{2n+6}$

2. *there exists an integer $t \in \{0, 1\}$ such that E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) $p \equiv 1 \pmod 4$;

	a_2	a_4	Δ
B1	0	$-p^{2t+1}$	$2^6 p^{3+6t}$
B2	0	$4p^{2t+1}$	$-2^{12} p^{3+6t}$

   (b) $p \equiv -1 \pmod 4$;

	a_2	a_4	Δ
C1	0	p^{2t+1}	$-2^6 p^{3+6t}$
C2	0	$-4p^{2t+1}$	$2^{12} p^{3+6t}$

3. *there exists an integer $n \geq 0$ such that $8p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$p\sqrt{8p^n + 1}$	$2p^{n+2}$	$2^6 p^{2n+6}$
D2	$-2p\sqrt{8p^n + 1}$	p^2	$2^9 p^{n+6}$
D1′	$-p\sqrt{8p^n + 1}$	$2p^{n+2}$	$2^6 p^{2n+6}$
D2′	$2p\sqrt{8p^n + 1}$	p^2	$2^9 p^{n+6}$

4. *there exists an integer $n \geq 0$ such that $8+p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$p\sqrt{8 + p^n}$	$2p^2$	$2^6 p^{n+6}$
E2	$-2p\sqrt{8 + p^n}$	p^{n+2}	$2^9 p^{2n+6}$
E1′	$-p\sqrt{8 + p^n}$	$2p^2$	$2^6 p^{n+6}$
E2′	$2p\sqrt{8 + p^n}$	p^{n+2}	$2^9 p^{2n+6}$

5. *there exists an integer $n \geq 1$ such that $8-p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$p\sqrt{8 - p^n}$	$2p^2$	$-2^6 p^{n+6}$
F2	$-2p\sqrt{8 - p^n}$	$-p^{n+2}$	$2^9 p^{2n+6}$
F1′	$-p\sqrt{8 - p^n}$	$2p^2$	$-2^6 p^{n+6}$
F2′	$2p\sqrt{8 - p^n}$	$-p^{n+2}$	$2^9 p^{2n+6}$

6. *there exists an integer $n \geq 1$ such that $p^n - 8$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$p\sqrt{p^n - 8}$	$-2p^2$	$2^6 p^{n+6}$
G2	$-2p\sqrt{p^n - 8}$	p^{n+2}	$-2^9 p^{2n+6}$
G1′	$-p\sqrt{p^n - 8}$	$-2p^2$	$2^6 p^{n+6}$
G2′	$2p\sqrt{p^n - 8}$	p^{n+2}	$-2^9 p^{2n+6}$

7. *there exists an integer $t \in \{0, 1\}$ such that $\frac{8-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$p^{t+1}\sqrt{\frac{8-1}{p}}$	$2p^{2t+1}$	$2^6 p^{3+6t}$
H2	$-2p^{t+1}\sqrt{\frac{8-1}{p}}$	$-p^{2t+1}$	$2^9 p^{3+6t}$
H1′	$-p^{t+1}\sqrt{\frac{8-1}{p}}$	$2p^{2t+1}$	$2^6 p^{3+6t}$
H2′	$2p^{t+1}\sqrt{\frac{8-1}{p}}$	$-p^{2t+1}$	$2^9 p^{3+6t}$

Theorem 3.7 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $64p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exists an integer $n \geq 0$ such that $p^n - 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$2p\sqrt{p^n - 1}$	p^{n+2}	$-2^6 p^{2n+6}$
A2	$-4p\sqrt{p^n - 1}$	$-4p^2$	$2^{12} p^{n+6}$
A1′	$-2p\sqrt{p^n - 1}$	p^{n+2}	$-2^6 p^{2n+6}$
A2′	$4p\sqrt{p^n - 1}$	$-4p^2$	$2^{12} p^{n+6}$

2. *there exists an integer $t \in \{0, 1\}$ such that E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) $p \equiv 1 \pmod 4$*;*

	a_2	a_4	Δ
B1	0	p^{2t+1}	$-2^6 p^{3+6t}$
B2	0	$-4p^{2t+1}$	$2^{12} p^{3+6t}$

(b) $p \equiv -1 \pmod 4$*;*

	a_2	a_4	Δ
C1	0	$-p^{2t+1}$	$2^6 p^{3+6t}$
C2	0	$4p^{2t+1}$	$-2^{12} p^{3+6t}$

3. *there exist integers $m \geq 3$ and $n \geq 0$ such that $2^m p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$2p\sqrt{2^m p^n + 1}$	$2^m p^{n+2}$	$2^{2m+6} p^{2n+6}$
D2	$-4p\sqrt{2^m p^n + 1}$	$4p^2$	$2^{m+12} p^{n+6}$
D1′	$-2p\sqrt{2^m p^n + 1}$	$2^m p^{n+2}$	$2^{2m+6} p^{2n+6}$
D2′	$4p\sqrt{2^m p^n + 1}$	$4p^2$	$2^{m+12} p^{n+6}$

4. *there exist integers $m \geq 2$ and $n \geq 0$ such that $2^m + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$2p\sqrt{2^m + p^n}$	$2^m p^2$	$2^{2m+6} p^{n+6}$
E2	$-4p\sqrt{2^m + p^n}$	$4p^{n+2}$	$2^{m+12} p^{2n+6}$
E1′	$-2p\sqrt{2^m + p^n}$	$2^m p^2$	$2^{2m+6} p^{n+6}$
E2′	$4p\sqrt{2^m + p^n}$	$4p^{n+2}$	$2^{m+12} p^{2n+6}$

5. *there exist integers $m \geq 2$ and $n \geq 0$ such that $2^m - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$2p\sqrt{2^m - p^n}$	$2^m p^2$	$-2^{2m+6} p^{n+6}$
F2	$-4p\sqrt{2^m - p^n}$	$-4p^{n+2}$	$2^{m+12} p^{2n+6}$
F1′	$-2p\sqrt{2^m - p^n}$	$2^m p^2$	$-2^{2m+6} p^{n+6}$
F2′	$4p\sqrt{2^m - p^n}$	$-4p^{n+2}$	$2^{m+12} p^{2n+6}$

6. *there exist integers $m \geq 2$ and $n \geq 0$ such that $p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$2p\sqrt{3^\ell p^n - 2^m}$	$-2^m p^2$	$2^{2m+6} p^{n+6}$
G2	$-4p\sqrt{3^\ell p^n - 2^m}$	$4p^{n+2}$	$-2^{m+12} p^{2n+6}$
G1′	$-2p\sqrt{3^\ell p^n - 2^m}$	$-2^m p^2$	$2^{2m+6} p^{n+6}$
G2′	$4p\sqrt{3^\ell p^n - 2^m}$	$4p^{n+2}$	$-2^{m+12} p^{2n+6}$

7. *there exist integers $m \geq 2$ and $t \in \{0,1\}$ such that $\frac{2^m+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$2p^{t+1}\sqrt{\frac{2^m+1}{p}}$	$2^m p^{2t+1}$	$2^{2m+6}p^{3+6t}$
H2	$-4p^{t+1}\sqrt{\frac{2^m+1}{p}}$	$4p^{2t+1}$	$2^{m+12}p^{3+6t}$
H1′	$-2p^{t+1}\sqrt{\frac{2^m+1}{p}}$	$2^m p^{2t+1}$	$2^{2m+6}p^{3+6t}$
H2′	$4p^{t+1}\sqrt{\frac{2^m+1}{p}}$	$4p^{2t+1}$	$2^{m+12}p^{3+6t}$

8. *there exist integers $m \geq 2$ and $t \in \{0,1\}$ such that $\frac{2^m-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$2p^{t+1}\sqrt{\frac{2^m-1}{p}}$	$2^m p^{2t+1}$	$2^{2m+6}p^{3+6t}$
I2	$-4p^{t+1}\sqrt{\frac{2^m-1}{p}}$	$-4p^{2t+1}$	$-2^{m+12}p^{3+6t}$
I1′	$-2p^{t+1}\sqrt{\frac{2^m-1}{p}}$	$2^m p^{2t+1}$	$2^{2m+6}p^{3+6t}$
I2′	$4p^{t+1}\sqrt{\frac{2^m-1}{p}}$	$-4p^{2t+1}$	$-2^{m+12}p^{3+6t}$

Theorem 3.8 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $128p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exists an integer $n \geq 0$ such that $2p^n - 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$2p\sqrt{2p^n-1}$	$2p^{n+2}$	$2^{2m+6}p^{2n+6}$
A2	$-4p\sqrt{2p^n-1}$	$-4p^2$	$2^{m+12}p^{n+6}$
A1′	$-2p\sqrt{2p^n-1}$	$2p^{n+2}$	$2^{2m+6}p^{2n+6}$
A2′	$4p\sqrt{2p^n-1}$	$-4p^2$	$2^{m+12}p^{n+6}$
B1	$2p\sqrt{2p^n-1}$	$-p^2$	$2^{m+6}p^{n+6}$
B2	$-4p\sqrt{2p^n-1}$	$8p^{n+2}$	$2^{2m+12}p^{2n+6}$
B1′	$-2p\sqrt{2p^n-1}$	$-p^2$	$2^{m+6}p^{n+6}$
B2′	$4p\sqrt{2p^n-1}$	$8p^{n+2}$	$2^{2m+12}p^{2n+6}$

2. *there exists an integer $n \geq 0$ such that $2+p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$2p\sqrt{2+p^n}$	$2p^2$	$2^{2m+6}p^{n+6}$
C2	$-4p\sqrt{2+p^n}$	$4p^{n+2}$	$2^{m+12}p^{2n+6}$
C1′	$-2p\sqrt{2+p^n}$	$2p^2$	$2^{2m+6}p^{n+6}$
C2′	$4p\sqrt{2+p^n}$	$4p^{n+2}$	$2^{m+12}p^{2n+6}$
D1	$2p\sqrt{2+p^n}$	p^{n+2}	$2^{m+6}p^{2n+6}$
D2	$-4p\sqrt{2+p^n}$	$8p^2$	$2^{2m+12}p^{n+6}$
D1′	$-2p\sqrt{2+p^n}$	p^{n+2}	$2^{m+6}p^{2n+6}$
D2′	$4p\sqrt{2+p^n}$	$8p^2$	$2^{2m+12}p^{n+6}$

3. *there exists an integer $n \geq 0$ such that $2-p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$2p\sqrt{2-p^n}$	$2p^2$	$-2^{2m+6}p^{n+6}$
E2	$-4p\sqrt{2-p^n}$	$-4p^{n+2}$	$2^{m+12}p^{2n+6}$
E1′	$-2p\sqrt{2-p^n}$	$2p^2$	$-2^{2m+6}p^{n+6}$
E2′	$4p\sqrt{2-p^n}$	$-4p^{n+2}$	$2^{m+12}p^{2n+6}$
F1	$2p\sqrt{2-p^n}$	$-p^{n+2}$	$2^{m+6}p^{2n+6}$
F2	$-4p\sqrt{2-p^n}$	$8p^2$	$-2^{2m+12}p^{n+6}$
F1′	$-2p\sqrt{2-p^n}$	$-p^{n+2}$	$2^{m+6}p^{2n+6}$
F2′	$4p\sqrt{2-p^n}$	$8p^2$	$-2^{2m+12}p^{n+6}$

4. *there exists an integer $n \geq 0$ such that p^n-2 is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$2p\sqrt{p^n-2}$	p^{n+2}	$2^{2m+6}p^{n+6}$
G2	$-4p\sqrt{p^n-2}$	$-8p^2$	$-2^{m+12}p^{2n+6}$
G1′	$-2p\sqrt{p^n-2}$	p^{n+2}	$2^{2m+6}p^{n+6}$
G2′	$4p\sqrt{p^n-2}$	$-8p^2$	$-2^{m+12}p^{2n+6}$
H1	$2p\sqrt{p^n-2}$	$-2p^2$	$-2^{m+6}p^{2n+6}$
H2	$-4p\sqrt{p^n-2}$	$4p^{n+2}$	$2^{2m+12}p^{n+6}$
H1′	$-2p\sqrt{p^n-2}$	$-2p^2$	$-2^{m+6}p^{2n+6}$
H2′	$4p\sqrt{p^n-2}$	$4p^{n+2}$	$2^{2m+12}p^{n+6}$

Theorem 3.9 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $256p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exists an integer and $n \geq 0$ such that $\frac{p^n+1}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$4p\sqrt{\frac{p^n+1}{2}}$	$2p^2$	2^9p^{2n+6}
A2	$-8p\sqrt{\frac{p^n+1}{2}}$	$8p^{n+2}$	$2^{15}p^{n+6}$
A1′	$-4p\sqrt{\frac{p^n+1}{2}}$	$2p^2$	2^9p^{2n+6}
A2′	$8p\sqrt{\frac{p^n+1}{2}}$	$8p^{n+2}$	$2^{15}p^{n+6}$
B1	$4p\sqrt{\frac{p^n+1}{2}}$	$2p^{n+2}$	2^9p^{n+6}
B2	$-8p\sqrt{\frac{p^n+1}{2}}$	$8p^2$	$2^{15}p^{2n+6}$
B1′	$-4p\sqrt{\frac{p^n+1}{2}}$	$2p^{n+2}$	2^9p^{n+6}
B2′	$8p\sqrt{\frac{p^n+1}{2}}$	$8p^2$	$2^{15}p^{2n+6}$

2. *there exists an integer $n \geq 0$ such that $\frac{p^n-1}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$4p\sqrt{\frac{p^n-1}{2}}$	$2p^{n+2}$	-2^9p^{2n+6}
C2	$-8p\sqrt{\frac{p^n-1}{2}}$	$-8p^2$	$2^{15}p^{n+6}$
C1′	$-4p\sqrt{\frac{p^n-1}{2}}$	$2p^{n+2}$	-2^9p^{2n+6}
C2′	$8p\sqrt{\frac{p^n-1}{2}}$	$-8p^2$	$2^{15}p^{n+6}$
D1	$4p\sqrt{\frac{p^n-1}{2}}$	$-2p^2$	2^9p^{n+6}
D2	$-8p\sqrt{\frac{p^n-1}{2}}$	$8p^{n+2}$	$-2^{15}p^{2n+6}$
D1′	$-4p\sqrt{\frac{p^n-1}{2}}$	$-2p^2$	2^9p^{n+6}
D2′	$8p\sqrt{\frac{p^n-1}{2}}$	$8p^{n+2}$	$-2^{15}p^{2n+6}$

3. *E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	0	$2p^2$	-2^9p^6
E2	0	$-8p^2$	$2^{15}p^6$
F1	0	$-2p^2$	2^9p^6
F2	0	$8p^2$	$-2^{15}p^6$

4. *there exists an integer $t \in \{0, 1\}$ such that E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	0	$2p^{2t+1}$	2^9p^{3+6t}
G2	0	$-8p^{2t+1}$	$2^{15}p^{3+6t}$
H1	0	$-2p^{2t+1}$	2^9p^{3+6t}
H2	0	$8p^{2t+1}$	$2^{15}p^{3+6t}$

3.1.2 The Proof for Conductor $2^\alpha p^2$

3.1.3 List of $\mathbb{Q}$-isomorphism classes

Let E be an elliptic curve over $\mathbb{Q}$ of conductor $2^M p^2$ with $0 \leq M \leq 8$ and having at least one rational point of order 2. We may assume that E is given by a model of the form

$$y^2 = x^3 + ax^2 + bx,$$

where a and b are integers both divisible by p, a and b have no other common odd divisors, and that this model is minimal outside of 2. From the hypothesis on the conductor of E, there exist two natural numbers α and δ, with $\delta \geq 2$, such that

$$b^2(a^2 - 4b) = \pm 2^\alpha p^\delta. \tag{3.2}$$

It follows that $b \neq 0$ and its only possible divisors are 2 and p. We consider the two cases: (i) $b > 0$, (ii) $b < 0$.

Lemma 3.10 *Suppose $b > 0$. Then there exists an integer d, and non-negative integers m and n satisfying one of the equations in the first column and E is $\mathbb{Q}$-isomorphic to the corresponding curve in the second column, for some $r_1, r_3 \in \{0, 1\}$; except in cases 1, 2 and 5, where if $m = 1$ then $r_1 \in \{1, 2\}$.*

		$y^2 = x^3 + a_2x^2 + a_4x$	
	Diophantine Equation	a_2	a_4
1	$d^2 - 2^m p^n = \pm 1$	$2^{r_1}pd$	$2^{m+2r_1-2}p^{n+2}$
2	$d^2 - 2^m = \pm p^n$	$2^{r_1}pd$	$2^{m+2r_1-2}p^2$
5	$pd^2 - 2^m = \pm 1$	$2^{r_1}p^{r_3+1}d$	$2^{m+2r_1-2}p^{2r_3+1}$
10	$d^2 - p^n = \pm 2^m$	$2^{r_1+1}pd$	$2^{2r_1}p^{n+2}$
11	$d^2 - 1 = 2^m p^n$	$2^{r_1+1}pd$	$2^{2r_1}p^2$
14	$pd^2 - 1 = 2^m$	$2^{r_1+1}p^{r_3+1}d$	$2^{2r_1}p^{2r_3+1}$
19	$2d^2 - p^n = \pm 1$	$2^{r_1+2}pd$	$2^{2r_1+1}p^{n+2}$
20	$2d^2 - 1 = p^n$	$2^{r_1+2}pd$	$2^{2r_1+1}p^2$
23	$2pd^2 - 1 = \pm 1$	$2^{r_1+2}p^{r_3+1}d$	$2^{2r_1+1}p^{2r_3+1}$

Proof. This lemma follows immediately from Lemma A.1 in Appendix A by removing the prime factor 3 from all places and setting $r_3 = 1$. Of course doing this makes a number of the rows identical, so ignoring the redundant rows we end up with the table above. The numbers in the first column of the table above are included to indicate which row of the table in Lemma A.1 these rows correspond. □

Similarly, from Lemma A.2 we obtain the following.

Lemma 3.11 *Suppose $b < 0$. Then there exists an integer d, and non-negative integers m and n satisfying one of the equations in the first column and E is $\mathbb{Q}$-isomorphic to the corresponding curve in the second column, for some $r_1, r_3 \in \{0, 1\}$; except in case 2, where if $m = 1$ then $r_1 \in \{1, 2\}$.*

		$y^2 = x^3 + a_2x^2 + a_4x$	
	Diophantine Equation	a_2	a_4
2	$d^2 + 2^m = p^n$	$2^{r_1}pd$	$-2^{m+2r_1-2}p^2$
10	$d^2 + p^n = 2^m$	$2^{r_1+1}pd$	$-2^{2r_1}p^{n+2}$
11	$d^2 + 1 = 2^m p^n$	$2^{r_1+1}pd$	$-2^{2r_1}p^2$
14	$pd^2 + 1 = 2^m$	$2^{r_1+1}p^{r_3+1}d$	$-2^{2r_1}p^{2r_3+1}$
20	$2d^2 + 1 = p^n$	$2^{r_1+2}pd$	$-2^{2r_1+1}p^2$
24	$2pd^2 + 1 = 1$	$2^{r_1+2}p^{r_3+1}d$	$-2^{2r_1+1}p^{2r_3+1}$

3.1.4 The end of the proof

In this section, we verify that the elliptic curves appearing in Theorems 3.1–3.9 are the only curves, up to $\mathbb{Q}$ isomorphism, having the stated properties.

Our method of proof is similar to that of Ivorra [37]. It is sufficient to prove the following.

($\star$) *Let F be an elliptic curve appearing in one of the Lemmata 3.10 or 3.11. Then, F is $\mathbb{Q}$-isomorphic to one of the elliptic curves appearing in Theorems 1 through 9.*

In fact, let N be an integer such that $0 \leq N \leq 8$ and E and elliptic curve over $\mathbb{Q}$ of conductor $2^N p^2$, having at least one rational point of order 2. According to the work done in the previous section (and Appendix A), E is $\mathbb{Q}$-isomorphic to an elliptic curve F appearing in Lemmas 3.10 or 3.11. It follows from assertion ($\star$) that F is thus $\mathbb{Q}$-isomorphic to one of the curves in Theorems 1 through 9. Furthermore, such is also the case for E. Since E is of conductor $2^N p^2$, it follows that E is $\mathbb{Q}$-isomorphic to one of the curves in the tables of the theorem corresponding to the value of N. This finishes the proof of the theorems.

Assertion ($\star$) is a consequence of the following assertion:

($\star\star$) *Let F be an elliptic curve appearing in one of the lemmata 3.10 or 3.11. Let F' be the quadratic twist of F by $\sqrt{-1}$. Then, one of the curves F and F' is $\mathbb{Q}$-isomorphic to one of the elliptic curves appearing in Theorems 1 through 9.*

In fact, consider an elliptic curve F referenced in Lemma 3.10 or 3.11. From ($\star\star$), we can suppose that F' is $\mathbb{Q}$-isomorphic to one of the elliptic curves in Theorems 3.1 through 3.9.

a) If F' is isomorphic to a curve in theorem 3.1, then F is isomorphic to a curve in theorem 3.4.

b) Suppose that F' is $\mathbb{Q}$-isomorphic to a curve in Theorems 3.2 through 3.9.

b.1) If F' is isomorphic to a curve in Theorems 3.6 through 3.9, we see that the same must be true of F.

b.2) If F' is isomorphic to a curve in Theorems 3.3 or 3.4, then F is isomorphic to a curve in Theorem 3.5.

b.3) If F' is isomorphic to a curve in Theorem 3.2, then F is isomorphic to a curve in Theorem 3.5.

b.4) Suppose now that F' is $\mathbb{Q}$-isomorphic to an elliptic curve appearing in Theorem 3.5.

If F' is isomorphic to one of the curves A1 or A2: if $m \in \{4, 5\}$, then F is isomorphic to one of the curves A1 or A2 in Theorem 3.4; if $m = 6$, then $p = 17$ and F is isomorphic to one of the curves in 3.1; if $m \geq 7$ the curve F is isomorphic to one to the curves A1 or A2 of Theorem 3.2.

If F' is isomorphic to one of the curves B1 or B2 then the curve F is isomorphic to one of the curves B1 or B2 in Theorem 3.4.

If F' is isomorphic to one of the curves C1 or C2 of Theorem 3.5; if $m \in \{4, 5\}$, then F is isomorphic to one of the curves C1 or C2 in Theorem 3.4; if $m = 6$, then $p = 17$ and F is isomorphic to one of the curves in 3.1; if $m \geq 7$, then F is isomorphic to one of the curves B1 or B2 in Theorem 3.2.

If F' is isomorphic to the curve D1 or D2; if $m \in \{4, 5\}$, then F is isomorphic to the curve D1 or D2 of Theorem 3.4; if $m \geq 7$, then F is isomorphic to one of the curves C1 or C2 in Theorem 3.2.

If F' is isomorphic to one of the curves E1 or E2 then the curve F is isomorphic to one of the curves E1 or E2 in Theorem 3.4.

If F' is isomorphic to one of the curves F1 or F2 of Theorem 3.5; if $m \in \{4, 5\}$, then F is isomorphic to one of the curves F1 or F2 in Theorem 3.4; if $m = 6$, then either $p = 17$ or $p = d^2 + 64$ and F is isomorphic to one of the curves in 3.1; if $m \geq 7$, then F is isomorphic to one of the curves D1 or D2 in Theorem 3.2.

If F' is isomorphic to one of the curves G1 or G2 then the curve F is isomorphic to one of the curves G1 or G2 in Theorem 3.4.

If F' is isomorphic to one of the curves H1 or H2 of Theorem 3.5; if $m \in \{4, 5\}$, then F is isomorphic to one of the curves H1 or H2 in Theorem 3.4; if $m \geq 7$, then F is isomorphic to one of the curves E1 or E2 in Theorem 3.2.

If F' is isomorphic to one of the curves I1 or I2 of Theorem 3.5; if $m \in \{4, 5\}$, then F is isomorphic to one of the curves I1 or I2 in Theorem 3.4; if $m = 6$, then $p = 7$ and F is isomorphic to one of the curves in 3.1; if $m \geq 7$, then F is isomorphic to one of the curves F1 or F2 in Theorem 3.2.

This proves assertion ($\star$) in this case.

All that remains now is to show that assertion ($\star\star$) holds for Lemmata 3.10 and 3.11.

Assertion ($\star\star$) holds for Lemma 3.10:

Since assertion ($\star\star$) is concerned only with the curves up to quadratic twist we may choose the sign of a_2 which makes calculations most convenient. This usually involves specifying the congruence class of pd, a factor of a_2, modulo 4. We will make extensive use of the tables in Chapter 2 for computing conductors.

In what follows we will refer to the curves appearing in Lemma 3.10 by their numbers in the first column. In particular, for the Diophantine equations involving "$\pm$" we would like to consider the curves corresponding to the "$+$" equation separately from the curves corresponding to the "$-$" equation. In the former case, we put a superscript of "$+$" on the curve number, and in the latter, a superscript of "$-$". This is made clear in the first two cases below.

1^+) Suppose that (p, d, m, n)[1] satisfy $d^2 = 2^m p^n + 1$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1} pd$ and $a_4 = 2^{m+2r_1-2} p^{n+2}$. We may assume d is such that $pd \equiv -1 \pmod 4$. Thus, using the tables in Chapter 2, the conductor of E is $2^{f_2} p^2$ where

$$f_2 = \begin{cases} 5 & \text{if } r_1 = 0, m = 3; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 6 & \text{if } r_1 = 1, m \geq 2. \end{cases}$$

(Observe how the assumption $pd \equiv -1 \pmod 4$ reduced the number of possibilities for the value of f_2 in the case when $r_1 = 0$ and $m \geq 4$.)

Now we can easily see that E is curve D1, A1, or D1 in Theorems 3.6, 3.5, 3.7, respectively.

1^-) Suppose that (p, d, m, n) [2] satisfy $d^2 = 2^m p^n - 1$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1} pd$ and $a_4 = 2^{m+2r_1-2} p^{n+2}$. We may assume d is such that $pd \equiv -1 \pmod 4$. The conductor of E is $2^7 p^2$ and so E is curve A1, if $r_1 = 0$, and curve B2', if $r_1 = 2$, of Theorem 3.8.

Notice we could have just written "E is curve A1, if $r_1 = 0$, and curve B2', if $r_1 = 2$" from which it should be clear that the curve A1 and B2' to which we refer are the ones in Theorem 3.8, since E is of conductor $2^7 p^2$. In what

[1] Then $m \geq 3$.

[2] Then $m \in \{0, 1\}$.

follows, we will not explicitly note which of Theorems 3.1 through 3.9 we are referring; this is clear from the conductors under consideration.

2^+) Suppose that (p, d, m, n) satisfy $d^2 = 2^m + p^n$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1}pd$ and $a_4 = 2^{m+2r_1-2}p^2$. We may assume d is such that $pd \equiv -1 \pmod 4$. Thus, from Theorem 2.1, the conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 3 & \text{if } r_1 = 0, m = 2; \\ 5 & \text{if } r_1 = 0, m = 3; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 7 & \text{if } r_1 = 1, m = 1; \\ 6 & \text{if } r_1 = 1, m \geq 2; \\ 7 & \text{if } r_1 = 2, m = 1. \end{cases}$$

Thus E is curve B1, E1, C1, C1, E1 or B2', respectively.

2^-) Suppose that (p, d, m, n)[3] satisfy $d^2 = 2^m - p^n$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1}pd$ and $a_4 = 2^{m+2r_1-2}p^2$. We may assume d is such that $pd \equiv -1 \pmod 4$. The conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 5 & \text{if } r_1 = 0, m = 3; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 6 & \text{if } r_1 = 1, m \geq 2; \end{cases}$$

Thus E is curve F1, D1, or F1, respectively.

5^+) Suppose that (p, d, m, n)[4] satisfy $pd^2 = 2^m + 1$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1}p^{r_3+1}d$ and $a_4 = 2^{m+2r_1-2}p^{2r_3+1}$. We may assume d is such that $p^{r_3+1}d \equiv -1 \pmod 4$. The conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 3 & \text{if } r_1 = 0, m = 2; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 6 & \text{if } r_1 = 1, m \geq 2. \end{cases}$$

Thus, E is curve G1 (if $r_1 = 0$, $m = 2$), H1 (if $r_1 = 0$, $m \geq 4$) and H1 or H1' (if $r_1 = 1$, $m \geq 2$).

5^-) Suppose that (p, d, m, n)[5] satisfy $pd^2 = 2^m - 1$, and E is the elliptic

[3]Then $m \geq 3$.
[4]Then $m \neq 1, 3$.
[5]Then $m \geq 3$.

curve with coefficients $a_2 = 2^{r_1}p^{r_3+1}d$ and $a_4 = 2^{m+2r_1-2}p^{2r_3+1}$. We may assume d is such that $p^{r_3+1}d \equiv -1 \pmod 4$. The conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 5 & \text{if } r_1 = 0, m = 3; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 6 & \text{if } r_1 = 1, m \geq 2. \end{cases}$$

Thus E is curve H1 or H1′ (if $r_1 = 0$, $m = 3$), I1 (if $r_1 = 0$, $m \geq 4$) and I1 or I1′ (if $r_1 = 1$, $m \geq 2$).

10^+) Suppose that (p, d, m, n)[6] satisfy $d^2 = p^n + 2^m$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1+1}pd$ and $a_4 = 2^{2r_1}p^{n+2}$. We may assume d is such that $pd \equiv 1 \pmod 4$. The conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 7 & \text{if } r_1 = 0, m = 1; \\ 4 & \text{if } r_1 = 0, m = 2; \\ 5 & \text{if } r_1 = 0, m = 3; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 7 & \text{if } r_1 = 1, m = 1; \\ 6 & \text{if } r_1 = 1, m \geq 2. \end{cases}$$

Thus E is curve D1 (or D1′), B1, E2 (or E2′), C2, E2 (or E2′), and C2 (or C2′), respectively.

10^-) Suppose that (p, d, m, n) satisfy $d^2 = p^n - 2^m$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1+1}pd$ and $a_4 = 2^{2r_1}p^{n+2}$. We may assume d is such that $pd \equiv 1 \pmod 4$. The conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 6 & \text{if } r_1 = 0, m = 0; \\ 7 & \text{if } r_1 = 0, m = 1; \\ 4 & \text{if } r_1 = 0, m = 2; \\ 5 & \text{if } r_1 = 0, m = 3; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 5 & \text{if } r_1 = 1, m = 0; \\ 7 & \text{if } r_1 = 1, m = 1; \\ 6 & \text{if } r_1 = 1, m \geq 2. \end{cases}$$

[6]Then $m \neq 0$.

Thus E is curve A1 (or A1′), G1 (or G1′), E2, G2 (or G2′), F2, A2 (or A2′), G2 (G2′), and H2 (or H2′).

11) Suppose that (p, d, m, n)[7] satisfy $d^2 = 2^m p^n + 1$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1+1}pd$ and $a_4 = 2^{2r_1}p^2$. We may assume d is such that $pd \equiv 1 \pmod 4$. The conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 5 & \text{if } r_1 = 0, m = 3; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 6 & \text{if } r_1 = 1, m \geq 2. \end{cases}$$

Thus E is curve D2 (or D2′), A2, and D2 (or D2′), respectively.

14) Suppose that (p, d, m, n)[8] satisfy $pd^2 = 2^m + 1$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1+1}p^{r_3+1}d$ and $a_4 = 2^{2r_1}p^{2r_3+1}$. We may assume d is such that $p^{r_3+1}d \equiv 1 \pmod 4$. The conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 3 & \text{if } r_1 = 0, m = 2; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 6 & \text{if } r_1 = 1, m \geq 2. \end{cases}$$

Thus E is curve G2, H2, H2 (or H2′), respectively.

19^+) Suppose that (p, d, m, n) satisfy $2d^2 = p^n + 1$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1+2}pd$ and $a_4 = 2^{2r_1+1}p^{n+2}$. The conductor of E is 2^8p^2, thus E is curve B1 (or B1′) if $r_1 = 0$, and A2 (or A2′) if $r_1 = 1$.

19^-) Suppose that (p, d, m, n) satisfy $2d^2 = p^n - 1$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1+2}pd$ and $a_4 = 2^{2r_1+1}p^{n+2}$. The conductor of E is 2^8p^2, thus E is curve C1 (or C1′) if $r_1 = 0$, and D2 (or D2′) if $r_1 = 1$.

20) Suppose that (p, d, m, n) satisfy $2d^2 = p^n + 1$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1+2}pd$ and $a_4 = 2^{2r_1+1}p^2$. The conductor of E is 2^8p^2, thus E is curve A1 (or A1′) if $r_1 = 0$, and B2 (or B2′) if $r_1 = 1$.

23^+) There are no solutions to $2pd^2 = 1 + 1$ so we have no curves corresponding to this case.

23^-) Suppose that (p, d, m, n) satisfy $2pd^2 = 1 - 1$, then $d = 0$, and E is the elliptic curve with coefficients $a_2 = 0$ and $a_4 = 2^{2r_1}p^{2r_3+1}$. The conductor of E is 2^8p^2 and E is the curve $G1$ if $r_1 = 0$ or the curve $H2$ if $r_1 = 1$.

[7] Then $m \geq 3$.

[8] Then $m \neq 0, 1, 3$.

This completes the proof that assertion ($\star\star$) is satisfied for all curves in lemma 3.10.

Assertion ($\star\star$) holds for Lemma 3.11:

2) Suppose that (p, d, m, n) satisfy $d^2 = p^n - 2^m$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1}pd$ and $a_4 = -2^{m+2r_1-2}p^2$. We may assume d is such that $pd \equiv -1 \pmod 4$. Thus, using the tables in chapter 2, the conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 4 & \text{if } r_1 = 0, m = 2; \\ 5 & \text{if } r_1 = 0, m = 3; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 7 & \text{if } r_1 = 1, m = 1; \\ 6 & \text{if } r_1 = 1, m \geq 2; \\ 7 & \text{if } r_1 = 2, m = 1. \end{cases}$$

Thus E is curve E1, G1, F1, H1 (or H1′), G1 (or G1′) and G1 (or G1′), respectively.

10) Suppose that (p, d, m, n)[9] satisfy $d^2 = 2^m - p^n$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1+1}pd$ and $a_4 = -2^{2r_1}p^{n+2}$. We may assume d is such that $pd \equiv 1 \pmod 4$. The conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 5 & \text{if } r_1 = 0, m = 0 \text{ (i.e. } n = 0); \\ 7 & \text{if } r_1 = 0, m = 1; \\ 5 & \text{if } r_1 = 0, m = 3; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 6 & \text{if } r_1 = 1, m = 0 \text{ (i.e. } n = 0); \\ 7 & \text{if } r_1 = 1, m = 1; \\ 6 & \text{if } r_1 = 1, m \geq 2. \end{cases}$$

Thus E is curve A1 (or A1′), F1 (or F1′), F2 (or F2′), D2, A2 (or A2′), and F2 (or F2′), E2 (or E2′) respectively.

[9]Then $m \neq 2$.

11) Suppose that (p, d, m, n)[10] satisfy $d^2 = 2^m p^n - 1$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1+1}pd$ and $a_4 = -2^{2r_1}p^2$. We may assume d is such that $pd \equiv 1 \pmod 4$. The conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 5 & \text{if } r_1 = 0, m = 0; \\ 7 & \text{if } r_1 = 0, m = 1; \\ 6 & \text{if } r_1 = 1, m = 0; \\ 7 & \text{if } r_1 = 1, m = 1; \end{cases}$$

Thus E is curve A1 (or A1′), B1 (or B1′), A2 (or A2′) and A2 (or A2′), respectively.

14) Suppose that (p, d, m, n)[11] satisfy $pd^2 = 2^m - 1$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1+1}p^{r_3+1}d$ and $a_4 = -2^{2r_1}p^{2r_3+1}$. We may assume d is such that $p^{r_3+1}d \equiv 1 \pmod 4$. The conductor of E is $2^{f_2}p^2$ where

$$f_2 = \begin{cases} 6 & \text{if } r_1 = 0, m = 0, p \equiv -1 \pmod 4; \\ 5 & \text{if } r_1 = 0, m = 0, p \equiv 1 \pmod 4; \\ 5 & \text{if } r_1 = 0, m = 3; \\ 4 & \text{if } r_1 = 0, m \geq 4; \\ 5 & \text{if } r_1 = 1, m = 0, p \equiv -1 \pmod 4; \\ 6 & \text{if } r_1 = 1, m = 0, p \equiv 1 \pmod 4; \\ 6 & \text{if } r_1 = 1, m \geq 2. \end{cases}$$

Thus E is curve C1, B1, H2 (or H2′), I2, C2, B2, I2 (or H2′), respectively.

20) Suppose that (p, d, m, n) satisfy $2d^2 = p^n - 1$, and E is the elliptic curve with coefficients $a_2 = 2^{r_1+2}pd$ and $a_4 = -2^{2r_1+1}p^2$. The conductor of E is 2^8p^2, thus E is curve D1 (or D1′) if $r_1 = 0$, and C2 (or C2′) if $r_1 = 1$.

24) Suppose that (p, d, m, n) satisfy $2pd^2 = 1 - 1$, then $d = 0$, and E is the elliptic curve with coefficients $a_2 = 0$ and $a_4 = -2^{2r_1}p^{2r_3+1}$. The conductor of E is 2^8p^2 and E is the curve $H1$ if $r_1 = 0$ or the curve $G2$ if $r_1 = 1$.

This completes the proof that assertion $(\star\star)$ is satisfied for all curves in lemma 3.11.

This completes the proof of Theorems 3.1 through 3.9.

[10] Then $m \leq 1$.

[11] Then $m \neq 1, 2$.

3.2 Curves of Conductor $2^\alpha 3^\beta p$

As we mentioned in the introduction to this chapter, the models presented in the following table are minimal except in the case when the conductor is not divisible by 4. In these cases (i.e. Theorems 3.12 and 3.13) the model is minimal except at 2, and a minimal model can be found using Corollary 2.2. We choose not to do this here.

Theorem 3.12 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $3^b p$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $2^6 3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot 3^{b-1}\sqrt{2^6 3^\ell p^n + 1}$	$2^4 3^{\ell+2(b-1)} p^n$	$2^{12} 3^{2\ell+6(b-1)} p^{2n}$
A2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^6 3^\ell p^n + 1}$	$3^{2(b-1)}$	$2^{12} 3^{\ell+6(b-1)} p^n$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

2. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $2^6 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot 3^{b-1}\sqrt{2^6 3^\ell + p^n}$	$2^4 3^{\ell+2(b-1)}$	$2^{12} 3^{2\ell+6(b-1)} p^n$
B2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^6 3^\ell + p^n}$	$3^{2(b-1)} p^n$	$2^{12} 3^{\ell+6(b-1)} p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

3. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $2^6 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot 3^{b-1}\sqrt{2^6 3^\ell - p^n}$	$2^4 3^{\ell+2(b-1)}$	$-2^{12} 3^{2\ell+6(b-1)} p^n$
C2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^6 3^\ell - p^n}$	$-3^{2(b-1)} p^n$	$2^{12} 3^{\ell+6(b-1)} p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

4. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $2^6 p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon \cdot 3^{b-1}\sqrt{2^6 p^n + 3^\ell}$	$2^4 3^{2(b-1)} p^n$	$2^{12} 3^{\ell+6(b-1)} p^{2n}$
D2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^6 p^n + 3^\ell}$	$3^{\ell+2(b-1)}$	$2^{12} 3^{2\ell+6(b-1)} p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

5. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $2^6 + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon \cdot 3^{b-1}\sqrt{2^6 + 3^\ell p^n}$	$2^4 3^{2(b-1)}$	$2^{12} 3^{\ell+6(b-1)} p^n$
E2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^6 + 3^\ell p^n}$	$3^{\ell+2(b-1)} p^n$	$2^{12} 3^{2\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

6. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $2^6 - 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon \cdot 3^{b-1}\sqrt{2^6 - 3^\ell p^n}$	$2^4 3^{2(b-1)}$	$-2^{12} 3^{\ell+6(b-1)} p^n$
F2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^6 - 3^\ell p^n}$	$-3^{\ell+2(b-1)} p^n$	$2^{12} 3^{2\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

7. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $3^\ell - 2^6 p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$\epsilon \cdot 3^{b-1}\sqrt{3^\ell - 2^6 p^n}$	$-2^4 3^{2(b-1)} p^n$	$2^{12} 3^{\ell+6(b-1)} p^{2n}$
G2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{3^\ell - 2^6 p^n}$	$3^{\ell+2(b-1)}$	$-2^{12} 3^{2\ell+6(b-1)} p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

8. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $p^n - 2^6 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$\epsilon \cdot 3^{b-1}\sqrt{p^n - 2^6 3^\ell}$	$-2^4 3^{\ell+2(b-1)}$	$2^{12}3^{2\ell+6(b-1)}p^n$
H2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{p^n - 2^6 3^\ell}$	$3^{2(b-1)}p^n$	$-2^{12}3^{\ell+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

In the case that $b = 2$, i.e. $N = 2 \cdot 3^2 p^2$, we furthermore could have one of the following conditions satisfied:

9. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{2^6+p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{2^6+p^n}{3}}$	$2^4 3^{2s+1}$	$2^{12}3^{3+6s}p^n$
I2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{2^6+p^n}{3}}$	$3^{2s+1}p^n$	$2^{12}3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

10. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{2^6-p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
J1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{2^6-p^n}{3}}$	$2^4 3^{2s+1}$	$-2^{12}3^{3+6s}p^n$
J2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{2^6-p^n}{3}}$	$-3^{2s+1}p^n$	$2^{12}3^{3+6s}p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

11. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n-2^6}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{p^n-2^6}{3}}$	$-2^4 3^{2s+1}$	$2^{12}3^{3+6s}p^n$
K2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{p^n-2^6}{3}}$	$3^{2s+1}p^n$	$-2^{12}3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

Theorem 3.13 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2\cdot 3^b p$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m 3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot 3^{b-1}\sqrt{2^m 3^\ell p^n + 1}$	$2^{m-2}3^{\ell+2(b-1)}p^n$	$2^{2m}3^{2\ell+6(b-1)}p^{2n}$
A2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m 3^\ell p^n + 1}$	$3^{2(b-1)}$	$2^{m+6}3^{\ell+6(b-1)}p^n$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

2. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot 3^{b-1}\sqrt{2^m 3^\ell + p^n}$	$2^{m-2}3^{\ell+2(b-1)}$	$2^{2m}3^{2\ell+6(b-1)}p^n$
B2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m 3^\ell + p^n}$	$3^{2(b-1)}p^n$	$2^{m+6}3^{\ell+6(b-1)}p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

3. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot 3^{b-1}\sqrt{2^m 3^\ell - p^n}$	$2^{m-2}3^{\ell+2(b-1)}$	$-2^{2m}3^{2\ell+6(b-1)}p^n$
C2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m 3^\ell - p^n}$	$-3^{2(b-1)}p^n$	$2^{m+6}3^{\ell+6(b-1)}p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

4. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon \cdot 3^{b-1}\sqrt{2^m p^n + 3^\ell}$	$2^{m-2}3^{2(b-1)}p^n$	$2^{2m}3^{\ell+6(b-1)}p^{2n}$
D2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m p^n + 3^\ell}$	$3^{\ell+2(b-1)}$	$2^{m+6}3^{2\ell+6(b-1)}p^n$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

5. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon \cdot 3^{b-1}\sqrt{2^m + 3^\ell p^n}$	$2^{m-2}3^{2(b-1)}$	$2^{2m}3^{\ell+6(b-1)}p^n$
E2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m + 3^\ell p^n}$	$3^{\ell+2(b-1)}p^n$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

6. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m - 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon \cdot 3^{b-1}\sqrt{2^m - 3^\ell p^n}$	$2^{m-2}3^{2(b-1)}$	$-2^{2m}3^{\ell+6(b-1)}p^n$
F2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m - 3^\ell p^n}$	$-3^{\ell+2(b-1)}p^n$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

7. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 1$ such that $3^\ell p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$\epsilon \cdot 3^{b-1}\sqrt{3^\ell p^n - 2^m}$	$-2^{m-2}3^{2(b-1)}$	$2^{2m}3^{\ell+6(b-1)}p^n$
G2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2^m}$	$3^{\ell+2(b-1)}p^n$	$-2^{m+6}3^{2\ell+6(b-1)}p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

8. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 1$ such that $3^\ell - 2^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$\epsilon \cdot 3^{b-1}\sqrt{3^\ell - 2^m p^n}$	$-2^{m-2}3^{2(b-1)}p^n$	$2^{2m}3^{\ell+6(b-1)}p^{2n}$
H2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{3^\ell - 2^m p^n}$	$3^{\ell+2(b-1)}$	$-2^{m+6}3^{2\ell+6(b-1)}p^n$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

9. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 1$ such that $p^n - 2^m 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$\epsilon \cdot 3^{b-1}\sqrt{p^n - 2^m 3^\ell}$	$-2^{m-2}3^{\ell+2(b-1)}$	$2^{2m}3^{2\ell+6(b-1)}p^n$
I2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{p^n - 2^m 3^\ell}$	$3^{2(b-1)}p^n$	$-2^{m+6}3^{\ell+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

In the case that $b = 2$, i.e. $N = 2 \cdot 3^2 p$, we furthermore could have one of the following conditions satisfied:

10. *there exist integers $m \geq 7$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{2^m + p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
J1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{2^m + p^n}{3}}$	$2^{m-2}3^{2s+1}$	$2^{2m}3^{3+6s}p^n$
J2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{2^m + p^n}{3}}$	$3^{2s+1}p^n$	$2^{m+6}3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

11. *there exist integers $m \geq 7$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{2^m - p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{2^m - p^n}{3}}$	$2^{m-2}3^{2s+1}$	$-2^{2m}3^{3+6s}p^n$
K2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{2^m - p^n}{3}}$	$-3^{2s+1}p^n$	$2^{m+6}3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

12. *there exist integers $m \geq 7$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n - 2^m}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
L1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{p^n - 2^m}{3}}$	$-2^{m-2}3^{2s+1}$	$2^{2m}3^{3+6s}p^n$
L2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{p^n - 2^m}{3}}$	$3^{2s+1}p^n$	$-2^{m+6}3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

Theorem 3.14 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^2 3^b p$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $4 \cdot 3^\ell + p^n$ is a square, $3^\ell \equiv -1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell + p^n}$	$3^{\ell+2(b-1)}$	$2^4 3^{2\ell+6(b-1)} p^n$
A2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell + p^n}$	$3^{2(b-1)} p^n$	$2^8 3^{\ell+6(b-1)} p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

2. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $4 \cdot 3^\ell - p^n$ is a square, $3^\ell \equiv -1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell - p^n}$	$3^{\ell+2(b-1)}$	$-2^4 3^{2\ell+6(b-1)} p^n$
B2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell - p^n}$	$-3^{2(b-1)} p^n$	$2^8 3^{\ell+6(b-1)} p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

3. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $4p^n - 3^\ell$ is a square, $p^n \equiv -1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot 3^{b-1}\sqrt{4p^n - 3^\ell}$	$3^{2(b-1)} p^n$	$-2^4 3^{\ell+6(b-1)} p^{2n}$
C2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{4p^n - 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^8 3^{2\ell+6(b-1)} p^n$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

4. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $p^n - 4 \cdot 3^\ell$ is a square, $3^\ell \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon \cdot 3^{b-1}\sqrt{p^n - 4 \cdot 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^4 3^{2\ell+6(b-1)} p^n$
D2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{p^n - 4 \cdot 3^\ell}$	$3^{2(b-1)} p^n$	$-2^8 3^{\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

In the case that $b = 2$, i.e. $N = 2^2 3^2 p$, we furthermore could have one of the following conditions satisfied:

5. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{4p^n-1}{3}$ is a square, $p^n \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon 3^{s+1}\sqrt{\frac{4p^n-1}{3}}$	$3^{2s+1}p^n$	$-2^4 3^{3+6s} p^{2n}$
E2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{4p^n-1}{3}}$	-3^{2s+1}	$2^8 3^{3+6s} p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

6. *there exists an integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n+4}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon 3^{s+1}\sqrt{\frac{p^n+4}{3}}$	3^{2s+1}	$2^4 3^{3+6s} p^n$
F2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{p^n+4}{3}}$	$3^{2s+1}p^n$	$2^8 3^{3+6s} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

Theorem 3.15 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^3 3^b p$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $m \in \{4, 5\}$, $\ell \geq 2 - b$ and $n \geq 1$ such that $2^m 3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot 3^{b-1}\sqrt{2^m 3^\ell p^n + 1}$	$2^{m-2}3^{\ell+2(b-1)}p^n$	$2^{2m}3^{2\ell+6(b-1)}p^{2n}$
A2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m 3^\ell p^n + 1}$	$3^{2(b-1)}$	$2^{m+6}3^{\ell+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

2. *there exist integers $\ell \geq 2 - b$ and $n \geq 1$ such that $4 \cdot 3^\ell + p^n$ is a square, $3^\ell \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$-\epsilon \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell + p^n}$	$3^{\ell+2(b-1)}$	$2^4 3^{2\ell+6(b-1)} p^n$
B2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell + p^n}$	$3^{2(b-1)} p^n$	$2^8 3^{\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

3. *there exist integers $m \in \{4, 5\}$, $\ell \geq 2 - b$ and $n \geq 1$ such that $2^m 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot 3^{b-1}\sqrt{2^m 3^\ell + p^n}$	$2^{m-2} 3^{\ell+2(b-1)}$	$2^{2m} 3^{2\ell+6(b-1)} p^n$
C2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m 3^\ell + p^n}$	$3^{2(b-1)} p^n$	$2^{m+6} 3^{\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

4. *there exist integers $\ell \geq 2 - b$ and $n \geq 1$ such that $4 \cdot 3^\ell - p^n$ is a square, $3^\ell \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$-\epsilon \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell - p^n}$	$3^{\ell+2(b-1)}$	$-2^4 3^{2\ell+6(b-1)} p^n$
D2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell - p^n}$	$-3^{2(b-1)} p^n$	$2^8 3^{\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

5. *there exist integers $m \in \{4, 5\}$, $\ell \geq 2 - b$ and $n \geq 1$ such that $2^m 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon \cdot 3^{b-1}\sqrt{2^m 3^\ell - p^n}$	$2^{m-2} 3^{\ell+2(b-1)}$	$-2^{2m} 3^{2\ell+6(b-1)} p^n$
E2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m 3^\ell - p^n}$	$-3^{2(b-1)} p^n$	$2^{m+6} 3^{\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

6. *there exist integers $m \in \{4, 5\}$, $\ell \geq 2 - b$ and $n \geq 1$ such that $2^m p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon \cdot 3^{b-1}\sqrt{2^m p^n + 3^\ell}$	$2^{m-2} 3^{2(b-1)} p^n$	$2^{2m} 3^{\ell+6(b-1)} p^{2n}$
F2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m p^n + 3^\ell}$	$3^{\ell+2(b-1)}$	$2^{m+6} 3^{2\ell+6(b-1)} p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

7. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $4p^n - 3^\ell$ is a square, $p^n \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$-\epsilon \cdot 3^{b-1}\sqrt{4p^n - 3^\ell}$	$3^{2(b-1)}p^n$	$-2^4 3^{\ell+6(b-1)}p^{2n}$
G2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{4p^n - 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^8 3^{2\ell+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

8. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $4 + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$-\epsilon \cdot 3^{b-1}\sqrt{4 + 3^\ell p^n}$	$3^{2(b-1)}$	$2^4 3^{\ell+6(b-1)}p^n$
H2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{4 + 3^\ell p^n}$	$3^{\ell+2(b-1)}p^n$	$2^8 3^{2\ell+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

9. *there exist integers $m \in \{4, 5\}$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$\epsilon \cdot 3^{b-1}\sqrt{2^m + 3^\ell p^n}$	$2^{m-2}3^{2(b-1)}$	$2^{2m}3^{\ell+6(b-1)}p^n$
I2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m + 3^\ell p^n}$	$3^{\ell+2(b-1)}p^n$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

10. *there exist integers $m \in \{4, 5\}$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m - 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
J1	$\epsilon \cdot 3^{b-1}\sqrt{2^m - 3^\ell p^n}$	$2^{m-2}3^{2(b-1)}$	$-2^{2m}3^{\ell+6(b-1)}p^n$
J2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m - 3^\ell p^n}$	$-3^{\ell+2(b-1)}p^n$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

11. *there exist integers $m \in \{4, 5\}$, $\ell \geq 2-b$ and $n \geq 1$ such that $3^\ell p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$\epsilon \cdot 3^{b-1}\sqrt{3^\ell p^n - 2^m}$	$-2^{m-2}3^{2(b-1)}$	$2^{2m}3^{\ell+6(b-1)}p^n$
K2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2^m}$	$3^{\ell+2(b-1)}p^n$	$-2^{m+6}3^{2\ell+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

12. *there exist integers $m \in \{4, 5\}$, $\ell \geq 2 - b$ and $n \geq 1$ such that $3^\ell - 2^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
L1	$\epsilon \cdot 3^{b-1}\sqrt{3^\ell - 2^m p^n}$	$-2^{m-2}3^{2(b-1)}p^n$	$2^{2m}3^{\ell+6(b-1)}p^{2n}$
L2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{3^\ell - 2^m p^n}$	$3^{\ell+2(b-1)}$	$-2^{m+6}3^{2\ell+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

13. *there exist integers $\ell \geq 2 - b$ and $n \geq 1$ such that $p^n - 4 \cdot 3^\ell$ is a square, $3^\ell \equiv -1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$-\epsilon \cdot 3^{b-1}\sqrt{p^n - 4 \cdot 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^4 3^{2\ell+6(b-1)}p^n$
M2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{p^n - 4 \cdot 3^\ell}$	$3^{2(b-1)}p^n$	$-2^8 3^{\ell+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

14. *there exist integers $m \in \{4, 5\}$, $\ell \geq 2 - b$ and $n \geq 1$ such that $p^n - 2^m 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
N1	$\epsilon \cdot 3^{b-1}\sqrt{p^n - 2^m 3^\ell}$	$-2^{m-2}3^{\ell+2(b-1)}$	$2^{2m}3^{2\ell+6(b-1)}p^n$
N2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{p^n - 2^m 3^\ell}$	$3^{2(b-1)}p^n$	$-2^{m+6}3^{\ell+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

In the case that $b = 2$, i.e. $N = 2^3 3^2 p$, we furthermore could have one of the following conditions satisfied:

15. *there exist integers $m \in \{4, 5\}$, $n \geq 1$, and $s \in \{0, 1\}$ such that $\frac{2^m + p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{2^m+p^n}{3}}$	$2^{m-2}3^{2s+1}$	$2^{2m}3^{3+6s}p^n$
O2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{2^m+p^n}{3}}$	$3^{2s+1}p^n$	$2^{m+6}3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

16. *there exist integers $m \in \{4, 5\}$, $n \geq 1$, and $s \in \{0, 1\}$ such that $\frac{2^m-p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
P1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{2^m-p^n}{3}}$	$2^{m-2}3^{2s+1}$	$-2^{2m}3^{3+6s}p^n$
P2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{2^m-p^n}{3}}$	$-3^{2s+1}p^n$	$2^{m+6}3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

17. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{4p^n-1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	$-\epsilon \cdot 3^{s+1}\sqrt{\frac{4p^n-1}{3}}$	$3^{2s+1}p^n$	$-2^4 3^{3+6s}p^{2n}$
Q2	$\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{4p^n-1}{3}}$	-3^{2s+1}	$2^8 3^{3+6s}p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

18. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n-4}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
R1	$-\epsilon \cdot 3^{s+1}\sqrt{\frac{p^n-4}{3}}$	-3^{2s+1}	$2^4 3^{3+6s}p^n$
R2	$\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{p^n-4}{3}}$	$3^{2s+1}p^n$	$-2^8 3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

19. *there exist integers $m \in \{4, 5\}$, $n \geq 1$, and $s \in \{0, 1\}$ such that $\frac{p^n-2^m}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
S1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{p^n-2^m}{3}}$	$-2^{m-2}3^{2s+1}$	$2^{2m}3^{3+6s}p^n$
S2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{p^n-2^m}{3}}$	$3^{2s+1}p^n$	$-2^{m+6}3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{s+1} modulo 4.

Theorem 3.16 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^4 3^b p$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 1$ such that $2^m 3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$-\epsilon \cdot 3^{b-1}\sqrt{2^m 3^\ell p^n + 1}$	$2^{m-2}3^{\ell+2(b-1)}p^n$	$2^{2m}3^{2\ell+6(b-1)}p^{2n}$
A2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m 3^\ell p^n + 1}$	$3^{2(b-1)}$	$2^{m+6}3^{\ell+6(b-1)}p^n$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

2. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $4 \cdot 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell + p^n}$	$3^{\ell+2(b-1)}$	$2^4 3^{2\ell+6(b-1)}p^n$
B2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell + p^n}$	$3^{2(b-1)}p^n$	$2^8 3^{\ell+6(b-1)}p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{\ell+b-1}$ modulo 4.

3. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 1$ such that $2^m 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$-\epsilon \cdot 3^{b-1}\sqrt{2^m 3^\ell + p^n}$	$2^{m-2}3^{\ell+2(b-1)}$	$2^{2m}3^{2\ell+6(b-1)}p^n$
C2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m 3^\ell + p^n}$	$3^{2(b-1)}p^n$	$2^{m+6}3^{\ell+6(b-1)}p^{2n}$

   where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

4. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $4 \cdot 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell - p^n}$	$3^{\ell+2(b-1)}$	$-2^4 3^{2\ell+6(b-1)} p^n$
D2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{4 \cdot 3^\ell - p^n}$	$-3^{2(b-1)} p^n$	$2^8 3^{\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{\ell+b-1}$ modulo 4.

5. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 1$ such that $2^m 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$-\epsilon \cdot 3^{b-1}\sqrt{2^m 3^\ell - p^n}$	$2^{m-2} 3^{\ell+2(b-1)}$	$-2^{2m} 3^{2\ell+6(b-1)} p^n$
E2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m 3^\ell - p^n}$	$-3^{2(b-1)} p^n$	$2^{m+6} 3^{\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

6. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 1$ such that $2^m p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$-\epsilon \cdot 3^{b-1}\sqrt{2^m p^n + 3^\ell}$	$2^{m-2} 3^{2(b-1)} p^n$	$2^{2m} 3^{\ell+6(b-1)} p^{2n}$
F2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m p^n + 3^\ell}$	$3^{\ell+2(b-1)}$	$2^{m+6} 3^{2\ell+6(b-1)} p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

7. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $4p^n - 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$\epsilon \cdot 3^{b-1}\sqrt{4p^n - 3^\ell}$	$3^{2(b-1)} p^n$	$-2^4 3^{\ell+6(b-1)} p^{2n}$
G2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{4p^n - 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^8 3^{2\ell+6(b-1)} p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1} p^n$ modulo 4.

8. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $4 + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$\epsilon \cdot 3^{b-1}\sqrt{4 + 3^\ell p^n}$	$3^{2(b-1)}$	$2^4 3^{\ell+6(b-1)} p^n$
H2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{4 + 3^\ell p^n}$	$3^{\ell+2(b-1)} p^n$	$2^8 3^{2\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

9. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 1$ such that $2^m + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$-\epsilon \cdot 3^{b-1}\sqrt{2^m + 3^\ell p^n}$	$2^{m-2}3^{2(b-1)}$	$2^{2m}3^{\ell+6(b-1)}p^n$
I2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m + 3^\ell p^n}$	$3^{\ell+2(b-1)}p^n$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

10. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 1$ such that $2^m - 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
J1	$-\epsilon \cdot 3^{b-1}\sqrt{2^m - 3^\ell p^n}$	$2^{m-2}3^{2(b-1)}$	$-2^{2m}3^{\ell+6(b-1)}p^n$
J2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{2^m - 3^\ell p^n}$	$-3^{\ell+2(b-1)}p^n$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

11. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 1$ such that $3^\ell p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$-\epsilon \cdot 3^{b-1}\sqrt{3^\ell p^n - 2^m}$	$-2^{m-2}3^{2(b-1)}$	$2^{2m}3^{\ell+6(b-1)}p^n$
K2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2^m}$	$3^{\ell+2(b-1)}p^n$	$-2^{m+6}3^{2\ell+6(b-1)}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

12. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 1$ such that $3^\ell - 2^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
L1	$-\epsilon \cdot 3^{b-1}\sqrt{3^\ell - 2^m p^n}$	$-2^{m-2}3^{2(b-1)}p^n$	$2^{2m}3^{\ell+6(b-1)}p^{2n}$
L2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{3^\ell - 2^m p^n}$	$3^{\ell+2(b-1)}$	$-2^{m+6}3^{2\ell+6(b-1)}p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

13. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $p^n - 4 \cdot 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$\epsilon \cdot 3^{b-1}\sqrt{p^n - 4 \cdot 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^4 3^{2\ell+6(b-1)} p^n$
M2	$-\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{p^n - 4 \cdot 3^\ell}$	$3^{2(b-1)} p^n$	$-2^8 3^{\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{\ell+b}$ modulo 4.

14. *there exist integers $m \geq 4$, $\ell \geq 2 - b$, and $n \geq 1$ such that $p^n - 2^m 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
N1	$-\epsilon \cdot 3^{b-1}\sqrt{p^n - 2^m 3^\ell}$	$-2^{m-2} 3^{\ell+2(b-1)}$	$2^{2m} 3^{2\ell+6(b-1)} p^n$
N2	$\epsilon \cdot 2 \cdot 3^{b-1}\sqrt{p^n - 2^m 3^\ell}$	$3^{2(b-1)} p^n$	$-2^{m+6} 3^{\ell+6(b-1)} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^{b-1} modulo 4.

In the case that $b = 2$, i.e. $N = 2^4 3^2 p$, we furthermore could have one of the following conditions satisfied:

15. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{4p^n - 1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{4p^n - 1}{3}}$	$3^{2s+1} p^n$	$-2^4 3^{3+6s} p^{2n}$
O2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{4p^n - 1}{3}}$	-3^{2s+1}	$2^8 3^{3+6s} p^n$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^s p^n$ modulo 4.

16. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n + 4}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
P1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{p^n + 4}{3}}$	3^{2s+1}	$2^4 3^{3+6s} p^n$
P2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{p^n + 4}{3}}$	$3^{2s+1} p^n$	$2^8 3^{3+6s} p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^s modulo 4.

17. *there exist integers $m \geq 4$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{2^m + p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{2^m+p^n}{3}}$	$2^{m-2}3^{2s+1}$	$2^{2m}3^{3+6s}p^n$
Q2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{2^m+p^n}{3}}$	$3^{2s+1}p^n$	$2^{m+6}3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^s modulo 4.

18. *there exist integers $m \geq 4$, $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{2^m-p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
R1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{2^m-p^n}{3}}$	$2^{m-2}3^{2s+1}$	$-2^{2m}3^{3+6s}p^n$
R2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{2^m-p^n}{3}}$	$-3^{2s+1}p^n$	$2^{m+6}3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^s modulo 4.

19. *there exist integer $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n-4}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
S1	$-\epsilon \cdot 3^{s+1}\sqrt{\frac{p^n-4}{3}}$	-3^{2s+1}	$2^4 3^{3+6s}p^n$
S2	$\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{p^n-4}{3}}$	$3^{2s+1}p^n$	$-2^8 3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^s modulo 4.

20. *there exist integers $m \geq 4$, $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n-2^m}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
T1	$\epsilon \cdot 3^{s+1}\sqrt{\frac{p^n-2^m}{3}}$	$-2^{m-2}3^{2s+1}$	$2^{2m}3^{3+6s}p^n$
T2	$-\epsilon \cdot 2 \cdot 3^{s+1}\sqrt{\frac{p^n-2^m}{3}}$	$3^{2s+1}p^n$	$-2^{m+6}3^{3+6s}p^{2n}$

where $\epsilon \in \{\pm 1\}$ is the residue of 3^s modulo 4.

Theorem 3.17 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^5 3^b p$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$2 \cdot 3^{b-1}\sqrt{3^\ell p^n + 1}$	$3^{\ell+2(b-1)}p^n$	$2^6 3^{2\ell+6(b-1)}p^{2n}$
A2	$-4 \cdot 3^{b-1}\sqrt{3^\ell p^n + 1}$	$4 \cdot 3^{2(b-1)}$	$2^{12}3^{\ell+6(b-1)}p^n$
A1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell p^n + 1}$	$3^{\ell+2(b-1)}p^n$	$2^6 3^{2\ell+6(b-1)}p^{2n}$
A2′	$4 \cdot 3^{b-1}\sqrt{3^\ell p^n + 1}$	$4 \cdot 3^{2(b-1)}$	$2^{12}3^{\ell+6(b-1)}p^n$

2. *there exist integers $\ell \geq 1$ and $n \geq 1$ such that $3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) *ℓ is even;*

	a_2	a_4	Δ
B1	$2 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$3^{2(b-1)}p^n$	$2^6 3^{\ell+6(b-1)}p^{2n}$
B2	$-4 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$2^{12}3^{2\ell+6(b-1)}p^n$
B1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$3^{2(b-1)}p^n$	$2^6 3^{\ell+6(b-1)}p^{2n}$
B2′	$4 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$2^{12}3^{2\ell+6(b-1)}p^n$

   (b) *ℓ is odd;*

	a_2	a_4	Δ
C1	$2 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$3^{\ell+2(b-1)}$	$2^6 3^{2\ell+6(b-1)}p^n$
C2	$-4 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$4 \cdot 3^{2(b-1)}p^n$	$2^{12}3^{\ell+6(b-1)}p^{2n}$
C1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$3^{\ell+2(b-1)}$	$2^6 3^{2\ell+6(b-1)}p^n$
C2′	$4 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$4 \cdot 3^{2(b-1)}p^n$	$2^{12}3^{\ell+6(b-1)}p^{2n}$

3. *there exist integers $\ell \geq 1$ and $n \geq 1$ such that $3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) *ℓ is even;*

	a_2	a_4	Δ
D1	$2 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$-3^{2(b-1)}p^n$	$2^6 3^{\ell+6(b-1)}p^{2n}$
D2	$-4 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$-2^{12}3^{2\ell+6(b-1)}p^n$
D1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$-3^{2(b-1)}p^n$	$2^6 3^{\ell+6(b-1)}p^{2n}$
D2′	$4 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$-2^{12}3^{2\ell+6(b-1)}p^n$

   (b) *ℓ is odd;*

	a_2	a_4	Δ
E1	$2 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$3^{\ell+2(b-1)}$	$-2^6 3^{2\ell+6(b-1)} p^n$
E2	$-4 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^n$	$2^{12} 3^{\ell+6(b-1)} p^{2n}$
E1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$3^{\ell+2(b-1)}$	$-2^6 3^{2\ell+6(b-1)} p^n$
E2′	$4 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^n$	$2^{12} 3^{\ell+6(b-1)} p^{2n}$

4. *there exist integers $\ell \geq 2 - b$ and $n \geq 1$ such that $p^n - 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) *ℓ is even;*

	a_2	a_4	Δ
F1	$2 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^6 3^{2\ell+6(b-1)} p^n$
F2	$-4 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$4 \cdot 3^{2(b-1)} p^n$	$-2^{12} 3^{\ell+6(b-1)} p^{2n}$
F1′	$-2 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^6 3^{2\ell+6(b-1)} p^n$
F2′	$4 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$4 \cdot 3^{2(b-1)} p^n$	$-2^{12} 3^{\ell+6(b-1)} p^{2n}$

   (b) *ℓ is odd;*

	a_2	a_4	Δ
G1	$2 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$3^{2(b-1)} p^n$	$-2^6 3^{\ell+6(b-1)} p^{2n}$
G2	$-4 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)}$	$2^{12} 3^{2\ell+6(b-1)} p^n$
G1′	$-2 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$3^{2(b-1)} p^n$	$-2^6 3^{\ell+6(b-1)} p^{2n}$
G2′	$4 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)}$	$2^{12} 3^{2\ell+6(b-1)} p^n$

5. *there exist integers $\ell \geq 2 - b$ and $n \geq 1$ such that $8 \cdot 3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$3^{b-1}\sqrt{8 \cdot 3^\ell p^n + 1}$	$2 \cdot 3^{\ell+2(b-1)} p^n$	$2^6 3^{2\ell+6(b-1)} p^{2n}$
H2	$-2 \cdot 3^{b-1}\sqrt{8 \cdot 3^\ell p^n + 1}$	$3^{2(b-1)}$	$2^9 3^{\ell+6(b-1)} p^n$
H1′	$-3^{b-1}\sqrt{8 \cdot 3^\ell p^n + 1}$	$2 \cdot 3^{\ell+2(b-1)} p^n$	$2^6 3^{2\ell+6(b-1)} p^{2n}$
H2′	$2 \cdot 3^{b-1}\sqrt{8 \cdot 3^\ell p^n + 1}$	$3^{2(b-1)}$	$2^9 3^{\ell+6(b-1)} p^n$

6. *there exist integers $\ell \geq 2 - b$ and $n \geq 1$ such that $8 \cdot 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$3^{b-1}\sqrt{8\cdot 3^\ell + p^n}$	$2\cdot 3^{\ell+2(b-1)}$	$2^6 3^{2\ell+6(b-1)} p^n$
I2	$-2\cdot 3^{b-1}\sqrt{8\cdot 3^\ell + p^n}$	$3^{2(b-1)} p^n$	$2^9 3^{\ell+6(b-1)} p^{2n}$
I1′	$-3^{b-1}\sqrt{8\cdot 3^\ell + p^n}$	$2\cdot 3^{\ell+2(b-1)}$	$2^6 3^{2\ell+6(b-1)} p^n$
I2′	$2\cdot 3^{b-1}\sqrt{8\cdot 3^\ell + p^n}$	$3^{2(b-1)} p^n$	$2^9 3^{\ell+6(b-1)} p^{2n}$

7. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $8\cdot 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
J1	$3^{b-1}\sqrt{8\cdot 3^\ell - p^n}$	$2\cdot 3^{\ell+2(b-1)}$	$-2^6 3^{2\ell+6(b-1)} p^n$
J2	$-2\cdot 3^{b-1}\sqrt{8\cdot 3^\ell - p^n}$	$-3^{2(b-1)} p^n$	$2^9 3^{\ell+6(b-1)} p^{2n}$
J1′	$-3^{b-1}\sqrt{8\cdot 3^\ell - p^n}$	$2\cdot 3^{\ell+2(b-1)}$	$-2^6 3^{2\ell+6(b-1)} p^n$
J2′	$2\cdot 3^{b-1}\sqrt{8\cdot 3^\ell - p^n}$	$-3^{2(b-1)} p^n$	$2^9 3^{\ell+6(b-1)} p^{2n}$

8. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $8p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$3^{b-1}\sqrt{8p^n + 3^\ell}$	$2\cdot 3^{2(b-1)} p^n$	$2^6 3^{\ell+6(b-1)} p^{2n}$
K2	$-2\cdot 3^{b-1}\sqrt{8p^n + 3^\ell}$	$3^{\ell+2(b-1)}$	$2^9 3^{2\ell+6(b-1)} p^n$
K1′	$-3^{b-1}\sqrt{8p^n + 3^\ell}$	$2\cdot 3^{2(b-1)} p^n$	$2^6 3^{\ell+6(b-1)} p^{2n}$
K2′	$2\cdot 3^{b-1}\sqrt{8p^n + 3^\ell}$	$3^{\ell+2(b-1)}$	$2^9 3^{2\ell+6(b-1)} p^n$

9. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $3^\ell p^n - 8$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
L1	$3^{b-1}\sqrt{3^\ell p^n - 8}$	$-2\cdot 3^{2(b-1)}$	$2^6 3^{\ell+6(b-1)} p^n$
L2	$-2\cdot 3^{b-1}\sqrt{3^\ell p^n - 8}$	$3^{\ell+2(b-1)} p^n$	$-2^9 3^{2\ell+6(b-1)} p^{2n}$
L1′	$-3^{b-1}\sqrt{3^\ell p^n - 8}$	$-2\cdot 3^{2(b-1)}$	$2^6 3^{\ell+6(b-1)} p^n$
L2′	$2\cdot 3^{b-1}\sqrt{3^\ell p^n - 8}$	$3^{\ell+2(b-1)} p^n$	$-2^9 3^{2\ell+6(b-1)} p^{2n}$

10. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $3^\ell - 8p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$3^{b-1}\sqrt{3^\ell - 8p^n}$	$-2\cdot 3^{2(b-1)}p^n$	$2^6 3^{\ell+6(b-1)}p^{2n}$
M2	$-2\cdot 3^{b-1}\sqrt{3^\ell - 8p^n}$	$3^{\ell+2(b-1)}$	$-2^9 3^{2\ell+6(b-1)}p^n$
M1′	$-3^{b-1}\sqrt{3^\ell - 8p^n}$	$-2\cdot 3^{2(b-1)}p^n$	$2^6 3^{\ell+6(b-1)}p^{2n}$
M2′	$2\cdot 3^{b-1}\sqrt{3^\ell - 8p^n}$	$3^{\ell+2(b-1)}$	$-2^9 3^{2\ell+6(b-1)}p^n$

11. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $p^n - 8\cdot 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
N1	$3^{b-1}\sqrt{p^n - 8\cdot 3^\ell}$	$-2\cdot 3^{\ell+2(b-1)}$	$2^6 3^{2\ell+6(b-1)}p^n$
N2	$-2\cdot 3^{b-1}\sqrt{p^n - 8\cdot 3^\ell}$	$3^{2(b-1)}p^n$	$-2^9 3^{\ell+6(b-1)}p^{2n}$
N1′	$-3^{b-1}\sqrt{p^n - 8\cdot 3^\ell}$	$-2\cdot 3^{\ell+2(b-1)}$	$2^6 3^{2\ell+6(b-1)}p^n$
N2′	$2\cdot 3^{b-1}\sqrt{p^n - 8\cdot 3^\ell}$	$3^{2(b-1)}p^n$	$-2^9 3^{\ell+6(b-1)}p^{2n}$

In the case that $b = 2$, i.e. $N = 2^5 3^2 p$, we furthermore could have one of the following conditions satisfied:

12. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n+1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$2\cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	3^{2s+1}	$2^6 3^{3+6s}p^n$
O2	$-4\cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$4\cdot 3^{2s+1}p^n$	$2^{12}3^{3+6s}p^{2n}$
O1′	$-2\cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	3^{2s+1}	$2^6 3^{3+6s}p^n$
O2′	$4\cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$4\cdot 3^{2s+1}p^n$	$2^{12}3^{3+6s}p^{2n}$

13. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n-1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
P1	$2\cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$3^{2s+1}p^n$	$-2^6 3^{3+6s}p^{2n}$
P2	$-4\cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$-4\cdot 3^{2s+1}$	$2^{12}3^{3+6s}p^n$
P1′	$-2\cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$3^{2s+1}p^n$	$-2^6 3^{3+6s}p^{2n}$
P2′	$4\cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$-4\cdot 3^{2s+1}$	$2^{12}3^{3+6s}p^n$

14. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n+8}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	$3^{s+1}\sqrt{\frac{p^n+8}{3}}$	$2 \cdot 3^{2s+1}$	$2^6 3^{3+6s} p^n$
Q2	$-2 \cdot 3^{s+1}\sqrt{\frac{p^n+8}{3}}$	$3^{2s+1}p^n$	$2^9 3^{3+6s} p^{2n}$
Q1′	$-3^{s+1}\sqrt{\frac{p^n+8}{3}}$	$2 \cdot 3^{2s+1}$	$2^6 3^{3+6s} p^n$
Q2′	$2 \cdot 3^{s+1}\sqrt{\frac{p^n+8}{3}}$	$3^{2s+1}p^n$	$2^9 3^{3+6s} p^{2n}$

15. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{8-p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
R1	$3^{s+1}\sqrt{\frac{8-p^n}{3}}$	$2 \cdot 3^{2s+1}$	$-2^6 3^{3+6s} p^n$
R2	$-2 \cdot 3^{s+1}\sqrt{\frac{8-p^n}{3}}$	$-3^{2s+1}p^n$	$2^9 3^{3+6s} p^{2n}$
R1′	$-3^{s+1}\sqrt{\frac{8-p^n}{3}}$	$2 \cdot 3^{2s+1}$	$-2^6 3^{3+6s} p^n$
R2′	$2 \cdot 3^{s+1}\sqrt{\frac{8-p^n}{3}}$	$-3^{2s+1}p^n$	$2^9 3^{3+6s} p^{2n}$

16. *there exists an integer $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n-8}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
S1	$3^{s+1}\sqrt{\frac{p^n-8}{3}}$	$-2 \cdot 3^{2s+1}$	$2^6 3^{3+6s} p^n$
S2	$-2 \cdot 3^{s+1}\sqrt{\frac{p^n-8}{3}}$	$3^{2s+1}p^n$	$-2^9 3^{3+6s} p^{2n}$
S1′	$-3^{s+1}\sqrt{\frac{p^n-8}{3}}$	$-2 \cdot 3^{2s+1}$	$2^6 3^{3+6s} p^n$
S2′	$2 \cdot 3^{s+1}\sqrt{\frac{p^n-8}{3}}$	$3^{2s+1}p^n$	$-2^9 3^{3+6s} p^{2n}$

Theorem 3.18 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^6 3^b p$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$2 \cdot 3^{b-1}\sqrt{3^\ell p^n + 1}$	$3^{2(b-1)}$	$2^6 3^{\ell+6(b-1)} p^n$
A2	$-4 \cdot 3^{b-1}\sqrt{3^\ell p^n + 1}$	$4 \cdot 3^{\ell+2(b-1)} p^n$	$2^{12} 3^{2\ell+6(b-1)} p^{2n}$
A1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell p^n + 1}$	$3^{2(b-1)}$	$2^6 3^{\ell+6(b-1)} p^n$
A2′	$4 \cdot 3^{b-1}\sqrt{3^\ell p^n + 1}$	$4 \cdot 3^{\ell+2(b-1)} p^n$	$2^{12} 3^{2\ell+6(b-1)} p^{2n}$

2. *there exist integers $\ell \geq 1$ and $n \geq 1$ such that $3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) ℓ is even;

	a_2	a_4	Δ
B1	$2 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$3^{\ell+2(b-1)}$	$2^6 3^{2\ell+6(b-1)} p^n$
B2	$-4 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$4 \cdot 3^{2(b-1)} p^n$	$2^{12} 3^{\ell+6(b-1)} p^{2n}$
B1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$3^{2(b-1)}$	$2^6 3^{2\ell+6(b-1)} p^n$
B2′	$4 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$4 \cdot 3^{\ell+2(b-1)} p^n$	$2^{12} 3^{\ell+6(b-1)} p^{2n}$

   (b) ℓ is odd;

	a_2	a_4	Δ
C1	$2 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$3^{2(b-1)} p^n$	$2^6 3^{\ell+6(b-1)} p^{2n}$
C2	$-4 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$2^{12} 3^{2\ell+6(b-1)} p^n$
C1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$3^{2(b-1)} p^n$	$2^6 3^{\ell+6(b-1)} p^{2n}$
C2′	$4 \cdot 3^{b-1}\sqrt{3^\ell + p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$2^{12} 3^{2\ell+6(b-1)} p^n$

3. *there exist integers $\ell \geq 1$ and $n \geq 1$ such that $3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) ℓ is even;

	a_2	a_4	Δ
D1	$2 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$3^{\ell+2(b-1)}$	$-2^6 3^{2\ell+6(b-1)} p^n$
D2	$-4 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^n$	$2^{12} 3^{\ell+6(b-1)} p^{2n}$
D1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$3^{\ell+2(b-1)}$	$-2^6 3^{2\ell+6(b-1)} p^n$
D2′	$4 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^n$	$2^{12} 3^{\ell+6(b-1)} p^{2n}$

   (b) ℓ is odd;

	a_2	a_4	Δ
E1	$2 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$-3^{2(b-1)}p^n$	$2^6 3^{\ell+6(b-1)}p^{2n}$
E2	$-4 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$-2^{12}3^{2\ell+6(b-1)}p^n$
E1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$-3^{2(b-1)}p^n$	$2^6 3^{\ell+6(b-1)}p^{2n}$
E2′	$4 \cdot 3^{b-1}\sqrt{3^\ell - p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$-2^{12}3^{2\ell+6(b-1)}p^n$

4. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $p^n - 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) *ℓ is even;*

	a_2	a_4	Δ
F1	$2 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$3^{2(b-1)}p^n$	$-2^6 3^{\ell+6(b-1)}p^{2n}$
F2	$-4 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)}$	$2^{12}3^{2\ell+6(b-1)}p^n$
F1′	$-2 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$3^{2(b-1)}p^n$	$-2^6 3^{\ell+6(b-1)}p^{2n}$
F2′	$4 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)}$	$2^{126}3^{2\ell+6(b-1)}p^n$

   (b) *ℓ is odd;*

	a_2	a_4	Δ
G1	$2 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^6 3^{2\ell+6(b-1)}p^n$
G2	$-4 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$4 \cdot 3^{2(b-1)}p^n$	$-2^{12}3^{\ell+6(b-1)}p^{2n}$
G1′	$-2 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^6 3^{2\ell+6(b-1)}p^n$
G2′	$4 \cdot 3^{b-1}\sqrt{p^n - 3^\ell}$	$4 \cdot 3^{2(b-1)}p^n$	$-2^{12}3^{\ell+6(b-1)}p^{2n}$

5. *there exist integers $m \geq 3$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m 3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$2 \cdot 3^{b-1}\sqrt{2^m 3^\ell p^n + 1}$	$2^m 3^{\ell+2(b-1)}p^n$	$2^{2m+6}3^{2\ell+6(b-1)}p^{2n}$
H2	$-4 \cdot 3^{b-1}\sqrt{2^m 3^\ell p^n + 1}$	$4 \cdot 3^{2(b-1)}$	$2^{m+12}3^{\ell+6(b-1)}p^n$
H1′	$-2 \cdot 3^{b-1}\sqrt{2^m 3^\ell p^n + 1}$	$2^m 3^{\ell+2(b-1)}p^n$	$2^{2m+6}3^{2\ell+6(b-1)}p^{2n}$
H2′	$4 \cdot 3^{b-1}\sqrt{2^m 3^\ell p^n + 1}$	$4 \cdot 3^{2(b-1)}$	$2^{m+12}3^{\ell+6(b-1)}p^n$

6. *there exist integers $m \geq 2$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$2 \cdot 3^{b-1}\sqrt{2^m 3^\ell + p^n}$	$2^m 3^{\ell+2(b-1)}$	$2^{2m+6}3^{2\ell+6(b-1)}p^n$
I2	$-4 \cdot 3^{b-1}\sqrt{2^m 3^\ell + p^n}$	$4 \cdot 3^{2(b-1)}p^n$	$2^{m+12}3^{\ell+6(b-1)}p^{2n}$
I1′	$-2 \cdot 3^{b-1}\sqrt{2^m 3^\ell + p^n}$	$2^m 3^{\ell+2(b-1)}$	$2^{2m+6}3^{2\ell+6(b-1)}p^n$
I2′	$4 \cdot 3^{b-1}\sqrt{2^m 3^\ell + p^n}$	$4 \cdot 3^{2(b-1)}p^n$	$2^{m+12}3^{\ell+6(b-1)}p^{2n}$

7. *there exist integers $m \geq 2$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
J1	$2 \cdot 3^{b-1}\sqrt{2^m 3^\ell - p^n}$	$2^m 3^{\ell+2(b-1)}$	$-2^{2m+6}3^{2\ell+6(b-1)}p^n$
J2	$-4 \cdot 3^{b-1}\sqrt{2^m 3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)}p^n$	$2^{m+12}3^{\ell+6(b-1)}p^{2n}$
J1′	$-2 \cdot 3^{b-1}\sqrt{2^m 3^\ell - p^n}$	$2^m 3^{\ell+2(b-1)}$	$-2^{2m+6}3^{2\ell+6(b-1)}p^n$
J2′	$4 \cdot 3^{b-1}\sqrt{2^m 3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)}p^n$	$2^{m+12}3^{\ell+6(b-1)}p^{2n}$

8. *there exist integers $m \geq 3$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$2 \cdot 3^{b-1}\sqrt{2^m p^n + 3^\ell}$	$2^m 3^{2(b-1)}p^n$	$2^{2m+6}3^{\ell+6(b-1)}p^{2n}$
K2	$-4 \cdot 3^{b-1}\sqrt{2^m p^n + 3^\ell}$	$4 \cdot 3^{\ell+2(b-1)}$	$2^{m+12}3^{2\ell+6(b-1)}p^n$
K1′	$-2 \cdot 3^{b-1}\sqrt{2^m p^n + 3^\ell}$	$2^m 3^{2(b-1)}p^n$	$2^{2m+6}3^{\ell+6(b-1)}p^{2n}$
K2′	$4 \cdot 3^{b-1}\sqrt{2^m p^n + 3^\ell}$	$4 \cdot 3^{\ell+2(b-1)}$	$2^{m+12}3^{2\ell+6(b-1)}p^n$

9. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $4p^n - 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
L1	$2 \cdot 3^{b-1}\sqrt{4p^n - 3^\ell}$	$4 \cdot 3^{2(b-1)}p^n$	$-2^{10}3^{\ell+6(b-1)}p^{2n}$
L2	$-4 \cdot 3^{b-1}\sqrt{4p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)}$	$2^{14}3^{2\ell+6(b-1)}p^n$
L1′	$-2 \cdot 3^{b-1}\sqrt{4p^n - 3^\ell}$	$4 \cdot 3^{2(b-1)}p^n$	$-2^{10}3^{\ell+6(b-1)}p^{2n}$
L2′	$4 \cdot 3^{b-1}\sqrt{4p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)}$	$2^{14}3^{2\ell+6(b-1)}p^n$

10. *there exist integers $m \geq 2$, $\ell \geq 2-b$ and $n \geq 1$ such that $2^m + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$2 \cdot 3^{b-1}\sqrt{2^m + 3^\ell p^n}$	$2^m 3^{2(b-1)}$	$2^{2m+6}3^{\ell+6(b-1)}p^n$
M2	$-4 \cdot 3^{b-1}\sqrt{2^m + 3^\ell p^n}$	$4 \cdot 3^{\ell+2(b-1)}p^n$	$2^{m+12}3^{2\ell+6(b-1)}p^{2n}$
M1′	$-2 \cdot 3^{b-1}\sqrt{2^m + 3^\ell p^n}$	$2^m 3^{2(b-1)}$	$2^{2m+6}3^{\ell+6(b-1)}p^n$
M2′	$4 \cdot 3^{b-1}\sqrt{2^m + 3^\ell p^n}$	$4 \cdot 3^{\ell+2(b-1)}p^n$	$2^{m+12}3^{2\ell+6(b-1)}p^{2n}$

11. *there exist integers $m \geq 2$, $\ell \geq 2 - b$ and $n \geq 1$ such that $2^m - 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
N1	$2 \cdot 3^{b-1}\sqrt{2^m - 3^\ell p^n}$	$2^m 3^{2(b-1)}$	$-2^{2m+6}3^{\ell+6(b-1)}p^n$
N2	$-4 \cdot 3^{b-1}\sqrt{2^m - 3^\ell p^n}$	$-4 \cdot 3^{\ell+2(b-1)}p^n$	$2^{m+12}3^{2\ell+6(b-1)}p^{2n}$
N1′	$-2 \cdot 3^{b-1}\sqrt{2^m - 3^\ell p^n}$	$2^m 3^{2(b-1)}$	$-2^{2m+6}3^{\ell+6(b-1)}p^n$
N2′	$4 \cdot 3^{b-1}\sqrt{2^m - 3^\ell p^n}$	$-4 \cdot 3^{\ell+2(b-1)}p^n$	$2^{m+12}3^{2\ell+6(b-1)}p^{2n}$

12. *there exist integers $m \geq 2$, $\ell \geq 2 - b$ and $n \geq 1$ such that $3^\ell p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$2 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2^m}$	$-2^m 3^{2(b-1)}$	$2^{2m+6}3^{\ell+6(b-1)}p^n$
O2	$-4 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2^m}$	$4 \cdot 3^{\ell+2(b-1)}p^n$	$-2^{m+12}3^{2\ell+6(b-1)}p^{2n}$
O1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2^m}$	$-2^m 3^{2(b-1)}$	$2^{2m+6}3^{\ell+6(b-1)}p^n$
O2′	$4 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2^m}$	$4 \cdot 3^{\ell+2(b-1)}p^n$	$-2^{m+12}3^{2\ell+6(b-1)}p^{2n}$

13. *there exist integers $m \geq 2$, $\ell \geq 2 - b$ and $n \geq 1$ such that $3^\ell - 2^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
P1	$2 \cdot 3^{b-1}\sqrt{3^\ell - 2^m p^n}$	$-2^m 3^{2(b-1)}p^n$	$2^{2m+6}3^{\ell+6(b-1)}p^{2n}$
P2	$-4 \cdot 3^{b-1}\sqrt{3^\ell - 2^m p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$-2^{m+12}3^{2\ell+6(b-1)}p^n$
P1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell - 2^m p^n}$	$-2^m 3^{2(b-1)}p^n$	$2^{2m+6}3^{\ell+6(b-1)}p^{2n}$
P2′	$4 \cdot 3^{b-1}\sqrt{3^\ell - 2^m p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$-2^{m+12}3^{2\ell+6(b-1)}p^n$

14. *there exist integers $m \geq 2$, $\ell \geq 2 - b$ and $n \geq 1$ such that $p^n - 2^m 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	$2 \cdot 3^{b-1}\sqrt{p^n - 2^m 3^\ell}$	$-2^m 3^{\ell+2(b-1)}$	$2^{2m+6}3^{2\ell+6(b-1)}p^n$
Q2	$-4 \cdot 3^{b-1}\sqrt{p^n - 2^m 3^\ell}$	$4 \cdot 3^{2(b-1)}p^n$	$-2^{m+12}3^{\ell+6(b-1)}p^{2n}$
Q1′	$-2 \cdot 3^{b-1}\sqrt{p^n - 2^m 3^\ell}$	$-2^m 3^{\ell+2(b-1)}$	$2^{2m+6}3^{2\ell+6(b-1)}p^n$
Q2′	$4 \cdot 3^{b-1}\sqrt{p^n - 2^m 3^\ell}$	$4 \cdot 3^{2(b-1)}p^n$	$-2^{m+12}3^{\ell+6(b-1)}p^{2n}$

In the case that $b = 2$, i.e. $N = 2^6 3^2 p$, we furthermore could have one of the following conditions satisfied:

15. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n+1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
R1	$2 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$3^{2s+1}p^n$	$2^6 3^{3+6s}p^{2n}$
R2	$-4 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$4 \cdot 3^{2s+1}$	$2^{12}3^{3+6s}p^n$
R1′	$-2 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$3^{2s+1}p^n$	$2^6 3^{3+6s}p^{2n}$
R2′	$4 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$4 \cdot 3^{2s+1}$	$2^{12}3^{3+6s}p^n$

16. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n-1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
S1	$2 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	-3^{2s+1}	$2^6 3^{3+6s}p^n$
S2	$-4 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$4 \cdot 3^{2s+1}p^n$	$-2^{12}3^{3+6s}p^{2n}$
S1′	$-2 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	-3^{2s+1}	$2^6 3^{3+6s}p^n$
S2′	$4 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$4 \cdot 3^{2s+1}p^n$	$-2^{12}3^{3+6s}p^{2n}$

17. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{4p^n-1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
T1	$2 \cdot 3^{s+1}\sqrt{\frac{4p^n-1}{3}}$	$4 \cdot 3^{2s+1)}p^n$	$-2^{10}3^{3+6s}p^{2n}$
T2	$-4 \cdot 3^{s+1}\sqrt{\frac{4p^n-1}{3}}$	$-4 \cdot 3^{2s+1)}$	$2^{14}3^{3+6s}p^n$
T1′	$-2 \cdot 3^{s+1}\sqrt{\frac{4p^n-1}{3}}$	$4 \cdot 3^{2s+1)}p^n$	$-2^{10}3^{3+6s}p^{2n}$
T2′	$4 \cdot 3^{s+1}\sqrt{\frac{4p^n-1}{3}}$	$-4 \cdot 3^{2s+1)}$	$2^{14}3^{3+6s}p^n$

18. *there exist integers $m \geq 2$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n+2^m}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
U1	$2 \cdot 3^{s+1}\sqrt{\frac{p^n+2^m}{3}}$	$2^m 3^{2s+1}$	$2^{2m+6}3^{3+6s}p^n$
U2	$-4 \cdot 3^{s+1}\sqrt{\frac{p^n+2^m}{3}}$	$4 \cdot 3^{2s+1}p^n$	$2^{m+12}3^{3+6s}p^{2n}$
U1′	$-2 \cdot 3^{s+1}\sqrt{\frac{p^n+2^m}{3}}$	$2^m 3^{2s+1}$	$2^{2m+6}3^{3+6s}p^n$
U2′	$4 \cdot 3^{s+1}\sqrt{\frac{p^n+2^m}{3}}$	$4 \cdot 3^{2s+1}p^n$	$2^{m+12}3^{3+6s}p^{2n}$

19. *there exist integers $m \geq 2$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{2^m-p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
V1	$2 \cdot 3^{s+1}\sqrt{\frac{2^m-p^n}{3}}$	$2^m 3^{2s+1}$	$-2^{2m+6}3^{3+6s}p^n$
V2	$-4 \cdot 3^{s+1}\sqrt{\frac{2^m-p^n}{3}}$	$-4 \cdot 3^{2s+1}p^n$	$2^{m+12}3^{3+6s}p^{2n}$
V1′	$-2 \cdot 3^{s+1}\sqrt{\frac{2^m-p^n}{3}}$	$2^m 3^{2s+1}$	$-2^{2m+6}3^{3+6s}p^n$
V2′	$4 \cdot 3^{s+1}\sqrt{\frac{2^m-p^n}{3}}$	$-4 \cdot 3^{2s+1}p^n$	$2^{m+12}3^{3+6s}p^{2n}$

20. *there exist integers $m \geq 2$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n-2^m}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
W1	$2 \cdot 3^{s+1}\sqrt{\frac{p^n-2^m}{3}}$	$-2^m 3^{2s+1}$	$2^{2m+6}3^{3+6s}p^n$
W2	$-4 \cdot 3^{s+1}\sqrt{\frac{p^n-2^m}{3}}$	$4 \cdot 3^{2s+1}p^n$	$-2^{m+12}3^{3+6s}p^{2n}$
W1′	$-2 \cdot 3^{s+1}\sqrt{\frac{p^n-2^m}{3}}$	$-2^m 3^{2s+1}$	$2^{2m+6}3^{3+6s}p^n$
W2′	$4 \cdot 3^{s+1}\sqrt{\frac{p^n-2^m}{3}}$	$4 \cdot 3^{2s+1}p^n$	$-2^{m+12}3^{3+6s}p^{2n}$

Theorem 3.19 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^7 3^b p$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $2 \cdot 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$2 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell + p^n}$	$2 \cdot 3^{\ell+2(b-1)}$	$2^8 3^{2\ell+6(b-1)} p^n$
A2	$-4 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell + p^n}$	$4 \cdot 3^{2(b-1)} p^n$	$2^{13} 3^{\ell+6(b-1)} p^{2n}$
A1′	$-2 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell + p^n}$	$2 \cdot 3^{\ell+2(b-1)}$	$2^8 3^{2\ell+6(b-1)} p^n$
A2′	$4 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell + p^n}$	$4 \cdot 3^{2(b-1)} p^n$	$2^{13} 3^{\ell+6(b-1)} p^{2n}$
B1	$2 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell + p^n}$	$3^{2(b-1)} p^n$	$2^7 3^{\ell+6(b-1)} p^{2n}$
B2	$-4 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell + p^n}$	$8 \cdot 3^{\ell+2(b-1)}$	$2^{14} 3^{2\ell+6(b-1)} p^n$
B1′	$-2 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell + p^n}$	$3^{2(b-1)} p^n$	$2^7 3^{\ell+6(b-1)} p^{2n}$
B2′	$4 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell + p^n}$	$8 \cdot 3^{\ell+2(b-1)}$	$2^{14} 3^{2\ell+6(b-1)} p^n$

2. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $2 \cdot 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$2 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell - p^n}$	$2 \cdot 3^{\ell+2(b-1)}$	$-2^8 3^{2\ell+6(b-1)} p^n$
C2	$-4 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^n$	$2^{13} 3^{\ell+6(b-1)} p^{2n}$
C1′	$-2 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell - p^n}$	$2 \cdot 3^{\ell+2(b-1)}$	$-2^8 3^{2\ell+6(b-1)} p^n$
C2′	$4 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^n$	$2^{13} 3^{\ell+6(b-1)} p^{2n}$
D1	$2 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell - p^n}$	$-3^{2(b-1)} p^n$	$2^7 3^{\ell+6(b-1)} p^{2n}$
D2	$-4 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell - p^n}$	$8 \cdot 3^{\ell+2(b-1)}$	$-2^{14} 3^{2\ell+6(b-1)} p^n$
D1′	$-2 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell - p^n}$	$-3^{2(b-1)} p^n$	$2^7 3^{\ell+6(b-1)} p^{2n}$
D2′	$4 \cdot 3^{b-1}\sqrt{2 \cdot 3^\ell - p^n}$	$8 \cdot 3^{\ell+2(b-1)}$	$-2^{14} 3^{2\ell+6(b-1)} p^n$

3. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $2p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$2 \cdot 3^{b-1}\sqrt{2p^n + 3^\ell}$	$2 \cdot 3^{2(b-1)}p^n$	$2^8 3^{\ell+6(b-1)}p^{2n}$
E2	$-4 \cdot 3^{b-1}\sqrt{2p^n + 3^\ell}$	$4 \cdot 3^{\ell+2(b-1)}$	$2^{13}3^{2\ell+6(b-1)}p^n$
E1′	$-2 \cdot 3^{b-1}\sqrt{2p^n + 3^\ell}$	$2 \cdot 3^{2(b-1)}p^n$	$2^8 3^{\ell+6(b-1)}p^{2n}$
E2′	$4 \cdot 3^{b-1}\sqrt{2p^n + 3^\ell}$	$4 \cdot 3^{\ell+2(b-1)}$	$2^{13}3^{2\ell+6(b-1)}p^n$
F1	$2 \cdot 3^{b-1}\sqrt{2p^n + 3^\ell}$	$3^{\ell+2(b-1)}$	$2^7 3^{2\ell+6(b-1)}p^n$
F2	$-4 \cdot 3^{b-1}\sqrt{2p^n + 3^\ell}$	$8 \cdot 3^{2(b-1)}p^n$	$2^{14}3^{\ell+6(b-1)}p^{2n}$
F1′	$-2 \cdot 3^{b-1}\sqrt{2p^n + 3^\ell}$	$3^{\ell+2(b-1)}$	$2^7 3^{2\ell+6(b-1)}p^n$
F2′	$4 \cdot 3^{b-1}\sqrt{2p^n + 3^\ell}$	$8 \cdot 3^{2(b-1)}p^n$	$2^{14}3^{\ell+6(b-1)}p^{2n}$

4. *there exist integers $\ell \geq 2 - b$ and $n \geq 1$ such that $2p^n - 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$2 \cdot 3^{b-1}\sqrt{2p^n - 3^\ell}$	$2 \cdot 3^{2(b-1)}p^n$	$-2^8 3^{\ell+6(b-1)}p^{2n}$
G2	$-4 \cdot 3^{b-1}\sqrt{2p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)}$	$2^{13}3^{2\ell+6(b-1)}p^n$
G1′	$-2 \cdot 3^{b-1}\sqrt{2p^n - 3^\ell}$	$2 \cdot 3^{2(b-1)}p^n$	$-2^8 3^{\ell+6(b-1)}p^{2n}$
G2′	$4 \cdot 3^{b-1}\sqrt{2p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)}$	$2^{13}3^{2\ell+6(b-1)}p^n$
H1	$2 \cdot 3^{b-1}\sqrt{2p^n - 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^7 3^{2\ell+6(b-1)}p^n$
H2	$-4 \cdot 3^{b-1}\sqrt{2p^n - 3^\ell}$	$8 \cdot 3^{2(b-1)}p^n$	$-2^{14}3^{\ell+6(b-1)}p^{2n}$
H1′	$-2 \cdot 3^{b-1}\sqrt{2p^n - 3^\ell}$	$-3^{\ell+2(b-1)}$	$2^7 3^{2\ell+6(b-1)}p^n$
H2′	$4 \cdot 3^{b-1}\sqrt{2p^n - 3^\ell}$	$8 \cdot 3^{2(b-1)}p^n$	$-2^{14}3^{\ell+6(b-1)}p^{2n}$

5. *there exist integers $\ell \geq 2 - b$ and $n \geq 1$ such that $2 + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$2 \cdot 3^{b-1}\sqrt{2 + 3^\ell p^n}$	$2 \cdot 3^{2(b-1)}$	$2^8 3^{\ell+6(b-1)}p^n$
I2	$-4 \cdot 3^{b-1}\sqrt{2 + 3^\ell p^n}$	$4 \cdot 3^{\ell+2(b-1)}p^n$	$2^{13}3^{2\ell+6(b-1)}p^{2n}$
I1′	$-2 \cdot 3^{b-1}\sqrt{2 + 3^\ell p^n}$	$2 \cdot 3^{2(b-1)}$	$2^8 3^{\ell+6(b-1)}p^n$
I2′	$4 \cdot 3^{b-1}\sqrt{2 + 3^\ell p^n}$	$4 \cdot 3^{\ell+2(b-1)}p^n$	$2^{13}3^{2\ell+6(b-1)}p^{2n}$
J1	$2 \cdot 3^{b-1}\sqrt{2 + 3^\ell p^n}$	$3^{\ell+2(b-1)}p^n$	$2^7 3^{2\ell+6(b-1)}p^{2n}$
J2	$-4 \cdot 3^{b-1}\sqrt{2 + 3^\ell p^n}$	$8 \cdot 3^{2(b-1)}$	$2^{14}3^{\ell+6(b-1)}p^n$
J1′	$-2 \cdot 3^{b-1}\sqrt{2 + 3^\ell p^n}$	$3^{\ell+2(b-1)}p^n$	$2^7 3^{2\ell+6(b-1)}p^{2n}$
J2′	$4 \cdot 3^{b-1}\sqrt{2 + 3^\ell p^n}$	$8 \cdot 3^{2(b-1)}$	$2^{14}3^{\ell+6(b-1)}p^n$

6. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $3^\ell p^n - 2$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$2 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2}$	$-2 \cdot 3^{2(b-1)}$	$2^8 3^{\ell+6(b-1)} p^n$
K2	$-4 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2}$	$4 \cdot 3^{\ell+2(b-1)} p^n$	$-2^{13} 3^{2\ell+6(b-1)} p^{2n}$
K1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2}$	$-2 \cdot 3^{2(b-1)}$	$2^8 3^{\ell+6(b-1)} p^n$
K2′	$4 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2}$	$4 \cdot 3^{\ell+2(b-1)} p^n$	$-2^{13} 3^{2\ell+6(b-1)} p^{2n}$
L1	$2 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2}$	$3^{\ell+2(b-1)} p^n$	$-2^7 3^{2\ell+6(b-1)} p^{2n}$
L2	$-4 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2}$	$-8 \cdot 3^{2(b-1)}$	$2^{14} 3^{\ell+6(b-1)} p^n$
L1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2}$	$3^{\ell+2(b-1)} p^n$	$-2^7 3^{2\ell+6(b-1)} p^{2n}$
L2′	$4 \cdot 3^{b-1}\sqrt{3^\ell p^n - 2}$	$-8 \cdot 3^{2(b-1)}$	$2^{14} 3^{\ell+6(b-1)} p^n$

7. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $3^\ell - 2p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$2 \cdot 3^{b-1}\sqrt{3^\ell - 2p^n}$	$-2 \cdot 3^{2(b-1)} p^n$	$2^8 3^{\ell+6(b-1)} p^{2n}$
M2	$-4 \cdot 3^{b-1}\sqrt{3^\ell - 2p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$-2^{13} 3^{2\ell+6(b-1)} p^n$
M1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell - 2p^n}$	$-2 \cdot 3^{2(b-1)} p^n$	$2^8 3^{\ell+6(b-1)} p^{2n}$
M2′	$4 \cdot 3^{b-1}\sqrt{3^\ell - 2p^n}$	$4 \cdot 3^{\ell+2(b-1)}$	$-2^{13} 3^{2\ell+6(b-1)} p^n$
N1	$2 \cdot 3^{b-1}\sqrt{3^\ell - 2p^n}$	$3^{\ell+2(b-1)}$	$-2^7 3^{2\ell+6(b-1)} p^n$
N2	$-4 \cdot 3^{b-1}\sqrt{3^\ell - 2p^n}$	$-8 \cdot 3^{2(b-1)} p^n$	$2^{14} 3^{\ell+6(b-1)} p^{2n}$
N1′	$-2 \cdot 3^{b-1}\sqrt{3^\ell - 2p^n}$	$3^{\ell+2(b-1)}$	$-2^7 3^{2\ell+6(b-1)} p^n$
N2′	$4 \cdot 3^{b-1}\sqrt{3^\ell - 2p^n}$	$-8 \cdot 3^{2(b-1)} p^n$	$2^{14} 3^{\ell+6(b-1)} p^{2n}$

8. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $p^n - 2 \cdot 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$2 \cdot 3^{b-1}\sqrt{p^n - 2 \cdot 3^\ell}$	$-2 \cdot 3^{\ell+2(b-1)}$	$2^8 3^{2\ell+6(b-1)} p^n$
O2	$-4 \cdot 3^{b-1}\sqrt{p^n - 2 \cdot 3^\ell}$	$4 \cdot 3^{2(b-1)} p^n$	$-2^{13} 3^{\ell+6(b-1)} p^{2n}$
O1′	$-2 \cdot 3^{b-1}\sqrt{p^n - 2 \cdot 3^\ell}$	$-2 \cdot 3^{\ell+2(b-1)}$	$2^8 3^{2\ell+6(b-1)} p^n$
O2′	$4 \cdot 3^{b-1}\sqrt{p^n - 2 \cdot 3^\ell}$	$4 \cdot 3^{2(b-1)} p^n$	$-2^{13} 3^{\ell+6(b-1)} p^{2n}$
P1	$2 \cdot 3^{b-1}\sqrt{p^n - 2 \cdot 3^\ell}$	$3^{2(b-1)} p^n$	$-2^7 3^{\ell+6(b-1)} p^{2n}$
P2	$-4 \cdot 3^{b-1}\sqrt{p^n - 2 \cdot 3^\ell}$	$-8 \cdot 3^{\ell+2(b-1)}$	$2^{14} 3^{2\ell+6(b-1)} p^n$
P1′	$-2 \cdot 3^{b-1}\sqrt{p^n - 2 \cdot 3^\ell}$	$3^{2(b-1)} p^n$	$-2^7 3^{\ell+6(b-1)} p^{2n}$
P2′	$4 \cdot 3^{b-1}\sqrt{p^n - 2 \cdot 3^\ell}$	$-8 \cdot 3^{\ell+2(b-1)}$	$2^{14} 3^{2\ell+6(b-1)} p^n$

In the case that $b = 2$, i.e. $N = 2^7 3^2 p$, we furthermore could have one of the following conditions satisfied:

9. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{2p^n+1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	$2 \cdot 3^{s+1}\sqrt{\frac{2p^n+1}{3}}$	$2 \cdot 3^{2s+1} p^n$	$2^8 3^{3+6s} p^{2n}$
Q2	$-4 \cdot 3^{s+1}\sqrt{\frac{2p^n+1}{3}}$	$4 \cdot 3^{2s+1}$	$2^{13} 3^{3+6s} p^n$
Q1′	$-2 \cdot 3^{s+1}\sqrt{\frac{2p^n+1}{3}}$	$2 \cdot 3^{2s+1} p^n$	$2^8 3^{3+6s} p^{2n}$
Q2′	$4 \cdot 3^{s+1}\sqrt{\frac{2p^n+1}{3}}$	$4 \cdot 3^{2s+1}$	$2^{13} 3^{3+6s} p^n$
R1	$2 \cdot 3^{s+1}\sqrt{\frac{2p^n+1}{3}}$	3^{2s+1}	$2^7 3^{3+6s} p^n$
R2	$-4 \cdot 3^{s+1}\sqrt{\frac{2p^n+1}{3}}$	$8 \cdot 3^{2s+1} p^n$	$2^{14} 3^{3+6s} p^{2n}$
R1′	$-2 \cdot 3^{s+1}\sqrt{\frac{2p^n+1}{3}}$	3^{2s+1}	$2^7 3^{3+6s} p^n$
R2′	$4 \cdot 3^{s+1}\sqrt{\frac{2p^n+1}{3}}$	$8 \cdot 3^{2s+1} p^n$	$2^{14} 3^{3+6s} p^{2n}$

10. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n+2}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
S1	$2\cdot 3^{s+1}\sqrt{\frac{p^n+2}{3}}$	$2\cdot 3^{2s+1}$	$2^8 3^{3+6s} p^n$
S2	$-4\cdot 3^{s+1}\sqrt{\frac{p^n+2}{3}}$	$4\cdot 3^{2s+1}p^n$	$2^{13} 3^{3+6s} p^{2n}$
S1′	$-2\cdot 3^{s+1}\sqrt{\frac{p^n+2}{3}}$	$2\cdot 3^{2s+1}$	$2^8 3^{3+6s} p^n$
S2′	$4\cdot 3^{s+1}\sqrt{\frac{p^n+2}{3}}$	$4\cdot 3^{2s+1}p^n$	$2^{13} 3^{3+6s} p^{2n}$
T1	$2\cdot 3^{s+1}\sqrt{\frac{p^n+2}{3}}$	$3^{2s+1}p^n$	$2^7 3^{3+6s} p^{2n}$
T2	$-4\cdot 3^{s+1}\sqrt{\frac{p^n+2}{3}}$	$8\cdot 3^{2s+1}$	$2^{14} 3^{3+6s} p^n$
T1′	$-2\cdot 3^{s+1}\sqrt{\frac{p^n+2}{3}}$	$3^{2s+1}p^n$	$2^7 3^{3+6s} p^{2n}$
T2′	$4\cdot 3^{s+1}\sqrt{\frac{p^n+2}{3}}$	$8\cdot 3^{2s+1}$	$2^{14} 3^{3+6s} p^n$

11. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n-2}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
U1	$2\cdot 3^{s+1}\sqrt{\frac{p^n-2}{3}}$	$-2\cdot 3^{2s+1}$	$2^8 3^{3+6s} p^n$
U2	$-4\cdot 3^{s+1}\sqrt{\frac{p^n-2}{3}}$	$4\cdot 3^{2s+1}p^n$	$-2^{13} 3^{3+6s} p^{2n}$
U1′	$-2\cdot 3^{s+1}\sqrt{\frac{p^n-2}{3}}$	$-2\cdot 3^{2s+1}$	$2^8 3^{3+6s} p^n$
U2′	$4\cdot 3^{s+1}\sqrt{\frac{p^n-2}{3}}$	$4\cdot 3^{2s+1}p^n$	$-2^{13} 3^{3+6s} p^{2n}$
V1	$2\cdot 3^{s+1}\sqrt{\frac{p^n-2}{3}}$	$3^{2s+1}p^n$	$-2^7 3^{3+6s} p^{2n}$
V2	$-4\cdot 3^{s+1}\sqrt{\frac{p^n-2}{3}}$	$-8\cdot 3^{2s+1}$	$2^{14} 3^{3+6s} p^n$
V1′	$-2\cdot 3^{s+1}\sqrt{\frac{p^n-2}{3}}$	$3^{2s+1}p^n$	$-2^7 3^{3+6s} p^{2n}$
V2′	$4\cdot 3^{s+1}\sqrt{\frac{p^n-2}{3}}$	$-8\cdot 3^{2s+1}$	$2^{14} 3^{3+6s} p^n$

Theorem 3.20 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^8 3^b p$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $\frac{3^\ell p^n - 1}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$4 \cdot 3^{b-1}\sqrt{\frac{3^\ell p^n - 1}{2}}$	$2 \cdot 3^{\ell+2(b-1)} p^n$	$-2^9 3^{2\ell+6(b-1)} p^{2n}$
A2	$-8 \cdot 3^{b-1}\sqrt{\frac{3^\ell p^n - 1}{2}}$	$-8 \cdot 3^{2(b-1)}$	$2^{15} 3^{\ell+6(b-1)} p^n$
A1′	$-4 \cdot 3^{b-1}\sqrt{\frac{3^\ell p^n - 1}{2}}$	$2 \cdot 3^{\ell+2(b-1)} p^n$	$-2^9 3^{2\ell+6(b-1)} p^{2n}$
A2′	$8 \cdot 3^{b-1}\sqrt{\frac{3^\ell p^n - 1}{2}}$	$-8 \cdot 3^{2(b-1)}$	$2^{15} 3^{\ell+6(b-1)} p^n$
B1	$4 \cdot 3^{b-1}\sqrt{\frac{3^\ell p^n - 1}{2}}$	$-2 \cdot 3^{2(b-1)}$	$2^9 3^{\ell+6(b-1)} p^n$
B2	$-8 \cdot 3^{b-1}\sqrt{\frac{3^\ell p^n - 1}{2}}$	$8 \cdot 3^{\ell+2(b-1)} p^n$	$-2^{15} 3^{2\ell+6(b-1)} p^{2n}$
B1′	$-4 \cdot 3^{b-1}\sqrt{\frac{3^\ell p^n - 1}{2}}$	$-2 \cdot 3^{2(b-1)}$	$2^9 3^{\ell+6(b-1)} p^n$
B2′	$8 \cdot 3^{b-1}\sqrt{\frac{3^\ell p^n - 1}{2}}$	$8 \cdot 3^{\ell+2(b-1)} p^n$	$-2^{15} 3^{2\ell+6(b-1)} p^{2n}$

2. *there exist integers $\ell \geq 2 - b$ and $n \geq 1$ such that $\frac{3^\ell + p^n}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$4 \cdot 3^{b-1}\sqrt{\frac{3^\ell + p^n}{2}}$	$2 \cdot 3^{\ell+2(b-1)}$	$2^9 3^{2\ell+6(b-1)} p^n$
C2	$-8 \cdot 3^{b-1}\sqrt{\frac{3^\ell + p^n}{2}}$	$8 \cdot 3^{2(b-1)} p^n$	$2^{15} 3^{\ell+6(b-1)} p^{2n}$
C1′	$-4 \cdot 3^{b-1}\sqrt{\frac{3^\ell + p^n}{2}}$	$2 \cdot 3^{\ell+2(b-1)}$	$2^9 3^{2\ell+6(b-1)} p^n$
C2′	$8 \cdot 3^{b-1}\sqrt{\frac{3^\ell + p^n}{2}}$	$8 \cdot 3^{2(b-1)} p^n$	$2^{15} 3^{\ell+6(b-1)} p^{2n}$
D1	$4 \cdot 3^{b-1}\sqrt{\frac{3^\ell + p^n}{2}}$	$2 \cdot 3^{2(b-1)} p^n$	$2^9 3^{\ell+6(b-1)} p^{2n}$
D2	$-8 \cdot 3^{b-1}\sqrt{\frac{3^\ell + p^n}{2}}$	$8 \cdot 3^{\ell+2(b-1)}$	$2^{15} 3^{2\ell+6(b-1)} p^n$
D1′	$-4 \cdot 3^{b-1}\sqrt{\frac{3^\ell + p^n}{2}}$	$2 \cdot 3^{2(b-1)} p^n$	$2^9 3^{\ell+6(b-1)} p^{2n}$
D2′	$8 \cdot 3^{b-1}\sqrt{\frac{3^\ell + p^n}{2}}$	$8 \cdot 3^{\ell+2(b-1)}$	$2^{15} 3^{2\ell+6(b-1)} p^n$

3. *there exist integers $\ell \geq 2 - b$ and $n \geq 1$ such that $\frac{3^\ell - p^n}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$4 \cdot 3^{b-1}\sqrt{\frac{3^\ell - p^n}{2}}$	$2 \cdot 3^{\ell+2(b-1)}$	$-2^9 3^{2\ell+6(b-1)} p^n$
E2	$-8 \cdot 3^{b-1}\sqrt{\frac{3^\ell - p^n}{2}}$	$-8 \cdot 3^{2(b-1)} p^n$	$2^{15} 3^{\ell+6(b-1)} p^{2n}$
E1′	$-4 \cdot 3^{b-1}\sqrt{\frac{3^\ell - p^n}{2}}$	$2 \cdot 3^{\ell+2(b-1)}$	$-2^9 3^{2\ell+6(b-1)} p^n$
E2′	$8 \cdot 3^{b-1}\sqrt{\frac{3^\ell - p^n}{2}}$	$-8 \cdot 3^{2(b-1)} p^n$	$2^{15} 3^{\ell+6(b-1)} p^{2n}$
F1	$4 \cdot 3^{b-1}\sqrt{\frac{3^\ell - p^n}{2}}$	$-2 \cdot 3^{2(b-1)} p^n$	$2^9 3^{\ell+6(b-1)} p^{2n}$
F2	$-8 \cdot 3^{b-1}\sqrt{\frac{3^\ell - p^n}{2}}$	$8 \cdot 3^{\ell+2(b-1)}$	$-2^{15} 3^{2\ell+6(b-1)} p^n$
F1′	$-4 \cdot 3^{b-1}\sqrt{\frac{3^\ell - p^n}{2}}$	$-2 \cdot 3^{2(b-1)} p^n$	$2^9 3^{\ell+6(b-1)} p^{2n}$
F2′	$8 \cdot 3^{b-1}\sqrt{\frac{3^\ell - p^n}{2}}$	$8 \cdot 3^{\ell+2(b-1)}$	$-2^{15} 3^{2\ell+6(b-1)} p^n$

4. *there exist integers $\ell \geq 2 - b$ and $n \geq 1$ such that $\frac{p^n - 3^\ell}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$4 \cdot 3^{b-1}\sqrt{\frac{p^n - 3^\ell}{2}}$	$2 \cdot 3^{2(b-1)} p^n$	$-2^9 3^{\ell+6(b-1)} p^{2n}$
G2	$-8 \cdot 3^{b-1}\sqrt{\frac{p^n - 3^\ell}{2}}$	$-8 \cdot 3^{\ell+2(b-1)}$	$2^{15} 3^{2\ell+6(b-1)} p^n$
G1′	$-4 \cdot 3^{b-1}\sqrt{\frac{p^n - 3^\ell}{2}}$	$2 \cdot 3^{2(b-1)} p^n$	$-2^9 3^{\ell+6(b-1)} p^{2n}$
G2′	$8 \cdot 3^{b-1}\sqrt{\frac{p^n - 3^\ell}{2}}$	$-8 \cdot 3^{\ell+2(b-1)}$	$2^{15} 3^{2\ell+6(b-1)} p^n$
H1	$4 \cdot 3^{b-1}\sqrt{\frac{p^n - 3^\ell}{2}}$	$-2 \cdot 3^{\ell+2(b-1)}$	$2^9 3^{2\ell+6(b-1)} p^n$
H2	$-8 \cdot 3^{b-1}\sqrt{\frac{p^n - 3^\ell}{2}}$	$8 \cdot 3^{2(b-1)} p^n$	$-2^{15} 3^{\ell+6(b-1)} p^{2n}$
H1′	$-4 \cdot 3^{b-1}\sqrt{\frac{p^n - 3^\ell}{2}}$	$-2 \cdot 3^{\ell+2(b-1)}$	$2^9 3^{2\ell+6(b-1)} p^n$
H2′	$8 \cdot 3^{b-1}\sqrt{\frac{p^n - 3^\ell}{2}}$	$8 \cdot 3^{2(b-1)} p^n$	$-2^{15} 3^{\ell+6(b-1)} p^{2n}$

In the case that $b = 2$, i.e. $N = 2^8 3^2 p$, we furthermore could have one of the following conditions satisfied:

5. *there exists an integer $n \geq 1$ such that $\frac{p^n + 1}{6}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$4 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$2 \cdot 3^{2s+1}p^n$	$2^9 3^{3+6s} p^{2n}$
I2	$-8 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$8 \cdot 3^{2s+1}$	$2^{15} 3^{3+6s} p^n$
I1′	$-4 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$2 \cdot 3^{2s+1}p^n$	$2^9 3^{3+6s} p^{2n}$
I2′	$8 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$8 \cdot 3^{2s+1}$	$2^{15} 3^{3+6s} p^n$
J1	$4 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$2 \cdot 3^{2s+1}$	$2^9 3^{3+6s} p^n$
J2	$-8 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$8 \cdot 3^{2s+1}p^n$	$2^{15} 3^{3+6s} p^{2n}$
J1′	$-4 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$2 \cdot 3^{2s+1}$	$2^9 3^{3+6s} p^n$
J2′	$8 \cdot 3^{s+1}\sqrt{\frac{p^n+1}{3}}$	$8 \cdot 3^{2s+1}p^n$	$2^{15} 3^{3+6s} p^{2n}$

6. *there exists an integer $n \geq 1$ such that $\frac{p^n-1}{6}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$4 \cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$2 \cdot 3^{2s+1}p^n$	$-2^9 3^{3+6s} p^{2n}$
K2	$-8 \cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$-8 \cdot 3^{2s+1}$	$2^{15} 3^{3+6s} p^n$
K1′	$-4 \cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$2 \cdot 3^{2s+1}p^n$	$-2^9 3^{3+6s} p^{2n}$
K2′	$8 \cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$-8 \cdot 3^{2s+1}$	$2^{15} 3^{3+6s} p^n$
L1	$4 \cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$-2 \cdot 3^{2s+1}$	$2^9 3^{3+6s} p^n$
L2	$-8 \cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$8 \cdot 3^{2s+1}p^n$	$-2^{15} 3^{3+6s} p^{2n}$
L1′	$-4 \cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$-2 \cdot 3^{2s+1}$	$2^9 3^{3+6s} p^n$
L2′	$8 \cdot 3^{s+1}\sqrt{\frac{p^n-1}{3}}$	$8 \cdot 3^{2s+1}p^n$	$-2^{15} 3^{3+6s} p^{2n}$

3.3 Curves of Conductor $2^\alpha 3^\beta p^2$

As we mentioned in the introduction to this chapter the models presented in the following table are minimal except in the case when the conductor is not divisible by 4. In these cases (i.e. Theorems 3.21 and 3.22) the model is minimal except at 2, and a minimal model can be found using Corollary 2.2. We choose not to do this here.

Theorem 3.21 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $3^b p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $2^6 3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot 3^{b-1} p \sqrt{2^6 3^\ell p^n + 1}$	$2^4 3^{\ell+2(b-1)} p^{n+2}$	$2^{12} 3^{2\ell+6(b-1)} p^{2n+6}$
A2	$-\epsilon \cdot 2 \cdot 3^{b-1} p \sqrt{2^6 3^\ell p^n + 1}$	$3^{2(b-1)} p^2$	$2^{12} 3^{\ell+6(b-1)} p^{n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

2. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $2^6 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot 3^{b-1} p \sqrt{2^6 3^\ell + p^n}$	$2^4 3^{\ell+2(b-1)} p^2$	$2^{12} 3^{2\ell+6(b-1)} p^{n+6}$
B2	$-\epsilon \cdot 2 \cdot 3^{b-1} p \sqrt{2^6 3^\ell + p^n}$	$3^{2(b-1)} p^{n+2}$	$2^{12} 3^{\ell+6(b-1)} p^{2n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

3. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $2^6 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot 3^{b-1} p \sqrt{2^6 3^\ell - p^n}$	$2^4 3^{\ell+2(b-1)} p^2$	$-2^{12} 3^{2\ell+6(b-1)} p^{n+6}$
C2	$-\epsilon \cdot 2 \cdot 3^{b-1} p \sqrt{2^6 3^\ell - p^n}$	$-3^{2(b-1)} p^{n+2}$	$2^{12} 3^{\ell+6(b-1)} p^{2n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

4. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $2^6 p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon \cdot 3^{b-1} p \sqrt{2^6 p^n + 3^\ell}$	$2^4 3^{2(b-1)} p^{n+2}$	$2^{12} 3^{\ell+6(b-1)} p^{2n+6}$
D2	$-\epsilon \cdot 2 \cdot 3^{b-1} p \sqrt{2^6 p^n + 3^\ell}$	$3^{\ell+2(b-1)} p^2$	$2^{12} 3^{2\ell+6(b-1)} p^{n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

5. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $2^6 + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon \cdot 3^{b-1} p \sqrt{2^6 + 3^\ell p^n}$	$2^4 3^{2(b-1)} p^2$	$2^{12} 3^{\ell+6(b-1)} p^{n+6}$
E2	$-\epsilon \cdot 2 \cdot 3^{b-1} p \sqrt{2^6 + 3^\ell p^n}$	$3^{\ell+2(b-1)} p^{n+2}$	$2^{12} 3^{2\ell+6(b-1)} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

6. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $2^6 - 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon \cdot 3^{b-1} p \sqrt{2^6 - 3^\ell p^n}$	$2^4 3^{2(b-1)} p^2$	$-2^{12} 3^{\ell+6(b-1)} p^{n+6}$
F2	$-\epsilon \cdot 2 \cdot 3^{b-1} p \sqrt{2^6 - 3^\ell p^n}$	$-3^{\ell+2(b-1)} p^{n+2}$	$2^{12} 3^{2\ell+6(b-1)} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

7. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $3^\ell - 2^6 p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$\epsilon \cdot 3^{b-1} p \sqrt{3^\ell - 2^6 p^n}$	$-2^4 3^{2(b-1)} p^{n+2}$	$2^{12} 3^{\ell+6(b-1)} p^{2n+6}$
G2	$-\epsilon \cdot 2 \cdot 3^{b-1} p \sqrt{3^\ell - 2^6 p^n}$	$3^{\ell+2(b-1)} p^2$	$-2^{12} 3^{2\ell+6(b-1)} p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

8. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $p^n - 2^6 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$\epsilon \cdot 3^{b-1} p \sqrt{p^n - 2^6 3^\ell}$	$-2^4 3^{\ell+2(b-1)} p^2$	$2^{12} 3^{2\ell+6(b-1)} p^{n+6}$
H2	$-\epsilon \cdot 2 \cdot 3^{b-1} p \sqrt{p^n - 2^6 3^\ell}$	$3^{2(b-1)} p^{n+2}$	$-2^{12} 3^{\ell+6(b-1)} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

9. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^6 3^\ell + 1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^6 3^\ell+1}{p}}$	$2^4 3^{\ell+2(b-1)}p^{2t+1}$	$2^{12}3^{2\ell+6(b-1)}p^{3+6t}$
I2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^6 3^\ell+1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^{12}3^{\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

10. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^6 3^\ell - 1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
J1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^6 3^\ell-1}{p}}$	$2^4 3^{\ell+2(b-1)}p^{2t+1}$	$-2^{12}3^{2\ell+6(b-1)}p^{3+6t}$
J2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^6 3^\ell-1}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^{12}3^{\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

11. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^6+3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^6+3^\ell}{p}}$	$2^4 3^{2(b-1)}p^{2t+1}$	$2^{12}3^{\ell+6(b-1)}p^{3+6t}$
K2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^6+3^\ell}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^{12}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

12. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^6-3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
L1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^6-3^\ell}{p}}$	$2^4 3^{2(b-1)}p^{2t+1}$	$-2^{12}3^{\ell+6(b-1)}p^{3+6t}$
L2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^6-3^\ell}{p}}$	$-3^{\ell+2(b-1)}p^{2t+1}$	$2^{12}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

13. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{3^\ell-2^6}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-2^6}{p}}$	$-2^4 3^{2(b-1)}p^{2t+1}$	$2^{12}3^{\ell+6(b-1)}p^{3+6t}$
M2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-2^6}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^{12}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

In the case that $b = 2$, i.e. $N = 2 \cdot 3^2 p^2$, we furthermore could have one of the following conditions satisfied:

14. *there exist integers $n \geq 0$ and $s \in \{0, 1\}$ such that $\frac{2^6+p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
N1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{2^6+p^n}{3}}$	$2^4 3^{2s+1}p^2$	$2^{12}3^{3+6s}p^{n+6}$
N2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{2^6+p^n}{3}}$	$3^{2s+1}p^{n+2}$	$2^{12}3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p$ modulo 4.

15. *there exist integers $n \geq 0$ and $s \in \{0, 1\}$ such that $\frac{2^6-p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{2^6-p^n}{3}}$	$2^4 3^{2s+1}p^2$	$-2^{12}3^{3+6s}p^{n+6}$
O2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{2^6-p^n}{3}}$	$-3^{2s+1}p^{n+2}$	$2^{12}3^{3+6s}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p$ modulo 4.

16. *there exist integers $n \geq 0$ and $s \in \{0, 1\}$ such that $\frac{p^n-2^6}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
P1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{p^n-2^6}{3}}$	$-2^4 3^{2s+1}p^2$	$2^{12}3^{3+6s}p^{n+6}$
P2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{p^n-2^6}{3}}$	$3^{2s+1}p^{n+2}$	$-2^{12}3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p$ modulo 4.

Theorem 3.22 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2\cdot 3^b p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 0$ such that $2^m 3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot 3^{b-1} p\sqrt{2^m 3^\ell p^n + 1}$	$2^{m-2}3^{\ell+2(b-1)}p^{n+2}$	$2^{2m}3^{2\ell+6(b-1)}p^{2n+6}$
A2	$-\epsilon \cdot 2 \cdot 3^{b-1} p\sqrt{2^m 3^\ell p^n + 1}$	$3^{2(b-1)}p^2$	$2^{m+6}3^{\ell+6(b-1)}p^{n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

2. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 0$ such that $2^m 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot 3^{b-1} p\sqrt{2^m 3^\ell + p^n}$	$2^{m-2}3^{\ell+2(b-1)}p^2$	$2^{2m}3^{2\ell+6(b-1)}p^{n+6}$
B2	$-\epsilon \cdot 2 \cdot 3^{b-1} p\sqrt{2^m 3^\ell + p^n}$	$3^{2(b-1)}p^{n+2}$	$2^{m+6}3^{\ell+6(b-1)}p^{2n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

3. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 0$ such that $2^m 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot 3^{b-1} p\sqrt{2^m 3^\ell - p^n}$	$2^{m-2}3^{\ell+2(b-1)}p^2$	$-2^{2m}3^{2\ell+6(b-1)}p^{n+6}$
C2	$-\epsilon \cdot 2 \cdot 3^{b-1} p\sqrt{2^m 3^\ell - p^n}$	$-3^{2(b-1)}p^{n+2}$	$2^{m+6}3^{\ell+6(b-1)}p^{2n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

4. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 0$ such that $2^m p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon \cdot 3^{b-1} p\sqrt{2^m p^n + 3^\ell}$	$2^{m-2}3^{2(b-1)}p^{n+2}$	$2^{2m}3^{\ell+6(b-1)}p^{2n+6}$
D2	$-\epsilon \cdot 2 \cdot 3^{b-1} p\sqrt{2^m p^n + 3^\ell}$	$3^{\ell+2(b-1)}p^2$	$2^{m+6}3^{2\ell+6(b-1)}p^{n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

5. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 0$ such that $2^m + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon \cdot 3^{b-1}p\sqrt{2^m + 3^\ell p^n}$	$2^{m-2}3^{2(b-1)}p^2$	$2^{2m}3^{\ell+6(b-1)}p^{n+6}$
E2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m + 3^\ell p^n}$	$3^{\ell+2(b-1)}p^{n+2}$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

6. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 0$ such that $2^m - 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon \cdot 3^{b-1}p\sqrt{2^m - 3^\ell p^n}$	$2^{m-2}3^{2(b-1)}p^2$	$-2^{2m}3^{\ell+6(b-1)}p^{n+6}$
F2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m - 3^\ell p^n}$	$-3^{\ell+2(b-1)}p^{n+2}$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

7. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 0$ such that $3^\ell p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$\epsilon \cdot 3^{b-1}p\sqrt{3^\ell p^n - 2^m}$	$-2^{m-2}3^{2(b-1)}p^2$	$2^{2m}3^{\ell+6(b-1)}p^{n+6}$
G2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{3^\ell p^n - 2^m}$	$3^{\ell+2(b-1)}p^{n+2}$	$-2^{m+6}3^{2\ell+6(b-1)}p^{2n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

8. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 0$ such that $3^\ell - 2^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$\epsilon 3^{b-1}p\sqrt{3^\ell - 2^m p^n}$	$-2^{m-2}3^{2(b-1)}p^{n+2}$	$2^{2m}3^{\ell+6(b-1)}p^{2n+6}$
H2	$-\epsilon 2 \cdot 3^{b-1}p\sqrt{3^\ell - 2^m p^n}$	$3^{\ell+2(b-1)}p^2$	$-2^{m+6}3^{2\ell+6(b-1)}p^{n+6}$

   where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

9. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $n \geq 0$ such that $p^n - 2^m 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$\epsilon \cdot 3^{b-1}p\sqrt{p^n - 2^m 3^\ell}$	$-2^{m-2}3^{\ell+2(b-1)}p^2$	$2^{2m}3^{2\ell+6(b-1)}p^{n+6}$
I2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{p^n - 2^m 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^{m+6}3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

10. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m 3^\ell + 1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
J1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m 3^\ell + 1}{p}}$	$2^{m-2}3^{\ell+2(b-1)}p^{2t+1}$	$2^{2m}3^{2\ell+6(b-1)}p^{3+6t}$
J2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m 3^\ell + 1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^{m+6}3^{\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

11. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m 3^\ell - 1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$\epsilon 3^{b-1}p^{t+1}\sqrt{\frac{2^m 3^\ell - 1}{p}}$	$2^{m-2}3^{\ell+2(b-1)}p^{2t+1}$	$-2^{2m}3^{2\ell+6(b-1)}p^{3+6t}$
K2	$-\epsilon 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m 3^\ell - 1}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^{m+6}3^{\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

12. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m + 3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
L1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m + 3^\ell}{p}}$	$2^{m-2}3^{2(b-1)}p^{2t+1}$	$2^{2m}3^{\ell+6(b-1)}p^{3+6t}$
L2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m + 3^\ell}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^{m+6}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

13. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m - 3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m-3^\ell}{p}}$	$2^{m-2}3^{2(b-1)}p^{2t+1}$	$-2^{2m}3^{\ell+6(b-1)}p^{3+6t}$
M2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m-3^\ell}{p}}$	$-3^{\ell+2(b-1)}p^{2t+1}$	$2^{m+6}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

14. *there exist integers $m \geq 7$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{3^\ell-2^m}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
N1	$\epsilon 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-2^m}{p}}$	$-2^{m-2}3^{2(b-1)}p^{2t+1}$	$2^{2m}3^{\ell+6(b-1)}p^{3+6t}$
N2	$-\epsilon 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-2^m}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^{m+6}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

In the case that $b = 2$, i.e. $N = 2 \cdot 3^2 p^2$, we furthermore could have one of the following conditions satisfied:

15. *there exist integers $m \geq 7$, $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{2^m+p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{2^m+p^n}{3}}$	$2^{m-2}3^{2s+1}p^2$	$2^{2m}3^{3+6s}p^{n+6}$
O2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{2^m+p^n}{3}}$	$3^{2s+1}p^{n+2}$	$2^{m+6}3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p$ modulo 4.

16. *there exist integers $m \geq 7$, $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{2^m-p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
P1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{2^m-p^n}{3}}$	$2^{m-2}3^{2s+1}p^2$	$-2^{2m}3^{3+6s}p^{n+6}$
P2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{2^m-p^n}{3}}$	$-3^{2s+1}p^{n+2}$	$2^{m+6}3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p$ modulo 4.

17. *there exist integers $m \geq 7$, $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{p^n-2^m}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	$\epsilon \cdot 3^{s+1} p \sqrt{\frac{p^n-2^m}{3}}$	$-2^{m-2} 3^{2s+1} p^2$	$2^{2m} 3^{3+6s} p^{n+6}$
Q2	$-\epsilon \cdot 2 \cdot 3^{s+1} p \sqrt{\frac{p^n-2^m}{3}}$	$3^{2s+1} p^{n+2}$	$-2^{m+6} 3^{3+6s} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p$ modulo 4.

18. *there exist integers $m \geq 7$ and $s,t \in \{0,1\}$ such that $\frac{2^m+1}{3p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
R1	$\epsilon \cdot 3^{s+1} p^{t+1} \sqrt{\frac{2^m-p^n}{3}}$	$2^{m-2} 3^{2s+1} p^{2t+1}$	$2^{2m} 3^{3+6s} p^{3+6t}$
R2	$-\epsilon \cdot 2 \cdot 3^{s+1} p^{t+1} \sqrt{\frac{2^m-p^n}{3}}$	$3^{2s+1} p^{2t+1}$	$2^{m+6} 3^{3+6s} p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p^{t+1}$ modulo 4.

19. *there exist integers $m \geq 7$ and $s,t \in \{0,1\}$ such that $\frac{2^m-1}{3p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
S1	$\epsilon \cdot 3^{s+1} p^{t+1} \sqrt{\frac{2^m-p^n}{3}}$	$2^{m-2} 3^{2s+1} p^{2t+1}$	$-2^{2m} 3^{3+6s} p^{3+6t}$
S2	$-\epsilon \cdot 2 \cdot 3^{s+1} p^{t+1} \sqrt{\frac{2^m-p^n}{3}}$	$-3^{2s+1} p^{2t+1}$	$2^{m+6} 3^{3+6s} p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p^{t+1}$ modulo 4.

Theorem 3.23 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^2 3^b p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $4 \cdot 3^\ell + p^n$ is a square, $3^\ell \equiv -1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot 3^{b-1} p \sqrt{4 \cdot 3^\ell + p^n}$	$3^{\ell+2(b-1)} p^2$	$2^4 3^{2\ell+6(b-1)} p^{n+6}$
A2	$-\epsilon \cdot 2 \cdot 3^{b-1} p \sqrt{4 \cdot 3^\ell + p^n}$	$3^{2(b-1)} p^{n+2}$	$2^8 3^{\ell+6(b-1)} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

2. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $4 \cdot 3^\ell - p^n$ is a square, $3^\ell \equiv -1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot 3^{b-1}p\sqrt{4 \cdot 3^\ell - p^n}$	$3^{\ell+2(b-1)}p^2$	$-2^4 3^{2\ell+6(b-1)}p^{n+6}$
B2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{4 \cdot 3^\ell - p^n}$	$-3^{2(b-1)}p^{n+2}$	$2^8 3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

3. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $4p^n - 3^\ell$ is a square, $p^n \equiv -1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot 3^{b-1}p\sqrt{4p^n - 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^4 3^{\ell+6(b-1)}p^{2n+6}$
C2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{4p^n - 3^\ell}$	$-3^{\ell+2(b-1)}p^2$	$2^8 3^{2\ell+6(b-1)}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

4. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $p^n - 4 \cdot 3^\ell$ is a square, $3^\ell \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon \cdot 3^{b-1}p\sqrt{p^n - 4 \cdot 3^\ell}$	$-3^{\ell+2(b-1)}p^2$	$2^4 3^{2\ell+6(b-1)}p^{n+6}$
D2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{p^n - 4 \cdot 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^8 3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

5. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{4 \cdot 3^\ell + 1}{p}$ is a square, $3^\ell p \equiv -1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4 \cdot 3^\ell + 1}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^4 3^{2\ell+6(b-1)}p^{3+6t}$
E2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4 \cdot 3^\ell + 1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^8 3^{\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

6. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{4\cdot 3^\ell - 1}{p}$ is a square, $3^\ell p \equiv -1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4\cdot 3^\ell-1}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^4 3^{2\ell+6(b-1)}p^{3+6t}$
F2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4\cdot 3^\ell-1}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^8 3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

7. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{4+3^\ell}{p}$ is a square, $p \equiv -1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4+3^\ell}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^4 3^{\ell+6(b-1)}p^{3+6t}$
G2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4+3^\ell}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^8 3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

8. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{3^\ell-4}{p}$ is a square, $p \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-4}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^4 3^{\ell+6(b-1)}p^{3+6t}$
H2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-4}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^8 3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

In the case that $b = 2$, i.e. $N = 2^2 3^2 p^2$, we furthermore could have one of the following conditions satisfied:

9. *there exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{4p^n-1}{3}$ is a square, $p^n \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$\epsilon 3^{s+1}p\sqrt{\frac{4p^n-1}{3}}$	$3^{2s+1}p^{n+2}$	$-2^4 3^{3+6s}p^{2n+6}$
I2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{4p^n-1}{3}}$	$-3^{2s+1}p^2$	$2^8 3^{3+6s}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s-1}p$ modulo 4.

10. *there exists an integers $n \geq 0$ and $s \in \{0, 1\}$ such that $\frac{p^n+4}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
J1	$\epsilon 3^{s+1}p\sqrt{\frac{p^n+4}{3}}$	$3^{2s+1}p^2$	$2^4 3^{3+6s}p^{n+6}$
J2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{p^n+4}{3}}$	$3^{2s+1}p^{n+2}$	$2^8 3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s-1}p$ modulo 4.

Theorem 3.24 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^3 3^b p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $m \in \{4, 5\}$, $\ell \geq 2 - b$ and $n \geq 0$ such that $2^m 3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$\epsilon \cdot 3^{b-1}p\sqrt{2^m 3^\ell p^n + 1}$	$2^{m-2}3^{\ell+2(b-1)}p^{n+2}$	$2^{2m}3^{2\ell+6(b-1)}p^{2n+6}$
A2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m 3^\ell p^n + 1}$	$3^{2(b-1)}p^2$	$2^{m+6}3^{\ell+6(b-1)}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

2. *there exist integers $\ell \geq 2 - b$ and $n \geq 0$ such that $4 \cdot 3^\ell + p^n$ is a square, $3^\ell \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$-\epsilon \cdot 3^{b-1}p\sqrt{4 \cdot 3^\ell + p^n}$	$3^{\ell+2(b-1)}p^2$	$2^4 3^{2\ell+6(b-1)}p^{n+6}$
B2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{4 \cdot 3^\ell + p^n}$	$3^{2(b-1)}p^{n+2}$	$2^8 3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

3. *there exist integers $m \in \{4, 5\}$, $\ell \geq 2 - b$ and $n \geq 0$ such that $2^m 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$\epsilon \cdot 3^{b-1}p\sqrt{2^m 3^\ell + p^n}$	$2^{m-2}3^{\ell+2(b-1)}p^2$	$2^{2m}3^{2\ell+6(b-1)}p^{n+6}$
C2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m 3^\ell + p^n}$	$3^{2(b-1)}p^{n+2}$	$2^{m+6}3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

4. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $4 \cdot 3^\ell - p^n$ is a square, $3^\ell \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$-\epsilon \cdot 3^{b-1}p\sqrt{4 \cdot 3^\ell - p^n}$	$3^{\ell+2(b-1)}p^2$	$-2^4 3^{2\ell+6(b-1)}p^{n+6}$
D2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{4 \cdot 3^\ell - p^n}$	$-3^{2(b-1)}p^{n+2}$	$2^8 3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

5. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $n \geq 0$ such that $2^m 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$\epsilon \cdot 3^{b-1}p\sqrt{2^m 3^\ell - p^n}$	$2^{m-2}3^{\ell+2(b-1)}p^2$	$-2^{2m}3^{2\ell+6(b-1)}p^{n+6}$
E2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m 3^\ell - p^n}$	$-3^{2(b-1)}p^{n+2}$	$2^{m+6}3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

6. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $n \geq 0$ such that $2^m p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$\epsilon \cdot 3^{b-1}p\sqrt{2^m p^n + 3^\ell}$	$2^{m-2}3^{2(b-1)}p^{n+2}$	$2^{2m}3^{\ell+6(b-1)}p^{2n+6}$
F2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m p^n + 3^\ell}$	$3^{\ell+2(b-1)}p^2$	$2^{m+6}3^{2\ell+6(b-1)}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

7. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $4p^n - 3^\ell$ is a square, $p^n \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$-\epsilon \cdot 3^{b-1}p\sqrt{4p^n - 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^4 3^{\ell+6(b-1)}p^{2n+6}$
G2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{4p^n - 3^\ell}$	$-3^{\ell+2(b-1)}p^2$	$2^8 3^{2\ell+6(b-1)}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

8. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $4 + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$-\epsilon \cdot 3^{b-1}p\sqrt{4+3^\ell p^n}$	$3^{2(b-1)}p^2$	$2^4 3^{\ell+6(b-1)}p^{n+6}$
H2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{4+3^\ell p^n}$	$3^{\ell+2(b-1)}p^{n+2}$	$2^8 3^{2\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

9. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $n \geq 0$ such that $2^m + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$\epsilon \cdot 3^{b-1}p\sqrt{2^m+3^\ell p^n}$	$2^{m-2}3^{2(b-1)}p^2$	$2^{2m}3^{\ell+6(b-1)}p^{n+6}$
I2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m+3^\ell p^n}$	$3^{\ell+2(b-1)}p^{n+2}$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

10. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $n \geq 0$ such that $2^m - 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
J1	$\epsilon \cdot 3^{b-1}p\sqrt{2^m-3^\ell p^n}$	$2^{m-2}3^{2(b-1)}p^2$	$-2^{2m}3^{\ell+6(b-1)}p^{n+6}$
J2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m-3^\ell p^n}$	$-3^{\ell+2(b-1)}p^{n+2}$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

11. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $n \geq 0$ such that $3^\ell p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$\epsilon \cdot 3^{b-1}p\sqrt{3^\ell p^n-2^m}$	$-2^{m-2}3^{2(b-1)}p^2$	$2^{2m}3^{\ell+6(b-1)}p^{n+6}$
K2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{3^\ell p^n-2^m}$	$3^{\ell+2(b-1)}p^{n+2}$	$-2^{m+6}3^{2\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

12. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $n \geq 0$ such that $3^\ell - 2^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
L1	$\epsilon \cdot 3^{b-1}p\sqrt{3^\ell-2^m p^n}$	$-2^{m-2}3^{2(b-1)}p^{n+2}$	$2^{2m}3^{\ell+6(b-1)}p^{2n+6}$
L2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{3^\ell-2^m p^n}$	$3^{\ell+2(b-1)}p^2$	$-2^{m+6}3^{2\ell+6(b-1)}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

13. *there exist integers $\ell \geq 2-b$ and $n \geq 1$ such that $p^n - 4 \cdot 3^\ell$ is a square, $3^\ell \equiv -1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$-\epsilon \cdot 3^{b-1}p\sqrt{p^n - 4 \cdot 3^\ell}$	$-3^{\ell+2(b-1)}p^2$	$2^4 3^{2\ell+6(b-1)}p^{n+6}$
M2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{p^n - 4 \cdot 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^8 3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

14. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $n \geq 0$ such that $p^n - 2^m 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
N1	$\epsilon \cdot 3^{b-1}p\sqrt{p^n - 2^m 3^\ell}$	$-2^{m-2}3^{\ell+2(b-1)}p^2$	$2^{2m}3^{2\ell+6(b-1)}p^{n+6}$
N2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{p^n - 2^m 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^{m+6}3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

15. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{4\cdot 3^\ell+1}{p}$ is a square, $3^\ell p \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$-\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4\cdot 3^\ell+1}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^4 3^{2\ell+6(b-1)}p^{3+6t}$
O2	$\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4\cdot 3^\ell+1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^8 3^{\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

16. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m 3^\ell+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
P1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m 3^\ell+1}{p}}$	$2^{m-2}3^{\ell+2(b-1)}p^{2t+1}$	$2^{2m}3^{2\ell+6(b-1)}p^{3+6t}$
P2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m 3^\ell+1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^{m+6}3^{\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

17. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{4\cdot 3^\ell - 1}{p}$ is a square, $3^\ell p \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	$-\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4\cdot 3^\ell-1}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^4 3^{2\ell+6(b-1)}p^{3+6t}$
Q2	$\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4\cdot 3^\ell-1}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^8 3^{\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

18. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m 3^\ell - 1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
R1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m 3^\ell-1}{p}}$	$2^{m-2}3^{\ell+2(b-1)}p^{2t+1}$	$-2^{2m}3^{2\ell+6(b-1)}p^{3+6t}$
R2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m 3^\ell-1}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^{m+6}3^{\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

19. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{4+3^\ell}{p}$ is a square, $p \equiv 1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
S1	$-\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4+3^\ell}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^4 3^{\ell+6(b-1)}p^{3+6t}$
S2	$\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4+3^\ell}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^8 3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

20. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m+3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
T1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m+3^\ell}{p}}$	$2^{m-2}3^{2(b-1)}p^{2t+1}$	$2^{2m}3^{\ell+6(b-1)}p^{3+6t}$
T2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m+3^\ell}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^{m+6}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

21. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m-3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
U1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m-3^\ell}{p}}$	$2^{m-2}3^{2(b-1)}p^{2t+1}$	$-2^{2m}3^{\ell+6(b-1)}p^{3+6t}$
U2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m-3^\ell}{p}}$	$-3^{\ell+2(b-1)}p^{2t+1}$	$2^{m+6}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

22. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{3^\ell-4}{p}$ is a square, $p \equiv -1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
V1	$-\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-4}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^4 3^{2\ell+6(b-1)}p^{3+6t}$
V2	$\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-4}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^8 3^{\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

23. *there exist integers $m \in \{4,5\}$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{3^\ell-2^m}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
W1	$\epsilon 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-2^m}{p}}$	$-2^{m-2}3^{2(b-1)}p^{2t+1}$	$2^{2m}3^{\ell+6(b-1)}p^{3+6t}$
W2	$-\epsilon 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-2^m}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^{m+6}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

In the case that $b = 2$, i.e. $N = 2^3 3^2 p^2$, we furthermore could have one of the following conditions satisfied:

24. *there exist integers $m \in \{4,5\}$, $n \geq 0$, and $s \in \{0,1\}$ such that $\frac{2^m+p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
X1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{2^m+p^n}{3}}$	$2^{m-2}3^{2s+1}p^2$	$2^{2m}3^{3+6s}p^{n+6}$
X2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{2^m+p^n}{3}}$	$3^{2s+1}p^{n+2}$	$2^{m+6}3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p$ modulo 4.

25. *there exist integers $m \in \{4, 5\}$, $n \geq 0$, and $s \in \{0, 1\}$ such that $\frac{2^m - p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Y1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{2^m - p^n}{3}}$	$2^{m-2}3^{2s+1}p^2$	$-2^{2m}3^{3+6s}p^{n+6}$
Y2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{2^m - p^n}{3}}$	$-3^{2s+1}p^{n+2}$	$2^{m+6}3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p$ modulo 4.

26. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{4p^n - 1}{3}$ is a square, $p^n \equiv -1 \pmod 4$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Z1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{4p^n - 1}{3}}$	$3^{2s+1}p^{n+2}$	$-2^4 3^{3+6s}p^{2n+6}$
Z2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{4p^n - 1}{3}}$	$-3^{2s+1}p^2$	$2^8 3^{3+6s}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p$ modulo 4.

27. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n - 4}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Z1	$-\epsilon \cdot 3^{s+1}p\sqrt{\frac{p^n - 4}{3}}$	$-3^{2s+1}p^2$	$2^4 3^{3+6s}p^{n+6}$
Z2	$\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{p^n - 4}{3}}$	$3^{2s+1}p^{n+2}$	$-2^8 3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p$ modulo 4.

28. *there exist integers $m \in \{4, 5\}$, $n \geq 1$, and $s \in \{0, 1\}$ such that $\frac{p^n - 2^m}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
AA1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{p^n - 2^m}{3}}$	$-2^{m-2}3^{2s+1}p^2$	$2^{2m}3^{3+6s}p^{n+6}$
AA2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{p^n - 2^m}{3}}$	$3^{2s+1}p^{n+2}$	$-2^{m+6}3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p$ modulo 4.

29. *there exist integers $m \in \{5\}$, $s \in \{0,1\}$ and $t \in \{0,1\}$ such that $\frac{2^m+1}{3p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
BB1	$\epsilon \cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m+1}{3p}}$	$2^{m-2}3^{2s+1}p^{2t+1}$	$2^{2m}3^{3+6s}p^{3+6t}$
BB2	$-\epsilon \cdot 2 \cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m+1}{3p}}$	$3^{2s+1}p^{2t+1}$	$2^{m+6}3^{3+6s}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p^{t+1}$ modulo 4.

30. *there exist integers $m \in \{4\}$, $s \in \{0,1\}$ and $t \in \{0,1\}$ such that $\frac{2^m-1}{3p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
CC1	$\epsilon \cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m-1}{3p}}$	$2^{m-2}3^{2s+1}p^{2t+1}$	$-2^{2m}3^{3+6s}p^{3+6t}$
CC2	$-\epsilon \cdot 2 \cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m-1}{3p}}$	$-3^{2s+1}p^{2t+1}$	$2^{m+6}3^{3+6s}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{s+1}p^{t+1}$ modulo 4.

Theorem 3.25 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^4 3^b p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 0$ such that $2^m 3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$-\epsilon \cdot 3^{b-1}p\sqrt{2^m 3^\ell p^n + 1}$	$2^{m-2}3^{\ell+2(b-1)}p^{n+2}$	$2^{2m}3^{2\ell+6(b-1)}p^{2n+6}$
A2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m 3^\ell p^n + 1}$	$3^{2(b-1)}p^2$	$2^{m+6}3^{\ell+6(b-1)}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

2. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $4 \cdot 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
B1	$\epsilon \cdot 3^{b-1}p\sqrt{4 \cdot 3^\ell + p^n}$	$3^{\ell+2(b-1)}p^2$	$2^4 3^{2\ell+6(b-1)}p^{n+6}$
B2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{4 \cdot 3^\ell + p^n}$	$3^{2(b-1)}p^{n+2}$	$2^8 3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{\ell+b-1}p$ modulo 4.

3. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 0$ such that $2^m 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$-\epsilon \cdot 3^{b-1}p\sqrt{2^m 3^\ell + p^n}$	$2^{m-2}3^{\ell+2(b-1)}p^2$	$2^{2m}3^{2\ell+6(b-1)}p^{n+6}$
C2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m 3^\ell + p^n}$	$3^{2(b-1)}p^{n+2}$	$2^{m+6}3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

4. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $4 \cdot 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
D1	$\epsilon \cdot 3^{b-1}p\sqrt{4 \cdot 3^\ell - p^n}$	$3^{\ell+2(b-1)}p^2$	$-2^4 3^{2\ell+6(b-1)}p^{n+6}$
D2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{4 \cdot 3^\ell - p^n}$	$-3^{2(b-1)}p^{n+2}$	$2^8 3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{\ell+b-1}p$ modulo 4.

5. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 0$ such that $2^m 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$-\epsilon \cdot 3^{b-1}p\sqrt{2^m 3^\ell - p^n}$	$2^{m-2}3^{\ell+2(b-1)}p^2$	$-2^{2m}3^{2\ell+6(b-1)}p^{n+6}$
E2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m 3^\ell - p^n}$	$-3^{2(b-1)}p^{n+2}$	$2^{m+6}3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

6. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 0$ such that $2^m p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
F1	$-\epsilon \cdot 3^{b-1}p\sqrt{2^m p^n + 3^\ell}$	$2^{m-2}3^{2(b-1)}p^{n+2}$	$2^{2m}3^{\ell+6(b-1)}p^{2n+6}$
F2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m p^n + 3^\ell}$	$3^{\ell+2(b-1)}p^2$	$2^{m+6}3^{2\ell+6(b-1)}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

7. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $4p^n - 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$\epsilon \cdot 3^{b-1}p\sqrt{4p^n - 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^4 3^{\ell+6(b-1)}p^{2n+6}$
G2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{4p^n - 3^\ell}$	$-3^{\ell+2(b-1)}p^2$	$2^8 3^{2\ell+6(b-1)}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{n+1}$ modulo 4.

8. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $4 + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
H1	$\epsilon \cdot 3^{b-1}p\sqrt{4 + 3^\ell p^n}$	$3^{2(b-1)}p^2$	$2^4 3^{\ell+6(b-1)}p^{n+6}$
H2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{4 + 3^\ell p^n}$	$3^{\ell+2(b-1)}p^{n+2}$	$2^8 3^{2\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

9. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 0$ such that $2^m + 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$-\epsilon \cdot 3^{b-1}p\sqrt{2^m + 3^\ell p^n}$	$2^{m-2}3^{2(b-1)}p^2$	$2^{2m}3^{\ell+6(b-1)}p^{n+6}$
I2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m + 3^\ell p^n}$	$3^{\ell+2(b-1)}p^{n+2}$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

10. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 0$ such that $2^m - 3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
J1	$-\epsilon \cdot 3^{b-1}p\sqrt{2^m - 3^\ell p^n}$	$2^{m-2}3^{2(b-1)}p^2$	$-2^{2m}3^{\ell+6(b-1)}p^{n+6}$
J2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{2^m - 3^\ell p^n}$	$-3^{\ell+2(b-1)}p^{n+2}$	$2^{m+6}3^{2\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

11. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 0$ such that $3^\ell p^n - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$-\epsilon \cdot 3^{b-1}p\sqrt{3^\ell p^n - 2^m}$	$-2^{m-2}3^{2(b-1)}p^2$	$2^{2m}3^{\ell+6(b-1)}p^{n+6}$
K2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{3^\ell p^n - 2^m}$	$3^{\ell+2(b-1)}p^{n+2}$	$-2^{m+6}3^{2\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

12. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 0$ such that $3^\ell - 2^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
L1	$-\epsilon \cdot 3^{b-1}p\sqrt{3^\ell - 2^m p^n}$	$-2^{m-2}3^{2(b-1)}p^{n+2}$	$2^{2m}3^{\ell+6(b-1)}p^{2n+6}$
L2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{3^\ell - 2^m p^n}$	$3^{\ell+2(b-1)}p^2$	$-2^{m+6}3^{2\ell+6(b-1)}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

13. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $p^n - 4 \cdot 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$\epsilon \cdot 3^{b-1}p\sqrt{p^n - 4 \cdot 3^\ell}$	$-3^{\ell+2(b-1)}p^2$	$2^4 3^{2\ell+6(b-1)}p^{n+6}$
M2	$-\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{p^n - 4 \cdot 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^8 3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{\ell+b}p$ modulo 4.

14. *there exist integers $m \geq 4$, $\ell \geq 2-b$, and $n \geq 0$ such that $p^n - 2^m 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
N1	$-\epsilon \cdot 3^{b-1}p\sqrt{p^n - 2^m 3^\ell}$	$-2^{m-2}3^{\ell+2(b-1)}p^2$	$2^{2m}3^{2\ell+6(b-1)}p^{n+6}$
N2	$\epsilon \cdot 2 \cdot 3^{b-1}p\sqrt{p^n - 2^m 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^{m+6}3^{\ell+6(b-1)}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p$ modulo 4.

15. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{4\cdot 3^\ell+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4\cdot 3^\ell+1}{p}}$	$2^m 3^{\ell+2(b-1)}p^{2t+1}$	$2^4 3^{2\ell+6(b-1)}p^{3+6t}$
O2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{4\cdot 3^\ell+1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^8 3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{\ell+b-1}p^t$ modulo 4.

16. *there exist integers $m \geq 4$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m 3^\ell+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
P1	$-\epsilon \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell+1}{p}}$	$2^m 3^{\ell+2(b-1)} p^{2t+1}$	$2^{2m} 3^{2\ell+6(b-1)} p^{3+6t}$
P2	$\epsilon \cdot 2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell+1}{p}}$	$3^{2(b-1)} p^{2t+1}$	$2^{m+6} 3^{\ell+6(b-1)} p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

17. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{4 \cdot 3^\ell-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	$\epsilon \cdot 3^{b-1} p^{t+1} \sqrt{\frac{4 \cdot 3^\ell-1}{p}}$	$2^m 3^{\ell+2(b-1)} p^{2t+1}$	$-2^4 3^{2\ell+6(b-1)} p^{3+6t}$
Q2	$-\epsilon \cdot 2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{4 \cdot 3^\ell-1}{p}}$	$-3^{2(b-1)} p^{2t+1}$	$2^8 3^{\ell+6(b-1)} p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{\ell+b-1}p^t$ modulo 4.

18. *there exist integers $m \geq 4$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m 3^\ell-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
R1	$-\epsilon \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell-1}{p}}$	$2^m 3^{\ell+2(b-1)} p^{2t+1}$	$-2^{2m} 3^{2\ell+6(b-1)} p^{3+6t}$
R2	$\epsilon \cdot 2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell-1}{p}}$	$-3^{2(b-1)} p^{2t+1}$	$2^{m+6} 3^{\ell+6(b-1)} p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

19. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{4+3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
S1	$\epsilon \cdot 3^{b-1} p^{t+1} \sqrt{\frac{4+3^\ell}{p}}$	$3^{2(b-1)} p^{2t+1}$	$2^4 3^{\ell+6(b-1)} p^{3+6t}$
S2	$-\epsilon \cdot 2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{4+3^\ell}{p}}$	$3^{\ell+2(b-1)} p^{2t+1}$	$2^8 3^{2\ell+6(b-1)} p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^t$ modulo 4.

20. *there exist integers $m \geq 4$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m+3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
T1	$-\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m+3^\ell}{p}}$	$2^{m-2}3^{2(b-1)}p^{2t+1}$	$2^{2m}3^{\ell+6(b-1)}p^{3+6t}$
T2	$\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m+3^\ell}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^{m+6}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

21. *there exist integers $m \geq 4$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m-3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
U1	$-\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m-3^\ell}{p}}$	$2^{m-2}3^{2(b-1)}p^{2t+1}$	$-2^{2m}3^{\ell+6(b-1)}p^{3+6t}$
U2	$\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{2^m-3^\ell}{p}}$	$-3^{\ell+2(b-1)}p^{2t+1}$	$2^{m+6}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

22. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{3^\ell-4}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
V1	$\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-4}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^4 3^{\ell+6(b-1)}p^{3+6t}$
V2	$-\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-4}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^8 3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^b p^t$ modulo 4.

23. *there exist integers $m \geq 4$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{3^\ell-2^m}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
W1	$-\epsilon \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-2^m}{p}}$	$-2^{m-2}3^{2(b-1)}p^{2t+1}$	$2^{2m}3^{\ell+6(b-1)}p^{3+6t}$
W2	$\epsilon \cdot 2 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-2^m}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^{m+6}3^{2\ell+6(b-1)}p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^{b-1}p^{t+1}$ modulo 4.

In the case that $b = 2$, i.e. $N = 2^4 3^2 p^2$, we furthermore could have one of the following conditions satisfied:

24. *there exist integers $n \geq 0$ and $s \in \{0, 1\}$ such that $\frac{4p^n-1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
X1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{4p^n-1}{3}}$	$3^{2s+1}p^{n+2}$	$-2^4 3^{3+6s}p^{2n+6}$
X2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{4p^n-1}{3}}$	$-3^{2s+1}p^2$	$2^8 3^{3+6s}p^{n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^s p^{n+1}$ modulo 4.

25. *there exist integers $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n+4}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Y1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{p^n+4}{3}}$	$3^{2s+1}p^2$	$2^4 3^{3+6s}p^{n+6}$
Y2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{p^n+4}{3}}$	$3^{2s+1}p^{n+2}$	$2^8 3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^s p$ modulo 4.

26. *there exist integers $m \geq 4$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{2^m+p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Z1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{2^m+p^n}{3}}$	$2^{m-2}3^{2s+1}p^2$	$2^{2m}3^{3+6s}p^{n+6}$
Z2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{2^m+p^n}{3}}$	$3^{2s+1}p^{n+2}$	$2^{m+6}3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^s p$ modulo 4.

27. *there exist integers $m \geq 4$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{2^m-p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
AA1	$\epsilon \cdot 3^{s+1}p\sqrt{\frac{2^m-p^n}{3}}$	$2^{m-2}3^{2s+1}p^2$	$-2^{2m}3^{3+6s}p^{n+6}$
AA2	$-\epsilon \cdot 2 \cdot 3^{s+1}p\sqrt{\frac{2^m-p^n}{3}}$	$-3^{2s+1}p^{n+2}$	$2^{m+6}3^{3+6s}p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^s p$ modulo 4.

28. *there exist integer $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n-4}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
BB1	$-\epsilon \cdot 3^{s+1} p \sqrt{\frac{p^n-4}{3}}$	$-3^{2s+1}p^2$	$2^4 3^{3+6s} p^{n+6}$
BB2	$\epsilon \cdot 2 \cdot 3^{s+1} p \sqrt{\frac{p^n-4}{3}}$	$3^{2s+1}p^{n+2}$	$-2^8 3^{3+6s} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^s p$ modulo 4.

29. *there exist integers $m \geq 4$, $n \geq 1$ and $s \in \{0, 1\}$ such that $\frac{p^n-2^m}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
CC1	$\epsilon \cdot 3^{s+1} p \sqrt{\frac{p^n-2^m}{3}}$	$-2^{m-2}3^{2s+1}p^2$	$2^{2m} 3^{3+6s} p^{n+6}$
CC2	$-\epsilon \cdot 2 \cdot 3^{s+1} p \sqrt{\frac{p^n-2^m}{3}}$	$3^{2s+1}p^{n+2}$	$-2^{m+6} 3^{3+6s} p^{2n+6}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^s p$ modulo 4.

30. *there exist integers $m \geq 4$ and $s, t \in \{0, 1\}$ such that $\frac{2^m+1}{3p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
DD1	$\epsilon \cdot 3^{s+1} p^{t+1} \sqrt{\frac{2^m+1}{3p}}$	$2^{m-2}3^{2s+1}p^{2t+1}$	$2^{2m} 3^{3+6s} p^{3+6t}$
DD2	$-\epsilon \cdot 2 \cdot 3^{s+1} p^{t+1} \sqrt{\frac{2^m+1}{3p}}$	$3^{2s+1}p^{2t+1}$	$2^{m+6} 3^{3+6s} p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^s p^{t+1}$ modulo 4.

31. *there exist integers $m \geq 4$ and $s, t \in \{0, 1\}$ such that $\frac{2^m-1}{3p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
EE1	$\epsilon \cdot 3^{s+1} p^{t+1} \sqrt{\frac{2^m-1}{3p}}$	$2^{m-2}3^{2s+1}p^{2t+1}$	$-2^{2m} 3^{3+6s} p^{3+6t}$
EE2	$-\epsilon \cdot 2 \cdot 3^{s+1} p^{t+1} \sqrt{\frac{2^m-1}{3p}}$	$-3^{2s+1}p^{2t+1}$	$2^{m+6} 3^{3+6s} p^{3+6t}$

where $\epsilon \in \{\pm 1\}$ is the residue of $3^s p^{t+1}$ modulo 4.

Theorem 3.26 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^5 3^b p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$2 \cdot 3^{b-1} p \sqrt{3^\ell p^n + 1}$	$3^{\ell+2(b-1)} p^{n+2}$	$2^6 3^{2\ell+6(b-1)} p^{2n+6}$
A2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell p^n + 1}$	$4 \cdot 3^{2(b-1)} p^2$	$2^{12} 3^{\ell+6(b-1)} p^{n+6}$
A1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell p^n + 1}$	$3^{\ell+2(b-1)} p^{n+2}$	$2^6 3^{2\ell+6(b-1)} p^{2n+6}$
A2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell p^n + 1}$	$4 \cdot 3^{2(b-1)} p^2$	$2^{12} 3^{\ell+6(b-1)} p^{n+6}$

2. *there exist integers $\ell \geq 1$ and $n \geq 0$ such that $3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) *ℓ is even;*

	a_2	a_4	Δ
B1	$2 \cdot 3^{b-1} p \sqrt{3^\ell + p^n}$	$3^{2(b-1)} p^{n+2}$	$2^6 3^{\ell+6(b-1)} p^{2n+6}$
B2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell + p^n}$	$4 \cdot 3^{\ell+2(b-1)} p^2$	$2^{12} 3^{2\ell+6(b-1)} p^{n+6}$
B1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell + p^n}$	$3^{2(b-1)} p^{n+2}$	$2^6 3^{\ell+6(b-1)} p^{2n+6}$
B2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell + p^n}$	$4 \cdot 3^{\ell+2(b-1)} p^2$	$2^{12} 3^{2\ell+6(b-1)} p^{n+6}$

   (b) *ℓ is odd;*

	a_2	a_4	Δ
C1	$2 \cdot 3^{b-1} p \sqrt{3^\ell + p^n}$	$3^{\ell+2(b-1)} p^2$	$2^6 3^{2\ell+6(b-1)} p^{n+6}$
C2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell + p^n}$	$4 \cdot 3^{2(b-1)} p^{n+2}$	$2^{12} 3^{\ell+6(b-1)} p^{2n+6}$
C1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell + p^n}$	$3^{\ell+2(b-1)} p^2$	$2^6 3^{2\ell+6(b-1)} p^{n+6}$
C2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell + p^n}$	$4 \cdot 3^{2(b-1)} p^{n+2}$	$2^{12} 3^{\ell+6(b-1)} p^{2n+6}$

3. *there exist integers $\ell \geq 1$ and $n \geq 0$ such that $3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) *ℓ is even;*

	a_2	a_4	Δ
D1	$2 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$-3^{2(b-1)} p^{n+2}$	$2^6 3^{\ell+6(b-1)} p^{2n+6}$
D2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$4 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{12} 3^{2\ell+6(b-1)} p^{n+6}$
D1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$-3^{2(b-1)} p^{n+2}$	$2^6 3^{\ell+6(b-1)} p^{2n+6}$
D2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$4 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{12} 3^{2\ell+6(b-1)} p^{n+6}$

(b) ℓ is odd;

	a_2	a_4	Δ
E1	$2 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$3^{\ell+2(b-1)} p^2$	$-2^6 3^{2\ell+6(b-1)} p^{n+6}$
E2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^{n+2}$	$2^{12} 3^{\ell+6(b-1)} p^{2n+6}$
E1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$3^{\ell+2(b-1)} p^2$	$-2^6 3^{2\ell+6(b-1)} p^{n+6}$
E2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^{n+2}$	$2^{12} 3^{\ell+6(b-1)} p^{2n+6}$

4. *there exist integers $\ell \geq 2 - b$ and $n \geq 0$ such that $p^n - 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

(a) ℓ is even;

	a_2	a_4	Δ
F1	$2 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$-3^{\ell+2(b-1)} p^2$	$2^6 3^{2\ell+6(b-1)} p^{n+6}$
F2	$-4 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$4 \cdot 3^{2(b-1)} p^{n+2}$	$-2^{12} 3^{\ell+6(b-1)} p^{2n+6}$
F1′	$-2 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$-3^{\ell+2(b-1)} p^2$	$2^6 3^{2\ell+6(b-1)} p^{n+6}$
F2′	$4 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$4 \cdot 3^{2(b-1)} p^{n+2}$	$-2^{12} 3^{\ell+6(b-1)} p^{2n+6}$

(b) ℓ is odd;

	a_2	a_4	Δ
G1	$2 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$3^{2(b-1)} p^{n+2}$	$-2^6 3^{\ell+6(b-1)} p^{2n+6}$
G2	$-4 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)} p^2$	$2^{12} 3^{2\ell+6(b-1)} p^{n+6}$
G1′	$-2 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$3^{2(b-1)} p^{n+2}$	$-2^6 3^{\ell+6(b-1)} p^{2n+6}$
G2′	$4 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)} p^2$	$2^{12} 3^{2\ell+6(b-1)} p^{n+6}$

5. *there exist integers $\ell \geq 1$ and $t \in \{0, 1\}$ such that $\frac{3^\ell+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

(a) $p \equiv 1 \pmod 4$;

	a_2	a_4	Δ
H1	$2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell+1}{p}}$	$3^{\ell+2(b-1)} p^{2t+1}$	$2^6 3^{2\ell+6(b-1)} p^{3+6t}$
H2	$-4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell+1}{p}}$	$4 \cdot 3^{2(b-1)} p^{2t+1}$	$2^{12} 3^{\ell+6(b-1)} p^{3+6t}$
H1′	$-2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell+1}{p}}$	$3^{\ell+2(b-1)} p^{2t+1}$	$2^6 3^{2\ell+6(b-1)} p^{3+6t}$
H2′	$4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell+1}{p}}$	$4 \cdot 3^{2(b-1)} p^{2t+1}$	$2^{12} 3^{\ell+6(b-1)} p^{3+6t}$

(b) $p \equiv -1 \pmod 4$;

	a_2	a_4	Δ
I1	$2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell+1}{p}}$	$3^{2(b-1)} p^{2t+1}$	$2^6 3^{\ell+6(b-1)} p^{3+6t}$
I2	$-4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell+1}{p}}$	$4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$2^{12} 3^{2\ell+6(b-1)} p^{3+6t}$
I1′	$-2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell+1}{p}}$	$3^{2(b-1)} p^{2t+1}$	$2^6 3^{\ell+6(b-1)} p^{3+6t}$
I2′	$4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell+1}{p}}$	$4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$2^{12} 3^{2\ell+6(b-1)} p^{3+6t}$

6. *there exist integers $\ell \geq 1$ and $t \in \{0, 1\}$ such that $\frac{3^\ell-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) $p \equiv 1 \pmod 4$;

	a_2	a_4	Δ
J1	$2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-1}{p}}$	$-3^{2(b-1)} p^{2t+1}$	$2^6 3^{\ell+6(b-1)} p^{3+6t}$
J2	$-4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-1}{p}}$	$4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$-2^{12} 3^{2\ell+6(b-1)} p^{3+6t}$
J1′	$-2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-1}{p}}$	$-3^{2(b-1)} p^{2t+1}$	$2^6 3^{\ell+6(b-1)} p^{3+6t}$
J2′	$4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-1}{p}}$	$4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$-2^{12} 3^{2\ell+6(b-1)} p^{3+6t}$

   (b) $p \equiv -1 \pmod 4$;

	a_2	a_4	Δ
K1	$2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-1}{p}}$	$3^{\ell+2(b-1)} p^{2t+1}$	$-2^6 3^{2\ell+6(b-1)} p^{3+6t}$
K2	$-4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-1}{p}}$	$-4 \cdot 3^{2(b-1)} p^{2t+1}$	$2^{12} 3^{\ell+6(b-1)} p^{3+6t}$
K1′	$-2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-1}{p}}$	$3^{\ell+2(b-1)} p^{2t+1}$	$-2^6 3^{2\ell+6(b-1)} p^{3+6t}$
K2′	$4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-1}{p}}$	$-4 \cdot 3^{2(b-1)} p^{2t+1}$	$2^{12} 3^{\ell+6(b-1)} p^{3+6t}$

7. *there exist integers $\ell \geq 2 - b$ and $n \geq 0$ such that $8 \cdot 3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
L1	$3^{b-1} p \sqrt{8 \cdot 3^\ell p^n + 1}$	$2 \cdot 3^{\ell+2(b-1)} p^{n+2}$	$2^6 3^{2\ell+6(b-1)} p^{2n+6}$
L2	$-2 \cdot 3^{b-1} p \sqrt{8 \cdot 3^\ell p^n + 1}$	$3^{2(b-1)} p^2$	$2^9 3^{\ell+6(b-1)} p^{n+6}$
L1′	$-3^{b-1} p \sqrt{8 \cdot 3^\ell p^n + 1}$	$2 \cdot 3^{\ell+2(b-1)} p^{n+2}$	$2^6 3^{2\ell+6(b-1)} p^{2n+6}$
L2′	$2 \cdot 3^{b-1} p \sqrt{8 \cdot 3^\ell p^n + 1}$	$3^{2(b-1)} p^2$	$2^9 3^{\ell+6(b-1)} p^{n+6}$

8. *there exist integers $\ell \geq 2 - b$ and $n \geq 0$ such that $8 \cdot 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$3^{b-1}p\sqrt{8\cdot 3^\ell + p^n}$	$2\cdot 3^{\ell+2(b-1)}p^2$	$2^6 3^{2\ell+6(b-1)}p^{n+6}$
M2	$-2\cdot 3^{b-1}p\sqrt{8\cdot 3^\ell + p^n}$	$3^{2(b-1)}p^{n+2}$	$2^9 3^{\ell+6(b-1)}p^{2n+6}$
M1′	$-3^{b-1}p\sqrt{8\cdot 3^\ell + p^n}$	$2\cdot 3^{\ell+2(b-1)}p^2$	$2^6 3^{2\ell+6(b-1)}p^{n+6}$
M2′	$2\cdot 3^{b-1}p\sqrt{8\cdot 3^\ell + p^n}$	$3^{2(b-1)}p^{n+2}$	$2^9 3^{\ell+6(b-1)}p^{2n+6}$

9. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $8\cdot 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
N1	$3^{b-1}p\sqrt{8\cdot 3^\ell - p^n}$	$2\cdot 3^{\ell+2(b-1)}p^2$	$-2^6 3^{2\ell+6(b-1)}p^{n+6}$
N2	$-2\cdot 3^{b-1}p\sqrt{8\cdot 3^\ell - p^n}$	$-3^{2(b-1)}p^{n+2}$	$2^9 3^{\ell+6(b-1)}p^{2n+6}$
N1′	$-3^{b-1}p\sqrt{8\cdot 3^\ell - p^n}$	$2\cdot 3^{\ell+2(b-1)}p^2$	$-2^6 3^{2\ell+6(b-1)}p^{n+6}$
N2′	$2\cdot 3^{b-1}p\sqrt{8\cdot 3^\ell - p^n}$	$-3^{2(b-1)}p^{n+2}$	$2^9 3^{\ell+6(b-1)}p^{2n+6}$

10. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $8p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$3^{b-1}p\sqrt{8p^n + 3^\ell}$	$2\cdot 3^{2(b-1)}p^{n+2}$	$2^6 3^{\ell+6(b-1)}p^{2n+6}$
O2	$-2\cdot 3^{b-1}p\sqrt{8p^n + 3^\ell}$	$3^{\ell+2(b-1)p^2}$	$2^9 3^{2\ell+6(b-1)}p^{n+6}$
O1′	$-3^{b-1}p\sqrt{8p^n + 3^\ell}$	$2\cdot 3^{2(b-1)}p^{n+2}$	$2^6 3^{\ell+6(b-1)}p^{2n+6}$
O2′	$2\cdot 3^{b-1}p\sqrt{8p^n + 3^\ell}$	$3^{\ell+2(b-1)p^2}$	$2^9 3^{2\ell+6(b-1)}p^{n+6}$

11. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $3^\ell p^n - 8$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
P1	$3^{b-1}p\sqrt{3^\ell p^n - 8}$	$-2\cdot 3^{2(b-1)}p^2$	$2^6 3^{\ell+6(b-1)}p^{n+6}$
P2	$-2\cdot 3^{b-1}p\sqrt{3^\ell p^n - 8}$	$3^{\ell+2(b-1)}p^{n+2}$	$-2^9 3^{2\ell+6(b-1)}p^{2n+6}$
P1′	$-3^{b-1}p\sqrt{3^\ell p^n - 8}$	$-2\cdot 3^{2(b-1)}p^2$	$2^6 3^{\ell+6(b-1)}p^{n+6}$
P2′	$2\cdot 3^{b-1}p\sqrt{3^\ell p^n - 8}$	$3^{\ell+2(b-1)}p^{n+2}$	$-2^9 3^{2\ell+6(b-1)}p^{2n+6}$

12. *there exist integers $\ell \geq 1$ and $n \geq 0$ such that $3^\ell - 8p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	$3^{b-1}p\sqrt{3^\ell - 8p^n}$	$-2\cdot 3^{2(b-1)}p^{n+2}$	$2^6 3^{\ell+6(b-1)}p^{2n+6}$
Q2	$-2\cdot 3^{b-1}p\sqrt{3^\ell - 8p^n}$	$3^{\ell+2(b-1)}p^2$	$-2^9 3^{2\ell+6(b-1)}p^{n+6}$
Q1′	$-3^{b-1}p\sqrt{3^\ell - 8p^n}$	$-2\cdot 3^{2(b-1)}p^{n+2}$	$2^6 3^{\ell+6(b-1)}p^{2n+6}$
Q2′	$2\cdot 3^{b-1}p\sqrt{3^\ell - 8p^n}$	$3^{\ell+2(b-1)}p^2$	$-2^9 3^{2\ell+6(b-1)}p^{n+6}$

13. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $p^n - 8\cdot 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
R1	$3^{b-1}p\sqrt{p^n - 8\cdot 3^\ell}$	$-2\cdot 3^{\ell+2(b-1)}p^2$	$2^6 3^{2\ell+6(b-1)}p^{n+6}$
R2	$-2\cdot 3^{b-1}p\sqrt{p^n - 8\cdot 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^9 3^{\ell+6(b-1)}p^{2n+6}$
R1′	$-3^{b-1}p\sqrt{p^n - 8\cdot 3^\ell}$	$-2\cdot 3^{\ell+2(b-1)}p^2$	$2^6 3^{2\ell+6(b-1)}p^{n+6}$
R2′	$2\cdot 3^{b-1}p\sqrt{p^n - 8\cdot 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^9 3^{\ell+6(b-1)}p^{2n+6}$

14. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{8\cdot 3^\ell+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
S1	$3^{b-1}p^{t+1}\sqrt{\frac{8\cdot 3^\ell+1}{p}}$	$2\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^6 3^{2\ell+6(b-1)}p^{3+6t}$
S2	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{8\cdot 3^\ell+1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^9 3^{\ell+6(b-1)}p^{3+6t}$
S1′	$-3^{b-1}p^{t+1}\sqrt{\frac{8\cdot 3^\ell+1}{p}}$	$2\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^6 3^{2\ell+6(b-1)}p^{3+6t}$
S2′	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{8\cdot 3^\ell+1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^9 3^{\ell+6(b-1)}p^{3+6t}$

15. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{8\cdot 3^\ell-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
T1	$3^{b-1}p^{t+1}\sqrt{\frac{8\cdot 3^\ell-1}{p}}$	$2\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^6 3^{2\ell+6(b-1)}p^{3+6t}$
T2	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{8\cdot 3^\ell-1}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^9 3^{\ell+6(b-1)}p^{3+6t}$
T1′	$-3^{b-1}p^{t+1}\sqrt{\frac{8\cdot 3^\ell-1}{p}}$	$2\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^6 3^{2\ell+6(b-1)}p^{3+6t}$
T2′	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{8\cdot 3^\ell-1}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^9 3^{\ell+6(b-1)}p^{3+6t}$

16. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{8+3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
U1	$3^{b-1}p^{t+1}\sqrt{\frac{8+3^\ell}{p}}$	$2\cdot 3^{2(b-1)}p^{2t+1}$	$2^6 3^{\ell+6(b-1)}p^{3+6t}$
U2	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{8+3^\ell}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^9 3^{2\ell+6(b-1)}p^{3+6t}$
U1′	$-3^{b-1}p^{t+1}\sqrt{\frac{8+3^\ell}{p}}$	$2\cdot 3^{2(b-1)}p^{2t+1}$	$2^6 3^{\ell+6(b-1)}p^{3+6t}$
U2′	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{8+3^\ell}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^9 3^{2\ell+6(b-1)}p^{3+6t}$

17. *there exist integers $\ell \geq 2-b$ and $t\in\{0,1\}$ such that $\frac{8-3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
V1	$3^{b-1}p^{t+1}\sqrt{\frac{8-3^\ell}{p}}$	$2\cdot 3^{2(b-1)}p^{2t+1}$	$-2^6 3^{\ell+6(b-1)}p^{3+6t}$
V2	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{8-3^\ell}{p}}$	$-3^{\ell+2(b-1)}p^{2t+1}$	$2^9 3^{2\ell+6(b-1)}p^{3+6t}$
V1′	$-3^{b-1}p^{t+1}\sqrt{\frac{8-3^\ell}{p}}$	$2\cdot 3^{2(b-1)}p^{2t+1}$	$-2^6 3^{\ell+6(b-1)}p^{3+6t}$
V2′	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{8-3^\ell}{p}}$	$-3^{\ell+2(b-1)}p^{2t+1}$	$2^9 3^{2\ell+6(b-1)}p^{3+6t}$

18. *there exist integers $\ell \geq 2-b$ and $t\in\{0,1\}$ such that $\frac{3^\ell-8}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
W1	$3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-8}{p}}$	$-2\cdot 3^{2(b-1)}p^{2t+1}$	$2^6 3^{\ell+6(b-1)}p^{3+6t}$
W2	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-8}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^9 3^{2\ell+6(b-1)}p^{3+6t}$
W1′	$-3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-8}{p}}$	$-2\cdot 3^{2(b-1)}p^{2t+1}$	$2^6 3^{\ell+6(b-1)}p^{3+6t}$
W2′	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-8}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^9 3^{2\ell+6(b-1)}p^{3+6t}$

In the case that $b=2$, i.e. $N=2^5 3^2 p^2$, we furthermore could have one of the following conditions satisfied:

19. *there exist integers $n\geq 0$ and $s\in\{0,1\}$ such that $\frac{p^n+1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
X1	$2 \cdot 3^{s+1} p \sqrt{\frac{p^n+1}{3}}$	$3^{2s+1} p^2$	$2^6 3^{3+6s} p^{n+6}$
X2	$-4 \cdot 3^{s+1} p \sqrt{\frac{p^n+1}{3}}$	$4 \cdot 3^{2s+1} p^{n+2}$	$2^{12} 3^{3+6s} p^{2n+6}$
X1′	$-2 \cdot 3^{s+1} p \sqrt{\frac{p^n+1}{3}}$	$3^{2s+1} p^2$	$2^6 3^{3+6s} p^{n+6}$
X2′	$4 \cdot 3^{s+1} p \sqrt{\frac{p^n+1}{3}}$	$4 \cdot 3^{2s+1} p^{n+2}$	$2^{12} 3^{3+6s} p^{2n+6}$

20. *there exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{p^n-1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Y1	$2 \cdot 3^{s+1} p \sqrt{\frac{p^n-1}{3}}$	$3^{2s+1} p^{n+2}$	$-2^6 3^{3+6s} p^{2n+6}$
Y2	$-4 \cdot 3^{s+1} p \sqrt{\frac{p^n-1}{3}}$	$-4 \cdot 3^{2s+1} p^2$	$2^{12} 3^{3+6s} p^{n+6}$
Y1′	$-2 \cdot 3^{s+1} p \sqrt{\frac{p^n-1}{3}}$	$3^{2s+1} p^{n+2}$	$-2^6 3^{3+6s} p^{2n+6}$
Y2′	$4 \cdot 3^{s+1} p \sqrt{\frac{p^n-1}{3}}$	$-4 \cdot 3^{2s+1} p^2$	$2^{12} 3^{3+6s} p^{n+6}$

21. *there exist integers $s, t \in \{0,1\}$ such that E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

    (a) $p \equiv 1 \pmod 4$:

	a_2	a_4	Δ
Z1	0	$3^{2s+1} p^{2t+1}$	$-2^6 3^{3+6s} p^{3+6t}$
Z2	0	$-4 \cdot 3^{2s+1} p^{2t+1}$	$2^{12} 3^{3+6s} p^{3+6t}$

    (b) $p \equiv -1 \pmod 4$:

	a_2	a_4	Δ
AA1	0	$-3^{2s+1} p^{2t+1}$	$2^6 3^{3+6s} p^{3+6t}$
AA2	0	$4 \cdot 3^{2s+1} p^{2t+1}$	$-2^{12} 3^{3+6s} p^{n+6}$

22. *E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
BB1	0	$-3^{2(b-1)} p^2$	$2^6 3^{6(b-1)} p^6$
BB2	0	$4 \cdot 3^{2(b-1)} p^2$	$-2^{12} 3^{6(b-1)} p^6$

23. *there exists an integer $t \in \{0,1\}$ such that E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

(a) $p \equiv 1 \pmod 4$*:*

	a_2	a_4	Δ
CC1	0	$-3^{2(b-1)}p^{2t+1}$	$2^6 3^{6(b-1)}p^{3+6t}$
CC2	0	$4 \cdot 3^{2(b-1)}p^{2t+1}$	$-2^{12}3^{6(b-1)}p^{3+6t}$

(b) $p \equiv -1 \pmod 4$*:*

	a_2	a_4	Δ
DD1	0	$3^{2(b-1)}p^{2t+1}$	$-2^6 3^{6(b-1)}p^{3+6t}$
DD2	0	$-4 \cdot 3^{2(b-1)}p^{2t+1}$	$2^{12}3^{6(b-1)}p^{3+6t}$

24. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n+8}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
EE1	$3^{s+1}p\sqrt{\frac{p^n+8}{3}}$	$2 \cdot 3^{2s+1}p^2$	$2^6 3^{3+6s}p^{n+6}$
EE2	$-2 \cdot 3^{s+1}p\sqrt{\frac{p^n+8}{3}}$	$3^{2s+1}p^{n+2}$	$2^9 3^{3+6s}p^{2n+6}$
EE1′	$-3^{s+1}p\sqrt{\frac{p^n+8}{3}}$	$2 \cdot 3^{2s+1}p^2$	$2^6 3^{3+6s}p^{n+6}$
EE2′	$2 \cdot 3^{s+1}p\sqrt{\frac{p^n+8}{3}}$	$3^{2s+1}p^{n+2}$	$2^9 3^{3+6s}p^{2n+6}$

25. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{8-p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
FF1	$3^{s+1}p\sqrt{\frac{8-p^n}{3}}$	$2 \cdot 3^{2s+1}p^2$	$-2^6 3^{3+6s}p^{n+6}$
FF2	$-2 \cdot 3^{s+1}p\sqrt{\frac{8-p^n}{3}}$	$-3^{2s+1}p^{n+2}$	$2^9 3^{3+6s}p^{2n+6}$
FF1′	$-3^{s+1}p\sqrt{\frac{8-p^n}{3}}$	$2 \cdot 3^{2s+1}p^2$	$-2^6 3^{3+6s}p^{n+6}$
FF2′	$2 \cdot 3^{s+1}p\sqrt{\frac{8-p^n}{3}}$	$-3^{2s+1}p^{n+2}$	$2^9 3^{3+6s}p^{2n+6}$

26. *there exists an integer $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n-8}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
GG1	$3^{s+1}p\sqrt{\frac{p^n-8}{3}}$	$-2\cdot 3^{2s+1}p^2$	$2^6 3^{3+6s}p^{n+6}$
GG2	$-2\cdot 3^{s+1}p\sqrt{\frac{p^n-8}{3}}$	$3^{2s+1}p^{n+2}$	$-2^9 3^{3+6s}p^{2n+6}$
GG1′	$-3^{s+1}p\sqrt{\frac{p^n-8}{3}}$	$-2\cdot 3^{2s+1}p^2$	$2^6 3^{3+6s}p^{n+6}$
GG2′	$2\cdot 3^{s+1}p\sqrt{\frac{p^n-8}{3}}$	$3^{2s+1}p^{n+2}$	$-2^9 3^{3+6s}p^{2n+6}$

Theorem 3.27 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^6 3^b p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $3^\ell p^n + 1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$2\cdot 3^{b-1}p\sqrt{3^\ell p^n+1}$	$3^{2(b-1)}p^2$	$2^6 3^{\ell+6(b-1)}p^{n+6}$
A2	$-4\cdot 3^{b-1}p\sqrt{3^\ell p^n+1}$	$4\cdot 3^{\ell+2(b-1)}p^{n+2}$	$2^{12}3^{2\ell+6(b-1)}p^{2n+6}$
A1′	$-2\cdot 3^{b-1}p\sqrt{3^\ell p^n+1}$	$3^{2(b-1)}p^2$	$2^6 3^{\ell+6(b-1)}p^{n+6}$
A2′	$4\cdot 3^{b-1}p\sqrt{3^\ell p^n+1}$	$4\cdot 3^{\ell+2(b-1)}p^{n+2}$	$2^{12}3^{2\ell+6(b-1)}p^{2n+6}$

2. *there exist integers $\ell \geq 1$ and $n \geq 0$ such that $3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) ℓ is even;

	a_2	a_4	Δ
B1	$2\cdot 3^{b-1}p\sqrt{3^\ell+p^n}$	$3^{\ell+2(b-1)}p^2$	$2^6 3^{2\ell+6(b-1)}p^{n+6}$
B2	$-4\cdot 3^{b-1}p\sqrt{3^\ell+p^n}$	$4\cdot 3^{2(b-1)}p^{n+2}$	$2^{12}3^{\ell+6(b-1)}p^{2n+6}$
B1′	$-2\cdot 3^{b-1}p\sqrt{3^\ell+p^n}$	$3^{2(b-1)}p^2$	$2^6 3^{2\ell+6(b-1)}p^{n+6}$
B2′	$4\cdot 3^{b-1}p\sqrt{3^\ell+p^n}$	$4\cdot 3^{\ell+2(b-1)}p^{n+2}$	$2^{12}3^{\ell+6(b-1)}p^{2n+6}$

   (b) ℓ is odd;

	a_2	a_4	Δ
C1	$2\cdot 3^{b-1}p\sqrt{3^\ell+p^n}$	$3^{2(b-1)}p^{n+2}$	$2^6 3^{\ell+6(b-1)}p^{2n+6}$
C2	$-4\cdot 3^{b-1}p\sqrt{3^\ell+p^n}$	$4\cdot 3^{\ell+2(b-1)}p^2$	$2^{12}3^{2\ell+6(b-1)}p^{n+6}$
C1′	$-2\cdot 3^{b-1}p\sqrt{3^\ell+p^n}$	$3^{2(b-1)}p^{n+2}$	$2^6 3^{\ell+6(b-1)}p^{2n+6}$
C2′	$4\cdot 3^{b-1}p\sqrt{3^\ell+p^n}$	$4\cdot 3^{\ell+2(b-1)}p^2$	$2^{12}3^{2\ell+6(b-1)}p^{n+6}$

3. *there exist integers $\ell \geq 1$ and $n \geq 0$ such that $3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) *ℓ is even;*

	a_2	a_4	Δ
D1	$2 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$3^{\ell+2(b-1)} p^2$	$-2^6 3^{2\ell+6(b-1)} p^{n+6}$
D2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^{n+2}$	$2^{12} 3^{\ell+6(b-1)} p^{2n+6}$
D1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$3^{\ell+2(b-1)} p^2$	$-2^6 3^{2\ell+6(b-1)} p^{n+6}$
D2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^{n+2}$	$2^{12} 3^{\ell+6(b-1)} p^{2n+6}$

   (b) *ℓ is odd;*

	a_2	a_4	Δ
E1	$2 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$-3^{2(b-1)} p^{n+2}$	$2^6 3^{\ell+6(b-1)} p^{2n+6}$
E2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$4 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{12} 3^{2\ell+6(b-1)} p^{n+6}$
E1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$-3^{2(b-1)} p^{n+2}$	$2^6 3^{\ell+6(b-1)} p^{2n+6}$
E2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell - p^n}$	$4 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{12} 3^{2\ell+6(b-1)} p^{n+6}$

4. *there exist integers $\ell \geq 2 - b$ and $n \geq 0$ such that $p^n - 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) *ℓ is even;*

	a_2	a_4	Δ
F1	$2 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$3^{2(b-1)} p^{n+2}$	$-2^6 3^{\ell+6(b-1)} p^{2n+6}$
F2	$-4 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)} p^2$	$2^{12} 3^{2\ell+6(b-1)} p^{n+6}$
F1′	$-2 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$3^{2(b-1)} p^{n+2}$	$-2^6 3^{\ell+6(b-1)} p^{2n+6}$
F2′	$4 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$-4 \cdot 3^{\ell+2(b-1)} p^2$	$2^{12} 3^{2\ell+6(b-1)} p^{n+6}$

   (b) *ℓ is odd;*

	a_2	a_4	Δ
G1	$2 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$-3^{\ell+2(b-1)} p^2$	$2^6 3^{2\ell+6(b-1)} p^{n+6}$
G2	$-4 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$4 \cdot 3^{2(b-1)} p^{n+2}$	$-2^{12} 3^{\ell+6(b-1)} p^{2n+6}$
G1′	$-2 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$-3^{\ell+2(b-1)} p^2$	$2^6 3^{2\ell+6(b-1)} p^{n+6}$
G2′	$4 \cdot 3^{b-1} p \sqrt{p^n - 3^\ell}$	$4 \cdot 3^{2(b-1)} p^{n+2}$	$-2^{12} 3^{\ell+6(b-1)} p^{2n+6}$

5. *there exist integers $\ell \geq 1$ and $t \in \{0, 1\}$ such that $\frac{3^\ell+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) *$p \equiv 1 \pmod 4$;*

	a_2	a_4	Δ
H1	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^6 3^{\ell+6(b-1)}p^{3+6t}$
H2	$-4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{p}}$	$4\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^{12}3^{2\ell+6(b-1)}p^{3+6t}$
H1′	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^6 3^{\ell+6(b-1)}p^{3+6t}$
H2′	$4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{p}}$	$4\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^{12}3^{2\ell+6(b-1)}p^{3+6t}$

(b) $p\equiv -1 \pmod 4$*;*

	a_2	a_4	Δ
I1	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^6 3^{2\ell+6(b-1)}p^{3+6t}$
I2	$-4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{p}}$	$4\cdot 3^{2(b-1)}p^{2t+1}$	$2^{12}3^{\ell+6(b-1)}p^{3+6t}$
I1′	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^6 3^{2\ell+6(b-1)}p^{3+6t}$
I2′	$4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{p}}$	$4\cdot 3^{2(b-1)}p^{2t+1}$	$2^{12}3^{\ell+6(b-1)}p^{3+6t}$

6. *there exist integers $\ell\geq 1$ and $t\in\{0,1\}$ such that $\frac{3^\ell-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (a) $p\equiv 1 \pmod 4$*;*

	a_2	a_4	Δ
J1	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^6 3^{2\ell+6(b-1)}p^{3+6t}$
J2	$-4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{p}}$	$-4\cdot 3^{2(b-1)}p^{2t+1}$	$2^{12}3^{\ell+6(b-1)}p^{3+6t}$
J1′	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$-2^6 3^{2\ell+6(b-1)}p^{3+6t}$
J2′	$4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{p}}$	$-4\cdot 3^{2(b-1)}p^{2t+1}$	$2^{12}3^{\ell+6(b-1)}p^{3+6t}$

   (b) $p\equiv -1 \pmod 4$*;*

	a_2	a_4	Δ
K1	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^6 3^{\ell+6(b-1)}p^{3+6t}$
K2	$-4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{p}}$	$4\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^{12}3^{2\ell+6(b-1)}p^{3+6t}$
K1′	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^6 3^{\ell+6(b-1)}p^{3+6t}$
K2′	$4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{p}}$	$4\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^{12}3^{2\ell+6(b-1)}p^{3+6t}$

7. *there exist integers $m\geq 3$, $\ell\geq 2-b$ and $n\geq 0$ such that $2^m 3^\ell p^n+1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
L1	$2\cdot 3^{b-1}p\sqrt{2^m3^\ell p^n+1}$	$2^m3^{\ell+2(b-1)}p^{n+2}$	$2^{2m+6}3^{2\ell+6(b-1)}p^{2n+6}$
L2	$-4\cdot 3^{b-1}p\sqrt{2^m3^\ell p^n+1}$	$4\cdot 3^{2(b-1)}p^2$	$2^{m+12}3^{\ell+6(b-1)}p^{n+6}$
L1′	$-2\cdot 3^{b-1}p\sqrt{2^m3^\ell p^n+1}$	$2^m3^{\ell+2(b-1)}p^{n+2}$	$2^{2m+6}3^{2\ell+6(b-1)}p^{2n+6}$
L2′	$4\cdot 3^{b-1}p\sqrt{2^m3^\ell p^n+1}$	$4\cdot 3^{2(b-1)}p^2$	$2^{m+12}3^{\ell+6(b-1)}p^{n+6}$

8. *there exist integers $m\geq 2$, $\ell\geq 2-b$ and $n\geq 0$ such that $2^m3^\ell+p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$2\cdot 3^{b-1}p\sqrt{2^m3^\ell+p^n}$	$2^m3^{\ell+2(b-1)}p^2$	$2^{2m+6}3^{2\ell+6(b-1)}p^{n+6}$
M2	$-4\cdot 3^{b-1}p\sqrt{2^m3^\ell+p^n}$	$4\cdot 3^{2(b-1)}p^{n+2}$	$2^{m+12}3^{\ell+6(b-1)}p^{2n+6}$
M1′	$-2\cdot 3^{b-1}p\sqrt{2^m3^\ell+p^n}$	$2^m3^{\ell+2(b-1)}p^2$	$2^{2m+6}3^{2\ell+6(b-1)}p^{n+6}$
M2′	$4\cdot 3^{b-1}p\sqrt{2^m3^\ell+p^n}$	$4\cdot 3^{2(b-1)}p^{n+2}$	$2^{m+12}3^{\ell+6(b-1)}p^{2n+6}$

9. *there exist integers $m\geq 2$, $\ell\geq 2-b$ and $n\geq 0$ such that $2^m3^\ell-p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
N1	$2\cdot 3^{b-1}p\sqrt{2^m3^\ell-p^n}$	$2^m3^{\ell+2(b-1)}p^2$	$-2^{2m+6}3^{2\ell+6(b-1)}p^{n+6}$
N2	$-4\cdot 3^{b-1}p\sqrt{2^m3^\ell-p^n}$	$-4\cdot 3^{2(b-1)}p^{n+2}$	$2^{m+12}3^{\ell+6(b-1)}p^{2n+6}$
N1′	$-2\cdot 3^{b-1}p\sqrt{2^m3^\ell-p^n}$	$2^m3^{\ell+2(b-1)}p^2$	$-2^{2m+6}3^{2\ell+6(b-1)}p^{n+6}$
N2′	$4\cdot 3^{b-1}p\sqrt{2^m3^\ell-p^n}$	$-4\cdot 3^{2(b-1)}p^{n+2}$	$2^{m+12}3^{\ell+6(b-1)}p^{2n+6}$

10. *there exist integers $m\geq 3$, $\ell\geq 2-b$ and $n\geq 0$ such that $2^mp^n+3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$2\cdot 3^{b-1}p\sqrt{2^mp^n+3^\ell}$	$2^m3^{2(b-1)}p^{n+2}$	$2^{2m+6}3^{\ell+6(b-1)}p^{2n+6}$
O2	$-4\cdot 3^{b-1}p\sqrt{2^mp^n+3^\ell}$	$4\cdot 3^{\ell+2(b-1)}p^2$	$2^{m+12}3^{2\ell+6(b-1)}p^{n+6}$
O1′	$-2\cdot 3^{b-1}p\sqrt{2^mp^n+3^\ell}$	$2^m3^{2(b-1)}p^{n+2}$	$2^{2m+6}3^{\ell+6(b-1)}p^{2n+6}$
O2′	$4\cdot 3^{b-1}p\sqrt{2^mp^n+3^\ell}$	$4\cdot 3^{\ell+2(b-1)}p^2$	$2^{m+12}3^{2\ell+6(b-1)}p^{n+6}$

11. *there exist integers $\ell\geq 2-b$ and $n\geq 0$ such that $4p^n-3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
P1	$2\cdot 3^{b-1}p\sqrt{4p^n-3^\ell}$	$4\cdot 3^{2(b-1)}p^{n+2}$	$-2^{10}3^{\ell+6(b-1)}p^{2n+6}$
P2	$-4\cdot 3^{b-1}p\sqrt{4p^n-3^\ell}$	$-4\cdot 3^{\ell+2(b-1)}p^2$	$2^{14}3^{2\ell+6(b-1)}p^{n+6}$
P1′	$-2\cdot 3^{b-1}p\sqrt{4p^n-3^\ell}$	$4\cdot 3^{2(b-1)}p^{n+2}$	$-2^{10}3^{\ell+6(b-1)}p^{2n+6}$
P2′	$4\cdot 3^{b-1}p\sqrt{4p^n-3^\ell}$	$-4\cdot 3^{\ell+2(b-1)}p^2$	$2^{14}3^{2\ell+6(b-1)}p^{n+6}$

12. *there exist integers $m\geq 2$, $\ell\geq 2-b$ and $n\geq 0$ such that $2^m+3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	$2\cdot 3^{b-1}p\sqrt{2^m+3^\ell p^n}$	$2^m3^{2(b-1)}p^2$	$2^{2m+6}3^{\ell+6(b-1)}p^{n+6}$
Q2	$-4\cdot 3^{b-1}p\sqrt{2^m+3^\ell p^n}$	$4\cdot 3^{\ell+2(b-1)}p^{n+2}$	$2^{m+12}3^{2\ell+6(b-1)}p^{2n+6}$
Q1′	$-2\cdot 3^{b-1}p\sqrt{2^m+3^\ell p^n}$	$2^m3^{2(b-1)}p^2$	$2^{2m+6}3^{\ell+6(b-1)}p^{n+6}$
Q2′	$4\cdot 3^{b-1}p\sqrt{2^m+3^\ell p^n}$	$4\cdot 3^{\ell+2(b-1)}p^{n+2}$	$2^{m+12}3^{2\ell+6(b-1)}p^{2n+6}$

13. *there exist integers $m\geq 2$, $\ell\geq 2-b$ and $n\geq 0$ such that $2^m-3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
R1	$2\cdot 3^{b-1}p\sqrt{2^m-3^\ell p^n}$	$2^m3^{2(b-1)}p^2$	$-2^{2m+6}3^{\ell+6(b-1)}p^{n+6}$
R2	$-4\cdot 3^{b-1}p\sqrt{2^m-3^\ell p^n}$	$-4\cdot 3^{\ell+2(b-1)}p^{n+2}$	$2^{m+12}3^{2\ell+6(b-1)}p^{2n+6}$
R1′	$-2\cdot 3^{b-1}p\sqrt{2^m-3^\ell p^n}$	$2^m3^{2(b-1)}p^2$	$-2^{2m+6}3^{\ell+6(b-1)}p^{n+6}$
R2′	$4\cdot 3^{b-1}p\sqrt{2^m-3^\ell p^n}$	$-4\cdot 3^{\ell+2(b-1)}p^{n+2}$	$2^{m+12}3^{2\ell+6(b-1)}p^{2n+6}$

14. *there exist integers $m\geq 2$, $\ell\geq 2-b$ and $n\geq 0$ such that $3^\ell p^n-2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
S1	$2\cdot 3^{b-1}p\sqrt{3^\ell p^n-2^m}$	$-2^m3^{2(b-1)}p^2$	$2^{2m+6}3^{\ell+6(b-1)}p^{n+6}$
S2	$-4\cdot 3^{b-1}p\sqrt{3^\ell p^n-2^m}$	$4\cdot 3^{\ell+2(b-1)}p^{n+2}$	$-2^{m+12}3^{2\ell+6(b-1)}p^{2n+6}$
S1′	$-2\cdot 3^{b-1}p\sqrt{3^\ell p^n-2^m}$	$-2^m3^{2(b-1)}p^2$	$2^{2m+6}3^{\ell+6(b-1)}p^{n+6}$
S2′	$4\cdot 3^{b-1}p\sqrt{3^\ell p^n-2^m}$	$4\cdot 3^{\ell+2(b-1)}p^{n+2}$	$-2^{m+12}3^{2\ell+6(b-1)}p^{2n+6}$

15. *there exist integers $m\geq 2$, $\ell\geq 2-b$ and $n\geq 0$ such that $3^\ell-2^m p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
T1	$2 \cdot 3^{b-1} p \sqrt{3^\ell - 2^m p^n}$	$-2^m 3^{2(b-1)} p^{n+2}$	$2^{2m+6} 3^{\ell+6(b-1)} p^{2n+6}$
T2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell - 2^m p^n}$	$4 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{m+12} 3^{2\ell+6(b-1)} p^{n+6}$
T1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell - 2^m p^n}$	$-2^m 3^{2(b-1)} p^{n+2}$	$2^{2m+6} 3^{\ell+6(b-1)} p^{2n+6}$
T2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell - 2^m p^n}$	$4 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{m+12} 3^{2\ell+6(b-1)} p^{n+6}$

16. *there exist integers $m \geq 2$, $\ell \geq 2 - b$ and $n \geq 0$ such that $p^n - 2^m 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
U1	$2 \cdot 3^{b-1} p \sqrt{p^n - 2^m 3^\ell}$	$-2^m 3^{\ell+2(b-1)} p^2$	$2^{2m+6} 3^{2\ell+6(b-1)} p^{n+6}$
U2	$-4 \cdot 3^{b-1} p \sqrt{p^n - 2^m 3^\ell}$	$4 \cdot 3^{2(b-1)} p^{n+2}$	$-2^{m+12} 3^{\ell+6(b-1)} p^{2n+6}$
U1′	$-2 \cdot 3^{b-1} p \sqrt{p^n - 2^m 3^\ell}$	$-2^m 3^{\ell+2(b-1)} p^2$	$2^{2m+6} 3^{2\ell+6(b-1)} p^{n+6}$
U2′	$4 \cdot 3^{b-1} p \sqrt{p^n - 2^m 3^\ell}$	$4 \cdot 3^{2(b-1)} p^{n+2}$	$-2^{m+12} 3^{\ell+6(b-1)} p^{2n+6}$

17. *there exist integers $m \geq 2$, $\ell \geq 2 - b$ and $t \in \{0, 1\}$ such that $\frac{2^m 3^\ell + 1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
V1	$2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell + 1}{p}}$	$2^m 3^{\ell+2(b-1)} p^{2t+1}$	$2^{2m+6} 3^{2\ell+6(b-1)} p^{3+6t}$
V2	$-4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell + 1}{p}}$	$4 \cdot 3^{2(b-1)} p^{2t+1}$	$2^{m+12} 3^{\ell+6(b-1)} p^{3+6t}$
V1′	$-2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell + 1}{p}}$	$2^m 3^{\ell+2(b-1)} p^{2t+1}$	$2^{2m+6} 3^{2\ell+6(b-1)} p^{3+6t}$
V2′	$4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell + 1}{p}}$	$4 \cdot 3^{2(b-1)} p^{2t+1}$	$2^{m+12} 3^{\ell+6(b-1)} p^{3+6t}$

18. *there exist integers $m \geq 2$, $\ell \geq 2 - b$ and $t \in \{0, 1\}$ such that $\frac{2^m 3^\ell - 1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
W1	$2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell - 1}{p}}$	$2^m 3^{\ell+2(b-1)} p^{2t+1}$	$-2^{2m+6} 3^{2\ell+6(b-1)} p^{3+6t}$
W2	$-4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell - 1}{p}}$	$-4 \cdot 3^{2(b-1)} p^{2t+1}$	$2^{m+12} 3^{\ell+6(b-1)} p^{3+6t}$
W1′	$-2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell - 1}{p}}$	$2^m 3^{\ell+2(b-1)} p^{2t+1}$	$-2^{2m+6} 3^{2\ell+6(b-1)} p^{3+6t}$
W2′	$4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m 3^\ell - 1}{p}}$	$-4 \cdot 3^{2(b-1)} p^{2t+1}$	$2^{m+12} 3^{\ell+6(b-1)} p^{3+6t}$

19. *there exist integers $m \geq 2$, $\ell \geq 2 - b$ and $t \in \{0, 1\}$ such that $\frac{2^m + 3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
X1	$2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m+3^\ell}{p}}$	$2^m 3^{2(b-1)} p^{2t+1}$	$2^{2m+6} 3^{\ell+6(b-1)} p^{3+6t}$
X2	$-4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m+3^\ell}{p}}$	$4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$2^{m+12} 3^{2\ell+6(b-1)} p^{3+6t}$
X1′	$-2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m+3^\ell}{p}}$	$2^m 3^{2(b-1)} p^{2t+1}$	$2^{2m+6} 3^{\ell+6(b-1)} p^{3+6t}$
X2′	$4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m+3^\ell}{p}}$	$4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$2^{m+12} 3^{2\ell+6(b-1)} p^{3+6t}$

20. *there exist integers $m \geq 2$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{2^m-3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Y1	$2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m-3^\ell}{p}}$	$2^m 3^{2(b-1)} p^{2t+1}$	$-2^{2m+6} 3^{\ell+6(b-1)} p^{3+6t}$
Y2	$-4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m-3^\ell}{p}}$	$-4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$2^{m+12} 3^{2\ell+6(b-1)} p^{3+6t}$
Y1′	$-2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m-3^\ell}{p}}$	$2^m 3^{2(b-1)} p^{2t+1}$	$-2^{2m+6} 3^{\ell+6(b-1)} p^{3+6t}$
Y2′	$4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{2^m-3^\ell}{p}}$	$-4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$2^{m+12} 3^{2\ell+6(b-1)} p^{3+6t}$

21. *there exist integers $m \geq 2$, $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{3^\ell-2^m}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Z1	$2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-2^m}{p}}$	$-2^m 3^{2(b-1)} p^{2t+1}$	$2^{2m+6} 3^{\ell+6(b-1)} p^{3+6t}$
Z2	$-4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-2^m}{p}}$	$4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$-2^{m+12} 3^{2\ell+6(b-1)} p^{3+6t}$
Z1′	$-2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-2^m}{p}}$	$-2^m 3^{2(b-1)} p^{2t+1}$	$2^{2m+6} 3^{\ell+6(b-1)} p^{3+6t}$
Z2′	$4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell-2^m}{p}}$	$4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$-2^{m+12} 3^{2\ell+6(b-1)} p^{3+6t}$

In the case that $b = 2$, i.e. $N = 2^6 3^2 p^2$, we furthermore could have one of the following conditions satisfied:

22. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n+1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
AA1	$2\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$3^{2s+1}p^{n+2}$	$2^6 3^{3+6s}p^{2n+6}$
AA2	$-4\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$4\cdot 3^{2s+1}p^2$	$2^{12}3^{3+6s}p^{n+6}$
AA1′	$-2\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$3^{2s+1}p^{n+2}$	$2^6 3^{3+6s}p^{2n+6}$
AA2′	$4\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$4\cdot 3^{2s+1}p^2$	$2^{12}3^{3+6s}p^{n+6}$

23. *there exist integers $n \geq 1$ and $s \in \{0,1\}$ such that $\frac{p^n-1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
BB1	$2\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$-3^{2s+1}p^2$	$2^6 3^{3+6s}p^{n+6}$
BB2	$-4\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$4\cdot 3^{2s+1}p^{n+2}$	$-2^{12}3^{3+6s}p^{2n+6}$
BB1′	$-2\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$-3^{2s+1}p^2$	$2^6 3^{3+6s}p^{n+6}$
BB2′	$4\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$4\cdot 3^{2s+1}p^{n+2}$	$-2^{12}3^{3+6s}p^{2n+6}$

24. *there exist integers $s,t \in \{0,1\}$ such that E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

    (a) $p \equiv 1 \pmod 4$:

	a_2	a_4	Δ
CC1	0	$-3^{2s+1}p^{2t+1}$	$2^6 3^{3+6s}p^{3+6t}$
CC2	0	$4\cdot 3^{2s+1}p^{2t+1}$	$-2^{12}3^{3+6s}p^{3+6t}$

    (b) $p \equiv -1 \pmod 4$:

	a_2	a_4	Δ
DD1	0	$3^{2s+1}p^{2t+1}$	$-2^6 3^{3+6s}p^{3+6t}$
DD2	0	$-4\cdot 3^{2s+1}p^{2t+1}$	$2^{12}3^{3+6s}p^{3+6t}$

25. *E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
EE1	0	$3^{2(b-1)}p^2$	$-2^6 3^{6(b-1)}p^6$
EE2	0	$-4\cdot 3^{2(b-1)}p^2$	$2^{12}3^{6(b-1)}p^6$

26. *there exists an integer $t \in \{0,1\}$ such that E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

(a) $p \equiv 1 \pmod 4$*:*

	a_2	a_4	Δ
FF1	0	$3^{2(b-1)}p^{2t+1}$	$-2^6 3^{6(b-1)}p^{3+6t}$
FF2	0	$-4 \cdot 3^{2(b-1)}p^{2t+1}$	$2^{12}3^{6(b-1)}p^{3+6t}$

(b) $p \equiv -1 \pmod 4$*:*

	a_2	a_4	Δ
GG1	0	$-3^{2(b-1)}p^{2t+1}$	$2^6 3^{6(b-1)}p^{3+6t}$
GG2	0	$4 \cdot 3^{2(b-1)}p^{2t+1}$	$-2^{12}3^{6(b-1)}p^{3+6t}$

27. *there exist integers $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{4p^n-1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
HH1	$2 \cdot 3^{s+1}p\sqrt{\frac{4p^n-1}{3}}$	$4 \cdot 3^{2s+1)}p^{n+2}$	$-2^{10}3^{3+6s}p^{2n+6}$
HH2	$-4 \cdot 3^{s+1}p\sqrt{\frac{4p^n-1}{3}}$	$-4 \cdot 3^{2s+1)}p^2$	$2^{14}3^{3+6s}p^{n+6}$
HH1′	$-2 \cdot 3^{s+1}p\sqrt{\frac{4p^n-1}{3}}$	$4 \cdot 3^{2s+1)}p^{n+2}$	$-2^{10}3^{3+6s}p^{2n+6}$
HH2′	$4 \cdot 3^{s+1}p\sqrt{\frac{4p^n-1}{3}}$	$-4 \cdot 3^{2s+1)}p^2$	$2^{14}3^{3+6s}p^{n+6}$

28. *there exist integers $m \geq 2$, $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{p^n+2^m}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
II1	$2 \cdot 3^{s+1}p\sqrt{\frac{p^n+2^m}{3}}$	$2^m 3^{2s+1}p^2$	$2^{2m+6}3^{3+6s}p^{n+6}$
II2	$-4 \cdot 3^{s+1}p\sqrt{\frac{p^n+2^m}{3}}$	$4 \cdot 3^{2s+1}p^{n+2}$	$2^{m+12}3^{3+6s}p^{2n+6}$
II1′	$-2 \cdot 3^{s+1}p\sqrt{\frac{p^n+2^m}{3}}$	$2^m 3^{2s+1}p^2$	$2^{2m+6}3^{3+6s}p^{n+6}$
II2′	$4 \cdot 3^{s+1}p\sqrt{\frac{p^n+2^m}{3}}$	$4 \cdot 3^{2s+1}p^{n+2}$	$2^{m+12}3^{3+6s}p^{2n+6}$

29. *there exist integers $m \geq 2$, $n \geq 0$ and $s \in \{0,1\}$ such that $\frac{2^m-p^n}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
JJ1	$2\cdot 3^{s+1}p\sqrt{\frac{2^m-p^n}{3}}$	$2^m 3^{2s+1}p^2$	$-2^{2m+6}3^{3+6s}p^{n+6}$
JJ2	$-4\cdot 3^{s+1}p\sqrt{\frac{2^m-p^n}{3}}$	$-4\cdot 3^{2s+1}p^{n+2}$	$2^{m+12}3^{3+6s}p^{2n+6}$
JJ1′	$-2\cdot 3^{s+1}p\sqrt{\frac{2^m-p^n}{3}}$	$2^m 3^{2s+1}p^2$	$-2^{2m+6}3^{3+6s}p^{n+6}$
JJ2′	$4\cdot 3^{s+1}p\sqrt{\frac{2^m-p^n}{3}}$	$-4\cdot 3^{2s+1}p^{n+2}$	$2^{m+12}3^{3+6s}p^{2n+6}$

30. *there exist integers $m\geq 2$, $n\geq 0$ and $s\in\{0,1\}$ such that $\frac{p^n-2^m}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
KK1	$2\cdot 3^{s+1}p\sqrt{\frac{p^n-2^m}{3}}$	$-2^m 3^{2s+1}p^2$	$2^{2m+6}3^{3+6s}p^{n+6}$
KK2	$-4\cdot 3^{s+1}p\sqrt{\frac{p^n-2^m}{3}}$	$4\cdot 3^{2s+1}p^{n+2}$	$-2^{m+12}3^{3+6s}p^{2n+6}$
KK1′	$-2\cdot 3^{s+1}p\sqrt{\frac{p^n-2^m}{3}}$	$-2^m 3^{2s+1}p^2$	$2^{2m+6}3^{3+6s}p^{n+6}$
KK2′	$4\cdot 3^{s+1}p\sqrt{\frac{p^n-2^m}{3}}$	$4\cdot 3^{2s+1}p^{n+2}$	$-2^{m+12}3^{3+6s}p^{2n+6}$

31. *there exist integers $m\geq 2$ and $s,t\in\{0,1\}$ such that $\frac{2^m+1}{3p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
LL1	$2\cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m+1}{3p}}$	$2^m 3^{2s+1}p^{2t+1}$	$2^{2m+6}3^{3+6s}p^{3+6t}$
LL2	$-4\cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m+1}{3p}}$	$4\cdot 3^{2s+1}p^{2t+1}$	$2^{m+12}3^{3+6s}p^{3+6t}$
LL1′	$-2\cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m+1}{3p}}$	$2^m 3^{2s+1}p^{2t+1}$	$2^{2m+6}3^{3+6s}p^{3+6t}$
LL2′	$4\cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m+1}{3p}}$	$4\cdot 3^{2s+1}p^{2t+1}$	$2^{m+12}3^{3+6s}p^{3+6t}$

32. *there exist integers $m\geq 2$ and $s,t\in\{0,1\}$ such that $\frac{2^m-1}{3p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
MM1	$2\cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m-1}{3p}}$	$2^m 3^{2s+1}p^{2t+1}$	$-2^{2m+6}3^{3+6s}p^{3+6t}$
MM2	$-4\cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m-1}{3p}}$	$-4\cdot 3^{2s+1}p^{2t+1}$	$2^{m+12}3^{3+6s}p^{3+6t}$
MM1′	$-2\cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m-1}{3p}}$	$2^m 3^{2s+1}p^{2t+1}$	$-2^{2m+6}3^{3+6s}p^{3+6t}$
MM2′	$4\cdot 3^{s+1}p^{t+1}\sqrt{\frac{2^m-1}{3p}}$	$-4\cdot 3^{2s+1}p^{2t+1}$	$2^{m+12}3^{3+6s}p^{3+6t}$

Theorem 3.28 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^7 3^b p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $2 \cdot 3^\ell + p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$2 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell + p^n}$	$2 \cdot 3^{\ell+2(b-1)} p^2$	$2^8 3^{2\ell+6(b-1)} p^{n+6}$
A2	$-4 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell + p^n}$	$4 \cdot 3^{2(b-1)} p^{n+2}$	$2^{13} 3^{\ell+6(b-1)} p^{2n+6}$
A1′	$-2 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell + p^n}$	$2 \cdot 3^{\ell+2(b-1)} p^2$	$2^8 3^{2\ell+6(b-1)} p^{n+6}$
A2′	$4 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell + p^n}$	$4 \cdot 3^{2(b-1)} p^{n+2}$	$2^{13} 3^{\ell+6(b-1)} p^{2n+6}$
B1	$2 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell + p^n}$	$3^{2(b-1)} p^{n+2}$	$2^7 3^{\ell+6(b-1)} p^{2n+6}$
B2	$-4 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell + p^n}$	$8 \cdot 3^{\ell+2(b-1)} p^2$	$2^{14} 3^{2\ell+6(b-1)} p^{n+6}$
B1′	$-2 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell + p^n}$	$3^{2(b-1)} p^{n+2}$	$2^7 3^{\ell+6(b-1)} p^{2n+6}$
B2′	$4 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell + p^n}$	$8 \cdot 3^{\ell+2(b-1)} p^2$	$2^{14} 3^{2\ell+6(b-1)} p^{n+6}$

2. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $2 \cdot 3^\ell - p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$2 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell - p^n}$	$2 \cdot 3^{\ell+2(b-1)} p^2$	$-2^8 3^{2\ell+6(b-1)} p^{n+6}$
C2	$-4 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^{n+2}$	$2^{13} 3^{\ell+6(b-1)} p^{2n+6}$
C1′	$-2 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell - p^n}$	$2 \cdot 3^{\ell+2(b-1)} p^2$	$-2^8 3^{2\ell+6(b-1)} p^{n+6}$
C2′	$4 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell - p^n}$	$-4 \cdot 3^{2(b-1)} p^{n+2}$	$2^{13} 3^{\ell+6(b-1)} p^{2n+6}$
D1	$2 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell - p^n}$	$-3^{2(b-1)} p^{n+2}$	$2^7 3^{\ell+6(b-1)} p^{2n+6}$
D2	$-4 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell - p^n}$	$8 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{14} 3^{2\ell+6(b-1)} p^{n+6}$
D1′	$-2 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell - p^n}$	$-3^{2(b-1)} p^{n+2}$	$2^7 3^{\ell+6(b-1)} p^{2n+6}$
D2′	$4 \cdot 3^{b-1} p\sqrt{2 \cdot 3^\ell - p^n}$	$8 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{14} 3^{2\ell+6(b-1)} p^{n+6}$

3. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $2p^n + 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$2\cdot 3^{b-1}p\sqrt{2p^n+3^\ell}$	$2\cdot 3^{2(b-1)}p^{n+2}$	$2^8 3^{\ell+6(b-1)}p^{2n+6}$
E2	$-4\cdot 3^{b-1}p\sqrt{2p^n+3^\ell}$	$4\cdot 3^{\ell+2(b-1)}p^2$	$2^{13}3^{2\ell+6(b-1)}p^{n+6}$
E1′	$-2\cdot 3^{b-1}p\sqrt{2p^n+3^\ell}$	$2\cdot 3^{2(b-1)}p^{n+2}$	$2^8 3^{\ell+6(b-1)}p^{2n+6}$
E2′	$4\cdot 3^{b-1}p\sqrt{2p^n+3^\ell}$	$4\cdot 3^{\ell+2(b-1)}p^2$	$2^{13}3^{2\ell+6(b-1)}p^{n+6}$
F1	$2\cdot 3^{b-1}p\sqrt{2p^n+3^\ell}$	$3^{\ell+2(b-1)}p^2$	$2^7 3^{2\ell+6(b-1)}p^{n+6}$
F2	$-4\cdot 3^{b-1}p\sqrt{2p^n+3^\ell}$	$8\cdot 3^{2(b-1)}p^{n+2}$	$2^{14}3^{\ell+6(b-1)}p^{2n+6}$
F1′	$-2\cdot 3^{b-1}p\sqrt{2p^n+3^\ell}$	$3^{\ell+2(b-1)}p^2$	$2^7 3^{2\ell+6(b-1)}p^{n+6}$
F2′	$4\cdot 3^{b-1}p\sqrt{2p^n+3^\ell}$	$8\cdot 3^{2(b-1)}p^{n+2}$	$2^{14}3^{\ell+6(b-1)}p^{2n+6}$

4. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $2p^n - 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$2\cdot 3^{b-1}p\sqrt{2p^n-3^\ell}$	$2\cdot 3^{2(b-1)}p^{n+2}$	$-2^8 3^{\ell+6(b-1)}p^{2n+6}$
G2	$-4\cdot 3^{b-1}p\sqrt{2p^n-3^\ell}$	$-4\cdot 3^{\ell+2(b-1)}p^2$	$2^{13}3^{2\ell+6(b-1)}p^{n+6}$
G1′	$-2\cdot 3^{b-1}p\sqrt{2p^n-3^\ell}$	$2\cdot 3^{2(b-1)}p^{n+2}$	$-2^8 3^{\ell+6(b-1)}p^{2n+6}$
G2′	$4\cdot 3^{b-1}p\sqrt{2p^n-3^\ell}$	$-4\cdot 3^{\ell+2(b-1)p^2}$	$2^{13}3^{2\ell+6(b-1)}p^{n+6}$
H1	$2\cdot 3^{b-1}p\sqrt{2p^n-3^\ell}$	$-3^{\ell+2(b-1)}p^2$	$2^7 3^{2\ell+6(b-1)}p^{n+6}$
H2	$-4\cdot 3^{b-1}p\sqrt{2p^n-3^\ell}$	$8\cdot 3^{2(b-1)}p^{n+2}$	$-2^{14}3^{\ell+6(b-1)}p^{2n+6}$
H1′	$-2\cdot 3^{b-1}p\sqrt{2p^n-3^\ell}$	$-3^{\ell+2(b-1)}p^2$	$2^7 3^{2\ell+6(b-1)}p^{n+6}$
H2′	$4\cdot 3^{b-1}p\sqrt{2p^n-3^\ell}$	$8\cdot 3^{2(b-1)}p^{n+2}$	$-2^{14}3^{\ell+6(b-1)}p^{2n+6}$

5. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $2+3^\ell p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$2\cdot 3^{b-1}p\sqrt{2+3^\ell p^n}$	$2\cdot 3^{2(b-1)}p^2$	$2^8 3^{\ell+6(b-1)}p^{n+6}$
I2	$-4\cdot 3^{b-1}p\sqrt{2+3^\ell p^n}$	$4\cdot 3^{\ell+2(b-1)}p^{n+2}$	$2^{13}3^{2\ell+6(b-1)}p^{2n+6}$
I1′	$-2\cdot 3^{b-1}p\sqrt{2+3^\ell p^n}$	$2\cdot 3^{2(b-1)}p^2$	$2^8 3^{\ell+6(b-1)}p^{n+6}$
I2′	$4\cdot 3^{b-1}p\sqrt{2+3^\ell p^n}$	$4\cdot 3^{\ell+2(b-1)}p^{n+2}$	$2^{13}3^{2\ell+6(b-1)}p^{2n+6}$
J1	$2\cdot 3^{b-1}p\sqrt{2+3^\ell p^n}$	$3^{\ell+2(b-1)}p^{n+2}$	$2^7 3^{2\ell+6(b-1)}p^{2n+6}$
J2	$-4\cdot 3^{b-1}p\sqrt{2+3^\ell p^n}$	$8\cdot 3^{2(b-1)}p^2$	$2^{14}3^{\ell+6(b-1)}p^{n+6}$
J1′	$-2\cdot 3^{b-1}p\sqrt{2+3^\ell p^n}$	$3^{\ell+2(b-1)}p^{n+2}$	$2^7 3^{2\ell+6(b-1)}p^{2n+6}$
J2′	$4\cdot 3^{b-1}p\sqrt{2+3^\ell p^n}$	$8\cdot 3^{2(b-1)}p^2$	$2^{14}3^{\ell+6(b-1)}p^{n+6}$

6. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $3^\ell p^n - 2$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$2 \cdot 3^{b-1} p \sqrt{3^\ell p^n - 2}$	$-2 \cdot 3^{2(b-1)} p^2$	$2^8 3^{\ell+6(b-1)} p^{n+6}$
K2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell p^n - 2}$	$4 \cdot 3^{\ell+2(b-1)} p^{n+2}$	$-2^{13} 3^{2\ell+6(b-1)} p^{2n+6}$
K1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell p^n - 2}$	$-2 \cdot 3^{2(b-1)} p^2$	$2^8 3^{\ell+6(b-1)} p^{n+6}$
K2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell p^n - 2}$	$4 \cdot 3^{\ell+2(b-1)} p^{n+2}$	$-2^{13} 3^{2\ell+6(b-1)} p^{2n+6}$
L1	$2 \cdot 3^{b-1} p \sqrt{3^\ell p^n - 2}$	$3^{\ell+2(b-1)} p^{n+2}$	$-2^7 3^{2\ell+6(b-1)} p^{2n+6}$
L2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell p^n - 2}$	$-8 \cdot 3^{2(b-1)} p^2$	$2^{14} 3^{\ell+6(b-1)} p^{n+6}$
L1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell p^n - 2}$	$3^{\ell+2(b-1)} p^{n+2}$	$-2^7 3^{2\ell+6(b-1)} p^{2n+6}$
L2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell p^n - 2}$	$-8 \cdot 3^{2(b-1)} p^2$	$2^{14} 3^{\ell+6(b-1)} p^{n+6}$

7. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $3^\ell - 2p^n$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$2 \cdot 3^{b-1} p \sqrt{3^\ell - 2p^n}$	$-2 \cdot 3^{2(b-1)} p^{n+2}$	$2^8 3^{\ell+6(b-1)} p^{2n+6}$
M2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell - 2p^n}$	$4 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{13} 3^{2\ell+6(b-1)} p^{n+6}$
M1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell - 2p^n}$	$-2 \cdot 3^{2(b-1)} p^{n+2}$	$2^8 3^{\ell+6(b-1)} p^{2n+6}$
M2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell - 2p^n}$	$4 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{13} 3^{2\ell+6(b-1)} p^{n+6}$
N1	$2 \cdot 3^{b-1} p \sqrt{3^\ell - 2p^n}$	$3^{\ell+2(b-1)} p^2$	$-2^7 3^{2\ell+6(b-1)} p^{n+6}$
N2	$-4 \cdot 3^{b-1} p \sqrt{3^\ell - 2p^n}$	$-8 \cdot 3^{2(b-1)} p^{n+2}$	$2^{14} 3^{\ell+6(b-1)} p^{2n+6}$
N1′	$-2 \cdot 3^{b-1} p \sqrt{3^\ell - 2p^n}$	$3^{\ell+2(b-1)} p^2$	$-2^7 3^{2\ell+6(b-1)} p^{n+6}$
N2′	$4 \cdot 3^{b-1} p \sqrt{3^\ell - 2p^n}$	$-8 \cdot 3^{2(b-1)} p^{n+2}$	$2^{14} 3^{\ell+6(b-1)} p^{2n+6}$

8. *there exist integers $\ell \geq 2-b$ and $n \geq 0$ such that $p^n - 2 \cdot 3^\ell$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$2\cdot 3^{b-1}p\sqrt{p^n-2\cdot 3^\ell}$	$-2\cdot 3^{\ell+2(b-1)}p^2$	$2^8 3^{2\ell+6(b-1)}p^{n+6}$
O2	$-4\cdot 3^{b-1}p\sqrt{p^n-2\cdot 3^\ell}$	$4\cdot 3^{2(b-1)}p^{n+2}$	$-2^{13}3^{\ell+6(b-1)}p^{2n+6}$
O1′	$-2\cdot 3^{b-1}p\sqrt{p^n-2\cdot 3^\ell}$	$-2\cdot 3^{\ell+2(b-1)}p^2$	$2^8 3^{2\ell+6(b-1)}p^{n+6}$
O2′	$4\cdot 3^{b-1}p\sqrt{p^n-2\cdot 3^\ell}$	$4\cdot 3^{2(b-1)}p^{n+2}$	$-2^{13}3^{\ell+6(b-1)}p^{2n+6}$
P1	$2\cdot 3^{b-1}p\sqrt{p^n-2\cdot 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^7 3^{\ell+6(b-1)}p^{2n+6}$
P2	$-4\cdot 3^{b-1}p\sqrt{p^n-2\cdot 3^\ell}$	$-8\cdot 3^{\ell+2(b-1)}p^2$	$2^{14}3^{2\ell+6(b-1)}p^{n+6}$
P1′	$-2\cdot 3^{b-1}p\sqrt{p^n-2\cdot 3^\ell}$	$3^{2(b-1)}p^{n+2}$	$-2^7 3^{\ell+6(b-1)}p^{2n+6}$
P2′	$4\cdot 3^{b-1}p\sqrt{p^n-2\cdot 3^\ell}$	$-8\cdot 3^{\ell+2(b-1)}p^2$	$2^{14}3^{2\ell+6(b-1)}p^{n+6}$

9. *there exist integers $\ell \geq 2-b$ and $t\in\{0,1\}$ such that $\frac{2\cdot 3^\ell+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell+1}{p}}$	$2\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^8 3^{2\ell+6(b-1)}p^{3+6t}$
Q2	$-4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell+1}{p}}$	$4\cdot 3^{2(b-1)}p^{2t+1}$	$2^{13}3^{\ell+6(b-1)}p^{3+6t}$
Q1′	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell+1}{p}}$	$2\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^8 3^{2\ell+6(b-1)}p^{3+6t}$
Q2′	$4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell+1}{p}}$	$4\cdot 3^{2(b-1)}p^{2t+1}$	$2^{13}3^{\ell+6(b-1)}p^{3+6t}$
R1	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell+1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^7 3^{\ell+6(b-1)}p^{3+6t}$
R2	$-4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell+1}{p}}$	$8\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^{14}3^{2\ell+6(b-1)}p^{3+6t}$
R1′	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell+1}{p}}$	$3^{2(b-1)}p^{2t+1}$	$2^7 3^{\ell+6(b-1)}p^{3+6t}$
R2′	$4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell+1}{p}}$	$8\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^{14}3^{2\ell+6(b-1)}p^{3+6t}$

10. *there exist integers $\ell \geq 2-b$ and $t\in\{0,1\}$ such that $\frac{2\cdot 3^\ell-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
S1	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell-1}{p}}$	$2\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^8 3^{2\ell+6(b-1)}p^{3+6t}$
S2	$-4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell-1}{p}}$	$-4\cdot 3^{2(b-1)}p^{2t+1}$	$2^{13}3^{\ell+6(b-1)}p^{3+6t}$
S1′	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell-1}{p}}$	$2\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^8 3^{2\ell+6(b-1)}p^{3+6t}$
S2′	$4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell-1}{p}}$	$-4\cdot 3^{2(b-1)}p^{2t+1}$	$2^{13}3^{\ell+6(b-1)}p^{3+6t}$
T1	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell-1}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^7 3^{\ell+6(b-1)}p^{3+6t}$
T2	$-4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell-1}{p}}$	$8\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^{14}3^{2\ell+6(b-1)}p^{3+6t}$
T1′	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell-1}{p}}$	$-3^{2(b-1)}p^{2t+1}$	$2^7 3^{\ell+6(b-1)}p^{3+6t}$
T2′	$4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2\cdot 3^\ell-1}{p}}$	$8\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^{14}3^{2\ell+6(b-1)}p^{3+6t}$

11. *there exist integers $\ell \geq 2-b$ and $t\in\{0,1\}$ such that $\frac{2+3^\ell}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
U1	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2+3^\ell}{p}}$	$2\cdot 3^{2(b-1)}p^{2t+1}$	$2^8 3^{\ell+6(b-1)}p^{3+6t}$
U2	$-4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2+3^\ell}{p}}$	$4\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^{13}3^{2\ell+6(b-1)}p^{3+6t}$
U1′	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2+3^\ell}{p}}$	$2\cdot 3^{2(b-1)}p^{2t+1}$	$2^8 3^{\ell+6(b-1)}p^{3+6t}$
U2′	$4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2+3^\ell}{p}}$	$4\cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^{13}3^{2\ell+6(b-1)}p^{3+6t}$
V1	$2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2+3^\ell}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^7 3^{2\ell+6(b-1)}p^{3+6t}$
V2	$-4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2+3^\ell}{p}}$	$8\cdot 3^{2(b-1)}p^{2t+1}$	$2^{14}3^{\ell+6(b-1)}p^{3+6t}$
V1′	$-2\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2+3^\ell}{p}}$	$3^{\ell+2(b-1)}p^{2t+1}$	$2^7 3^{2\ell+6(b-1)}p^{3+6t}$
V2′	$4\cdot 3^{b-1}p^{t+1}\sqrt{\frac{2+3^\ell}{p}}$	$8\cdot 3^{2(b-1)}p^{2t+1}$	$2^{14}3^{\ell+6(b-1)}p^{3+6t}$

12. *there exist integers $\ell \geq 2-b$ and $t\in\{0,1\}$ such that $\frac{3^\ell-2}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
W1	$2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell - 2}{p}}$	$-2 \cdot 3^{2(b-1)} p^{2t+1}$	$2^8 3^{\ell+6(b-1)} p^{3+6t}$
W2	$-4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell - 2}{p}}$	$4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$-2^{13} 3^{2\ell+6(b-1)} p^{3+6t}$
W1′	$-2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell - 2}{p}}$	$-2 \cdot 3^{2(b-1)} p^{2t+1}$	$2^8 3^{\ell+6(b-1)} p^{3+6t}$
W2′	$4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell - 2}{p}}$	$4 \cdot 3^{\ell+2(b-1)} p^{2t+1}$	$-2^{13} 3^{2\ell+6(b-1)} p^{3+6t}$
X1	$2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell - 2}{p}}$	$3^{\ell+2(b-1)} p^{2t+1}$	$-2^7 3^{2\ell+6(b-1)} p^{3+6t}$
X2	$-4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell - 2}{p}}$	$-8 \cdot 3^{2(b-1)} p^{2t+1}$	$2^{14} 3^{\ell+6(b-1)} p^{3+6t}$
X1′	$-2 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell - 2}{p}}$	$3^{\ell+2(b-1)} p^{2t+1}$	$-2^7 3^{2\ell+6(b-1)} p^{3+6t}$
X2′	$4 \cdot 3^{b-1} p^{t+1} \sqrt{\frac{3^\ell - 2}{p}}$	$-8 \cdot 3^{2(b-1)} p^{2t+1}$	$2^{14} 3^{\ell+6(b-1)} p^{3+6t}$

In the case that $b = 2$, i.e. $N = 2^7 3^2 p^2$, we furthermore could have one of the following conditions satisfied:

13. *there exist integers $n \geq 0$ and $s \in \{0, 1\}$ such that $\frac{2p^n+1}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Y1	$2 \cdot 3^{s+1} p \sqrt{\frac{2p^n+1}{3}}$	$2 \cdot 3^{2s+1} p^{n+2}$	$2^8 3^{3+6s} p^{2n+6}$
Y2	$-4 \cdot 3^{s+1} p \sqrt{\frac{2p^n+1}{3}}$	$4 \cdot 3^{2s+1} p^2$	$2^{13} 3^{3+6s} p^{n+6}$
Y1′	$-2 \cdot 3^{s+1} p \sqrt{\frac{2p^n+1}{3}}$	$2 \cdot 3^{2s+1} p^{n+2}$	$2^8 3^{3+6s} p^{2n+6}$
Y2′	$4 \cdot 3^{s+1} p \sqrt{\frac{2p^n+1}{3}}$	$4 \cdot 3^{2s+1} p^2$	$2^{13} 3^{3+6s} p^{n+6}$
Z1	$2 \cdot 3^{s+1} p \sqrt{\frac{2p^n+1}{3}}$	$3^{2s+1} p^2$	$2^7 3^{3+6s} p^{n+6}$
Z2	$-4 \cdot 3^{s+1} p \sqrt{\frac{2p^n+1}{3}}$	$8 \cdot 3^{2s+1} p^{n+2}$	$2^{14} 3^{3+6s} p^{2n+6}$
Z1′	$-2 \cdot 3^{s+1} p \sqrt{\frac{2p^n+1}{3}}$	$3^{2s+1} p^2$	$2^7 3^{3+6s} p^{n+6}$
Z2′	$4 \cdot 3^{s+1} p \sqrt{\frac{2p^n+1}{3}}$	$8 \cdot 3^{2s+1} p^{n+2}$	$2^{14} 3^{3+6s} p^{2n+6}$

14. *there exist integers $n \geq 0$ and $s \in \{0, 1\}$ such that $\frac{p^n+2}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
AA1	$2\cdot 3^{s+1}p\sqrt{\frac{p^n+2}{3}}$	$2\cdot 3^{2s+1}p^2$	$2^8 3^{3+6s}p^{n+6}$
AA2	$-4\cdot 3^{s+1}p\sqrt{\frac{p^n+2}{3}}$	$4\cdot 3^{2s+1}p^{n+2}$	$2^{13}3^{3+6s}p^{2n+6}$
AA1′	$-2\cdot 3^{s+1}p\sqrt{\frac{p^n+2}{3}}$	$2\cdot 3^{2s+1}p^2$	$2^8 3^{3+6s}p^{n+6}$
AA2′	$4\cdot 3^{s+1}p\sqrt{\frac{p^n+2}{3}}$	$4\cdot 3^{2s+1}p^{n+2}$	$2^{13}3^{3+6s}p^{2n+6}$
BB1	$2\cdot 3^{s+1}p\sqrt{\frac{p^n+2}{3}}$	$3^{2s+1}p^{n+2}$	$2^7 3^{3+6s}p^{2n+6}$
BB2	$-4\cdot 3^{s+1}p\sqrt{\frac{p^n+2}{3}}$	$8\cdot 3^{2s+1}p^2$	$2^{14}3^{3+6s}p^{n+6}$
BB1′	$-2\cdot 3^{s+1}p\sqrt{\frac{p^n+2}{3}}$	$3^{2s+1}p^{n+2}$	$2^7 3^{3+6s}p^{2n+6}$
BB2′	$4\cdot 3^{s+1}p\sqrt{\frac{p^n+2}{3}}$	$8\cdot 3^{2s+1}p^2$	$2^{14}3^{3+6s}p^{n+6}$

15. *there exist integers $n\geq 0$ and $s\in\{0,1\}$ such that $\frac{p^n-2}{3}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
CC1	$2\cdot 3^{s+1}p\sqrt{\frac{p^n-2}{3}}$	$-2\cdot 3^{2s+1}p^2$	$2^8 3^{3+6s}p^{n+6}$
CC2	$-4\cdot 3^{s+1}p\sqrt{\frac{p^n-2}{3}}$	$4\cdot 3^{2s+1}p^{n+2}$	$-2^{13}3^{3+6s}p^{2n+6}$
CC1′	$-2\cdot 3^{s+1}p\sqrt{\frac{p^n-2}{3}}$	$-2\cdot 3^{2s+1}p^2$	$2^8 3^{3+6s}p^{n+6}$
CC2′	$4\cdot 3^{s+1}p\sqrt{\frac{p^n-2}{3}}$	$4\cdot 3^{2s+1}p^{n+2}$	$-2^{13}3^{3+6s}p^{2n+6}$
DD1	$2\cdot 3^{s+1}p\sqrt{\frac{p^n-2}{3}}$	$3^{2s+1}p^{n+2}$	$-2^7 3^{3+6s}p^{2n+6}$
DD2	$-4\cdot 3^{s+1}p\sqrt{\frac{p^n-2}{3}}$	$-8\cdot 3^{2s+1}p^2$	$2^{14}3^{3+6s}p^{n+6}$
DD1′	$-2\cdot 3^{s+1}p\sqrt{\frac{p^n-2}{3}}$	$3^{2s+1}p^{n+2}$	$-2^7 3^{3+6s}p^{2n+6}$
DD2′	$4\cdot 3^{s+1}p\sqrt{\frac{p^n-2}{3}}$	$-8\cdot 3^{2s+1}p^2$	$2^{14}3^{3+6s}p^{n+6}$

Theorem 3.29 *The elliptic curves E defined over $\mathbb{Q}$, of conductor $2^8 3^b p^2$, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *there exist integers $\ell\geq 2-b$ and $n\geq 0$ such that $\frac{3^\ell p^n-1}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
A1	$4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell p^n - 1}{2}}$	$2 \cdot 3^{\ell+2(b-1)} p^{n+2}$	$-2^9 3^{2\ell+6(b-1)} p^{2n+6}$
A2	$-8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell p^n - 1}{2}}$	$-8 \cdot 3^{2(b-1)} p^2$	$2^{15} 3^{\ell+6(b-1)} p^{n+6}$
A1′	$-4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell p^n - 1}{2}}$	$2 \cdot 3^{\ell+2(b-1)} p^{n+2}$	$-2^9 3^{2\ell+6(b-1)} p^{2n+6}$
A2′	$8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell p^n - 1}{2}}$	$-8 \cdot 3^{2(b-1)} p^2$	$2^{15} 3^{\ell+6(b-1)} p^{n+6}$
B1	$4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell p^n - 1}{2}}$	$-2 \cdot 3^{2(b-1)} p^2$	$2^9 3^{\ell+6(b-1)} p^{n+6}$
B2	$-8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell p^n - 1}{2}}$	$8 \cdot 3^{\ell+2(b-1)} p^{n+2}$	$-2^{15} 3^{2\ell+6(b-1)} p^{2n+6}$
B1′	$-4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell p^n - 1}{2}}$	$-2 \cdot 3^{2(b-1)} p^2$	$2^9 3^{\ell+6(b-1)} p^{n+6}$
B2′	$8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell p^n - 1}{2}}$	$8 \cdot 3^{\ell+2(b-1)} p^{n+2}$	$-2^{15} 3^{2\ell+6(b-1)} p^{2n+6}$

2. *there exist integers $\ell \geq 2 - b$ and $n \geq 0$ such that $\frac{3^\ell + p^n}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
C1	$4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell + p^n}{2}}$	$2 \cdot 3^{\ell+2(b-1)} p^2$	$2^9 3^{2\ell+6(b-1)} p^{n+6}$
C2	$-8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell + p^n}{2}}$	$8 \cdot 3^{2(b-1)} p^{n+2}$	$2^{15} 3^{\ell+6(b-1)} p^{2n+6}$
C1′	$-4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell + p^n}{2}}$	$2 \cdot 3^{\ell+2(b-1)} p^2$	$2^9 3^{2\ell+6(b-1)} p^{n+6}$
C2′	$8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell + p^n}{2}}$	$8 \cdot 3^{2(b-1)} p^{n+2}$	$2^{15} 3^{\ell+6(b-1)} p^{2n+6}$
D1	$4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell + p^n}{2}}$	$2 \cdot 3^{2(b-1)} p^{n+2}$	$2^9 3^{\ell+6(b-1)} p^{2n+6}$
D2	$-8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell + p^n}{2}}$	$8 \cdot 3^{\ell+2} p^2$	$2^{15} 3^{2\ell+6(b-1)} p^{n+6}$
D1′	$-4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell + p^n}{2}}$	$2 \cdot 3^{2(b-1)} p^{n+2}$	$2^9 3^{\ell+6(b-1)} p^{2n+6}$
D2′	$8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell + p^n}{2}}$	$8 \cdot 3^{\ell+2} p^2$	$2^{15} 3^{2\ell+6(b-1)} p^{n+6}$

3. *there exist integers $\ell \geq 2 - b$ and $n \geq 0$ such that $\frac{3^\ell - p^n}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
E1	$4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell - p^n}{2}}$	$2 \cdot 3^{\ell+2(b-1)} p^2$	$-2^9 3^{2\ell+6(b-1)} p^{n+6}$
E2	$-8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell - p^n}{2}}$	$-8 \cdot 3^{2(b-1)} p^{n+2}$	$2^{15} 3^{\ell+6(b-1)} p^{2n+6}$
E1′	$-4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell - p^n}{2}}$	$2 \cdot 3^{\ell+2(b-1)} p^2$	$-2^9 3^{2\ell+6(b-1)} p^{n+6}$
E2′	$8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell - p^n}{2}}$	$-8 \cdot 3^{2(b-1)} p^{n+2}$	$2^{15} 3^{\ell+6(b-1)} p^{2n+6}$
F1	$4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell - p^n}{2}}$	$-2 \cdot 3^{2(b-1)} p^{n+2}$	$2^9 3^{\ell+6(b-1)} p^{2n+6}$
F2	$-8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell - p^n}{2}}$	$8 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{15} 3^{2\ell+6(b-1)} p^{n+6}$
F1′	$-4 \cdot 3^{b-1} p \sqrt{\frac{3^\ell - p^n}{2}}$	$-2 \cdot 3^{2(b-1)} p^{n+2}$	$2^9 3^{\ell+6(b-1)} p^{2n+6}$
F2′	$8 \cdot 3^{b-1} p \sqrt{\frac{3^\ell - p^n}{2}}$	$8 \cdot 3^{\ell+2(b-1)} p^2$	$-2^{15} 3^{2\ell+6(b-1)} p^{n+6}$

4. *there exist integers $\ell \geq 2 - b$ and $n \geq 0$ such that $\frac{p^n - 3^\ell}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
G1	$4 \cdot 3^{b-1} p \sqrt{\frac{p^n - 3^\ell}{2}}$	$2 \cdot 3^{2(b-1)} p^{n+2}$	$-2^9 3^{\ell+6(b-1)} p^{2n+6}$
G2	$-8 \cdot 3^{b-1} p \sqrt{\frac{p^n - 3^\ell}{2}}$	$-8 \cdot 3^{\ell+2(b-1)} p^2$	$2^{15} 3^{2\ell+6(b-1)} p^{n+6}$
G1′	$-4 \cdot 3^{b-1} p \sqrt{\frac{p^n - 3^\ell}{2}}$	$2 \cdot 3^{2(b-1)} p^{n+2}$	$-2^9 3^{\ell+6(b-1)} p^{2n+6}$
G2′	$8 \cdot 3^{b-1} p \sqrt{\frac{p^n - 3^\ell}{2}}$	$-8 \cdot 3^{\ell+2(b-1)} p^2$	$2^{15} 3^{2\ell+6(b-1)} p^{n+6}$
H1	$4 \cdot 3^{b-1} p \sqrt{\frac{p^n - 3^\ell}{2}}$	$-2 \cdot 3^{\ell+2(b-1)} p^2$	$2^9 3^{2\ell+6(b-1)} p^{n+6}$
H2	$-8 \cdot 3^{b-1} p \sqrt{\frac{p^n - 3^\ell}{2}}$	$8 \cdot 3^{2(b-1)} p^{n+2}$	$-2^{15} 3^{\ell+6(b-1)} p^{2n+6}$
H1′	$-4 \cdot 3^{b-1} p \sqrt{\frac{p^n - 3^\ell}{2}}$	$-2 \cdot 3^{\ell+2(b-1)} p^2$	$2^9 3^{2\ell+6(b-1)} p^{n+6}$
H2′	$8 \cdot 3^{b-1} p \sqrt{\frac{p^n - 3^\ell}{2}}$	$8 \cdot 3^{2(b-1)} p^{n+2}$	$-2^{15} 3^{\ell+6(b-1)} p^{2n+6}$

5. *there exist integers $\ell \geq 2 - b$ and $t \in \{0, 1\}$ such that $\frac{3^\ell + 1}{2p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
I1	$4 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{2p}}$	$2 \cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^9 3^{2\ell+6(b-1)}p^{3+6t}$
I2	$-8 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{2p}}$	$8 \cdot 3^{2(b-1)}p^{2t+1}$	$2^{15} 3^{\ell+6(b-1)}p^{3+6t}$
I1′	$-4 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{2p}}$	$2 \cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^9 3^{2\ell+6(b-1)}p^{3+6t}$
I2′	$8 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{2p}}$	$8 \cdot 3^{2(b-1)}p^{2t+1}$	$2^{15} 3^{\ell+6(b-1)}p^{3+6t}$
J1	$4 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{2p}}$	$2 \cdot 3^{2(b-1)}p^{2t+1}$	$2^9 3^{\ell+6(b-1)}p^{3+6t}$
J2	$-8 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{2p}}$	$8 \cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^{15} 3^{2\ell+6(b-1)}p^{3+6t}$
J1′	$-4 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{2p}}$	$2 \cdot 3^{2(b-1)}p^{2t+1}$	$2^9 3^{\ell+6(b-1)}p^{3+6t}$
J2′	$8 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell+1}{2p}}$	$8 \cdot 3^{\ell+2(b-1)}p^{2t+1}$	$2^{15} 3^{2\ell+6(b-1)}p^{3+6t}$

6. *there exist integers $\ell \geq 2-b$ and $t \in \{0,1\}$ such that $\frac{3^\ell-1}{2p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
K1	$4 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{2p}}$	$2 \cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^9 3^{2\ell+6(b-1)}p^{3+6t}$
K2	$-8 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{2p}}$	$-8 \cdot 3^{2(b-1)}p^{2t+1}$	$2^{15} 3^{\ell+6(b-1)}p^{3+6t}$
K1′	$-4 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{2p}}$	$2 \cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^9 3^{2\ell+6(b-1)}p^{3+6t}$
K2′	$8 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{2p}}$	$-8 \cdot 3^{2(b-1)}p^{2t+1}$	$2^{15} 3^{\ell+6(b-1)}p^{3+6t}$
L1	$4 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{2p}}$	$-2 \cdot 3^{2(b-1)}p^{2t+1}$	$2^9 3^{\ell+6(b-1)}p^{3+6t}$
L2	$-8 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{2p}}$	$8 \cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^{15} 3^{2\ell+6(b-1)}p^{3+6t}$
L1′	$-4 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{2p}}$	$-2 \cdot 3^{2(b-1)}p^{2t+1}$	$2^9 3^{\ell+6(b-1)}p^{3+6t}$
L2′	$8 \cdot 3^{b-1}p^{t+1}\sqrt{\frac{3^\ell-1}{2p}}$	$8 \cdot 3^{\ell+2(b-1)}p^{2t+1}$	$-2^{15} 3^{2\ell+6(b-1)}p^{3+6t}$

In the case that $b = 2$, i.e. $N = 2^8 3^2 p^2$, we furthermore could have one of the following conditions satisfied:

7. *there exists an integer $n \geq 0$ such that $\frac{p^n+1}{6}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
M1	$4\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$2\cdot 3^{2s+1}p^{n+2}$	$2^9 3^{3+6s}p^{2n+6}$
M2	$-8\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$8\cdot 3^{2s+1}p^2$	$2^{15}3^{3+6s}p^{n+6}$
M1′	$-4\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$2\cdot 3^{2s+1}p^{n+2}$	$2^9 3^{3+6s}p^{2n+6}$
M2′	$8\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$8\cdot 3^{2s+1}p^2$	$2^{15}3^{3+6s}p^{n+6}$
N1	$4\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$2\cdot 3^{2s+1}p^2$	$2^9 3^{3+6s}p^{n+6}$
N2	$-8\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$8\cdot 3^{2s+1}p^{n+2}$	$2^{15}3^{3+6s}p^{2n+6}$
N1′	$-4\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$2\cdot 3^{2s+1}p^2$	$2^9 3^{3+6s}p^{n+6}$
N2′	$8\cdot 3^{s+1}p\sqrt{\frac{p^n+1}{3}}$	$8\cdot 3^{2s+1}p^{n+2}$	$2^{15}3^{3+6s}p^{2n+6}$

8. *there exists an integer $n\geq 0$ such that $\frac{p^n-1}{6}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
O1	$4\cdot 3^{s+1}p\sqrt{\frac{p^n-1}{3}}$	$2\cdot 3^{2s+1}p^{n+2}$	$-2^9 3^{3+6s}p^{2n+6}$
O2	$-8\cdot 3^{s+1}p\sqrt{\frac{p^n-1}{3}}$	$-8\cdot 3^{2s+1}p^2$	$2^{15}3^{3+6s}p^{n+6}$
O1′	$-4\cdot 3^{s+1}p\sqrt{\frac{p^n-1}{3}}$	$2\cdot 3^{2s+1}p^{n+2}$	$-2^9 3^{3+6s}p^{2n+6}$
O2′	$8\cdot 3^{s+1}p\sqrt{\frac{p^n-1}{3}}$	$-8\cdot 3^{2s+1}p^2$	$2^{15}3^{3+6s}p^{n+6}$
P1	$4\cdot 3^{s+1}p\sqrt{\frac{p^n-1}{3}}$	$-2\cdot 3^{2s+1}p^2$	$2^9 3^{3+6s}p^{n+6}$
P2	$-8\cdot 3^{s+1}p\sqrt{\frac{p^n-1}{3}}$	$8\cdot 3^{2s+1}p^{n+2}$	$-2^{15}3^{3+6s}p^{2n+6}$
P1′	$-4\cdot 3^{s+1}p\sqrt{\frac{p^n-1}{3}}$	$-2\cdot 3^{2s+1}p^2$	$2^9 3^{3+6s}p^{n+6}$
P2′	$8\cdot 3^{s+1}p\sqrt{\frac{p^n-1}{3}}$	$8\cdot 3^{2s+1}p^{n+2}$	$-2^{15}3^{3+6s}p^{2n+6}$

9. *there exist integers $s,t\in\{0,1\}$ such that E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ
Q1	0	$2\cdot 3^{2s+1}p^{2t+1}$	$-2^9 3^{3+6s}p^{3+6t}$
Q2	0	$-8\cdot 3^{2s+1}p^{2t+1}$	$2^{15}3^{3+6s}p^{3+6t}$
R1	0	$-2\cdot 3^{2s+1}p^{2t+1}$	$2^9 3^{3+6s}p^{3+6t}$
R2	0	$8\cdot 3^{2s+1}p^{2t+1}$	$-2^{15}3^{3+6s}p^{3+6t}$

3.4 Proofs of $2^\alpha 3^\beta p$ and $2^\alpha 3^\beta p^2$

We sketch a constructive proof that the curves listed in the tables of Sections 3.2 and 3.3 are all the curves up to $\mathbb{Q}$-isomorphism of the stated conductor. Most of the work has already been done in Appendix A; there we have a classification of curves (up to $\mathbb{Q}$-isomorphism, and containing a point of order 2) with conductor of the *form* $2^\alpha 3^\beta p^\delta$. All that needs to be done now is to find the *exact* conductor, i.e. the values of $0 \leq \alpha \leq 8$, $1 \leq \beta \leq 2$ and $1 \leq \delta \leq 2$. These will depend on the values of m, ℓ, n and the congruence class of d modulo 4 in the defining Diophantine equation. To compute the conductors of each of the curves in the tables of Appendix A we make extensive use of the tables in Chapter 2. Rather than get bogged down in all the details of computing the conductors of the curves we will give a general overview of how the computations can be done. This should be enough to give the reader the flavor of the proof and allow us to save some trees in the process.

In what follows we refer to the elliptic curve $y^2 = x^3 + ax^2 + bx$ by its coefficients a and b.

We split the curves appearing in Lemma A.1 into three classes: let A.1.I be the class consisting of curves numbered 1 through 9, A.1.II be the class of curves numbered 10 through 18, and A.1.III be the class of curves numbered 19 through 27. It is straightforward to check that the 2-valuations of a, b and Δ for curves in each of the three classes are as follows.

	A.1.I	A.1.II	A.1.III
$v_2(a)$	r_1	$= r_1 + 1$ (if $m \geq 1$) $> r_1 + 1$ (if $m = 0$)	$r_1 + 2$
$v_2(b)$	$m + 2r_1 - 2$	$2r_1$	$2r_1 + 1$
$v_2(\Delta)$	$2m + 6r_1$	$2r_1 + 1$	$6r_1 + 9$

It follows directly from Theorem 2.1 that for curves in A.1.I

$$v_2(N) = \begin{cases} 4 & \text{if } r_1 = 0, m = 2, \quad a \equiv 1 \pmod 4, b \equiv 1 \pmod 4 \\ 2 & \text{if } r_1 = 0, m = 2, \quad a \equiv 1 \pmod 4, b \equiv -1 \pmod 4 \\ 3 & \text{if } r_1 = 0, m = 2, \quad a \equiv -1 \pmod 4, b \equiv 1 \pmod 4 \\ 4 & \text{if } r_1 = 0, m = 2, \quad a \equiv -1 \pmod 4, b \equiv -1 \pmod 4 \\ 5 & \text{if } r_1 = 0, m = 3, \\ 4 & \text{if } r_1 = 0, m \geq 4, \quad a \equiv -1 \pmod 4 \\ 3 & \text{if } r_1 = 0, m = 4, 5, \quad a \equiv 1 \pmod 4 \\ 0 & \text{if } r_1 = 0, m = 6, \quad a \equiv 1 \pmod 4 \\ 1 & \text{if } r_1 = 0, m \geq 7, \quad a \equiv 1 \pmod 4 \\ 7 & \text{if } r_1 = 1, m = 1, \\ 6 & \text{if } r_1 = 1, m \geq 2, \\ 7 & \text{if } r_1 = 2, m = 1, \end{cases}$$

and for the curves in A.1.II we have

$$v_2(N) = \begin{cases} 6 & \text{if } r_1 = 0, m = 0,\ b \equiv 1 \pmod 4 \\ 5 & \text{if } r_1 = 0, m = 0,\ b \equiv -1 \pmod 4 \\ 7 & \text{if } r_1 = 0, m = 1, \\ 4 & \text{if } r_1 = 0, m = 2,\ \ a - b \equiv 13 \pmod{16}, \\ 3 & \text{if } r_1 = 0, m = 2,\ \ a - b \equiv 5 \pmod{16}, \\ 4 & \text{if } r_1 = 0, m = 2,\ \ a - b \equiv 1 \pmod{16}, \\ 2 & \text{if } r_1 = 0, m = 2,\ \ a - b \equiv 9 \pmod{16}, \\ 5 & \text{if } r_1 = 0, m = 3, \\ 4 & \text{if } r_1 = 0, m \geq 4,\ \ a/2 \equiv 1 \pmod 4 \\ 3 & \text{if } r_1 = 0, m = 4, 5,\ \ a/2 \equiv -1 \pmod 4 \\ 0 & \text{if } r_1 = 0, m = 6,\ \ a/2 \equiv -1 \pmod 4 \\ 1 & \text{if } r_1 = 0, m \geq 7,\ \ a/2 \equiv -1 \pmod 4 \\ 5 & \text{if } r_1 = 1, m = 0,\ \ b/4 \equiv 1 \pmod 4 \\ 6 & \text{if } r_1 = 1, m = 0,\ \ b/4 \equiv -1 \pmod 4 \\ 6 & \text{if } r_1 = 1, m \geq 1,\ \ b/4 \equiv 1 \pmod 4 \\ 7 & \text{if } r_1 = 2, m \geq 1.\ \ b/4 \equiv -1 \pmod 4. \end{cases}$$

As for the curves in A.1.III we simply have $v_2(N) = 8$.

The values of $v_3(N)$ can be directly computed from Theorem 2.3. We find that if E is one of the curves in Lemma A.1 and DE the corresponding Diophantine equation which p satisfies, then, if 3 appears as a coefficient of d^2 in DE then $v_3(N) = 2$, otherwise

$$v_3(N) = \begin{cases} 0 & \text{if } r_2 = 0 \text{ and } \ell = 0 \\ 1 & \text{if } r_2 = 0 \text{ and } \ell \neq 0 \\ 2 & \text{if } r_2 = 1. \end{cases}$$

Similarly, we find that if p appears as a coefficient of d^2 in DE then $v_p(N) = 2$,

otherwise

$$v_p(N) = \begin{cases} 0 & \text{if } r_3 = 0 \text{ and } n = 0 \\ 1 & \text{if } r_3 = 0 \text{ and } n \neq 0 \\ 2 & \text{if } r_3 = 1. \end{cases}$$

Recall, we also made the convention in Appendix A that, in the Diophantine equations listed in Lemma A.1, ℓ, m, or n can only be zero if they appear on the right-hand side of the equation. This just avoids redundancy in our list of curves.

This is all the information needed to distribute the curves in A.1 across the appropriate theorems in Sections 3.2 and 3.3. Notice that, by taking $\ell = 0$, we get curves of conductor $2^\alpha p^2$. This is how the curves in the theorems of Section 3.1 were originally found, though the proof we gave there did not reflect this.

Similar considerations can be applied to the curves in Lemma A.2.

This completes the proof of the theorems in Sections 3.2 and 3.3.

Chapter 4
Diophantine Lemmata

In this chapter we prepare all the Diophantine lemmata we will need in subsequent chapters.

4.1 Useful Results

In this section we collect together, for the convenience of the reader, all the results that we will need to solve the Diophantine equations in the next section.

The first result we will need is Catalan's Conjecture, which is now a theorem of Mihailescu [52]. In this work we will refer to it as "Catalan's Theorem", or simply as "Catalan".

Theorem 4.1 (Mihailescu) *The only solution to the diophantine equation*

$$x^n - y^m = 1$$

in positive integers x, y, m, n with $n, m > 1$ is given by $3^2 - 2^3 = 1$.

Some results of Cohn and Ljunggren that we will make use of are the following.

Theorem 4.2 (Cohn [19]) *Let k be odd. The only solutions to $x^2 + 2^k = y^n$ in positive integers x, y and $n \geq 3$ are*

k	x	y	n
$6\alpha + 1$	$5 \cdot 2^{3\alpha}$	$3 \cdot 2^{2\alpha}$	3
$4\alpha + 5$	$7 \cdot 2^{2\alpha}$	$3 \cdot 2^{\alpha}$	4
$10\alpha + 5$	$11 \cdot 2^{5\alpha+3}$	$3 \cdot 2^{2\alpha+1}$	5

with $\alpha \geq 0$.

Theorem 4.3 (Ljunggren [48]) *The equation* $x^4 - 3y^2 = 1$ *has no solution in positive integers.*

The main results that we will use in attacking the diophantine equations arising in the table of the previous chapter are the results of Bennett, Skinner, Vatsal and Yazdani. Here we restate the relevant parts of their results.

Theorem 4.4 (Bennett, Skinner [5]) *If* $n \geq 4$ *and* $C \in \{1, 2, 3, 6\}$ *then the equation*

$$x^n + y^n = Cz^2$$

has no solutions in nonzero pairwise coprime integers (x, y, z) *with, say,* $x > y$ *unless* $C = 2$ *and* $(n, x, y, z) \in \{(5, 3, -1, \pm 11), (4, 1, -1, \pm 1)\}$.

Theorem 4.5 (Bennett, Vatsal, Yazdani [6]) *If* $C \in \{1, 2, 3\}$, $n \geq 5$ *is prime and* α, β *are nonnegative integers, then the diophantine equation*

$$x^n + 3^\alpha y^n = C^\beta z^3$$

has no solutions in coprime integers (x, y, z) *with* $|xy| > 1$, *unless*

$$(|x|, |y|, \alpha, n, |Cz^3|) = (2, 1, 1, 7, 125)$$

or, possibly, $(\alpha, C) = (1, 2)$.

Theorem 4.6 (Bennett [3]) *Suppose that* $a < b$ *are positive integers with* $ab = 2^\alpha 3^\beta$ *for nonegative integers* α, β. *If* $n \geq 3$ *is an integer, then the only solutions in positive integers* x *and* y *to the diophantine equation* $ax^n - by^n = \pm 1$ *are given by*

$$(a, b, x, y, n) = \begin{cases} (1, 2, 1, 1, n), (2, 3, 1, 1, n), (3, 4, 1, 1, n), \\ (8, 9, 1, 1, n), (1, 9, 2, 1, 3). \end{cases}$$

The proofs of the above theorem rely heavily on results on ternary diophantine equations coming from the theory of Galois representations and modular forms. In a few cases of the proofs of the results in the next section we will need to make use of this theory, so we briefly outline the main idea as it applies here. See [5] for the general details.

Consider the equation $3^\ell x^q + 2^m y^q = d^2$ with ℓ, m, q fixed integers. We want to show this equation has no solutions for x, y, d, with $|xy| > 1$, in the case that $q \geq 7$ is prime and $m \geq 6$. Suppose that $(x, y, d) = (a, b, c)$ is a solution in this case. Without loss of generality we may assume $c \equiv 1 \pmod 4$. Then, as in [5], we associate to this solution the elliptic curve

$$E_{a,b,c} : Y^2 + XY = X^3 + \frac{c-1}{4}X^2 + 2^{m-2}b^q X,$$

whose discriminant is

$$\Delta = 2^{2m-12}3^\ell (ab^2)^q$$

and conductor is

$$N(E_{a,b,c}) = 2^\alpha 3 \prod_{p|ab} p,$$

where $\alpha \in \{-1, 0\}$. We then associate to $E_{a,b,c}$ a Galois representation $\rho_q^{E_{a,b,c}}$ which is irreducible (see [5] corollary 3.1 , this is where $|xy| > 1$ and $q \geq 7$ is required). The representation $\rho_q^{E_{a,b,c}}$ arises from a cuspidal newform of weight 2 and level $N = 2^{\alpha+1}3$ (see [5] Lemma 3.3). This is where we reach a contradiction, since there are no newforms at level 3 or 6.

So how does this help us with the diophantine equations we will be considering in the next section? Well, the above result applies to the equations

$$d^2 = 3^\ell p^n + 2^m \text{ and } d^2 = 3^\ell + 2^m p^n$$

to show that there are no solutions with both $m \geq 6$ and n having a prime divisor ≥ 7. Then we'll use other methods to deal with the other cases of n and m.

4.2 Diophantine lemmata

In the following p denotes a prime ≥ 5.

The following results generalize those of Ivorra [37] (and of Hadano [34]). In particular, Ivorra's work concerns the case when $\ell = 0$, thus in our proofs we can refer to Ivorra's work and assume $\ell \geq 1$.

For an integer n, let $P_{\min}(n)$ denote its smallest prime factor and $P_{\max}(n)$ denote its largest prime factor. This notation will be used throughout the rest of this section.

Lemma 4.7 *1. The solutions to*

$$d^2 - 2^m 3^\ell p^n = 1$$

with $m, \ell, n \geq 0$ and $d \geq 1$ satisfy one of the following

(i) $n = 0$ *and* $(d, m, \ell) \in \{(2, 0, 1), (3, 3, 0), (5, 3, 1), (7, 4, 1), (17, 5, 2)\}$,

(ii) $n = 1$ *and*

(a) $p = 5$ *and* $(d, m, \ell) \in \{(9, 4, 0), (161, 6, 4)\}$,

(b) $p = 3^\ell \pm 2$ *with* $\ell \geq 1$ *and* $(d, m) = (p \mp 1, 0)$,

(c) $p = \frac{3^\ell - 1}{2}$ *with* ℓ *odd and* $(d, m) = (4p + 1, 3)$,

(d) $p = \frac{3^\ell + 1}{2}$ *with* ℓ *even and* $(d, m) = (4p - 1, 3)$,

(e) $p = \frac{3^\ell + 1}{4}$ *with* ℓ *odd and* $(d, m) = (8p - 1, 4)$,

(f) $p = 2^{m-2} 3^\ell \pm 1$ *with* $m \geq 3$ *and* $d = 2p \mp 1$,

(g) $p = 2^{m-2} \pm 1$ *with* $m \geq 5$ *and* $(d, \ell) = (2p \mp 1, 0)$,

(h) $p = \frac{2^{m-2} + 1}{3^\ell}$ *with* $m \geq 5$, $\ell \geq 1$ *and* $d = 2^{m-1} + 1$, *where* $3^\ell \mid m - 2$.

(iii) $n = 2$ *and* $(p, m, \ell, d) \in \{(5, 0, 3, 26), (5, 5, 1, 49), (7, 6, 1, 97),$
$(11, 3, 5, 485), (17, 7, 2, 577)\}$.

2. The solutions to

$$d^2 - 2^m 3^\ell p^n = -1$$

with $m, \ell, n \geq 0$ and $d \geq 1$ must have $\ell = 0$ and satisfy one of the following

(i) $p \geq 5$ *and* $(d, m, n) = (1, 1, 0)$,

(ii) $p = 13$ *and* $(d, m, n) \in \{(5, 1, 1), (239, 1, 4)\}$,

(iii) $p \neq 13$, $p \equiv 1 \pmod 4$ *and* $(m, n) \in \{(0, 1), (1, 1), (1, 2)\}$.

Proof. 1) It follows from Corollary 1.4 of [3] that $n \in \{0, 1, 2\}$. By considering the equation modulo 8 either $m = 0$ or $m \geq 3$, since 3 and 5 are quadratic non-residues modulo 8. If $m = 0$ then the equation can be written

$$(d + 1)(d - 1) = 3^\ell p^n.$$

It follows $d + 1$ and $d - 1$ are coprime and so

$$\begin{cases} d + 1 = 3^\ell \\ d - 1 = p^n \end{cases} \quad \text{or} \quad \begin{cases} d - 1 = 3^\ell \\ d + 1 = p^n. \end{cases}$$

We will consider such cases many times throughout the proofs in this section so to save space we will collapse them into one single pair of equations:

$$\begin{cases} d \pm 1 = 3^\ell \\ d \mp 1 = p^n. \end{cases}$$

Subtracting the two equations gives

$$\pm 2 = 3^\ell - p^n.$$

If $n = 0$ then $\ell = 1$ and $d = 2$; if $n = 1$ then $p = 3^\ell \mp 2$. Finally, if $n = 2$ then $p^2 = 3^\ell \mp 2$, but modulo 3 implies the sign must be negative, and modulo 4 implies ℓ is odd.

For the rest of the proof we assume $m \geq 3$ and consider the cases $n = 0$, 1, and 2 separately.

$n = 0$: Again, we could write the equation as $d^2 - 1 = 2^m 3^\ell$ and factor the left-hand side to obtain the solutions in an elementary way, however, a direct application of Corollary 1.4 of [3] suffices to show the only solutions are

$$(d, m, \ell) = \{(3, 3, 0), (5, 3, 1), (7, 4, 1), (17, 5, 2)\}.$$

$n = 1$ or 2: The equation can be written as

$$(d + 1)(d - 1) = 2^m 3^\ell p^n$$

where $\gcd(d + 1, d - 1) = 2$, so one of the following three cases must hold:

$$\begin{cases} d \pm 1 = 2 \cdot 3^\ell p^n \\ d \mp 1 = 2^{m-1} \end{cases}, \begin{cases} d \pm 1 = 2 \cdot p^n \\ d \mp 1 = 3^\ell \end{cases} \text{ or } \begin{cases} d \pm 1 = 2 \cdot 3^\ell \\ d \mp 1 = p^n \end{cases} \tag{4.1}$$

Case 1 of (4.1): Subtracting the equations and dividing through by 2 gives

$$3^\ell p^n - 2^{m-2} = \pm 1. \tag{4.2}$$

Suppose $3^\ell p^n - 2^{m-2} = -1$, then consideration modulo 3 implies m is even. Writing $m - 2 = 2k$ the equation can be written as $3^\ell p^n = (2^k + 1)(2^k - 1)$, thus

$$\begin{cases} 2^k \pm 1 = 3^\ell \\ 2^k \mp 1 = p^n \end{cases}$$

The second equation has no solutions by Catalan's theorem. Thus (4.2) is $3^\ell p^n - 2^{m-2} = 1$. Clearly $m \geq 5$ and consideration modulo 3 implies m odd. If $n = 1$ then we are in case (ii)(g) or (ii)(h) of the lemma. In this case $2^{2(m-2)} \equiv 1 \pmod{3^\ell}$, and so $3^{\ell-1} \mid m-2$ (see, for instance, [Be00] Lemma 3.1). On the other hand, if $n = 2$ then ℓ is even (look modulo 3). The equation can then be written

$$(3^{\ell/2}p)^2 - 2^{m-2} = 1$$

which has no solutions with $m \geq 5$ by Catalan's theorem.

Case 2 of (4.1): Subtracting the equations and dividing through by 2 gives

$$p^n - 2^{m-2}3^\ell = \pm 1.$$

If $n = 1$ then $p = 2^{m-2}3^\ell \pm 1$ which is case (ii)(f) of the lemma. If $n = 2$ then $p^2 = 2^{m-2}3^\ell \pm 1$. A simple inspection modulo 4 reveals that the negative sign cannot occur, therefore

$$p^2 = 2^{m-2}3^\ell + 1.$$

Moving the 1 to the left-hand side and factoring, or simply applying corollary 1.4 of [Be:2004], reveals the only solutions are

$$(m, \ell, p) \in \{(5, 1, 5), (6, 1, 7), (7, 2, 17)\}.$$

Case 3 of (4.1): Subtracting the equations and dividing through by 2 gives

$$3^\ell - 2^{m-2}p^n = \pm 1.$$

$n = 1$: If $m = 3$ then we are in (ii)(c) or (ii)(d) of the lemma. If $m = 4$ then we are in case (ii)(e) of the lemma. Now suppose $m \geq 5$, so the equation is

$$3^\ell - 2^{m-2}p = \pm 1. \tag{4.3}$$

The right-hand side must be positive and ℓ must be even by considering the equation modulo 8. Letting $\ell = 2k$ we may write

$$(3^k + 1)(3^k - 1) = 2^{m-2}p.$$

Since $\gcd(3^k + 1, 3^k - 1) = 2$ we are in one of the two cases:

$$\begin{cases} 3^k \pm 1 = 2 \\ 3^k \mp 1 = 2^{m-3}p \end{cases} \quad \text{or} \quad \begin{cases} 3^k \pm 1 = 2p \\ 3^k \mp 1 = 2^{m-3}. \end{cases}$$

The first case has no solutions, so we must be in the second case. Subtracting the two equations and dividing through by 2 gives $p - 2^{m-4} = \pm 1$, and so

$$p = 2^{m-4} \pm 1 \text{ with } m \geq 6.$$

Going back to (4.3) (recall the right-hand side must be positive) where we now know $m \geq 6$ we get $3^\ell \equiv 1 \pmod{16}$. Thus $4 \mid \ell$. Finally, taking (4.3) modulo 5 results in $2^{m-2}p \equiv 0 \pmod{5}$, hence $p = 5$. Thus the only solution with $m \geq 5$ is $(p, n, m, \ell, d) = (5, 1, 6, 4, 161)$.

$n = 2$: In this case the equation is

$$2^{m-2}p^2 = 3^\ell \pm 1.$$

If m is even then the equation is $(2^{(m-2)/2}p)^2 - 3^\ell = \pm 1$ which has no solutions by Catalan's theorem. Therefore m is odd and the equation can be written as

$$2x^2 - 3^\ell = \pm 1,$$

where $x = 2^{(m-3)/2}p$. Clearly there are no solutions, with x of the desired form, when $\ell = 0$, so assume $\ell \geq 1$. The left-hand side must be negative by considering the equation modulo 3:

$$2x^2 - 3^\ell = -1.$$

Certainly the only solutions with $\ell \leq 2$ are $(x, \ell) \in \{(1, 1), (2, 2)\}$. As for $\ell \geq 3$, Nagell [54] has shown the only solution is $(x, \ell) = (11, 5)$. Of these three solutions only one has x of the desired form, namely $(x, \ell) = (11, 5)$. Thus $2^{m-2}p^2 = 3^\ell \pm 1$ has only the solution $(p, m, \ell) = (11, 3, 5)$. This completes the proof (1).

2) Considering the equation $d^2 - 2^m 3^\ell p^n = -1$ modulo 3 implies $\ell = 0$. Therefore, the lemma follows from Lemma 3 in [37]. □

Lemma 4.8 *1. The solutions to*

$$d^2 - 2^m p^n = 3^\ell$$

with $\ell, n \geq 0$, $m \geq 2$, and $d \geq 1$ satisfy one of the following:

(i) $n = 0$ *and* $(d, m, \ell) = (3, 3, 0), (5, 4, 2)$,

(ii) $n = 1$ *and*

(a) $p = \frac{3^{\ell/2}+1}{2}$ *with* $\ell/2$ *even and* $(d, m) = (3^{\ell/2} + 2, 3)$,

(b) $p = \frac{3^{\ell/2}+1}{4}$ *with* $\ell/2$ *odd and* $(d, m) = (3^{\ell/2} + 2, 4)$,

(c) $p = 2^{m-2} \pm 3^{\ell/2}$ *with* $m \geq 3$ *and* $d = 2p \mp 3^{\ell/2}$,

(iii) $n = 2$, *and* $(p, m, \ell, d) = (5, 6, 4, 41)$.

(iv) $n = 3$ *and* $(p, m, \ell, d) = (5, 9, 2, 253)$.

2. *The solutions to*

$$d^2 + 3^\ell = 2^m p^n$$

with $m \geq 2$, $\ell \geq 1$ *and* $n \geq 0$ *satisfy one of the following:*

(i) $n = 0$, $m = 2$ *and* $\ell = 1$,

(ii) $n = 2$, $p = \frac{3^\ell+1}{4}$, ℓ *odd*, $m = 2$, *and* $d = 2p - 1$,

(iii) n *odd*, $n = 1$ *or* $P_{\min}(n) \geq 7$, $p \equiv 1 \pmod 3$, $m = 2$ *and* ℓ *odd.*

3. *The solutions to*

$$d^2 + 2^m p^n = 3^\ell$$

with $m \geq 2$, $\ell \geq 1$ *and* $n \geq 0$ *satisfy one of the following:*

(i) $n = 0$ *and* $(m, \ell, d) \in \{(3, 2, 1), (5, 4, 7)\}$,

(ii) $n = 1$ *and*

(a) $p = 5$ *and* $(m, \ell, d) = (6, 8, 79)$,

(b) $p = \frac{3^{\ell/2}-1}{2}$, $\ell/2$ *odd*, $m = 3$, *and* $d = \pm(4p - 3^{\ell/2})$,

(c) $p = 3^{\ell/2} - 2^{m-2}$, $m \geq 3$, ℓ *even, and* $d = \pm(2p - 3^{\ell/2})$,

(iii) $n = 2$ *and*

(a) $p = 5$ *and* $(m, \ell, d) = (3, 6, 23)$,

(b) $p = 7$ *and* $(m, \ell, d) = (7, 8, 17)$.,

(c) $p^2 = \frac{3^{\ell/2}-1}{2}$, $\ell/2$ *odd*, $m = 3$, *and* $d = \pm(4p^2 - 3^{\ell/2})$,

Proof. 1) The case when $\ell = 0$ is done in [37], so we may assume $\ell \geq 1$ henceforth. We break up the proof into a series of statements or "assertions".

Assertion 1: If $m \geq 6$ and $P_{\max}(n) \geq 7$ then there are no solutions.

Write the equation as

$$3^{\ell}(\pm 1)^q + 2^m y^q = d^2$$

where $q = P_{\max}(n) \geq 7$ and $y = p^{n/q}$. This is a particular form of the equation

$$3^{\ell} x^q + 2^m y^q = d^2.$$

Let $E_{a,b,c}$ be the elliptic curve associated to a solution $(x, y, d) = (a, b, c)$ of this equation as described in case (v) of [5]. It follows from Lemma 3.3 in [5] that $E_{a,b,c}$ has conductor

$$N(E_{a,b,c}) = \begin{cases} 3p & \text{if } m = 6 \\ 6p & \text{if } m \geq 7. \end{cases}$$

and corresponds to a cuspidal newform of weight 2, and level

$$\begin{cases} 3 & \text{if } m = 6 \\ 6 & \text{if } m \geq 7. \end{cases}$$

This gives a contradiction since there are no cuspidal newforms of weight 2 at these levels.

Assertion 2: If $m \geq 2$ then ℓ is even and $m \neq 2$.

This follows by inspection of the equation modulo 4 and 8.

Assertion 3: If $m \geq 2$ and $P_{\max}(n) \geq 5$ then $\ell = 2$. Furthermore, $m \geq 8$.

By assertion 2 it follows that ℓ is even so we may write $\ell = 2k$ and factor the equation as

$$(d + 3^{\ell})(d - 3^{\ell}) = 2^m p^n.$$

Either one of the following two cases holds:

$$\begin{cases} d \pm 3^k = 2 \\ d \mp 3^k = 2^{m-1} p^n \end{cases} \quad \text{or} \quad \begin{cases} d \pm 3^k = 2p^n \\ d \mp 3^k = 2^{m-1}. \end{cases}$$

Suppose we are in the first case. Subtracting the two equations and dividing through by 2 gives

$$2^{m-2} p^n \pm 3^k = 1.$$

Clearly there are no solutions when the sign is positive, and when the sign is negative there are no solutions by Theorem 1.2 of [3]. Now suppose we are in the second case. Subtracting the two equations and dividing through by 2 gives

$$x^t + 3^k(1)^t = 2^{m-2}(-1)^3,$$

where $t = P_{\max}(n)$ and $x = \pm p^{n/t}$. By Theorem 1.5 in [6] it follows that $k = 1$, i.e. $\ell = 2$. Additionally, one may easily check by hand that there are no solutions for $m \leq 7$. This proves assertion 3.

Assertion 4: If $m \geq 2$ and $P_{\max}(n) \geq 7$ then there are no solutions.

This is a direct consequence of assertions 1 and 3.

Assertion 5: If $m \geq 2$ and $P_{\max}(n) = 5$ then there are no solutions.

Recall $\ell = 2$ by assertion 3 so the equation can be written as $d^3 - 2^m x^5 = 9$ where $x = p^{n/5}$. Letting $0 \leq a \leq 4$ be the residue of m modulo 5 we may write

$$(2^{2m}d)^2 = (2^{\frac{m+4a}{5}}x)^5 + 2^{4a}9.$$

If $a \geq 3$ we may scale through by 2^{-10b} where $4a = 10b + r$, and $0 \leq r \leq 9$ is even, to get

$$\left(\frac{2^{2m}d}{2^{5b}}\right)^2 = \left(\frac{2^{\frac{m+4a}{5}}x}{2^{2b}}\right)^5 + 2^r 9.$$

The point is that solutions to our original equation correspond to rational points of a particular form on a genus 2 hyperelliptic curve: $Y^2 = X^5 + 2^{2s}9$, $0 \leq s \leq 4$. We show in Chapter 5 (see Theorem 5.1) that the rational points on these curves all have $X \in \{-2, 0, 4\}$. Thus, there are no solutions to our original equation. This proves assertion 5.

Assertion 6: If $m \geq 2$ and $P_{\max}(n) = 3$ then the only solution is $(p, n, m, \ell) = (5, 3, 9, 2)$.

In this case the equation can be written as $d^2 = 2^m x^3 + 3^\ell$ where $x = p^{n/3}$. Let $0 \leq a \leq 2$ be the residue of m modulo 3 and $0 \leq b \leq 5$ be the residue of ℓ modulo 6. Recall ℓ is even, so b must be even also. Making the change of variables

$$X = \frac{2^{(m+2a)/4}x}{3^{(\ell-b)/3}} \text{ and } D = \frac{2^a d}{3^{(\ell-b)/2}},$$

the equation becomes

$$D^2 = X^3 + 2^{2a}3^b \quad \text{where } 2a, b \in \{0, 2, 4\}.$$

We are only interested in solutions where X and D are of the form above, in particular (X, D) is to be a $\{3, \infty\}$-integral solution. The table in appendix B lists all the S-integral points on these elliptic curves. The only solution to this equation of the desired form occurs when $(a, b) = (0, 2)$ and it is $(X, D) = (40, 253)$. This pulls back to the solution $(p, n, m, \ell, d) = (5, 3, 9, 2, 253)$ of the original equation. This proves assertion 6.

Assertion 7: If $m \geq 2$ and $n = 2^a$ where $a \geq 1$ then $p = 5$ and $(m, \ell, d) = (6, 4, 41)$.

By considering the equation modulo 3 it follows that m is even ($2 \mid n$ means $p^n \equiv 1 \pmod 3$). Write $m = 2s$ and $n = 2t$ so equation becomes

$$(d + 2^s p^t)(d - 2^s p^t) = 3^\ell.$$

It follows that

$$\begin{cases} d + 2^s p^t = 3^\ell \\ d - 2^s p^t = 1, \end{cases}$$

and subtracting these equations gives

$$2^{s+1} p^t = 3^\ell - 1.$$

By assertion 2 we know ℓ is even so we may write $\ell = 2k$ and factor the right-hand side:

$$2^{s+1} p^t = (3^k + 1)(3^k - 1).$$

It follows that

$$\begin{cases} 3^k + 1 = 2^s p^t \\ 3^k - 1 = 2 \end{cases} \quad \text{or} \quad \begin{cases} 3^k \pm 1 = 2p^t \\ 3^k \mp 1 = 2^s. \end{cases}$$

The first case only has the solution $(k, s, t) = (1, 2, 0)$ which implies $n = 0$, a contradiction. In the second case, it follows from Catalan and the second equation that $(s, k) \in \{(1, 1), (2, 1), (3, 2)\}$, hence $p = 5$ and $(m, \ell, d) = (6, 4, 41)$. This proves assertion 7.

Assertion 8: If $m \geq 2$ and $n = 1$, then the only solutions are the ones stated in the lemma.

Since ℓ is even (assertion 2) the equation can be written as

$$(d + 3^k)(d - 3^k) = 2^m p,$$

where $\ell = 2k$. It follows that

$$\begin{cases} d \pm 3^k = 2p \\ d \mp 3^k = 2^{m-1} \end{cases} \quad \text{or} \quad \begin{cases} d - 3^k = 2 \\ d + 3^k = 2^{m-1}p. \end{cases}$$

Eliminating d in the first case gives $\pm 3^k = p - 2^{m-2}$. Thus $p = 2^{m-2} \pm 3^k$. In the second case eliminating d gives $-3^k = 1 - 2^{m-2}p$, that is

$$2^{m-2}p = 3^k + 1.$$

Considering this equation modulo 8 implies $m \leq 4$, so $m \in \{3, 4\}$. This proves assertion 8.

Finally, if $n = 0$ then the equation is $d^2 = 2^m + 3^\ell$ which only has the solution $(m, \ell, d) = (4, 2, 5)$ by Lemma 5 in [37]. This completes the proof of (1).

2) Considering the equation modulo 4 implies ℓ is odd, and considering the equation modulo 8 implies $m = 2$. If n is even then we may write $n = 2s$ and the equation becomes

$$(d + 2p^s)(d - 2p^2) = -3^\ell.$$

As we've done many times before in these arguments we eliminate d:

$$4p^s = 3^\ell + 1.$$

It follows from Theorem 1.2 in [3] that $s \in \{0, 1, 2\}$. If $s = 0$ or 1 then we are in case (i) or (ii) of the lemma, respectively. So assume $s = 2$. The equation can be factored as

$$(2p + 1)(2p - 1) = 3^\ell$$

and since we are to have $\gcd(2p + 1, 2p - 1) = 1$ it follows $2p - 1 = 1$ and hence there are no solutions. Now assume n is odd. Considering the equation

modulo 3 implies $p \equiv 1 \pmod 3$. It suffices to show 3 and 5 cannot divide n to complete the proof. If 3 divides n then the equation can be written as

$$d^2 = 4x^3 - 3^\ell,$$

where $x = p^{n/3}$. Changing variables we may write this as

$$\left(\frac{4d}{3^{3t}}\right)^2 = \left(\frac{2x}{3^{2t}}\right)^3 - 2^4 \cdot 3^a,$$

where $\ell = 6t + a$, $0 \leq a \leq 5$ is odd. By the tables in Appendix B there are no rational points on these elliptic curves of the desired form. If 5 divides n then a similar change of variables leads us to the equation

$$\left(\frac{16d}{3^{5t}}\right)^2 = \left(\frac{4x}{3^{2t}}\right)^5 - 2^8 \cdot 3^a,$$

where $x = p^{n/5}$ and $a \in \{1, 3, 5, 7, 9\}$. Again, there are no solutions of the desired form to these hyperelliptic curves as shown in Chapter 5. This completes the proof of (2).

3) If $n = 0$ then the equation is

$$d^2 = 3^\ell - 2^m.$$

Considering the equation modulo 3 it follows m must be odd. It is easy to check that the only solutions with $\ell \leq 2$ are

$$(m, \ell, d) \in \{(1, 1, 1), (3, 2, 1)\}.$$

As for the case when $\ell \geq 3$ it follows from [19] that the only solutions are $(m, \ell, d) \in \{(1, 3, 5), (5, 4, 7)\}$.

From now on we assume $n \geq 1$. It follows from the equation that $\ell \geq 3$ since the left-hand side is $d^2 + 2^m p^n \geq 1 + 10 = 11$. Furthermore, since $m \geq 2$ then considering the equation modulo 4 implies ℓ even, and further considerations modulo 8 imply $m \geq 3$.

Assertion: If $m \geq 2$ and $P_{\max}(n) \geq 3$ then the equation $d^2 + 2^m p^n = 3^\ell$ has no solutions.

Since ℓ is even we may factor the equation

$$(d-3^k)(d+3^k) = -2^m p^n,$$

where $\ell = 2k$. This leads to the two cases

$$\begin{cases} d \pm 3^k = \pm 2 \\ d \mp 3^k = \mp 2^{m-1} p^n \end{cases} \quad \text{or} \quad \begin{cases} d \pm 3^k = \pm 2p^n \\ d \mp 3^k = \mp 2^{m-1}. \end{cases}$$

Eliminating d in the first case gives

$$3^k - 2^{m-2} p^n = 1,$$

and by Theorem 1.2 in [3] there are no solutions, since $P_{\max}(n) \geq 3$. Eliminating d in the second case gives

$$3^k - p^n = 2^{m-2}.$$

If $P_{\max}(n) \geq 5$ then by Theorem 1.5 in [6] it follows that $k = 1$, i.e. $\ell = 2$, which contradicts $\ell \geq 3$. Now assume $P_{\max}(n) = 3$. We return to the original equation and write it as

$$d^2 = 2^m x^3 + 3^\ell,$$

where $x = p^{n/3}$. The solutions to this equation correspond to the rational points on the elliptic curves

$$Y^2 = X^3 + 2^{2a} 3^b$$

of the form

$$X = \frac{2^{a+s} p^{n/3}}{3^{2t}} \quad \text{and} \quad Y = \frac{2^a d}{3^{3t}},$$

where $m = 3s + a$, $\ell = 6t + b$ and $2a, b \in \{0, 2, 4\}$. From the tables in Appendix B we see there are no such points. This proves the assertion.

Finally, we consider the solutions with $n = 2^a$ for $a \geq 0$. Factoring the equation, as we did in the proof of the assertion above, we are in one of two cases:

$$3^k - 2^{m-2} p^n = 1 \quad \text{or} \quad 3^k - p^n = 2^{m-2}, \tag{4.4}$$

where $k = \ell/2$.

In the first case of (4.4), Theorem 1.2 of [3] implies $n \in \{1, 2\}$. If $m = 3$ then we are in case (ii)(b) or (ii)(b) of the lemma. So assume $m \geq 4$. Considering the equation modulo 4 implies k is even, i.e. $4 \mid \ell$, so we may factor the equation as

$$(3^s + 1)(3^s - 1) = 2^{m-2}p^n,$$

where $k = 2s$, i.e $s = \ell/4$. We are in one of two cases:

$$\begin{cases} 3^s + 1 = 2^{m-3}p^n \\ 3^s - 1 = 2 \end{cases} \quad \text{or} \quad \begin{cases} 3^s \pm 1 = 2^{m-3} \\ 3^s \mp 1 = 2p^n. \end{cases}$$

The first case clearly has no solutions (under our assumptions on p and n). Eliminating 3^s in the second case gives

$$\pm 1 = 2^{m-4} - p^n,$$

from which it follows from Catalan's Theorem that $n = 1$, and so $p = 2^{m-4} \pm 1$. It follows from assumptions on p that $m \geq 6$. Therefore, the equation in (4.4) becomes

$$3^k - 2^{m-2}p = 1,$$

where $m \geq 6$ and $4 \mid k$ (look modulo 16). Considering the equation modulo 5 implies $2^{m-2}p \equiv 0 \pmod 5$, thus $p = 5$ and we are in case (ii)(c) of the lemma.

Now suppose we are in the second case of (4.4). If $n = 1$ then we are in (ii)(c) of the lemma. So assume $n = 2^a$ with $a \geq 1$. If $m = 3$ then the equation is $3^k - p^n = 2$ which only has the solution $(p, n, k) = (5, 2, 3)$ in even n (see [19]). So assume $m \geq 4$. Considering the equation modulo 8 implies $m \geq 5$ and k is even, i.e. $4 \mid \ell$. Factor the equation as

$$(3^t + p^s)(3^t - p^s) = 2^{m-2},$$

where $k = 2t$ and $n = 2s$. It follows that

$$\begin{cases} 3^t + p^s = 2^{m-3} \\ 3^t - p^s = 2, \end{cases}$$

and so by eliminating p^s we get $3^t - 2^{m-4} = 1$. By Catalan's Theorem $(t, m) \in \{(1, 5), (2, 7)\}$, and solving for p, n, m and ℓ we get $(p, n, m, \ell) = (7, 2, 7, 8)$. This completes the proof of (3).

□

Lemma 4.9 *1. The solutions to*

$$d^2 - 2^m 3^\ell = p^n$$

with $m \geq 2$, $\ell \geq 0$ and $n \geq 1$ satisfy one of the following:

(i) $n = 2$ *and*
  (a) $p = 2^{m-2}3^\ell - 1$, $m \geq 3$, *and* $d = p + 2$,
  (b) $p = 3^\ell - 2^{m-2}$, $m \geq 3$, *and* $d = 2^{m-1} + p$,
  (c) $p = 2^{m-2} - 3^\ell$, $m \geq 5$, *and* $d = 2^{m-1} - p$,

(ii) $n = 3$, *and* $(p, m, \ell, d) \in \{(7, 1, 2, 19), (13, 2, 1, 47), (17, 7, 0, 71), (19, 1, 9, 215), (73, 15, 2, 827)\}$,

(iii) $n = 4$, *and* $(p, m, \ell, d) \in \{(5, 3, 3, 29), (7, 7, 4, 13)\}$,

(iv) $n = 6$, *and* $(p, m, \ell, d) = (5, 9, 1, 131)$,

(v) $P_{\min}(n) \geq 7$, $m \leq 5$ *and* $\ell \geq 1$,

(vi) $n = 1$.

2. The solutions to

$$d^2 + 2^m 3^\ell = p^n$$

with $m \geq 1$, $\ell \geq 0$ and $n \geq 1$ satisfy one of the following:

(i) $n = 2$ *and*
  (a) $p = 2^{m-2}3^\ell + 1$, $m \geq 3$, *and* $d = p - 2$,
  (b) $p = 3^\ell + 2^{m-2}$, $m \geq 3$, *and* $d = p - 2 \cdot 3^\ell$,

(ii) $n = 3$ *and* $(p, m, \ell, d) \in \{(5, 2, 0, 11), (7, 1, 3, 17), (13, 2, 5, 35), (73, 4, 7, 595), (97, 3, 4, 955), (193, 4, 4, 2681), (1153, 5, 5, 39151)\}$,

(iii) $n = 4$ *and* $(p, m, \ell, d) \in \{(5, 5, 1, 23), (5, 6, 2, 7), (7, 6, 1, 47), (17, 7, 2, 287)\}$,

(iv) $P_{\min}(n) \geq 7$ *and* $m \leq 5$,

(v) $n = 1$.

3. The solutions to

$$d^2 + p^n = 2^m 3^\ell$$

with $m \geq 1$, $\ell \geq 0$ and $n \geq 1$ satisfy one of the following:

(i) $n = 3$ *and* $(p, m, \ell, d) \in \{(23, 12, 1, 11), (5, 1, 5, 19), (7, 9, 0, 13), (23, 3, 7, 73), (47, 5, 11, 2359)\}$,

(ii) $P_{\min}(n) \geq 7$ *and* $m \leq 5$,

(iii) $n = 1$.

Proof. 1) The case when $\ell = 0$ is treated in [37], so we may assume $\ell \geq 1$. We break the proof up into the following sequence of "assertions".

Assertion 1: If $m \geq 6$ and $P_{\max}(n) \geq 7$ then there are no solutions.

Write the equation as

$$2^m 3^\ell (1)^q + y^q = d^2$$

where $q = P_{\max}(n) \geq 7$ and $y = p^{n/q}$. This is a particular form of the equation

$$2^m 3^\ell x^q + y^q = d^2.$$

Let $E_{a,b,c}$ be the elliptic curve associated to a solution $(x, y, d) = (a, b, c)$ of this equation as described in case (v) of [5]. It follows form Lemma 3.3 in [5] that $E_{a,b,c}$ has conductor

$$N(E_{a,b,c}) = \begin{cases} 3p & \text{if } m = 6 \\ 6p & \text{if } m \geq 7. \end{cases}$$

and corresponds to a cuspidal newform of weight 2, and level

$$\begin{cases} 3 & \text{if } m = 6 \\ 6 & \text{if } m \geq 7. \end{cases}$$

This gives a contradiction since there are no cuspidal newforms of weight 2 at these levels. This proves assertion 1.

Assertion 2: The only solutions with $3 \mid n$ are the ones with $n \in \{3, 6\}$ as stated in the lemma.

Applying the change of variables

$$X = \frac{p^{n/3}}{2^{2s}3^{2t}} \quad \text{and} \quad D = \frac{d}{2^{3s}3^{3t}},$$

to the equation $d^2 = p^n + 2^m 3^\ell$ where $m = 6s + a$ and $\ell = 6t + b$ with $0 \leq a, b \leq 5$, gives the equation

$$D^2 = X^3 + 2^a 3^b.$$

The rational points of the desired form on these elliptic curves can be found by inspection of the tables in Appendix B and are as follows:

$$(X, D, a, b) = \{(17/4, 71/8, 1, 0), (7, 19, 1, 2), (19/9, 215/27, 1, 3), (13, 47, 2, 1),$$

$$(25/4, 131/8, 3, 1), (73/16, 827/64, 3, 2)\}.$$

These pull back to the following solutions of the original equation:

$$(p, n, m, \ell, d) = \{(17, 3, 7, 0, 71), (7, 3, 1, 2, 19), (19, 3, 1, 9, 215), (13, 3, 2, 1, 47),$$

$$(5, 6, 9, 1, 131), (73, 3, 15, 2, 827)\}.$$

This proves assertion 2.

Assertion 3: There are no solutions with $5 \mid n$.

Solutions to $d^2 = p^n + 2^m 3^\ell$ with $5 \mid n$ correspond to rational points on $D^2 = X^5 + 2^a 3^b$, $0 \leq a, b \leq 9$, with x coordinate of the form

$$X = \frac{p^{n/5}}{2^{2s} 3^{2t}}.$$

We show in Chapter 5 that no such points exist.

Assertion 4: The only solutions with n even, $3 \nmid n$, are the ones with $n \in \{2, 4\}$ as stated in the lemma.

Considering the equation $d^2 = 2^m 3^\ell + p^n$ modulo 8 implies $m \geq 3$. Since n is even we may factor the equation as

$$(d + p^k)(d - p^k) = 2^m 3^\ell,$$

where $n = 2k$. It follows that we are in one of two cases

$$\begin{cases} d - p^n = 2 \\ d + p^k = 2^{m-1} 3^\ell, \end{cases} \quad \text{or} \quad \begin{cases} d \pm p^k = 2 \cdot 3^\ell \\ d \mp p^k = 2^{m-1}. \end{cases}$$

Eliminating d in the first case gives $2^{m-2}3^\ell - p^k = 1$, in which it follows from [3] that $k = 1$ or 2. However, considering this equation modulo 3 implies k is odd, therefore $k = 1$, and so $p = 2^{m-2}3^\ell - 1$.

In the second case, eliminating d gives

$$3^\ell \mp p^k = 2^{m-2}. \tag{4.5}$$

If $P_{\max}(k) \geq 5$ then it follows from Theorem 1.5 in [6] that $\ell = 1$. Recall $5 \nmid n$ by assertion 3, so we may assume $P_{\max}(k) \geq 7$. However, assertion 1 implies in this case that $m \leq 5$. It is now easy to see that there are no solutions with $P_{\max}(n) \geq 5$. So we must have that $k = 2^a$, $a \in \mathbb{N}$. If $k = 1$, i.e. $n = 2$, then we are are in case (i) of the lemma. So suppose $k = 2^a > 1$. If the equation in (4.5) is $3^\ell + p^k = 2^{m-2}$ then observe, by local considerations, that $m \geq 5$ is even and ℓ is odd. Factoring the equation, as we've done many times over, leads us to see there are no solutions. So equation (4.5) must be $3^\ell - p^k = 2^{m-2}$. If $m = 3$ then the equation is $3^\ell - p^k = 2$ which has only the solution $(p, \ell, k) = (5, 3, 2)$ (see [19]). So assume $m \geq 4$. Considering the equation modulo 4 implies ℓ is even and so we may factor as usual:

$$(3^{\ell/2} + p^{k/2})(3^{\ell/2} - p^{k/2}) = 2^{m-2},$$

from which it follows that

$$\begin{cases} 3^{\ell/2} + p^{k/2} = 2^{m-3} \\ 3^{\ell/2} - p^{k/2} = 2, \end{cases}$$

and so, eliminating $p^{k/2}$ we get $3^{\ell/2} - 2^{m-4} = 1$. By Catalan's Theorem $(m, \ell) \in \{(5, 2), (7, 4)\}$, only one of which pulls back to a solution of the original equation;

$$(p, n, m, \ell, d) = (7, 4, 7, 4, 113).$$

This proves assertion 4.

Finally, if n is odd it clearly follows from the equation $d^2 - 2^m 3^\ell = p^n$ that $p \equiv 1 \pmod{12}$.

2) Assertion 1 in the proof of (1) above also holds for this case, that is, there are no solutions if both $m \geq 6$ and $P_{\max}(n) \geq 7$. The case when $\ell = 0$ is

treated in [37] so we may assume $\ell \geq 1$. The solutions with $3 \mid n$ correspond to points on the elliptic curves

$$y^2 = x^3 - 2^a 3^b$$

of the form

$$x = \frac{p^{n/3}}{2^{2s}3^{2t}},$$

where $0 \leq a, b \leq 5$, $m = 6s + a$ and $\ell = 6t + b$. It follows from the tables in Appendix B that the only such points have $n = 1$ and correspond to the seven solutions in part (ii) of the lemma. The solutions with $5 \mid n$ correspond to points on the hyperelliptic curves

$$y^2 = x^5 - 2^a 3^b$$

of the form

$$x = \frac{p^{n/3}}{2^{2s}3^{2t}},$$

where $0 \leq a, b \leq 9$, $m = 10s + a$ and $\ell = 10t + b$. It follows from Chapter 5 that there are no rational points on these curves of this form. We break the rest of the proof up into two cases depending on the parity of n.

Assertion 5: The only solutions with n even are the ones with $n \in \{2, 4\}$ as stated in the lemma.

Since n is even we may factor the equation as

$$(d + p^k)(d - p^k) = -2^m 3^\ell,$$

where $n = 2k$, it follows that we are in one of the two cases

$$\begin{cases} d - p^k = -2 \\ d + p^k = 2^{m-1}3^\ell, \end{cases} \quad \text{or} \quad \begin{cases} d \pm p^k = 2 \cdot 3^\ell \\ d \mp p^k = 2^{m-1}. \end{cases}$$

Eliminating d in the first case gives $p^k - 2^{m-2}3^\ell = 1$ which has no solutions for $k \geq 3$ by [3], thus $k = 1$ or 2. If $k = 1$ then $p = 2^{m-2}3^\ell + 1$ and we are in case (ii)(a) of the lemma. If $k = 2$ then we may factor the equation as

$$(p + 1)(p - 1) = 2^{m-2}3^\ell,$$

where, as usual, eliminating p gives $\pm 1 = 3^\ell - 2^{m-4}$, so

$$(m, \ell) \in \{(5,1), (7,2), (6,1)\}$$

by Catalan. Thus,

$$(p, n, m, \ell) \in \{(5,4,5,1), (7,4,6,1), (17,4,7,2)\}.$$

In the second case, eliminating d gives

$$p^k = 3^\ell + 2^{m-2}.$$

We may assume $3, 5 \nmid k$ as these cases were already considered above. Suppose $P_{\max}(k) \geq 7$, then from Theorem 1.5 in [6] it follows that $\ell = 1$, and so $m \geq 7$. However, we have already seen that there are no solutions with $P_{\max}(n) \geq 7$ and $m \geq 7$. Therefore k, thus n, must be a power of 2. If $k = 1$ then we are in (i)(b) of the lemma. If $k = 2^a > 1$ then considering the equation $p^k = 3^\ell + 2^{m-2}$ modulo 3 implies $m \geq 4$ and even, and modulo 4 implies ℓ is even. As usual, factoring and applying Catalan gives $(p, n, m, \ell) = (5, 4, 6, 2)$. This proves assertion 5.

Finally, if n is odd and $(n, 15) = 1$ then either $n = 1$ or $P_{\max}(n) \geq 7$ (and $m \leq 5$ as we've argued using [5] many times before).

This proves (2).

3) As we've seen in (1) and (2) there are no solutions with both $m \geq 6$ and $P_{\max}(n) \geq 7$. The solutions with $3 \mid n$ correspond to rational points on the elliptic curves $y^2 = x^3 + 2^a 3^b$ of the form

$$x = \frac{-p^{n/3}}{2^{2s} 3^{2t}},$$

and these can be determined by consulting the tables in Appendix B. Similarly, the solutions with $5 \mid n$ correspond to rational points on the hyperelliptic curves $y^2 = x^5 + 2^a 3^b$ of the form

$$x = \frac{-p^{n/5}}{2^{2s} 3^{2t}},$$

of which there are none by Theorem 5.1. The solutions with n even must have $m = 1$ (looking modulo 3) and $\ell = 0$ (looking modulo 4), thus there are no solutions. This completes the proof of (3).

□

Lemma 4.10 *1. The solutions to*

$$d^2 - 2^m = 3^\ell p^n$$

with $m \geq 1$, $\ell \geq 0$ and $n \geq 1$ satisfy one of the following:

(i) $n = 1$ *and*

(a) $p = \frac{2^{m/2+1}+1}{3^\ell}$, $\ell \geq 1$, $d = 2^{m/2} + 1$,

(b) $p = 3^\ell \pm 2^{m/2+1}$, $\ell \geq 1$, $d = p \pm 2^{m/2}$,

(c) $\ell = 0$, m *odd.*

(ii) $n = 2$ *and*

(a) $(p, m, \ell, d) \in \{(5, 6, 2, 17), (7, 8, 4, 65)\}$,

(b) $p = 2^{m-2} - 1$, $m \geq 5$, $\ell = 0$ *and* $d = p + 2$,

(iii) $n = 3$ *and* $(p, m, \ell, d) = (17, 7, 0, 71)$.

2. The solutions to

$$d^2 - 2^m = -3^\ell p^n$$

with $m, \ell \geq 0$ and $n \geq 1$ satisfy one of the following:

(i) $n = 1$ *and*

(a) $(p, m, \ell, d) \in \{(5, 6, 1, 7), (7, 10, 2, 31)\}$,

(b) $p = 2^{m/2+1} - 3^\ell$, $m \geq 4$ *even*, $\ell \geq 1$, *and* $d = \pm(2^{m/2} - p)$,

(c) $\ell = 0$ *and* $m \geq 5$ *odd.*

(ii) $n = 3$ *and* $(p, m, \ell, d) \in \{(5, 12, 1, 61), (7, 9, 0, 13)\}$.

3. The solutions to

$$d^2 + 2^m = 3^\ell p^n$$

with $m \geq 1$, $\ell \geq 0$ and $n \geq 1$ satisfy one of the following:

(i) $n = 1$,

(ii) $n = 2$ *and*

(a) $(p, m, \ell, d) = (5, 4, 0, 3)$,

(b) $p = \frac{2^{m-1}+1}{3^{\ell/2}}$ *with* $m \geq 3$ *odd, and* $d = 3^{\ell/2}p - 2$,

(iii) $n = 3$ *and* $(p, m, \ell, d) \in \{(5, 2, 0, 11), (11, 9, 1, 59), (17, 15, 2, 107), (19, 7, 1, 143), (67, 5, 3, 8549), (73, 2, 9, 1871)\}$,

(iv) $P_{\max}(n) \geq 7$ *and* $m \in \{1, 3, 5\}$.

Proof. 1) The case when $\ell = 0$ is treated in [37] so we only need to consider $\ell \geq 1$. In this case it follows that m is even. As in the proofs of the other lemmata it follows from [5] there are no solutions with both $P_{\max}(n) \geq 7$ and $m \geq 6$. Also, there are no solutions in the case when $3 \mid n$ (resp. $5 \mid n$) since solutions would correspond to $\{2, \infty\}$-integral points on elliptic curves (resp. hyperelliptic curves) of a particular form of which there are none by Appendix B (resp. Theorem 5.1).

Assertion 1: The solutions with $P_{\max}(n) \geq 7$ must have $\ell = 1$.

Since m is even we can factor the equation as

$$(d + 2^k)(d - 2^k) = 3^\ell p^n,$$

where $m = 2k$. One of the following cases must hold:

$$\begin{cases} d + 2^k = 3^\ell p^n \\ d - 2^k = 1, \end{cases} \quad \text{or} \quad \begin{cases} d \pm 2^k = 3^\ell \\ d \mp 2^k = p^n. \end{cases}$$

Eliminating d in the first case gives $3^\ell p^n - 2^{k+1} = 1$ which has no solutions with $P_{\max}(n) \geq 7$ by Theorem 1.2 in [3]. Eliminating d in the second case gives

$$3^\ell - p^n = \pm 2^{k+1}, \tag{4.6}$$

from which $\ell = 1$ follows by Theorem 1.5 of [6]. This proves assertion 1.

Assertion 2: There are no solutions with $P_{\max}(n) \geq 7$.

It follows from remarks above that such solutions must have $m \in \{2, 4\}$ and $\ell = 1$. Furthermore, it follows from (4.6) that

$$p^n = 2^{m/2+1} + 3,$$

and so $p^n = 7$ or 11, which contradicts $P_{\max}(n) \geq 7$. This proves assertion 2.

Assertion 3: The solutions with n even are the ones with $n = 2$ as stated in the lemma .

Considering the equation modulo 4 implies ℓ is even, so we may factor the equation as

$$(d + 3^{\ell/2}p^{n/2})(d - 3^{\ell/2}p^{n/2}) = 2^m,$$

from which it follows that

$$\begin{cases} d \pm 3^{\ell/2}p^{n/2} = 2^{m-1} \\ d \mp 3^{\ell/2}p^{n/2} = 2. \end{cases}$$

Eliminating d give $3^{\ell/2}p^{n/2} = 2^{m-2} - 1$ and so $n \in \{2, 4\}$ by Theorem 1.2 of [3]. Furthermore, since m is even we may factor the right-hand side of this equation as

$$3^{\ell/2}p^{n/2} = (2^{(m-2)/2} + 1)(2^{(m-2)/2} - 1),$$

from which it follows that

$$\begin{cases} 2^{(m-2)/2} \pm 1 = 3^{\ell/2} \\ 2^{(m-2)/2} \mp 1 = p^{n/2}. \end{cases}$$

It follows from the first equation and Catalan that

$$(m, \ell) \in \{(4, 2), (6, 2), (8, 4)\},$$

and plugging these into the second equation gives $p = 5$ or 7. This proves assertion 3.

Finally, we need to consider the case when $n = 1$. Following the proof in assertion 1, where the fact that m even was used to factor the equation, we obtain the two cases:

$$3^{\ell}p - 2^{m/2+1} = 1 \quad \text{or} \quad 3^{\ell} - p = \pm 2^{m/2+1}.$$

This completes the proof of (1).

2) Clearly there are no solutions with $m \leq 3$. The case when $\ell = 0$ is treated in [37] so we only need to consider $\ell \geq 1$. In this case it follows that m is even and $m \geq 4$. Furthermore, n is odd. As in the proofs of the other lemmas it follows from [5] there are no solutions with both $P_{\max}(n) \geq 7$ and $m \geq 6$. Also, the only solution in the case when $3 \mid n$ is $(p, n, m, \ell, d) = (5, 3, 12, 1, 61)$ since solutions would correspond to $\{2, \infty\}$-integral points on elliptic curves which we can determine with the use of Appendix B.

Assertion 4: The solutions with $P_{\max}(n) \geq 5$ must have $\ell = 1$. Furthermore, there are no solutions with $P_{\max}(n) \geq 7$.

This follows by a similar argument as in assertions 1 and 2 of part (1) above.

If $5 \mid n$ then solutions to $d^2 - 2^m = -3p^n$ would correspond to $\{2, \infty\}$-integral points on hyperelliptic curves $y^2 = x^5 + 2^{2b}3^4$ with x of the form $x = (-3p^{n/5})/(2^{2k})$ and by Theorem 5.1 there are no such points.

The only case left to consider is $n = 1$. Since m is even we may factor the original equation as

$$(d + 2^{m/2})(d - 2^{m/2}) = -3^\ell p,$$

and so one of the following cases must hold:

$$\begin{cases} d + 2^{m/2} = 3^\ell p^n \\ d - 2^{m/2} = -1, \end{cases} \quad \text{or} \quad \begin{cases} d \pm 2^{m/2} = \pm 3^\ell \\ d \mp 2^{m/2} = \mp p^n. \end{cases}$$

Eliminating d in the first case gives $3^\ell p = 2^{m/2+1} - 1$ where $m/2 + 1$ must be even. By factoring the left-hand side we see the only solutions are $(p, m, \ell) \in \{(5, 6, 1), (7, 10, 2)\}$. Eliminating d in the second case gives $p = 2^{m/2+1} - 3^\ell$. This completes the proof of (2).

3) For the case when $\ell = 0$ see [37]. As usual, we can apply [5] to show there are no solutions with both $P_{\max}(n) \geq 7$ and $m \geq 6$. Also, local considerations at 3 imply m is odd.

The case when $3 \mid n$ (respectively $5 \mid n$) corresponds to finding $\{2, \infty\}$-integral points on elliptic curves (respectively hyperelliptic curves) so we can use the tables in Appendix B (respectively Theorem 5.1) to show the only solutions are the ones as stated in the lemma.

In the case when $2 \mid n$ we must have ℓ is even also and so we may factor the equation. A result of Bennett [3] shows $n = 2$ or 4, and a result of Cohn [19] shows $n \neq 4$. This completes the proof of (3).

□

Lemma 4.11 *1. The solutions to $3d^2 - 2^m = p^n$ with $m \geq 0$ and $n \geq 1$ satisfy one of the following:*

(i) $n = 3$ *and* $(p, m, d) = (11, 8, 23)$,

(ii) $P_{\max}(n) \geq 7$ *or* n *even, and* $m = 1$,

(iii) $n = 1$.

2. *The solutions to* $3d^2 - 2^m = -p^n$ *with* $m \geq 0$ *and* $n \geq 1$ *satisfy one of the following:*

   (i) $n = 3$ *and* $(p, m, d) = (5, 7, 1)$,

   (ii) $n = 1$.

3. *The solutions to* $3d^2 + 2^m = p^n$ *with* $m \geq 0$ *and* $n \geq 1$ *satisfy one of the following:*

   (i) $n = 3$ *and* $(p, m, d) = (11, 3, 21)$,

   (ii) $P_{\max}(n) \geq 7$ *and* $m = 1$,

   (iii) $n = 2$ *and* $m \in \{0, 1\}$,

   (iv) $n = 1$.

4. *The solutions to* $3d^2 - 2^m p^n = -1$ *with* $m \geq 0$ *and* $n \geq 1$ *satisfy* $m \in \{0, 2\}$ *and* $n \in \{1, 2\}$.

5. *The solutions to* $3d^2 - 2^m p^n = 1$ *with* $m \geq 0$ *and* $n \geq 1$ *satisfy* $m \in \{0, 1\}$ *and* $n \in \{1, 2\}$.

Proof. In the first three cases there are no solutions with $P_{\max}(n) \geq 7$ and $m \geq 2$ by Theorem 1.2 of [5].

1) First consider the case when $m = 0$, from which it follows that n is odd. There are no solutions with $n \geq 4$ by Theorem 1.1 of [5], and there are no solutions with $n = 3$ as shown in [18] (alternatively, this case corresponds to finding integral points on the Mordell curve $y^2 = x^3 + 27$). Thus $n = 1$ in this case. In what follows we may assume $m \geq 1$.

If $3 \mid n$ then the equation describes an elliptic curve (whose minimal model is of the form $y^2 = x^3 + 2^a 3^3$, $0 \leq a \leq 5$) and solutions correspond to $\{2, \infty\}$-integral points on the elliptic curve of a certain form. Using the tables in Appendix B we conclude that $(p, m, d) = (11, 8, 23)$ is the only solution in this case. Similarly, if $5 \mid n$ then the equation describes a hyperelliptic curve

(whose minimal model is of the form $y^2 = x^5 + 2^a 3^3$, $0 \leq a \leq 9$) and so we may apply results of Chapter 5 to conclude there are no solutions.

Finally, if n is even then considering the equations modulo 4 implies $m = 1$.

The proofs of (2) and (3) are very similar.

4) Considering the equation modulo 4 and 8 implies $m \in \{0, 2\}$. Suppose $m = 0$, then Theorem 1.1 of [5] implies $P_{\max}(n) \leq 3$. If $3 \mid n$ then the equation can be written as $(9d)^2 = (3p^{n/3})^3 - 27$ which, by the tables in Appendix B, has no solutions of the desired form. If $4 \mid n$ then the equation can be written as $3d^2 = x^4 - 1$ which has no solutions by [22]. Therefore, $n = 1, 2$. As for the case $m = 2$, Theorem 1.2 of [5] implies $P_{\max}(n) \in \{2, 3, 5\}$. If $5 \mid n$ then the equation can be written as $(2^4 3^3 d)^2 = (2^2 3 p^{n/5})^5 - 2^8 3^5$ which has no solutions by Theorem 5.1. If $3 \mid n$ then the equation can be written as $(2^2 3^2 d)^2 = (2 \cdot 3p^{n/3})^3 - 2^4 3^3$ which has no solutions by the tables in Appendix B. If $4 \mid n$ then by Theorem 1.2 of [7] there are no solutions. Therefore, $n = 1, 2$.

5) Considering the equations modulo 4 implies $m \in \{0, 1\}$. Suppose $m = 0$ then Theorem 1.1 of [5] implies $P_{\max}(n) \leq 3$, and considering the equation modulo 3 implies n odd. Thus, $n = 1$ or $3 \mid n$. If $3 \mid n$ then the equation can be written as $(9d)^2 = (3p^{n/3})^3 + 27$, and since $y^2 = x^3 + 27$ is a rank 0 elliptic curve with only one nontrivial point $(x, y) = (-3, 0)$, the equation has no solutions of the desired form. Therefore $n = 1$. As for the case $m = 1$, Theorem 1.2 of [5] implies $P_{\max}(n) \in \{2, 3, 5\}$. If $5 \mid n$ then the equation can be written as $(2^4 3^3 d)^2 = (2^2 3 p^{n/5})^5 + 2^8 3^5$ which has no solutions by Theorem 5.1. If $3 \mid n$ then the equation can be written as $(2^2 3^2 d)^2 = (2 \cdot 3p^{n/3})^3 - 2^4 3^3$ which has no solutions by the tables in Appendix B. If $4 \mid n$ then there are no solutions since the equation $3d^2 = 2x^4 + 1$ has only the trivial solution $d = x = 1$ (see [47]).

This completes the proof of the lemma.

□

Chapter 5
Rational points on $y^2 = x^5 \pm 2^\alpha 3^\beta$

In this chapter we are concerned with finding all the rational points on the genus 2 hyperelliptic curves $y^2 = x^5 \pm 2^\alpha 3^\beta$ where α and β are integers. The results obtained here were used in the proofs of the Diophantine lemmata of Chapter 4.

5.1 Introduction and Statement of Results

A celebrated theorem of Faltings states that a curve $\mathcal{C}$ of genus ≥ 2 has only finitely many rational points: $\#\mathcal{C}(K) < \infty$ for K a number field. For fixed α and β the curve $C : y^2 = x^5 \pm 2^\alpha 3^\beta$ is of genus 2 and so has finitely many rational points. We wish to determine all such points, i.e. $C(\mathbb{Q})$. It suffices to only consider the cases $0 \leq \alpha, \beta \leq 9$ since two curves $y^2 = x^5 + A$ and $y^2 = x^5 + B$ are $\mathbb{Q}$-isomorphic if A/B is a tenth power. Unfortunately, there is one curve we cannot say anything about, namely $y^2 = x^5 - 2^3 3^9$. We believe there are no (finite) rational points on this curve but are unable to prove this at this time. Of course, it can be shown that there are no integral points on it (see [71]). Keeping this curve aside for the time being we will prove the following theorem.

Theorem 5.1 *Let α and β be integers such that $0 \leq \alpha, \beta \leq 9$, and $\epsilon \in \{\pm 1\}$. Suppose $(\alpha, \beta, \epsilon) \neq (3, 9, -1)$. If $C : y^2 = x^5 + \epsilon 2^\alpha 3^\beta$ contains a (finite) rational point (x, y) then $\alpha, \beta, \epsilon, x, y$ are one of those listed in Table 5.1.*

C				C			
α	β	ϵ	$C(\mathbb{Q}) \setminus \{\infty\}$	α	β	ϵ	$C(\mathbb{Q}) \setminus \{\infty\}$
0	0	1	$(-1,0),(0,\pm1)$	6	6	1	$(0,\pm216)$
0	1	1	$(1,\pm2)$	6	8	1	$(0,\pm648)$
0	2	1	$(0,\pm3)$	8	0	1	$(0,\pm16)$
0	4	1	$(0,\pm9),(-2,\pm7),(3,\pm18))$	8	2	1	$(0,\pm48)$
0	5	1	$(-3,0)$	8	4	1	$(0,\pm144)$
0	6	1	$(0,\pm27)$	8	6	1	$(0,\pm432)$
0	8	1	$(0,\pm81),(18,\pm1377)$	8	8	1	$(0,\pm1296)$
1	0	1	$(-1,\pm1)$	0	0	-1	$(1,0)$
1	5	1	$(3,\pm27)$	0	5	-1	$(3,0)$
1	8	1	$(7,\pm173)$	1	2	-1	$(3,\pm15)$
2	0	1	$(0,\pm2),(2,\pm6)$	1	4	-1	$(3,\pm9)$
2	2	1	$(0,\pm6),(-2,\pm2)$	3	8	-1	$(9,\pm81)$
2	4	1	$(0,\pm18),(-3,\pm9),(6,\pm90)$	4	0	-1	$(2,\pm4)$
2	5	1	$(-3,\pm27)$	4	2	-1	$(10,\pm316)$
2	6	1	$(0,\pm54)$	5	0	-1	$(2,0),(6,\pm88)$
2	8	1	$(0,\pm162)$	5	4	-1	$(6,\pm72)$
3	0	1	$(1,\pm3)$	5	5	-1	$(6,0)$
3	1	1	$(1,\pm5)$	5	6	-1	$(9,\pm189)$
4	0	1	$(0,\pm4)$	5	8	-1	$(18,\pm1296)$
4	1	1	$(1,\pm7),(-2,\pm4)$	7	4	-1	$(33,\pm6255)$
4	2	1	$(0,\pm12)$	8	1	-1	$(4,\pm16)$
4	3	1	$(-2,\pm20)$	8	5	-1	$(12,\pm432)$
4	4	1	$(0,\pm36)$				
4	5	1	$(6,\pm108),(-2,\pm4)$				
4	6	1	$(0,\pm108)$				
4	8	1	$(1,\pm324),(9,\pm405)$				
5	0	1	$(-2,0),(2,\pm8)$				
5	1	1	$(-2,\pm8)$				
5	2	1	$(1,\pm17),(-2,\pm16)$				
5	5	1	$(-6,0),(-2,\pm88)$				
6	0	1	$(0,\pm8)$				
6	2	1	$(0,\pm24),(4,\pm40)$				
6	4	1	$(0,\pm72),(12,\pm504)$				

Table 5.1: Theorem 5.1: All points on $C : y^2 = x^5 \pm 2^\alpha 3^\beta$

5.2 Basic Theory of Jacobians of Curves

In this section we outline the basic theory of Jacobians of curves with a focus on computing in the Jacobian using MAGMA. The reader we have in mind is one who is familiar with the theory of, and computing with, elliptic curves and wants to start computing in Jacobians. We end this section with a discussion of Chabauty's technique for bounding the rational points on genus 2 curves and using its implementation in MAGMA. The reader already familiar with this material can skip directly to Section 5.3.

By a *hyperelliptic* curve we shall mean a curve $\mathcal{C}$ (with a model) of the form $y^2 = f(x)$, where $f(x)$ is a polynomial of degree $2g+1$, with distinct roots, and with coefficients in a field k of characteristic $\neq 2$. Here g is a positive integer, the *genus* of the curve $\mathcal{C}$. We will mostly be interested in the case of genus 2 curves over number fields k (especially $k = \mathbb{Q}$), however in stating the basic theory we won't restrict ourselves to genus 2 just yet.

When studying hyperelliptic curves one is chiefly concerned with determining the set of k-rational points on $\mathcal{C}$, denoted by $\mathcal{C}(k)$. This is the set of points (x, y) on $\mathcal{C}$ with $x, y \in k$. A celebrated theorem of Faltings says that if $g \geq 2$ and k is a number field, then this set is finite. Thus, one can hope to write down the set $\mathcal{C}(k)$ explicitly.

Faltings theorem clearly does not hold for genus 1 curves (elliptic curves). For example, it is well known that the elliptic curve $E : y^2 = x^3 + x + 1$ has infinitely many $\mathbb{Q}$-rational points. Some examples of rational points on E are:

$$(0, \pm 1), (1/4, \pm 9/8), (72, \pm 611), (-287/1296, \pm 40879/46656),$$

$$(43992/82369, \pm 30699397/23639903).$$

In the elliptic curve case the rational points on $\mathcal{C}$ form a finitely generated abelian group, so one is interested in determining the group structure of $\mathcal{C}(k)$, called the *Mordell-Weil group*. In our example above, $E(\mathbb{Q}) \simeq \mathbb{Z}$, with generator $P = (0, 1)$, and the points listed above are P, $2P$, $3P$, $4P$ and $5P$.

For curves $\mathcal{C}$ of genus ≥ 2 the set $\mathcal{C}(k)$ does not form a group. However, $\mathcal{C}(k)$ can be embedded into a finitely generated abelian group $J(k)$ called the *Jacobian* of $\mathcal{C}/k$ (also called the Mordell-Weil group of $\mathcal{C}$). We will briefly sketch how the Jacobian is constructed from $\mathcal{C}$ and state some of the basic facts that we will use.

5.2.1 Basic Setup

Let $\overline{k}$ be the algebraic closure of k. By a point on $\mathcal{C}$ we mean a pair (x, y) of elements in $\overline{k}$ satisfying $y^2 = f(x)$ or one other element; the point at infinity, denoted ∞. Let $\mathcal{C}(\overline{k})$ denote the set of all points on $\mathcal{C}$. We can define an action of $\mathrm{Aut}(\overline{k}/k)$ on $\mathcal{C}(\overline{k})$ as follows: if $\sigma \in \mathrm{Aut}(\overline{k}/k)$ and $P \in \mathcal{C}(\overline{k})$ then $P^\sigma = (x^\sigma, y^\sigma)$. The set of k-rational points on $\mathcal{C}$ can be defined as

$$\mathcal{C}(k) = \{P \in \mathcal{C}(\overline{k}) : P^\sigma = P \text{ for all } \sigma \in \mathrm{Aut}(\overline{k}/k)\}.$$

5.2.2 Divisors

The *divisor group* of $\mathcal{C}$ is the free abelian group generated by the points of $\mathcal{C}$. Thus a *divisor* D of $\mathcal{C}$ is a finite formal sum of the form

$$D = \sum_{P \in \mathcal{C}(\overline{k})} m_P(P),$$

where the m_P are integers (only finitely many of which are non-zero). The *degree* of D is $\deg(D) = \sum_P m_P$. If $m_P \geq 0$ for all P then we write $D \geq 0$ and call D an *effective* divisor. The *divisors of degree* 0 form a subgroup of $\mathrm{Div}(\mathcal{C})$ which we denote by

$$\mathrm{Div}^0(\mathcal{C}) = \{D \in \mathrm{Div}(\mathcal{C}) : \deg(D) = 0\}.$$

We can define an action of $\mathrm{Aut}(\overline{k}/k)$ on $\mathrm{Div}(\mathcal{C})$ in the obvious way

$$D^\sigma = \sum_P m_P(P^\sigma).$$

We say that D is defined over k if $D^\sigma = D$ for all $\sigma \in \mathrm{Aut}(\overline{k}/k)$. Note that if $D = \sum_P m_P(P)$ then to say D is defined over k does not mean all $P \in \mathcal{C}(k)$, it just means that $\mathrm{Aut}(\overline{k}/k)$ permutes the P in the appropriate way. The *group of divisors defined over* k is denoted by $\mathrm{Div}_k(\mathcal{C})$ and similarly for $\mathrm{Div}_k^0(\mathcal{C})$.

5.2.3 Principal Divisors and Jacobian

The (affine) *coordinate ring* $k[\mathcal{C}]$ of $\mathcal{C}$ is defined to be the quotient ring

$$k[\mathcal{C}] = k[x, y]/\langle y^2 - f(x)\rangle,$$

which is an integral domain. The field of fractions $k(\mathcal{C})$ is called the *function field* of $\mathcal{C}$. We can think of the function field as the set of all rational functions $p(x,y)/q(x,y)$, with q not divisible by $y^2 - f(x)$, where we identify two such functions if they agree at all points on $\mathcal{C}$. Over $\overline{k}$ we can similarly define $\overline{k}[\mathcal{C}]$ and $\overline{k}(\mathcal{C})$. If $P = (u,v)$ is a point on $\mathcal{C}$ then the *local ring* of $\mathcal{C}$ at P is subring of $\overline{k}(\mathcal{C})$ consisting of functions defined at P;

$$\overline{k}[\mathcal{C}]_P = \{F \in \overline{k}(\mathcal{C}) : F = g/h \text{ for some } g, h \in \overline{k}[\mathcal{C}] \text{ with } h(P) \neq 0\}.$$

This is a discrete valuation ring with (normalized) valuation denoted by ord_P, maximal ideal denoted M_P generated by t_P, a uniformizer (see, [69] chapter 2). We extend ord_P to $\overline{k}(\mathcal{C})$ by $\mathrm{ord}_P(g/h) = \mathrm{ord}_P(g) - \mathrm{ord}_P(h)$. The point of all this is that for $g \in \overline{k}(\mathcal{C})$ we can write

$$g = t_P^{\mathrm{ord}_P(g)} h,$$

for some $h \in \overline{k}(\mathcal{C})$ such that $h(P) \neq 0$, and this can be done at each point P on $\mathcal{C}$. The *order* of g at P is $\mathrm{ord}_P(g)$ and if $\mathrm{ord}_P(g) > 0$ then g has a zero at P; if $\mathrm{ord}_P(g) < 0$ then g has a pole at P. For the hyperelliptic curve $\mathcal{C}$ the uniformizer can be explicitly determined, it depends on the point $P = (u,v)$ as follows

$$t_P = \begin{cases} x - u & \text{if } v \neq 0 \\ y & \text{if } v = 0 \end{cases}$$

(see, for example [67]).

A function $g \in \overline{k}(\mathcal{C})$ has only a finite number of zeros and poles (see, for example [67]) so we can associate to g a divisor

$$\mathrm{div}(g) = \sum_{P \in \mathcal{C}(\overline{k})} \mathrm{ord}_P(g)(P).$$

A divisor of this form is called *principal* and the set of all principal divisors is denoted

$$\mathrm{Prin}(\mathcal{C}) = \{\mathrm{div}(g) : g \in \overline{k}(\mathcal{C})\}.$$

This is a subgroup of $\mathrm{Div}(\mathcal{C})$, since $\mathrm{div}(f) + \mathrm{div}(g) = \mathrm{div}(fg)$. In fact it is a subgroup of $\mathrm{Div}^0(\mathcal{C})$. We define the *Jacobian* of $\mathcal{C}$ to be the quotient

$$J(\mathcal{C}) = \mathrm{Div}^0(\mathcal{C})/\mathrm{Prin}(\mathcal{C}).$$

This is clearly an abelian group. This is going to be the main object we are concerned with. We will see in a little bit that there is a more natural way to view this object when $\mathcal{C}$ has genus 2. If D_1 and D_2 are degree 0 divisors then we write $D_1 \sim D_2$, and say D_1 and D_2 are *linearly equivalent*, if $D_1 - D_2 \in \mathrm{Prin}(\mathcal{C})$. For $D \in \mathrm{Div}^0(\mathcal{C})$ we write $[D]_\sim$ (or just [D]) for the element of $J(\mathcal{C})$ represented by D.

We can extend the action of $\mathrm{Aut}(\overline{k}/k)$ to $J(\mathcal{C})$ in the natural way. Then $J_k(\mathcal{C})$ is defined to be subgroup of $J(\mathcal{C})$ fixed by $\mathrm{Aut}(\overline{k}/k)$. When it is clear as to what curve we are referring, we shall denote $J(\mathcal{C})$ and $J_k(\mathcal{C})$ by $J(\overline{k})$ and $J(k)$, respectively.

5.2.4 Geometric representation of the Jacobian

In the case when $\mathcal{C}$ is an elliptic curve, say E, it is well known that there is a bijection between $E(\overline{k})$ and $J(\overline{k})$. To be more specific, the Riemann-Roch theorem tells us that every element of $J(\overline{k})$ has a unique representative of the form $(P) - (\infty)$, so the bijection $E(k) \longrightarrow J(\overline{k})$ is given by $P \mapsto [(P) - (\infty)]$. In this case, the points on $E(k)$ form a finitely generated abelian group (with identity ∞), and the group operation turns out to have a geometric description; $P + Q + R = \infty$ iff P, Q, and R are co-linear (with tangency requirements if the points aren't all distinct). This is sometimes stated as "an elliptic curve is its own Jacobian".

Let $\mathcal{C}$ be a hyperelliptic curve of genus g. If $P = (x_0, y_0)$ is a point on the curve then so is $P' = (x_0, -y_0)$. The points P and P' are zeros of the function $x - x_0$, which has a double pole at ∞. Thus the divisor $(P) + (P') - 2(\infty)$ is principal, that is $-(P') \sim (P) - 2(\infty)$. It follows that each element of $J(\overline{k})$ can be represented in the form

$$D = \sum_{i=1}^{r} (P_i) - r(\infty)$$

with the following condition satisfied: if the point $P_i = (x_i, y_i)$ appears in D, then the point $P_i' = (x_i, -y_i)$ does not appear as one of the P_j for $j \neq i$. This implies, in particular, that the points of the form $(x, 0)$ appear at most once in D. It follows from Riemann-Roch that each element of $J(\overline{k})$ can be represented uniquely by such a divisor with the additional condition that $r \leq g$. Such divisors are called *reduced*.

Now let's restrict out attention to the case when $\mathcal{C}$ has genus 2. In this case we then have that every element of $J(\overline{k})$ has a unique (reduced) representative of the form

$$D = (P) + (Q) - 2(\infty),$$

where $Q \neq P'$ (note $P = \infty$ or $Q = \infty$ is allowed). We denote the class of such a divisor as $\{P, Q\}$. Thus

$$J(\overline{k}) = \{\ \{P, Q\} : P, Q \in \mathcal{C}(\overline{k}), Q \neq P'\}. \tag{5.1}$$

The group operation on $J(\overline{k})$ can be described geometrically, much in the same way as for elliptic curves. The identity is $\mathcal{O} = \{\infty, \infty\}$ and

$$-\{P, Q\} = \{P', Q'\}. \tag{5.2}$$

Let $\{P_1, Q_1\}$ and $\{P_2, Q_2\}$ be two points in $J(\overline{k})$. There is a unique $M(x) \in \overline{k}[x]$ of degree 3 such that $y = M(x)$ passes through the four points P_1, Q_1, P_2, Q_2. This curve intersects $\mathcal{C}$ at another 2 points P_3 and Q_3 and so

$$\{P_1, Q_1\} + \{P_2, Q_2\} + \{P_3, Q_3\} = \mathcal{O}.$$

In other words

$$\{P_1, Q_1\} + \{P_2, Q_2\} = \{P_3', Q_3'\}. \tag{5.3}$$

5.2.5 2-torsion in the Jacobian

From the identity 5.2 it follows that the elements of the form $\{(\theta_1, 0), (\theta_2, 0)\}$, where θ_1 and θ_2 are distinct roots of $f(x)$, are of order 2 in $J(\overline{k})$. Also, elements of the form $\{(\theta, 0), \infty\}$, where θ is a root of $f(x)$, are of order 2. These are precisely all the 2-torsion elements. Thus, there are $\binom{6}{2} = 15$ elements of order 2 in $J(\overline{k})$.

5.2.6 Rational Points

The group $\mathrm{Aut}(\overline{k}/k)$ acts on $J(\overline{k})$ as follows

$$\{P, Q\}^\sigma = \{P^\sigma, Q^\sigma\}.$$

The set of *rational points* on the Jacobian is the set $J(k)$; the subset of $J(\overline{k})$ fixed under the action of $\mathrm{Aut}(\overline{k}/k)$ on $J(\overline{k})$. That is,

$$J(k) = \{\{P, Q\} \in J(\overline{k}) : (P^\sigma, Q^\sigma) = (P, Q) \text{ or } (Q, P) \text{ for all } \sigma \in \mathrm{Aut}(\overline{k}/k)\}.$$

It follows that an element $\{P, Q\} \in J(\overline{k})$ is rational if either

(i) $P, Q \in \mathcal{C}(k)$, or

(ii) P and Q are defined over a quadratic extension $k(\sqrt{d})$ of k and conjugate over $k(\sqrt{d})$,

As an example consider the curve $\mathcal{C} : y^2 = x^5 + 1$ over the base field $k = \mathbb{Q}$. Some points in $\mathcal{C}(\mathbb{Q})$ are $\infty, (0, \pm 1), (-1, 0)$, and so we have the following eight elements in $J(\mathbb{Q})$

$$\mathcal{O}, \{\infty, (0,1)\}, \{\infty, (0,-1)\}, \{\infty, (-1,0)\}, \{(0,1), (-1,0)\}$$
$$\{(0,-1), (-1,0)\}, \{(0,1), (0,1)\}, \{(0,-1), (0,-1)\}.$$

The element $\{\infty, (-1, 0)\}$ is the only element of order 2 in $J(\mathbb{Q})$, since $x = -1$ is the only rational root of $x^5 + 1$. Using (5.3) we can compute

$$\{\infty, (0,1)\} + \{\infty, (-1,0)\} = \{\infty, \infty\} + \{(0,1), (-1,0)\} = \{(0,1), (-1,0)\}.$$

Over the quadratic field $\mathbb{Q}(i)$ (where $i = \sqrt{-1}$) we have

$$(1 + i, \pm(-1 + 2i)), (1 - i, \pm(1 + 2i)) \in \mathcal{C}(\mathbb{Q}(i))$$

which gives two more points in $J(\mathbb{Q})$:

$$\{(1 + i, -1 + 2i), (1 - i, -1 - 2i)\}, \{(1 + i, 1 - 2i), (1 - i, 1 + 2i)\}.$$

Notice that, for example, $\{(1 + i, 1 - 2i), (0, 1)\}$ is in $J(\overline{\mathbb{Q}})$ but not $J(\mathbb{Q})$, since $(1 + i, 1 - 2i)$ and $(0, 1)$ are not quadratic conjugates over $\mathbb{Q}$.

5.2.7 Structure of the Jacobian: The Mordell-Weil theorem

By construction (as a quotient of a free abelian group) the Jacobian is an abelian group. In fact, the Mordell-Weil theorem states that $J(k)$ is finitely generated in the case when k is a number field. Thus, we can write it as

$$J(k) \simeq J(k)_{tors} \times \mathbb{Z}^r$$

where $J(k)_{tors}$ is the torsion subgroup of $J(k)$ (which is finite) and r is the *rank* of $J(k)$. Computing the torsion subgroup $J(k)_{tors}$ is a computationally straightforward task. $J(k)_{tors}$ embeds into $J(\mathbb{F}_p)$ for each prime p for which $\mathcal{C}$ has good reduction (p does not divide the discriminant of f). The finite groups $J(\mathbb{F}_p)$ are easy to compute and so piecing together the information at different primes we can usually, in practice, determine the structure of $J(k)_{tors}$. This procedure is not effective but does work quite well in many situations. There is a crude effective procedure involving the height function of $J(k)$ which can be used to compute $J(k)_{tors}$. For all the curves we will be considering, we will use MAGMA to compute the torsion subgroup.

There is no known effective procedure for computing the rank, however there are a number of heuristics for computing bounds on the rank. In practice one can usually bound the rank r by doing a 2-descent, and then find enough independent points in $J(k)$ which meets this bound, thus determining the rank. This will be the case in all the curves we consider (except for $y^2 = x^5 - 2^3 3^9$, where we obtain a rank bound of 1 but can't find a point on the Jacobian).

Coming back to the example we considered above, namely $y^2 = x^5 + 1$ over $\mathbb{Q}$, we found ten elements in $J(\mathbb{Q})$. It can be determined that a rank bound for $J(\mathbb{Q})$ is zero and that the torsion subgroup has size 10, thus we have found $J(\mathbb{Q})$ completely. It follows that the only integral solutions to $y^2 = x^5 + 1$ are $(0, \pm 1)$ and $(-1, 0)$. Of course this is certainly well known; it is a special case of Catalan's theorem.

5.2.8 Computer Representations of Jacobians

Any element $\{(u_1, v_1), (u_2, v_2)\} \in J(\overline{k})$ can be represented uniquely by a pair of polynomials $(a(x), b(x)) \in \overline{k}[x]^2$, where $a(x) = (x - u_1)(x - u_2)$ and $y = b(x)$ is the unique line through (u_1, v_1) and (u_2, v_2) (take $y = b(x)$ to be the tangent line to $\mathcal{C}$ if $(u_1, v_1) = (u_2, v_2)$). This is equivalent to requiring $f(x) - b(x)^2$ be divisible by $a(x)$. In the case when the point of $J(\overline{k})$ is of the form $\{\infty, (u, v)\}$ then $a(x) = x - u$ and $b(x) = v$. The identity $\mathcal{O} = \{\infty, \infty\}$ gets represented as $(1, 0)$. If we let $\overline{k}_d[x]$ denote the set of polynomials of degree at most d then we have a injection

$$\phi : J(\overline{k}) \longrightarrow \overline{k}_2[x] \times \overline{k}_1[x],$$

where the image is the set of all (a, b) such that a is monic and $a \mid f - b^2$.

An algorithm for adding two elements in $J(\overline{k})$ by adding their corresponding images (a_1, b_1), (a_2, b_2) in $\overline{k}_2[x] \times \overline{k}_1[x]$ has been given by Cantor [14].

The rational points $J(k)$ on $J(\overline{k})$ correspond to polynomials with rational coefficients (over k), that is, ϕ restricts to

$$\phi : J(k) \hookrightarrow k_2[x] \times k_1[x],$$

5.2.9 Some Examples (Using MAGMA)

Let's come back to our example $y^2 = x^5 + 1$ (where $k = \mathbb{Q}$). The elements in $J(\mathbb{Q})$ and their corresponding representations are as follows.

$$\begin{aligned}
\mathcal{O} = \{\infty, \infty\} &\longmapsto (1, 0) \\
\{\infty, (0, 1)\} &\longmapsto (x, 1) \\
\{\infty, (0, -1)\} &\longmapsto (x, -1) \\
\{\infty, (-1, 0)\} &\longmapsto (x + 1, 0) \\
\{(0, 1), (-1, 0)\} &\longmapsto (x^2 + x, x + 1) \\
\{(0, -1), (-1, 0)\} &\longmapsto (x^2 + x, -x - 1) \\
\{(0, 1), (0, 1)\} &\longmapsto (x^2, 1) \\
\{(0, -1), (0, -1)\} &\longmapsto (x^2, -1) \\
\{(1 + i, -1 + 2i), (1 - i, -1 - 2i)\} &\longmapsto (x^2 - 2x + 2, 2x - 3) \\
\{(1 + i, 1 - 2i), (1 - i, 1 + 2i)\} &\longmapsto (x^2 - 2x + 2, -2x + 3).
\end{aligned}$$

As another example consider the curve $y^2 = x^5 + 2^2 3^4$ over $\mathbb{Q}$. Some points

on $J(\mathbb{Q})$ and their corresponding representations are as follows.

$$\begin{aligned}
\{\infty, (0,18)\} &\longmapsto (x, 18)\\
\{\infty, (-3,9)\} &\longmapsto (x+3, 9)\\
\{\infty, (6,90)\} &\longmapsto (x-6, 90)\\
\{(0,18), (0,18)\} &\longmapsto (x^2, 18)\\
\{(-3,9), (-3,9)\} &\longmapsto (x^2+6x+9, 45/2x+153/2)\\
\{(0,18), (6,-90)\} &\longmapsto (x^2-6x, -18x+18)\\
\{(-1+\sqrt{11}i, 2+4\sqrt{11}i), &(-1-\sqrt{11}i, 2-4\sqrt{11}i)\}\\
&\longmapsto (x^2+2x+12, 4x+6).
\end{aligned}$$

We now show how MAGMA can be used to find the structure of $J(\mathbb{Q})$.

```
> _<x>:=PolynomialRing(Rationals());
> C:=HyperellipticCurve(x^5+2^2*3^4); J:=Jacobian(C);
> T,mapTtoJ:=TorsionSubgroup(J);
> T;
> {mapTtoJ(t):t in T};

Abelian Group isomorphic to Z/5
Defined on 1 generator
Relations:
 5*P[1] = 0
{ (x,18,1), (x^2,-18,2), (x^2,18,2), (x,-18,1), (1,0,0) ]
```

This tells us that $J(\mathbb{Q})_{tors} \simeq \mathbb{Z}/5$ and is generated by $(x, 18)$, i.e. the element $\{\infty, (0,18)\}$. All of $J(\mathbb{Q})_{tors}$ is also listed (elements in MAGMA are listed as triples $(a(x), b(x), \deg a)$). All that remains is to determine the rank r of $J(\mathbb{Q})$ and (if possible) the r free generators. We can use a 2-descent to compute an upper bound $\hat{r}$ on the rank, then search for independent points in $J(\mathbb{Q})$ and hope we get $\hat{r}$ of them, thus verifying $\hat{r}$ is the rank of $J(\mathbb{Q})$.

```
> r:=TwoSelmerGroupDatat(J);r;
> R:=RationalPoints(J:Bound:=1000);
> B:=ReducedBasis(R); B;
```

```
1
[ (x^2 - 6*x, -18*x + 18, 2) ]
```

We get an upper bound of 1 on the rank and we found a torsion-free element, thus $J(\mathbb{Q})$ has rank 1. Therefore

$$J(\mathbb{Q}) \simeq \mathbb{Z}/5 \times \mathbb{Z}.$$

Note, we can't conclude that $\mathcal{A} = (x^2 - 6x, -18x + 18)$ generates the free part, it could be a multiple of the generator. Let's suppose the generator of the free part is $\mathcal{G}$ and that $\mathcal{A} = n\mathcal{G}$ for some integer n. Then taking (canonical) heights we get $\hat{h}(\mathcal{A}) = n^2\hat{h}(\mathcal{G})$. If $\mathcal{A}$ is not a generator then $n \geq 2$ and so

$$\hat{h}(\mathcal{G}) < \frac{1}{4}\hat{h}(\mathcal{A}).$$

So we just need to search for points on $J(\mathbb{Q})$ up to canonical height $\frac{1}{4}\hat{h}(\mathcal{A})$ to find the generator. In MAGMA we can search for points by naive height h. Letting HC be the height constant of $J(\mathbb{Q})$, i.e. the maximum difference between the canonical and naive height, we have to search up to the bound

$$\exp\left(\frac{\hat{h}(\mathcal{A})}{4} + HC\right)$$

to find a generator.

```
> HC:=HeightConstant(J:Effort:=2);HC;
> A:=J![x^2 - 6*x, -18*x + 18];
> hA:=Height(A);hA;
> newbound:=Exp(hA/4+HC);newbound;
> R:=RationalPoints(J:Bound:=newbound);B:=ReducedBasis(R);B;

0.33387781394988171248019038929 1
7.08937355470437938278274010122
1303.54532976380801714115763662
[ (x^2 - 6*x, -18*x + 18, 2) ]
```

Therefore $\mathcal{A}$ is indeed a generator of the free part of $J(\mathbb{Q})$. Thus

$$J(\mathbb{Q}) = \langle (x, 18) \rangle \times \langle (x^2 - 6x, -18x + 18) \rangle \simeq \mathbb{Z}/5 \times \mathbb{Z}.$$

Other possible choices for the free generator are $\mathcal{A} + n\mathcal{P}$, where $\mathcal{P} = (x, 18)$ and n any integer, these can be listed as follows.

```
> [ n*P + A : n in {1..4} ];

[ (x^2-3*x-18, 9*x+36, 2), (x^2+2*x+12, -4*x-6, 2),
(x^2-6*x, -12*x-18, 2), (x-6, -90, 1) ]
```

5.2.10 Chabauty's theorem

Theorem 5.2 (Chabauty [16]) *Let C be a curve defined over genus $g > 1$ defined over a number field k. If the Jacobian of C has rank less than g, then $C(k)$ is finite.*

This result is superceded by Falting's work which gives the same conclusion without a condition on the rank. However, the methods of Chabauty can be used, in some situations, to give a sharp upper bound on the cardinality of $C(k)$, hence allowing us to determine the set $C(k)$.

In our situation, C is a genus 2 curve of rank 1 and we are interested in the set of rational points $C(\mathbb{Q})$. Consider $C(\mathbb{Q})$ as contained in $J(\mathbb{Q})$ via the embedding

$$P \mapsto \{P, \infty\}.$$

Suppose we have already found the torsion and free-generator of $J(\mathbb{Q})$:

$$J(\mathbb{Q}) = J(\mathbb{Q})_{tors} \times \langle \mathcal{D} \rangle.$$

The basic idea is to pick an odd prime p for which C has good reduction; i.e. $\widetilde{C} = C \pmod p$ is a curve of genus 2 over $\mathbb{F}_p$. Let $\widetilde{\mathcal{D}}$ be the reduction of $\mathcal{D}$ mod p, and let m be the order of $\widetilde{\mathcal{D}}$ in $J(\mathbb{F}_p)$. Then the divisor $\mathcal{F} = m\mathcal{D}$ is in the kernel of reduction. Anything in $J(\mathbb{Q})$ can be written uniquely in the form

$$\mathcal{U} + n \cdot \mathcal{F}, \;\; n \in \mathbb{Z},$$

where $\mathcal{U}$ is an element in the finite set

$$\{\mathcal{B} + i \cdot \mathcal{D} : \mathcal{B} \in J(\mathbb{Q})_{tors} \text{ and } 1 \leq i \leq m-1\}.$$

Fix $\mathcal{U}$ as a member of this set. The question is for how many integers n can $\mathcal{U} + n \cdot \mathcal{F}$ be of the form $\{P, \infty\}$? It turns out that this only happens if n is a root of a power series over $\mathbb{Z}_p$ (the power series will depend on $\mathcal{U}$). A theorem of Strassman can be used to bound the number of p-adic roots to this power series and hence one can find an upper bound $\ell(\mathcal{U})$ on the number of

integers n for which $\mathcal{U} + n \cdot \mathcal{F}$ is of the form $\{P, \infty\}$. Summing these bounds $\ell(\mathcal{U})$ over the finitely many $\mathcal{U}$ we get a bound on the number of possible elements of the form $\{P, \infty\}$, hence a bound on the cardinality of $C(\mathbb{Q})$. If this bound matches the number of known points we have found on the curve then we know we have found all the rational points. For a thorough account of Chabauty's method the reader is directed to [15] (or [25] for a similar procedure using differential forms) .

Let us consider the task of finding all the rational points on the curve $C_3 : y^2 = x^5 + 3$. First we input the curve into MAGMA and search for rational points.

```
> _<x>:=PolynomialRing(Rationals());
> C:=HyperellipticCurve(x^5+3);
> RationalPoints(C:Bound:=1000);

{@ (1 : 0 : 0), (1 : -2 : 1), (1 : 2 : 1) @}
```

One can check that increasing the search bound does not produce any more points. So we would like to show $C_3(\mathbb{Q}) = \{\infty, (1, 0), (1, \pm 2)\}$.

```
> J:=Jacobian(C);
> r:=TwoSelmerGroupData(J);r;
> T,mapTtoJ:=TorsionSubgroup(J);
> T;
> R:=RationalPoints(J:Bound:=1000);B:=ReducedBasis(R);B;


1
Abelian Group of order 1
[ (x - 1, 2, 1) ]
```

Thus $J(\mathbb{Q})$ has rank 1 and trivial torsion. Also, $(x - 1, 2)$ is a possible generator. By the procedure outlined in the previous section we can verify that $P = (x - 1, 2)$ is indeed a generator. With a generator in hand we can now apply Chabauty at a prime ≥ 7 to find an upper bound on the size of $C(\mathbb{Q})$. In fact, what Chabauty returns is a bound on half the number of non-Weierstrass points; Weierstrass points are the points $(x, 0)$ and the point at ∞, all of which

are easy to find. In this example the only Weierstrass point is ∞. Since we know two non-Weierstrass point on our curve, we are done if Chabauty returns the value 1. The function "Chabauty" actually returns an indexed set of tuples $< (x, z, v, k) >$ such that there are at most k pairs of rational points on C whose image in $\mathbb{P}^1$ under the x-coordinate map are congruent to $(x : z)$ modulo p^v, and such that the only rational points on C outside these congruences classes are Weierstrass points. We can just get a bound by using the prefix # on the command.

```
> P:=B[1];"\\
> #Chabauty(P,7)
> #Chabauty(P,11)
> #Chabauty(P,17)
> #Chabauty(P,19)


3
3
8
1
```

Thus, applying Chabauty's method at the prime 19 is enough to show that we have found all the rational points on C_3.

It is worth noting that Strassman's theorem bounds the number of p-adic roots, not just the integer roots, so it seems likely that the bound returned will be strictly greater than the number of rational points. This is what happened in the previous example for the primes 7, 11 and 17. For these primes the procedure could not decide whether the extra p-adic solutions were actually rational solutions. These p-adic points on the curve, which are not rational, are affectionately called "ghost" solutions; see [13].

As a second example let us consider the curve $C_{324} := y^2 = x^5 + 324$. (Note $324 = 2^2 3^4$.) This is the example we worked through in the previous section. We showed

$$J_{324}(\mathbb{Q}) \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}$$

with torsion generator $(x, 18)$ and free generator $(x^2 - 6x, -18x + 18)$. A simple search reveals the following points in $C_{324}(\mathbb{Q})$:

$$\{\infty, (0, \pm 18), (-3, \pm 9), (6, \pm 90)\}.$$

If we try to apply Chabauty's method we find that the smallest bound returned is 4, which occurs at the primes $7, 31, 139,$ and 191. This is not enough to conclude we have found all the points, but it does show there is at most one other pair of rational points on the curve. It may happen that trying larger primes will succeed in a bound of 3 but this simply becomes computational costly. So, how do we proceed? Well, we do have additional information given to us at the smaller primes, MAGMA returns p-adic information about these supposed "ghost" solutions, so it may be possible to piece information together at different primes to conclude no other rational point can exist. We refer to this as "multiple-prime" Chabauty and consider some examples in Section 5.5.

5.3 Data for the curves $y^2 = x^5 \pm 2^\alpha 3^\beta$

Let $A = \pm 2^\alpha 3^\beta$, $0 \leq \alpha, \beta \leq 9$, and C_A denote the curve $y^2 = x^5 + A$. For each value of A we can use MAGMA to compute the torsion group $J_A(\mathbb{Q})_{tors}$ and a rank bound $\overline{r_A}$ on the Mordell-Weil group $J_A(\mathbb{Q})$ of C_A (via a 2-descent). Furthermore, we use MAGMA to try to find $\overline{r_A}$ linearly independent points in $J_A(\mathbb{Q})$ thus concluding the rank is exactly $\overline{r_A}$. We have already successfully done this for $A = 2^2 3^4$ in Section 5.2.9 and moreover we found a generator for the free part of $J_A(\mathbb{Q})$.

For most of the two hundred curves we consider this works out quite well in determining $J_A(\mathbb{Q})$. However, in some cases MAGMA was unable to find a non-torsion point, simply because its height is just beyond the search range. In each case, Michael Stoll [73] was able to find such points for us.

In Tables 5.2 through 5.9 we list the results of the computations performed by MAGMA. Here $\overline{r}$ is the rank bound determined by MAGMA by doing a 2-descent (in the cases $A = -2 \cdot 3^3, -2^5 3^7$ we use the results of Stoll [72] to get a sharper bound, this is included in brackets). #LI is the number of linearly independent points found in $J_A(\mathbb{Q})$ by searching in MAGMA (and in some cases the data provided by Stoll [73]). $C_A(\mathbb{Q})_{\text{known}}$ is the set of known points on $C_A(\mathbb{Q})$ including the point at infinity ∞. For curves of rank 0, we have $C_A(\mathbb{Q}) = C_A(\mathbb{Q})_{known}$. For the curves of rank 1, we include in column p the first prime for which Chabauty returns a bound on $\#C_A(\mathbb{Q})$ which is equal to the number of known points in $C_A(\mathbb{Q})$. This verifies we have found $C_A(\mathbb{Q})$

exactly. In the case that two primes appears in column p, we were unable to find a single prime for which the Chabauty computation was successful in determining $C_A(\mathbb{Q})$. However, a multiple-prime Chabauty argument at the two primes works in these cases. This will be done in Section 5.5. Also, there we will discuss the curves of rank 2.

As shown in Tables 5.2 through 5.9 we have successfully determined the rank except in four cases:

$$A \in \{2^5 3^9, -3^9, -2^3 3^9, -2^4 3^6\}.$$

In the case $-2^3 3^9$ we have a rank bound of 1 but are unable to find a point in $J(\mathbb{Q})$. If a point does exist it can be shown (under Birch and Swinnerton-Dyer) to be just beyond the reach of computing at this time [73]. Thus, at this time we are unable to determine the rank. In the three other cases MAGMA has returned a rank bound of 2 but was unable to find any non-torsion points. We now show, in these cases, the rank is 0.

Let $A \in \{2^5 3^9, -3^9, -2^4 3^6\}$, and $C_A^{(d)}$ denote the twist $y^2 = d(x^5 + A)$ of C_A. Over $K = \mathbb{Q}(\sqrt{d})$ these two curves are isomorphic from which it follows

$$rkJ_A(K) = rkJ_A(\mathbb{Q}) + rkJ_A^{(d)}(\mathbb{Q}).$$

Taking $d = -3$ we get the following, where the curve $C_A^{(d)}$ is $\mathbb{Q}$-isomorphic to the one listed. The bounds for $rkJ_A(K)$ were computed in MAGMA by using a 2-descent, and the ranks $rkJ_A^{(d)}(\mathbb{Q})$ were computed above.

A	$C_A^{(d)}$	$rkJ_A(K)$	$rkJ_A^{(d)}(\mathbb{Q})$
$2^5 3^9$	$y^2 = x^5 - 2^5 3^4$	≤ 2	2
-3^9	$y^2 = x^5 + 3^4$	≤ 2	2
$-2^4 3^6$	$y^2 = x^5 + 2^4 3$	≤ 2	2

Thus $rkJ_A(\mathbb{Q}) = 0$ in each of these cases.

To summarize, in the case when that rank is ≤ 1 we have now shown (using classical Chabauty implemented in MAGMA) that $C(\mathbb{Q}) = C(\mathbb{Q})_{known}$ as listed in the tables except possibly in the cases[1]

$$A \in \{2^2 3^4, 2^5, 2^6 3^2, 2^6 3^3\}.$$

[1]And when $A = -2^3 3^9$ since we can't determine the exact rank in this case, as mentioned above.

$C:\ y^2 = x^5 + 2^\alpha 3^\beta$							
α	β	$\overline{r}$	#LI	rank	$J(\mathbb{Q})$	$C(\mathbb{Q})_{\text{known}} \setminus \infty$	p
0	0	0	0	0	$\mathbb{Z}/10$	$(-1,0),(0,\pm 1)$	
0	1	1	1	1	$\mathbb{Z}$	$(1,\pm 2)$	11
0	2	1	1	1	$\mathbb{Z}/5 \times \mathbb{Z}$	$(0,\pm 3)$	11
0	3	0	0	0	0		
0	4	2	2	2	$\mathbb{Z}/5 \times \mathbb{Z}^2$	$(0,\pm 9),(-2,\pm 7),(3,\pm 18)$	
0	5	1	1	1	$\mathbb{Z}/2 \times \mathbb{Z}$	$(-3,0)$	29
0	6	0	0	0	$\mathbb{Z}/5$	$(0,\pm 27)$	
0	7	0	0	0	0		
0	8	1	1	1	$\mathbb{Z}/5 \times \mathbb{Z}$	$(0,\pm 81),(18,\pm 1377)$	17
0	9	1	1	1	$\mathbb{Z}$		19
1	0	2	2	2	$\mathbb{Z}^2$	$(-1,\pm 1)$	
1	1	2	2	2	$\mathbb{Z}^2$		
1	2	0	0	0	0		
1	3	0	0	0	0		
1	4	1	1	1	$\mathbb{Z}$		19
1	5	1	1	1	$\mathbb{Z}$	$(3,\pm 27)$	19
1	6	0	0	0	0		
1	7	1	1	1	$\mathbb{Z}$		11
1	8	2	2	2	$\mathbb{Z}^2$	$(7,\pm 173)$	
1	9	1	1	1	$\mathbb{Z}$		31
2	0	1	1	1	$\mathbb{Z}/5 \times \mathbb{Z}$	$(0,\pm 2),(2,\pm 6)$	19
2	1	0	0	0	0		
2	2	1	1	1	$\mathbb{Z}/5 \times \mathbb{Z}$	$(0,\pm 6),(-2,\pm 2)$	61
2	3	1	1	1	$\mathbb{Z}$		19
2	4	1	1	1	$\mathbb{Z}/5 \times \mathbb{Z}$	$(0,\pm 18),(-3,\pm 9),(6,\pm 90)$	29, 59
2	5	1	1	1	$\mathbb{Z}$	$(-3,\pm 27)$	29

Table 5.2: Data for $y^2 = x^5 + 2^\alpha 3^\beta$

$C: y^2 = x^5 + 2^\alpha 3^\beta$							
α	β	$\overline{r}$	#LI	rank	$J(\mathbb{Q})$	$C(\mathbb{Q})_{\text{known}} \setminus \infty$	p
2	6	1	1	1	$\mathbb{Z}/5 \times \mathbb{Z}$	$(0, \pm 54)$	11
2	7	0	0	0	0		
2	8	0	0	0	$\mathbb{Z}/5$	$(0, \pm 162)$	
2	9	1	1	1	$\mathbb{Z}$		29
3	0	1	1	1	$\mathbb{Z}$	$(1, \pm 3)$	13
3	1	1	1	1	$\mathbb{Z}$	$(1, \pm 5)$	31
3	2	0	0	0	0		
3	3	1	1	1	$\mathbb{Z}$		11
3	4	1	1	1	$\mathbb{Z}$		11
3	5	0	0	0	0		
3	6	0	0	0	0		
3	7	0	0	0	0		
3	8	1	1	1	$\mathbb{Z}$		19
3	9	1	1	1	$\mathbb{Z}$		11
4	0	0	0	0	$\mathbb{Z}/5$	$(0, \pm 4)$	
4	1	2	2	2	$\mathbb{Z}^2$	$(1, \pm 7), (-2, \pm 4)$	
4	2	0	0	0	$\mathbb{Z}/5$	$(0, \pm 12)$	
4	3	1	1	1	$\mathbb{Z}$	$(-2, \pm 20)$	19
4	4	0	0	0	$\mathbb{Z}/5$	$(0, \pm 36)$	
4	5	2	2	2	$\mathbb{Z}^2$	$(6, \pm 108)$	
4	6	1	1	1	$\mathbb{Z}/5 \times \mathbb{Z}$	$(0, \pm 108)$	61
4	7	1	1	1	$\mathbb{Z}$		19
4	8	1	1	1	$\mathbb{Z}/5 \times \mathbb{Z}$	$(0, \pm 324), (9, \pm 405)$	47
4	9	1	1	1	$\mathbb{Z}$		17

Table 5.3: Data for $y^2 = x^5 + 2^\alpha 3^\beta$ (con't)

$C: y^2 = x^5 + 2^\alpha 3^\beta$							
α	β	$\overline{r}$	#LI	rank	$J(\mathbb{Q})$	$C(\mathbb{Q})_{\text{known}} \setminus \infty$	p
5	0	1	1	1	$\mathbb{Z}/2 \times \mathbb{Z}$	$(-2,0),(2,\pm 8)$	
5	1	2	2	2	$\mathbb{Z}^2$	$(-2,\pm 8)$	
5	2	3	3	3	$\mathbb{Z}^3$	$(1,\pm 17),(-2,\pm 16)$	
5	3	1	1	1	$\mathbb{Z}$		19
5	4	0	0	0	0		
5	5	1	1	1	$\mathbb{Z}/2 \times \mathbb{Z}$	$(-2,\pm 88),(-6,0)$	11
5	6	0	0	0	0		
5	7	1	1	1	$\mathbb{Z}$		
5	8	1	1	1	$\mathbb{Z}$		
5	9	2	0				
6	0	0	0	0	$\mathbb{Z}/5$	$(0,\pm 8)$	
6	1	1	1	1	$\mathbb{Z}$		19
6	2	1	1	1	$\mathbb{Z}/5 \times \mathbb{Z}$	$(0,\pm 24),(4,\pm 40)$	29,59
6	3	1	1	1	$\mathbb{Z}$		7,29
6	4	1	1	1	$\mathbb{Z}/5 \times \mathbb{Z}$	$(0,\pm 72),(12,\pm 504)$	7
6	5	0	0	0	0		
6	6	0	0	0	$\mathbb{Z}/5$	$(0,\pm 216)$	
6	7	1	1	1	$\mathbb{Z}$		17
6	8	0	0	0	$\mathbb{Z}/5$	$(0,\pm 648)$	
6	9	0	0	0	0		
7	0	1	1	1	$\mathbb{Z}$		11
7	1	1	1	1	$\mathbb{Z}$		11
7	2	1	1	1	$\mathbb{Z}$		31
7	3	0	0	0	0		
7	4	2	2	2	$\mathbb{Z}^2$		

Table 5.4: Data for $y^2 = x^5 + 2^\alpha 3^\beta$ (con't)

$C:\ y^2 = x^5 + 2^\alpha 3^\beta$							
α	β	$\overline{r}$	#LI	rank	$J(\mathbb{Q})$	$C(\mathbb{Q})_{\text{known}} \setminus \infty$	p
7	5	0	0	0	0		
7	6	1	1	1	$\mathbb{Z}$		19
7	7	1	1	1	$\mathbb{Z}$		19
7	8	0	0	0	0		
7	9	1	1	1	$\mathbb{Z}$		41
8	0	0	0	0	$\mathbb{Z}/5$	$(0, \pm 16)$	
8	1	1	1	1	$\mathbb{Z}$		29
8	2	1	1	1	$\mathbb{Z}/5 \times \mathbb{Z}$	$(0, \pm 48)$	29
8	3	0	0	0	0		
8	4	0	0	0	$\mathbb{Z}/5$	$(0, \pm 144)$	
8	5	1	1	1	$\mathbb{Z}$		11
8	6	0	0	0	$\mathbb{Z}/5$	$(0, \pm 432)$	
8	7	1	1	1	$\mathbb{Z}$		29
8	8	0	0	0	$\mathbb{Z}/5$	$(0, \pm 1296)$	
8	9	0	0	0	0		
9	0	0	0	0	0		
9	1	1	1	1	$\mathbb{Z}$		11
9	2	0	0	0	0		
9	3	1	1	1	$\mathbb{Z}$		59
9	4	0	0	0	0		
9	5	1	1	1	$\mathbb{Z}$		29
9	6	1	0	1	$\mathbb{Z}$		11
9	7	0	0	0	0		
9	8	0	0	0	0		
9	9	0	0	0	0		

Table 5.5: Data for $y^2 = x^5 + 2^\alpha 3^\beta$ (con't)

$C: y^2 = x^5 - 2^\alpha 3^\beta$							
α	β	$\overline{r}$	#LI	rank	$J(\mathbb{Q})$	$C(\mathbb{Q})_{\text{known}} \setminus \infty$	p
0	0	1	1	1	$\mathbb{Z}/2 \times \mathbb{Z}$	$(1, 0)$	11
0	1	0	0	0	0		
0	2	0	0	0	0		
0	3	1	1	1	$\mathbb{Z}$		17
0	4	1	1	1	$\mathbb{Z}$		11
0	5	0	0	0	$\mathbb{Z}/2$	$(3, 0)$	
0	6	1	1	1	$\mathbb{Z}$		19
0	7	1	1	1	$\mathbb{Z}$		17
0	8	0	0	0	0		
0	9	2	0				
1	0	0	0	0	0		
1	1	0	0	0	0		
1	2	2	2	2	$\mathbb{Z}^2$	$(3, \pm 15)$	
1	3	2 (0)	0	0	0		
1	4	1	1	1	$\mathbb{Z}$	$(3, \pm 9)$	13
1	5	1	1	1	$\mathbb{Z}$		11
1	6	2	2	2	$\mathbb{Z}^2$		
1	7	1	1	1	$\mathbb{Z}$		11
1	8	0	0	0	0		
1	9	1	1	1	$\mathbb{Z}$		7
2	0	0	0	0	0		
2	1	1	1	1	$\mathbb{Z}$		17
2	2	0	0	0	0		
2	3	0	0	0	0		
2	4	0	0	0	0		

Table 5.6: Data for $y^2 = x^5 - 2^\alpha 3^\beta$

$C: y^2 = x^5 - 2^\alpha 3^\beta$							
α	β	$\overline{r}$	#LI	rank	$J(\mathbb{Q})$	$C(\mathbb{Q})_{\text{known}} \setminus \infty$	p
2	5	0	0	0	0		
2	6	0	0	0	0		
2	7	1	1	1	$\mathbb{Z}$		17
2	8	1	1	1	$\mathbb{Z}$		41
2	9	0	0	0	0		
3	0	1	1	1	$\mathbb{Z}$		11
3	1	1	1	1	$\mathbb{Z}$		11
3	2	0	0	0	0		
3	3	1	1	1	$\mathbb{Z}$		11
3	4	1	1	1	$\mathbb{Z}$		19
3	5	0	0	0	0		
3	6	0	0	0	0		
3	7	0	0	0	0		
3	8	1	1	1	$\mathbb{Z}$	$(9, \pm 81)$	17
3	9	1	0				
4	0	1	1	1	$\mathbb{Z}$	$(2, \pm 4)$	29
4	1	1	1	1	$\mathbb{Z}$		11
4	2	1	1	1	$\mathbb{Z}$	$(10, \pm 316)$	11
4	3	0	0	0	0		
4	4	1	1	1	$\mathbb{Z}$		19
4	5	1	1	1	$\mathbb{Z}$		17
4	6	2	0				
4	7	0	0	0	0		
4	8	0	0	0	0		
4	9	0	0	0	0		

Table 5.7: Data for $y^2 = x^5 - 2^\alpha 3^\beta$ (con't)

$C: y^2 = x^5 - 2^\alpha 3^\beta$							
α	β	$\overline{r}$	#LI	rank	$J(\mathbb{Q})$	$C(\mathbb{Q})_{\text{known}} \setminus \infty$	p
5	0	1	1	1	$\mathbb{Z}/2 \times \mathbb{Z}$	$(2,0), (6, \pm 88)$	11
5	1	0	0	0	0		
5	2	1	1	1	$\mathbb{Z}$		19
5	3	1	1	1	$\mathbb{Z}$		11
5	4	2	2	2	$\mathbb{Z}^2$	$(6, \pm 72)$	
5	5	1	1	1	$\mathbb{Z}/2 \times \mathbb{Z}$	$(6, 0)$	11
5	6	2	2	2	$\mathbb{Z}^2$	$(9, \pm 189)$	
5	7	3 (1)	1	1	$\mathbb{Z}$		11
5	8	1	1	1	$\mathbb{Z}$	$(18, \pm 1296)$	11
5	9	0	0	0	0		
6	0	1	1	1	$\mathbb{Z}$		19
6	1	0	0	0	0		
6	2	0	0	0	0		
6	3	0	0	0	0		
6	4	0	0	0	0		
6	5	1	1	1	$\mathbb{Z}$		17
6	6	1	1	1	$\mathbb{Z}$		41
6	7	0	0	0	0		
6	8	1	1	1	$\mathbb{Z}$		41
6	9	1	1	1	$\mathbb{Z}$		17
7	0	1	1	1	$\mathbb{Z}$		11
7	1	1	1	1	$\mathbb{Z}$		11
7	2	1	1	1	$\mathbb{Z}$		11
7	3	0	0	0	0		
7	4	2	2	2	$\mathbb{Z}^2$	$(33, \pm 6255)$	

Table 5.8: Data for $y^2 = x^5 - 2^\alpha 3^\beta$ (con't)

$C: y^2 = x^5 - 2^\alpha 3^\beta$							
α	β	$\overline{r}$	#LI	rank	$J(\mathbb{Q})$	$C(\mathbb{Q})_{\text{known}} \setminus \infty$	p
7	5	0	0	0	0		
7	6	1	1	1	$\mathbb{Z}$		29
7	7	1	1	1	$\mathbb{Z}$		11
7	8	0	0	0	0		
7	9	1	1	1	$\mathbb{Z}$		11
8	0	0	0	0	0		
8	1	1	1	1	$\mathbb{Z}$	$(4, \pm 16)$	19
8	2	1	1	1	$\mathbb{Z}$		61
8	3	0	0	0	0		
8	4	0	0	0	0		
8	5	1	1	1	$\mathbb{Z}$	$(12, \pm 432)$	29
8	6	0	0	0	0		
8	7	1	1	1	$\mathbb{Z}$		29
8	8	0	0	0	0		
8	9	0	0	0	0		
9	0	0	0	0	0		
9	1	1	1	1	$\mathbb{Z}$		11
9	2	0	0	0	0		
9	3	1	1	1	$\mathbb{Z}$		11
9	4	0	0	0	0		
9	5	1	1	1	$\mathbb{Z}$		11
9	6	1	1	1	$\mathbb{Z}$		29
9	7	0	0	0	0		
9	8	0	0	0	0		
9	9	0	0	0	0		

Table 5.9: Data for $y^2 = x^5 - 2^\alpha 3^\beta$ (con't)

In fact, we will show that $C(\mathbb{Q}) = C(\mathbb{Q})_{known}$ in these cases as well. The first case is dealt with using the results of Stoll in the next section. The last two cases are dealt with in Section 5.5 by applying a multiple-prime Chabauty argument. The case $A = 2^5$ is dealt with using results on ternary diophantine equations, which we also do in Section 5.5.

5.4 The family of curves $y^2 = x^5 + A$

We take a digression in this section to mention some general results pertaining to our curves. The curves of interest in this chapter are a part of the family of curves

$$C_A : y^2 = x^5 + A,$$

where $A \neq 0$ is a rational number. Since C_A and C_B are isomorphic over $\mathbb{Q}$ if A/B is a tenth power we will assume that A is an integer and tenth-power free. Except for some fixed values of A not much is known about the rational points on this family of curves in general. However, recently Michael Stoll (see [75]) has announced some very interesting results regarding the number of rational points on these curves, in the case when the Jacobian $J_A(\mathbb{Q})$ of C_A has rank 1.

Before stating his results we'll fix a bit of notation. Let d_A be the number of *trivial* points on $C_A(\mathbb{Q})$; points $(x, y) \in C_A(\mathbb{Q})$ with $xy = 0$, or the point at infinity ∞. Non-trivial points occurs in pairs: (x, y), $(x, -y)$, so we let n_A be half the number of non-trivial points. Equivalently, n_A is the number of nontrivial points with positive y coordinate. Then $\#C_A(\mathbb{Q}) = 2n_A + d_A$, and d_A is given by

$$d_A = \begin{cases} 1 & \text{if } A \text{ is neither a square nor a fifth power,} \\ 2 & \text{if } A \text{ is a fifth power, } A \neq 1, \\ 3 & \text{if } A \text{ is a square, } A \neq 1, \\ 4 & \text{if } A = 1. \end{cases}$$

We have already seen that C_1 has rank zero and that $\#C_1(\mathbb{Q}) = 4$. Thus for $A \neq 1$ we have $\#C_A(\mathbb{Q}) \leq 2n_A + 3$. In [75] Stoll proves the following, where r_A denotes the Mordell-Weil rank of the Jacobian $J_A(\mathbb{Q})$ of C_A.

Theorem 5.3 (Stoll) *Let $A \neq 0$ be an integer such that $r_A = 1$. Then $n_A \leq 2$ and consequently $\#C_A(\mathbb{Q}) \leq 7$.*

More specifically he proves the following theorem, using a refinement of the method of Chabauty and Coleman. Here p is an odd prime and v_p denotes the p-adic valuation.

Theorem 5.4 (Stoll) *Let $A \neq 0$ be an integer such that $r_A = 1$.*

1. *if $v_p(A) \in \{1, 3, 7, 9\}$ for some $p \neq 11, 13$ then $n_A \leq 1$.*
2. *if $v_p(A) = 5$ for some $p \neq 3, 5$ then $n_A \leq 1$, if $v_3(A) = 5$ then $n_A \leq 2$.*
3. *if $v_p(A) \in \{2, 4, 6, 8\}$ for some $p \neq 2, 3, 7$, or if $v_3(A) \in \{6, 8\}$, or if $v_7(A) \in \{2, 6, 8\}$ then $n_A \leq 1$, otherwise if $v_3(A) \in \{2, 4\}$ then $n_A \leq 2$,*
4. *if $A \equiv 1 \pmod 3$ then $n_A \leq 1$, and if $A \equiv -1 \pmod 3$ then $n_A \leq 2$,*
5. *if $A \equiv 1, 3, 9 \pmod{11}$ then $n_A \leq 1$.*

In the case that $A = \pm 2^a 3^b$ the upper bounds on $\#C_A(\mathbb{Q})$ obtained by Stoll matches the number of known points on $C_A(\mathbb{Q})$ in the following cases:

$$A \in \{3, 3^8, 2^2 3^4, 2^3, 3, 2^4 3^3, 2^4 3^8, 2^6 3^4, -2 \cdot 3^4, -2^3 3^8, -2^5 3^8, -2^8 3\}.$$

Thus, our results in the previous section are superceded by Stoll's results, except in one case. Notice that in the case $A = 2^2 3^4 = 18^2$ we were unable to find a single prime at which the Chabauty bound is sufficient to determine $C_{18^2}(\mathbb{Q})$, thus Stoll's results now give us $C_{18^2}(\mathbb{Q})$.

The curve C_{18^2} has 7 rational points, so the bound in Theorem 5.3 is sharp. In fact, as shown in Stoll, this is the unique curve that attains this bound.

One may have noticed, in the tables of the previous section, the only torsion groups that arose were $\mathbb{Z}/2\mathbb{Z}$, $\mathbb{Z}/5\mathbb{Z}$, and, in the single case $A = 1$, $\mathbb{Z}/10\mathbb{Z}$. This is also governed by a general result. It follows from results of Poonen [58] that the torsion of $J_A(\mathbb{Q})$ is as follows.

1. If A is neither a square nor a fifth power then

$$J_A(\mathbb{Q})_{tors} = 0.$$

2. If $A = a^2$ for some integer $a \neq 1$ then

$$J_A(\mathbb{Q})_{tors} = \{\{(0,a),\infty\},\{(0,-a),\infty\},\{(0,a),(0,a)\},$$
$$\{(0,-a),(0,-a)\},O\} \simeq \mathbb{Z}/5\mathbb{Z}.$$

3. If $A = b^5$ for some integer $b \neq 1$ then

$$J_A(\mathbb{Q})_{tors} = \{\ \{(-b,0),\infty\}\ ,O\} \simeq \mathbb{Z}/2\mathbb{Z}.$$

5.5 Proof of Theorem 5.1

We have verified in Section 5.3 that Theorem 5.1 holds for all A except $A \in \{2^2 3^4, 2^5, 2^6 3^2, 2^6 3^3\}$. In the last section we verified, using a result of Stoll, the case $A = 2^2 3^4$. In this section we show that for $A \in \{2^5, 2^6 3^2, 2^6 3^3\}$ the set of known points $C(\mathbb{Q})_{known}$ listed in the tables of Section 5.3 are precisely all the rational points these curves. In the last two cases we do this by applying a multiple-prime Chabauty argument. Such an argument is scarcely found in the literature, indeed I only know of only two places it is applied: [59] and [13].

In what follows, we view $C_A(\mathbb{Q}) \subset J_A(\mathbb{Q})$ via the embedding $(x_0, y_0) \mapsto \{(x_0, y_0), \infty\}$.

5.5.1 $A = 2^6 3^2$

Let us first consider the case $A = 2^6 3^2$, where

$$C_A(\mathbb{Q})_{known} = \{\infty, (0, \pm 24), (4, \pm 40)\}$$

and

$$J_A(\mathbb{Q}) = \langle\{(0,-24),\infty\}\rangle \times \langle\{(4,-40),\infty\}\rangle \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}.$$

Let $T = \{(0,-24),\infty\}$ and $P = \{(4,-40),\infty\}$ be the generators for the torsion and free-part respectively.

Considering the reduction modulo 29,

$$\phi_{29} : J(\mathbb{Q}) \to J(\mathbb{F}_{29}) \simeq \mathbb{Z}/30\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}.$$

The reductions of T and P, denoted by T_{29} and P_{29}, have orders 5 and 30 respectively. We can input this into MAGMA as follows.

```
> _<x>:=PolynomialRing(Rationals());
> C:=HyperellipticCurve(x^5+2^6*3^2); J:=Jacobian(C);
> T:=J![x,-24]]; P:=J![x-4,-4x-24];
> J29:=BaseChange(J,GF(29));
> T29:=J29!T; P29:=J29!P;
> Order(T29); Order(P29);

5
30
```

It follows that the image of the Mordell-Weil group is $\phi_{29}(J(\mathbb{Q})) = \langle T_{29} \rangle \times \langle P_{29} \rangle \simeq \mathbb{Z}/5\mathbb{Z} \times \mathbb{Z}/30\mathbb{Z}$ (it is a simple computation to check $T_{29} \notin \langle P_{29} \rangle$). A rational point (x_0, y_0) on $C_A(\mathbb{Q})$ has image of the form $\{(\overline{x_0}, \overline{y_0}), \infty\}$ in $J(\mathbb{F}_{29})$ so we determine conditions on the integers a and b such that the element $aT + bP$ has this image.

```
> for a in [0..4] do;
for> for b in [0..29] do;
for|for> if (a*T29+b*P29)[3] le 1 then;
for|for|if> print(<a,b,a*T29+b*P29>);
for|for|if> end if;
for|for> end for;
for> end for;

<0, 0, (1, 0, 0)>
<0, 1, (x + 25, 18, 1)>
<0, 29, (x + 25, 11, 1)>
<1, 0, (x, 5, 1)>
<1, 10, (x + 7, 3, 1)>
<2, 8, (x + 1, 16, 1)>
<3, 22, (x + 1, 13, 1)>
<4, 0, (x , 24, 1)>
<4, 12, (x + 7, 26, 1)>
```

This tells us that the image of $aT+bP$ is $\{(\overline{x_0}, \overline{y_0}), \infty\}$ for a and b satisfying the following congruences.

$a \pmod 5$	$b \pmod{30}$	$\phi_{29}(aT + bP)$
0	0	$\{\infty, \infty\}$
0	1	$\{(4, 18), \infty\}$
0	29	$\{(4, 11), \infty\}$
1	0	$\{(0, 5), \infty\}$
0	18	$\{(22, 3), \infty\}$
2	8	$\{(28, 16), \infty\}$
3	22	$\{(28, 13), \infty\}$
4	0	$\{(0, 24), \infty\}$
4	12	$\{(22, 26), \infty\}$

Our five known rational points on $C(\mathbb{Q})$ are in the residue classes $\{\infty, \infty\}$, $\{(4, 18), \infty\}$, $\{(4, 11), \infty\}$, $\{(0, 5), \infty\}$ and $\{(0, 24), \infty\}$, to show there are no other rational points it suffices to show two things:
(i) each coset of $J(\mathbb{Q})/\ker\phi_{29}$ contains at most one rational point,
(ii) there are no rational points in the other four residue classes.

The first of these follows from the fact that the differential killing the Mordell-Weil group modulo 29, $\overline{\omega} = x + 18$, does not vanish on any of the residue classes. This is the Coleman-Chabauty part of the argument. As for (ii) we repeat the computations above with $p = 59$ and get the following classes of ($a \pmod{60}$, $b \pmod{60}$):

$$(0, 0), (0, 1), (0, 7), (0, 11), (0, 30), (0, 49), (0, 53),$$
$$(0, 59), (1, 0), (1, 36), (2, 44), (3, 16), (4, 0), (4, 24).$$

Considering b modulo 30, we see the four extraneous classes which appeared at the prime 29 do not appear here. Thus, these four classes do not contain a rational point. Therefore, for $A = 2^6 3^2$

$$C_A(\mathbb{Q}) = \{\infty, (0, \pm 24), (4, \pm 40)\}.$$

I would like to thank Michael Stoll for his help with this argument.

5.5.2 $A = 2^6 3^3$

In this case there are no known finite points on $C_A(\mathbb{Q})$. Using MAGMA we find

$$J_A(\mathbb{Q}) = \langle P \rangle \simeq \mathbb{Z},$$

where $P = \{x^2-24x+88, 116x-584\}$. Making a call, in MAGMA, to Chabauty at the prime 7 we find that there are at most two rational points on C. Similarly, we get the same information at the prime 29. In particular, applying the same type of computations as above, aP lies in a residue class of the form $\{r, \infty\}$ modulo 7 only when $a \equiv 0, 2, 3 \pmod 5$, and aP lies in a residue class of the form $\{r, \infty\}$ modulo 29 only when $a \equiv 0, 1, 4 \pmod 5$. Thus the only rational points on C_A lie in the coset of $J(\mathbb{Q})/\ker\phi_7$ which contains ∞. The differential killing the Mordell-Weil group modulo 7, $\overline{\omega} = x$, does not vanish on any of the residue classes thus each coset contains at most one rational point, and so ∞ is the only rational points on $C_A(\mathbb{Q})$.

5.5.3 $A = 2^5$

In this case we can apply results from the theory of ternary diophantine equations to get our result. Any rational solution to the equation $y^2 = x^5 + 2^5$ is of the form $(x, y) = (a/e^2, b/e^5)$ for some $a, b, e \in \mathbb{Z}$ with $(a, e) = (b, e) = 1$. Thus a, b, e is a solution to

$$b^2 = a^5 + (2e^2)^5. \tag{5.4}$$

Let $g = (a, b)$, then g^2 divides $(2e^2)^5$, but $(g, e) = 1$, so $g^2 \mid 2^5$. Therefore, $g = 1, 2, 4$. Since 5.4 has no solutions with $a, b, 2e^2$ pairwise coprime (see Darmon and Merel [28]) then $g \neq 1$. Also, $g \neq 4$ since otherwise $2 \mid (b, e)$, a contradiction. It must be the case that $g = 2$, and so dividing the equation through by 2^5 we have

$$2(b/8)^2 = (a/2)^5 + (e^2)^5,$$

where $b/8, a/2, e$ are pairwise coprime. By a result of Bennett and Skinner (see Theorem 4.4) the only solutions are with $(a/e^2, b/e^5) = (2, \pm 8), (-2, 0)$.

5.5.4 Rank ≥ 2 cases

We've shown in Section 5.3 that the curves of the form $y^2 = x^5 + 2^\alpha 3^\beta$, whose Mordell-Weil group has rank ≥ 2, correspond to the following values of α and β:

$$(\alpha, \beta) = (0, 4), (1, 0), (1, 1), (1, 8), (4, 1), (4, 5), (5, 1), (5, 2), (7, 4).$$

Similarly, the curves of the form $y^2 = x^5 - 2^\alpha 3^\beta$ with rank ≥ 2 are the following:

$$(\alpha, \beta) = (1, 2), (1, 6), (5, 4), (5, 6), (7, 4).$$

For these fourteen remaining curves the classical method of Chabauty cannot be applied to bound the number of rational points since the rank is not smaller that the genus. In this case, we would need to use *covering methods*. In this method, finitely many curves D_i are constructed which are unramified covers of C, $\phi_i : D_i \to C$. In such a situation, there is a number field K such that $C(\mathbb{Q}) \subset \bigcup_i \phi_i(D_i(K))$. Hence, determining K-rational points on all D_i will allow us to determine all $\mathbb{Q}$-rational points on C. The covering curves D_i that typically arise have genus 17 and thus it seems we have made the problem harder. However, D_i may possess maps down to some elliptic curve E, for which the *Elliptic Curve Chabauty* method may be applied. This method is described by Bruin in [9], [10], [11], and much of the method has been implemented in MAGMA by Bruin (some of which is still unavailable in the current release [12]). The methods, though implemented, require a high level of sophistication on the part of the user. Bruin verified the results for these final fourteen cures for us [12].

It is interesting to note that one of these curves can be taken care of using a result of Bruin [10]. A rational point (X, Y) on the curve $Y^2 = X^5 + 2$ has the form $X = x/s^2$, $Y = y/s^5$ for integers x, y, s such that $(x, s) = (y, s) = 1$. The equation can then be written as

$$y^2 = x^5 + 2(s^2)^5$$

where we are now interested in coprime integer solutions x, y, s. It follows from [10] (see also [36]) that the only solutions are with $(x, y, s^2) = (-1, \pm 1, 1)$. These pull back to the solutions $(X, Y) = (-1, \pm 1)$.

Chapter 6

Classification of Elliptic Curves over $\mathbb{Q}$ with 2-torsion and conductor $2^\alpha p^2$

As we mentioned before we have broken up our attempt to classify curves of conductor $2^\alpha p^2$ into two stages. In the first stage, we showed if there is an elliptic curve of conductor $2^\alpha p^2$ then p must satisfy one of finitely many explicitly determined Diophantine equations, and we have explicit formulae for the coefficients of the elliptic curve. All this information is given in the theorems of Section 3.1.1. The second stage is to refine the theorems of Section 3.1.1 by using Diophantine lemmata of Chapter 4. It is stage two that is the focus of this chapter.

In Section 6.1 we state the classification theorems for curves of conductor $2^\alpha p^2$. The novelty of these theorems is that, given a prime p, it is straightforward to check whether there are any elliptic curves of conductor $2^\alpha p^2$ (with 2-torsion), and to determine all such curves. Of course, for small values of p (say $p \leq 17$) one could (and should!) consult the tables of Cremona. For larger values, however, we believe the work in this chapter will prove valuable.

6.1 Statement of Results

Let p be a prime number and N an integer satisfying the inequalities

$$p \geq 5, \text{ and } 0 \leq N \leq 8.$$

In what follows, we announce nine theorems which describe, up to $\mathbb{Q}$-isomorphism, all the elliptic curves over $\mathbb{Q}$, of conductor $2^N p^2$, having a rational

point of order 2 over $\mathbb{Q}$. Each theorem corresponds to a value of N. The results obtained are presented in the form of tables analogous to those of [26] and [37]. Each row consists of an elliptic curve of $\mathbb{Q}$ realizing the desired conditions. The columns of the table consist of the following properties of E:

1. A minimal model of E of the form

$$y^2 + a_1xy = x^3 + a_2x^2 + a_4x + a_6,$$

where the a_i are in $\mathbb{Z}$. If $N \geq 2$, we can choose a model such that $a_1 = a_6 = 0$. In the statements of these theorems we omit the columns corresponding to these coefficients.

2. The order $|T_2|$ of the group T_2 consisting of $\mathbb{Q}$-rational 2-torsion points of E.

3. The factorization of the minimal discriminant Δ of E.

4. The j-invariant of E.

5. The Kodaira symbols of E at 2 and p.

Also appearing in the table are the letters of identification (A,B,...) for each elliptic curve. The curves which are labeled by the same letter are linked by an isogeny over $\mathbb{Q}$ of degree 2 or a composition of two such isogenies. Moreover, they are numbered in the order of how they are to be determined.

As in Chapter 3 we will use the following notation.

a. For each elliptic curve E over $\mathbb{Q}$, we denote by E' the elliptic curve over $\mathbb{Q}$ obtained from E by a twist by $\sqrt{-1}$.

b. Given an integer n which is a square in $\mathbb{Z}$ we denote, for the rest of this work, by $\sqrt{n}$ the square root of n satisfying the following condition:

$$\begin{cases} \sqrt{n} \equiv 1 \bmod 4 & \text{if } n \text{ is odd} \\ \sqrt{n} \geq 0 & \text{if } n \text{ is even .} \end{cases} \tag{6.1}$$

Theorem 6.1 *The elliptic curves E defined over $\mathbb{Q}$, of conductor p^2, and having at least one rational point of order 2, are the ones such that one of the following conditions is satisfied:*

1. *$p = 7$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	minimal model	T_2	j	Δ
A1	$[1,-1,0,-2,-1]$	2	-15^3	7^3
A2	$[1,-1,0,-107,552]$	2	-15^3	7^9
B1	$[1,-1,0,-37,-78]$	2	255^3	7^3
B2	$[1,-1,0,-1822,30393]$	2	255^3	7^9

2. *$p = 17$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	minimal model	T_2	j	Δ
C1	$[1,-1,1,-1644,-24922]$	4	$\frac{273^3}{17^2}$	17^8
C2	$[1,-1,1,-26209,-1626560]$	2	$\frac{18863^3}{17}$	17^7
C3	$[1,-1,1,-199,510]$	4	$\frac{33^3}{17}$	17^7
C4	$[1,-1,1,-199,-68272]$	2	$\frac{-33^3}{17^4}$	17^{10}

3. *$p - 64$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_1	a_2	a_4	a_6	$\lvert T_2\rvert$	Δ	j	*Kodaira*
A1	1	$\frac{p\sqrt{p-64}-1}{4}$	$-p^2$	0	2	p^7	$\frac{(p-16)^3}{p}$	$\mathrm{I}_0;\mathrm{I}_1^*$
A2	1	$\frac{p\sqrt{p-64}-1}{4}$	$4p^2$	$p^3\sqrt{p-64}$	2	$-p^8$	$\frac{(256-p)^3}{p^2}$	$\mathrm{I}_0;\mathrm{I}_2^*$

Theorem 6.2 *The elliptic curves $E/\mathbb{Q}$ of conductor $2p^2$ with a rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *$p = 7$ or 17 and E is $\mathbb{Q}$-isomorphic to one of the curves in the table in Appendix C.*
2. [1] *$p = 2^k + 1$, where $k \geq 5$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_1	a_2	a_4	a_6	Δ	j	*Kodaira*
A1	1	$\frac{p(2p-1)-1}{4}$	$\frac{p^3(p-1)}{16}$	0	$2^{2k-8}p^8$	$\frac{(2^kp+1)^3}{2^{2k-8}p^2}$	$\mathrm{I}_{2k-8};\mathrm{I}_2^*$
A2	1	$\frac{p(2p-1)-1}{4}$	$\frac{-p^3(p-1)}{4}$	$\frac{-p^4(p-1)(2p-1)}{16}$	$2^{k-4}p^7$	$\frac{(2^{k+4}p+1)^3}{2^{k-4}p}$	$\mathrm{I}_{k-4};\mathrm{I}_1^*$
B1	1	$\frac{-p(p-2)-1}{4}$	$\frac{-p^2(p-1)}{16}$	0	$2^{2k-8}p^8$	$\frac{(p^2-2^k)^3}{2^{2k-8}p^2}$	$\mathrm{I}_{2k-8};\mathrm{I}_2^*$
B2	1	$\frac{-p(p-2)-1}{4}$	$\frac{p^2(p-1)}{4}$	$\frac{-p^3(p-1)(p-2)}{16}$	$-2^{k-4}p^{10}$	$\frac{(2^{k+4}-p^2)^3}{2^{k-4}p^4}$	$\mathrm{I}_{k-4};\mathrm{I}_4^*$

[1] These are **Fermat primes**; it is necessary that k be a power of 2 for $2^k + 1$ to be prime.

$|T_2| = 4$ *for A1 and B1, and* $|T_2| = 2$ *for the other two.*

3. [2] $p = 2^q - 1$, *where* $q \geq 5$ *is a prime, and* E *is* $\mathbb{Q}$*-isomorphic to one of the elliptic curves:*

	a_1	a_2	a_4	a_6	Δ	j	*Kodaira*
C1	1	$\frac{p(2p+1)-1}{4}$	$\frac{p^3(p+1)}{16}$	0	$2^{2q-8}p^8$	$\frac{(2^qp+1)^3}{2^{2q-8}p^2}$	$\mathrm{I}_{2q-8}; \mathrm{I}_2^*$
C2	1	$\frac{p(2p+1)-1}{4}$	$\frac{-p^3(p+1)}{4}$	$\frac{-p^4(p+1)(2p+1)}{16}$	$2^{q-4}p^7$	$\frac{(2^{q+4}p+1)^3}{2^{q-4}p}$	$\mathrm{I}_{q-4}; \mathrm{I}_1^*$
D1	1	$\frac{-p(p+2)-1}{4}$	$\frac{p^2(p+1)}{16}$	0	$2^{2q-8}p^8$	$\frac{(p^2+2^q)^3}{2^{2q-8}p^2}$	$\mathrm{I}_{2q-8}; \mathrm{I}_2^*$
D2	1	$\frac{-p(p+2)-1}{4}$	$\frac{-p^2(p+1)}{4}$	$\frac{p^3(p+1)(p+2)}{16}$	$2^{q-4}p^{10}$	$\frac{(p^2+2^{q+4})^3}{2^{q-4}p^4}$	$\mathrm{I}_{q-4}; \mathrm{I}_4^*$

$|T_2| = 4$ *for C1 and D1, and* $|T_2| = 2$ *for the other two.*

4. *there exists* $m \geq 7$ *such that* $p - 2^m = d^2$, *for some* $d \equiv 1 \pmod 4$, *and* E *is* $\mathbb{Q}$*-isomorphic to one of the elliptic curves:*

	a_1	a_2	a_4	a_6	Δ	j	*Kodaira*
E1	1	$\frac{pd-1}{4}$	$-2^{m-6}p^2$	0	$2^{2m-12}p^7$	$\frac{(p-2^{m-2})^3}{2^{2m-12}p}$	$\mathrm{I}_{2m-12}; \mathrm{I}_1^*$
E2	1	$\frac{pd-1}{4}$	$2^{m-4}p^2$	$2^{m-6}p^3d$	$-2^{m-6}p^8$	$\frac{(2^{m+2}-p)^3}{2^{m-6}p^2}$	$\mathrm{I}_{m-6}; \mathrm{I}_2^*$

$|T_2|$ *is* 2 *for both curves.*

5. *there exists* $m \geq 7$ *such that* $p + 2^m = d^2$, *for some* $d \equiv 1 \pmod 4$, *and* E *is* $\mathbb{Q}$*-isomorphic to one of the elliptic curves:*

	a_1	a_2	a_4	a_6	Δ	j	*Kodaira*
F1	1	$\frac{pd-1}{4}$	$2^{m-6}p^2$	0	$2^{2m-12}p^7$	$\frac{(p+2^{m-2})^3}{2^{2(m-6)}p}$	$\mathrm{I}_{2m-12}; \mathrm{I}_1^*$
F2	1	$\frac{pd-1}{4}$	$-2^{m-4}p^2$	$-2^{m-6}p^3d$	$2^{m-6}p^8$	$\frac{(p+2^{m+2})^3}{2^{m-6}p^2}$	$\mathrm{I}_{m-6}; \mathrm{I}_2^*$

$|T_2|$ *is* 2 *for both curves.*

6. *there exists* $m \geq 7$ *such that* $2^m - p = d^2$, *for some* $d \equiv 1 \pmod 4$, *and* E *is* $\mathbb{Q}$*-isomorphic to one of the elliptic curves:*

	a_1	a_2	a_4	a_6	Δ	j	*Kodaira*
G1	1	$\frac{-pd-1}{4}$	$2^{m-6}p^2$	0	$2^{2m-12}p^7$	$\frac{(p-2^{m-2})^3}{2^{2m-12}p}$	$\mathrm{I}_{2m-12}; \mathrm{I}_1^*$
G2	1	$\frac{-pd-1}{4}$	$-2^{m-4}p^2$	$2^{m-6}p^3d$	$2^{m-6}p^8$	$\frac{(2^{m+2}-p)^3}{2^{m-6}p^2}$	$\mathrm{I}_{m-6}; \mathrm{I}_2^*$

[2] These are **Mersenne primes**; it is necessary that q be a prime for $2^q - 1$ to be prime.

$|T_2|$ is 2 for both curves.

7. *there exists $m \geq 7$ such that $\frac{2^m-1}{p}$ is a square integer, say $pd^2 = 2^m - 1$ with $d \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_1	a_2	a_4	a_6	Δ	*j-invariant*	*Kodaira*
H1	1	$\frac{-pd-1}{4}$	$2^{m-6}p$	0	$-2^{2m-12}p^3$	$\frac{(1-2^{m-2})^3}{2^{2m-12}}$	$\mathrm{I}_{2m-12}; \mathrm{III}$
H2	1	$\frac{-pd-1}{4}$	$-2^{m-4}p$	$2^{m-6}p^2d$	$2^{m-6}p^3$	$\frac{(2^{m+2}-1)^3}{2^{m-6}}$	$\mathrm{I}_{m-6}; \mathrm{III}$
I1	1	$\frac{p^2d-1}{4}$	$2^{m-6}p^3$	0	$-2^{2m-12}p^9$	$\frac{(1-2^{m-2})^3}{2^{2m-12}}$	$\mathrm{I}_{2m-12}; \mathrm{III}^*$
I2	1	$\frac{p^2d-1}{4}$	$-2^{m-4}p^3$	$-2^{m-6}p^5d$	$2^{m-6}p^9$	$\frac{(2^{m+2}-1)^3}{2^{m-6}}$	$\mathrm{I}_{m-6}; \mathrm{III}^*$

$|T_2|$ is 2 for all four curves.

8. *there exists $m \geq 7$ such that $\frac{2^m+1}{p}$ is a square integer, say $pd^2 = 2^m + 1$ with $d \equiv 1 \pmod 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_1	a_2	a_4	a_6	Δ	*j-invariant*	*Kodaira*
J1	1	$\frac{pd-1}{4}$	$2^{m-6}p$	0	$2^{2m-12}p^3$	$\frac{(2^{m-2}+1)^3}{2^{2m-12}}$	$\mathrm{I}_{2m-12}; \mathrm{III}$
J2	1	$\frac{pd-1}{4}$	$-2^{m-4}p$	$-2^{m-6}p^2d$	$2^{m-6}p^3$	$\frac{(2^{m+2}+1)^3}{2^{m-6}}$	$\mathrm{I}_{m-6}; \mathrm{III}$
K1	1	$\frac{p^2d-1}{4}$	$2^{m-6}p^3$	0	$2^{2m-12}p^9$	$\frac{(2^{m-2}+1)^3}{2^{2m-12}}$	$\mathrm{I}_{2m-12}; \mathrm{III}^*$
K2	1	$\frac{p^2d-1}{4}$	$-2^{m-4}p^3$	$-2^{m-6}p^5d$	$2^{m-6}p^9$	$\frac{(2^{m+2}+1)^3}{2^{m-6}}$	$\mathrm{I}_{m-6}; \mathrm{III}^*$

$|T_2|$ is 2 for all four curves.

Theorem 6.3 *The elliptic curves $E/\mathbb{Q}$ of conductor $4p^2$ with a rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *$p = 5$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves in the table in Appendix C.*
2. *$p - 4$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
A1	$p\sqrt{p-4}$	$-p^2$	2	2^4p^7	$\frac{256(p-1)^3}{p}$	$\mathrm{IV}; \mathrm{I}_1^*$
A2	$-2p\sqrt{p-4}$	p^3	2	-2^8p^8	$\frac{p^4(16-p)^3}{p^2}$	$\mathrm{IV}^*; \mathrm{I}_2^*$

Theorem 6.4 *The elliptic curves $E/\mathbb{Q}$ of conductor $8p^2$ with a rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *$p = 5, 7, 17, 23$ or 31 and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves in the table in Appendix C.*

2. *$p - 2^m$ is a square for $m = 4$ or 5 and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ	*j-invariant*	*Kodaira*
A1	$p\sqrt{p-2^m}$	$-2^{m-2}p^2$	$2^{2m}p^7$	$\frac{2^{12-2m}(p-2^{m-2})^3}{p}$	$\mathrm{I}_1^*, \mathrm{III}^*; \mathrm{I}_1^*$
A2	$-2p\sqrt{p-2^m}$	p^3	$-2^{m+6}p^8$	$\frac{2^{6-m}(2^{m+2}-p)^3}{p^2}$	$\mathrm{III}^*, \mathrm{II}^*; \mathrm{I}_2^*$

   $|T_2|$ is 2 for both curves.

3. *$p + 32$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
B1	$p\sqrt{p+32}$	2^3p^2	2	$2^{10}p^7$	$\frac{4(p+8)^3}{p}$	$\mathrm{III}^*; \mathrm{I}_1^*$
B2	$-2p\sqrt{p+32}$	p^3	2	$-2^{11}p^8$	$\frac{-2(p+128)^3}{p^2}$	$\mathrm{II}^*; \mathrm{I}_2^*$

Theorem 6.5 *The elliptic curves $E/\mathbb{Q}$ of conductor $16p^2$ with a rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *$p = 5, 7, 17, 23$ or 31 and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves in the table in Appendix C.*

2. *$p = 2^k + 1$, where $k \geq 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
A1	$-p(2p-1)$	$(p-1)p^3$	4	$2^{2k+4}p^8$	$\frac{(2^kp+1)^3}{2^{2k-8}p^2}$	$\mathrm{I}_{2k-4}^*; \mathrm{I}_2^*$
A2	$2p(2p-1)$	p^2	2	$2^{k+8}p^7$	$\frac{(2^{k+4}p+1)^3}{2^{k-4}p}$	$\mathrm{I}_k^*; \mathrm{I}_1^*$
A3	$-2p(p+1)$	$p^2(p-1)^2$	2	$2^{4k-4}p^7$	$\frac{(p+2^{2k-4})^3}{2^{2(2k-8)}p}$	$\mathrm{I}_{4k-12}^*; \mathrm{I}_1^*$
A4	$-2p(p-2)$	p^4	2	$-2^{k+8}p^{10}$	$\frac{(2^{k+4}-p^2)^3}{2^{k-4}p^4}$	$\mathrm{II}^*; \mathrm{I}_4^*$

3. *$p = 2^q - 1$, where $q \geq 3$ is a prime, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\|T_2\|$	Δ	*j-invariant*	*Kodaira*
B1	$-p(2p+1)$	$(p+1)p^3$	4	$2^{2q+4}p^8$	$\frac{(2^q p+1)^3}{2^{2q-8}p^2}$	$\mathrm{I}^*_{2q-4};\mathrm{I}^*_2$
B2	$2p(2p+1)$	p^2	2	$2^{q+8}p^7$	$\frac{(2^{q+4}p+1)^3}{2^{q-4}p^2}$	$\mathrm{I}^*_q;\mathrm{I}^*_1$
B3	$-2p(p-1)$	$p^2(p+1)^2$	2	$-2^{4q-4}p^7$	$\frac{(p-2^{2q-4})^3}{2^{2(2q-8)}p}$	$\mathrm{I}^*_{4q-12};\mathrm{I}^*_1$
B4	$-2p(p+2)$	p^4	2	$2^{q+8}p^7$	$\frac{(p^2+2^{q+4})^3}{2^{q-4}p^4}$	$\mathrm{II}^*;\mathrm{I}^*_4$

4. *$p-2^m$ is a square for $m=2$ or $m\geq 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ	*j-invariant*	*Kodaira*
C1	$-p\sqrt{p-2^m}$	$-2^{m-2}p^2$	$2^{2m}p^7$	$\frac{(p-2^{m-2})^3}{2^{2m-12}p}$	$\mathrm{II}^*,\mathrm{I}^*_{2m-8};\mathrm{I}^*_1$
C2	$2p\sqrt{p-2^m}$	p^3	$-2^{m+6}p^8$	$\frac{(2^{m+2}-p)^3}{2^{m-6}p^2}$	$\mathrm{I}^*_0,\mathrm{I}^*_{m-2};\mathrm{I}^*_2$

   $|T_2|$ is 2 for both curves.

5. *$p+32$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\|T_2\|$	Δ	*j-invariant*	*Kodaira*
D1	$-p\sqrt{p+32}$	2^3p^2	2	$2^{10}p^7$	$\frac{4(p+8)^3}{p}$	$\mathrm{I}^*_2;\mathrm{I}^*_1$
D2	$2p\sqrt{p+32}$	p^3	2	$2^{11}p^8$	$\frac{2(p+2^7)^3}{p^2}$	$\mathrm{I}^*_3;\mathrm{I}^*_2$

6. *there exists an odd integer $m\geq 7$ such that $p+2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\|T_2\|$	Δ	*j-invariant*	*Kodaira*
E1	$-p\sqrt{p+2^m}$	$2^{m-2}p^2$	2	$2^{2m}p^7$	$\frac{(p+2^{m-2})^3}{2^{2m-12}p}$	$\mathrm{I}^*_{2m-8};\mathrm{I}^*_1$
E2	$2p\sqrt{p+2^m}$	p^3	2	$2^{m+6}p^8$	$\frac{(p+2^{m+2})^3}{2^{m-6}p^2}$	$\mathrm{I}^*_{m-2};\mathrm{I}^*_2$

7. *there exists an odd integer $m\geq 7$ such that 2^m-p is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\|T_2\|$	Δ	*j-invariant*	*Kodaira*
F1	$p\sqrt{2^m-p}$	$2^{m-2}p^2$	2	$-2^{2m}p^7$	$\frac{(p-2^{m-2})^3}{2^{2(m-6)}p}$	$\mathrm{I}^*_{2m-8};\mathrm{I}^*_1$
F2	$-2p\sqrt{2^m-p}$	$-p^3$	2	$2^{m+6}p^8$	$\frac{(2^{m+2}-p)^3}{2^{m-6}p^2}$	$\mathrm{I}^*_{m-2};\mathrm{I}^*_2$

8. *there exists $m\geq 7$ such that $\frac{2^m-1}{p}$ is a square integer and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
G1	$p\sqrt{\frac{2^m-1}{p}}$	$2^{m-2}p$	2	$-2^{2m}p^3$	$\frac{(1-2^{m-2})^3}{2^{2m-12}}$	I^*_{2m-8}; III
G2	$-2p\sqrt{\frac{2^m-1}{p}}$	$-p$	2	$2^{m+6}p^3$	$\frac{(2^{m+2}-1)^3}{2^{m-6}}$	I^*_{m-2}; III
H1	$-p^2\sqrt{\frac{2^m-1}{p}}$	$2^{m-2}p^3$	2	$-2^{2m}p^9$	$\frac{(1-2^{m-2})^3}{2^{2m-12}}$	I^*_{2m-8}; III*
H2	$2p^2\sqrt{\frac{2^m-1}{p}}$	$-p^3$	2	$2^{m+6}p^9$	$\frac{(2^{m+2}-1)^3}{2^{m-6}}$	I^*_{m-2}; III*

9. *there exists $m \geq 5$ such that $\frac{2^m+1}{p}$ is a square integer and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
I1	$-p\sqrt{\frac{2^m+1}{p}}$	$2^{m-2}p$	2	$2^{2m}p^3$	$\frac{(2^{m-2}+1)^3}{2^{2m-12}}$	I^*_{2m-8}; III
I2	$2p\sqrt{\frac{2^m+1}{p}}$	p	2	$2^{m+6}p^3$	$\frac{(2^{m+2}+1)^3}{2^{m-6}}$	I^*_{m-2}; III
J1	$-p^2\sqrt{\frac{2^m+1}{p}}$	$2^{m-2}p^3$	2	$2^{2m}p^9$	$\frac{(2^{m-2}+1)^3}{2^{2m-12}}$	I^*_{2m-8}; III*
J2	$2p^2\sqrt{\frac{2^m+1}{p}}$	p^3	2	$2^{m+6}p^9$	$\frac{(2^{m+2}+1)^3}{2^{m-6}}$	I^*_{m-2}; III*

Theorem 6.6 *The elliptic curves $E/\mathbb{Q}$ of conductor $32p^2$ with a rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *$p = 7$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves in the table in Appendix C.*

2. *$p \geq 5$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (i) $p \equiv 1 \pmod 4$,

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
A1	0	$-p^2$	4	2^6p^6	1728	III; I^*_0
A2	0	2^2p^2	2	$-2^{12}p^6$	1728	I^*_3; I^*_0
A3	$6p$	p^2	2	2^9p^6	$2^33^311^3$	I^*_0; I^*_0
A4	$-6p$	p^2	2	2^9p^6	$2^33^311^3$	I^*_0; I^*_0
B1	0	$-p$	2	2^6p^3	1728	III; III
B2	0	2^2p	2	$-2^{12}p^3$	1728	I^*_3; III
C1	0	$-p^3$	2	2^6p^9	1728	III; III*
C2	0	2^2p^3	2	$-2^{12}p^9$	1728	I^*_3; III*

   (ii) $p \equiv 3 \pmod 4$,

	a_2	a_4	$\|T_2\|$	Δ	*j-invariant*	*Kodaira*
D1	0	$-p^2$	4	2^6p^6	1728	$\mathrm{III};\mathrm{I}_0^*$
D2	0	2^2p^2	2	$-2^{12}p^6$	1728	$\mathrm{I}_3^*;\mathrm{I}_0^*$
D3	$6p$	p^2	2	2^9p^6	$2^33^311^3$	$\mathrm{I}_0^*;\mathrm{I}_0^*$
D4	$-6p$	p^2	2	2^9p^6	$2^33^311^3$	$\mathrm{I}_0^*;\mathrm{I}_0^*$
E1	0	p	2	-2^6p^3	1728	$\mathrm{III};\mathrm{III}$
E2	0	-2^2p	2	$2^{12}p^3$	1728	$\mathrm{I}_3^*;\mathrm{III}$
F1	0	p^3	2	-2^6p^9	1728	$\mathrm{III};\mathrm{III}^*$
F2	0	-2^2p^3	2	$2^{12}p^9$	1728	$\mathrm{I}_3^*;\mathrm{III}^*$

3. *$p-1$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\|T_2\|$	Δ	*j-invariant*	*Kodaira*
G1	$2p\sqrt{p-1}$	$-p^2$	2	2^6p^7	$\frac{64(4p-1)^3}{p}$	$\mathrm{III};\mathrm{I}_1^*$
G2	$-2^2p\sqrt{p-1}$	2^2p^3	2	$-2^{12}p^8$	$\frac{64(4-p)^3}{p^2}$	$\mathrm{I}_3^*;\mathrm{I}_2^*$
G1′	$-2p\sqrt{p-1}$	$-p^2$	2	2^6p^7	$\frac{64(4p-1)^3}{p}$	$\mathrm{III};\mathrm{I}_1^*$
G2′	$2^2p\sqrt{p-1}$	2^2p^3	2	$-2^{12}p^8$	$\frac{64(4-p)^3}{p^2}$	$\mathrm{I}_3^*;\mathrm{I}_2^*$

4. *$p-8$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\|T_2\|$	Δ	*j-invariant*	*Kodaira*
H1	$p\sqrt{p-8}$	$-2p^2$	2	2^6p^7	$\frac{64(p-2)^3}{p}$	$\mathrm{III};\mathrm{I}_1^*$
H2	$-2p\sqrt{p-8}$	p^3	2	-2^9p^8	$\frac{-8(p-32)^3}{p^2}$	$\mathrm{I}_0^*;\mathrm{I}_2^*$
H1′	$-p\sqrt{p-8}$	$-2p^2$	2	2^6p^7	$\frac{64(p-2)^3}{p}$	$\mathrm{III};\mathrm{I}_1^*$
H2′	$2p\sqrt{p-8}$	p^3	2	-2^9p^8	$\frac{-8(p-32)^3}{p^2}$	$\mathrm{I}_0^*;\mathrm{I}_2^*$

5. *$p+8$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\|T_2\|$	Δ	*j-invariant*	*Kodaira*
I1	$p\sqrt{p+8}$	$2p^2$	2	2^6p^7	$\frac{64(p+2)^3}{p}$	$\mathrm{III};\mathrm{I}_1^*$
I2	$-2p\sqrt{p+8}$	p^3	2	2^9p^8	$\frac{8(p+32)^3}{p^2}$	$\mathrm{I}_0^*;\mathrm{I}_2^*$
I1′	$-p\sqrt{p+8}$	$2p^2$	2	2^6p^7	$\frac{64(p+2)^3}{p}$	$\mathrm{III};\mathrm{I}_1^*$
I2′	$2p\sqrt{p+8}$	p^3	2	2^9p^8	$\frac{8(p+32)^3}{p^2}$	$\mathrm{I}_0^*;\mathrm{I}_2^*$

Theorem 6.7 *The elliptic curves $E/\mathbb{Q}$ of conductor $64p^2$ with a rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *$p = 5, 7, 17$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves in the table in Appendix C.*

2. *$p \geq 5$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

   (i) $p \equiv 1 \pmod 4$,

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
A1	0	-2^2p^2	4	$2^{12}p^6$	1728	$\mathrm{I}_2^*;\mathrm{I}_0^*$
A2	0	p^2	2	-2^6p^6	1728	$\mathrm{II};\mathrm{I}_0^*$
A3	$12p$	2^2p^2	2	$2^{15}p^6$	$2^33^311^3$	$\mathrm{I}_5^*;\mathrm{I}_0^*$
A4	$-12p$	2^2p^2	2	$2^{15}p^6$	$2^33^311^3$	$\mathrm{I}_5^*;\mathrm{I}_0^*$
B1	0	p	2	-2^6p^3	1728	$\mathrm{II};\mathrm{III}$
B2	0	-2^2p	2	$2^{12}p^3$	1728	$\mathrm{I}_2^*;\mathrm{III}$
C1	0	p^3	2	-2^6p^9	1728	$\mathrm{II};\mathrm{III}^*$
C2	0	-2^2p^3	2	$2^{12}p^9$	1728	$\mathrm{I}_2^*;\mathrm{III}^*$

   (ii) $p \equiv 3 \pmod 4$,

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
D1	0	-2^2p^2	4	$2^{12}p^6$	1728	$\mathrm{I}_2^*;\mathrm{I}_0^*$
D2	0	p^2	2	-2^6p^6	1728	$\mathrm{II};\mathrm{I}_0^*$
D3	$12p$	2^2p^2	2	$2^{15}p^6$	$2^33^311^3$	$\mathrm{I}_5^*;\mathrm{I}_0^*$
D4	$-12p$	2^2p^2	2	$2^{15}p^6$	$2^33^311^3$	$\mathrm{I}_5^*;\mathrm{I}_0^*$
E1	0	$-p$	2	2^6p^3	1728	$\mathrm{II};\mathrm{III}$
E2	0	2^2p	2	$-2^{12}p^2$	1728	$\mathrm{I}_2^*;\mathrm{III}$
F1	0	$-p^3$	2	2^6p^9	1728	$\mathrm{II};\mathrm{III}^*$
F2	0	2^2p^3	2	$-2^{12}p^9$	1728	$\mathrm{I}_2^*;\mathrm{III}^*$

3. *$p = 2^k + 1$, where $k \geq 4$, and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ	*j-invariant*	*Kodaira*
G1	$2p(2p-1)$	$2^2(p-1)p^3$	$2^{2k+10}p^8$	$\frac{(2^kp+1)^3}{2^{2k-8}p^2}$	$\mathrm{I}_0^*;\mathrm{I}_2^*$
G2	$-2^2p(2p-1)$	2^2p^2	$2^{k+14}p^7$	$\frac{(2^{k+4}p+1)^3}{2^{k-4}p}$	$\mathrm{I}_{k+4}^*;\mathrm{I}_1^*$
G3	$p(p+1)$	$2^{2k-2}p^2$	$2^{4k+2}p^7$	$\frac{(p+2^{2k-4})^3}{2^{2(2k-8)}p}$	$\mathrm{I}_{4k-8}^*;\mathrm{I}_1^*$
G4	$2^2p(p-2)$	2^2p^4	$-2^{k+14}p^{10}$	$\frac{(2^{k+4}-p^2)^3}{2^{k-4}p^4}$	$\mathrm{I}_{k+4}^*;\mathrm{I}_4^*$
G1′	$-2p(2p-1)$	$2^2(p-1)p^3$	$2^{2k+10}p^8$	$\frac{(2^kp+1)^3)^3}{2^{2k-8}p^2}$	$\mathrm{I}_0^*;\mathrm{I}_2^*$
G2′	$2^2p(2p-1)$	2^2p^2	$2^{k+14}p^7$	$\frac{(2^{k+4}p+1)^3}{2^{k-4}p}$	$\mathrm{I}_{k+4}^*;\mathrm{I}_1^*$
G3′	$-p(p+1)$	$2^{2k-2}p^2$	$2^{4k+2}p^7$	$\frac{(p+2^{2k-4})^3}{2^{2(2k-8)}p}$	$\mathrm{I}_{4k-8}^*;\mathrm{I}_1^*$
G4′	$-2^2p(p-2)$	2^2p^4	$-2^{k+14}p^{10}$	$\frac{(2^{k+4}-p^2)^3}{2^{k-4}p^4}$	$\mathrm{I}_{k+4}^*;\mathrm{I}_4^*$

$|T_2|=4$ *for G1 and G1′, and* $|T_2|=2$ *for all others.*

4. $p=2^q-1$, *where* $q\geq 3$ *is a prime, and* E *is* $\mathbb{Q}$*-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ	*j-invariant*	*Kodaira*
H1	$2p(2p+1)$	$2^2(p+1)p^3$	$2^{2q+10}p^8$	$\frac{(2^qp+1)^3}{2^{2q-8}p^2}$	$\mathrm{I}_0^*;\mathrm{I}_2^*$
H2	$-2^2p(2p+1)$	2^2p^2	$2^{q+14}p^7$	$\frac{(2^{q+4}p+1)^3}{2^{q-4}p}$	$\mathrm{I}_{q+4}^*;\mathrm{I}_1^*$
H3	$p(p-1)$	$2^{2q-2}p^2$	$-2^{4q+2}p^7$	$\frac{(p-2^{2q-4})^3}{2^{2(2q-8)}p}$	$\mathrm{I}_{4q-8}^*;\mathrm{I}_1^*$
H4	$2^2p(p+2)$	2^2p^4	$2^{q+14}p^{10}$	$\frac{(p^2+2^{q+4})^3}{2^{q-4}p^4}$	$\mathrm{I}_{q+4}^*;\mathrm{I}_4^*$
H1′	$-2p(2p+1)$	$2^2(p+1)p^3$	$2^{2q+10}p^8$	$\frac{(2^qp+1)^3}{2^{2q-8}p^2}$	$\mathrm{I}_0^*;\mathrm{I}_2^*$
H2′	$2^2p(2p+1)$	2^2p^2	$2^{q+14}p^7$	$\frac{(2^{q+4}p+1)^3}{2^{q-4}p}$	$\mathrm{I}_{q+4}^*;\mathrm{I}_1^*$
H3′	$-p(p-1)$	$2^{2q-2}p^2$	$-2^{4q+2}p^7$	$\frac{(p-2^{2q-4})^3}{2^{2(2q-8)}p}$	$\mathrm{I}_{4q-8}^*;\mathrm{I}_1^*$
H4′	$-2^2p(p+2)$	2^2p^4	$2^{q+14}p^{10}$	$\frac{(p^2+2^{q+4})^3}{2^{q-4}p^4}$	$\mathrm{I}_{q+4}^*;\mathrm{I}_4^*$

$|T_2|=4$ *for H1 and H1′, and* $|T_2|=2$ *for all others.*

5. $p-1$ *is a square and* E *is* $\mathbb{Q}$*-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
I1	$2p\sqrt{p-1}$	p^3	2	-2^6p^8	$\frac{-64(p-4)^3}{p^2}$	$\mathrm{II};\mathrm{I}_2^*$
I2	$-2^2p\sqrt{p-1}$	-2^2p^2	2	$2^{12}p^7$	$\frac{64(4p-1)^3}{p}$	$\mathrm{I}_2^*;\mathrm{I}_1^*$
I1′	$-2p\sqrt{p-1}$	p^3	2	-2^6p^8	$\frac{-64(p-4)^3}{p^2}$	$\mathrm{II};\mathrm{I}_2^*$
I2′	$2^2p\sqrt{p-1}$	-2^2p^2	2	$2^{12}p^7$	$\frac{64(4p-1)^3}{p}$	$\mathrm{I}_2^*;\mathrm{I}_1^*$

6. *there exists $m \geq 2$ such that $p - 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
J1	$2p\sqrt{p-2^m}$	$-2^m p^2$	2	$2^{2m+6}p^7$	$\frac{(p-2^{m-2})^3}{2^{2m-12}p}$	$\mathrm{I}^*_{2m-4}; \mathrm{I}^*_1$
J2	$-2^2p\sqrt{p-2^m}$	2^2p^3	2	$-2^{m+12}p^8$	$\frac{(2^{m+2}-p)^3}{2^{m-6}p^2}$	$\mathrm{I}^*_{m+2}; \mathrm{I}^*_2$
J1′	$-2p\sqrt{p-2^m}$	$-2^m p^2$	2	$2^{2m+6}p^7$	$\frac{(p-2^{m-2})^3}{2^{2m-12}p}$	$\mathrm{I}^*_{2m-4}; \mathrm{I}^*_1$
J2′	$2^2p\sqrt{p-2^m}$	2^2p^3	2	$-2^{m+12}p^8$	$\frac{(2^{m+2}-p)^3}{2^{m-6}p^2}$	$\mathrm{I}^*_{m+2}; \mathrm{I}^*_2$

7. *there exists an odd integer $m \geq 2$ such that $p + 2^m$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
K1	$2p\sqrt{p+2^m}$	$2^m p^2$	2	$2^{2m+6}p^7$	$\frac{(p+2^{m-2})^3}{2^{2m-12}p}$	$\mathrm{I}^*_{2m-4}; \mathrm{I}^*_1$
K2	$-2^2p\sqrt{p+2^m}$	2^2p^3	2	$2^{m+12}p^8$	$\frac{(p+2^{m+2})^3}{2^{m-6}p^2}$	$\mathrm{I}^*_{m+2}; \mathrm{I}^*_2$
K1′	$-2p\sqrt{p+2^m}$	$2^m p^2$	2	$2^{2m+6}p^7$	$\frac{(p+2^{m-2})^3}{2^{2m-12}p}$	$\mathrm{I}^*_{2m-4}; \mathrm{I}^*_1$
K2′	$2^2p\sqrt{p+2^m}$	2^2p^3	2	$2^{m+12}p^8$	$\frac{(p+2^{m+2})^3}{2^{m-6}p^2}$	$\mathrm{I}^*_{m+2}; \mathrm{I}^*_2$

8. *there exists an odd integer $m \geq 3$ such that $2^m - p$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
L1	$2p\sqrt{2^m-p}$	$2^m p^2$	2	$-2^{2m+6}p^7$	$\frac{(p-2^{m-2})^3}{2^{2m-12}p}$	$\mathrm{I}^*_{2m-4}; \mathrm{I}^*_1$
L2	$-2^2p\sqrt{2^m-p}$	-2^2p^3	2	$2^{m+12}p^8$	$\frac{(2^{m+2}-p)^3}{2^{m-6}p^2}$	$\mathrm{I}^*_{m+2}; \mathrm{I}^*_2$
L1′	$-2p\sqrt{2^m-p}$	$2^m p^2$	2	$-2^{2m+6}p^7$	$\frac{(p-2^{m-2})^3}{2^{2m-12}p}$	$\mathrm{I}^*_{2m-4}; \mathrm{I}^*_1$
L2′	$2^2p\sqrt{2^m-p}$	-2^2p^3	2	$2^{m+12}p^8$	$\frac{(2^{m+2}-p)^3}{2^{m-6}p^2}$	$\mathrm{I}^*_{m+2}; \mathrm{I}^*_2$

9. *there exists $m \geq 3$ such that $\frac{2^m-1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	Δ	*j-invariant*	*Kodaira*
M1	$2p\sqrt{\frac{2^m-1}{p}}$	$2^m p$	$-2^{2m+6}p^3$	$\frac{-(2^{m-2}-1)^3}{2^{2m-12}}$	I^*_{2m-4}; III
M2	$-2^2p\sqrt{\frac{2^m-1}{p}}$	-2^2p	$2^{m+12}p^3$	$\frac{(2^{m+2}-1)^3}{2^{m-6}}$	I^*_{m+2}; III
M1′	$-2p\sqrt{\frac{2^m-1}{p}}$	$2^m p$	$-2^{2m+6}p^3$	$\frac{-(2^{m-2}-1)^3}{2^{2m-12}}$	I^*_{2m-4}; III
M2′	$2^2p\sqrt{\frac{2^m-1}{p}}$	-2^2p	$2^{m+12}p^3$	$\frac{(2^{m+2}-1)^3}{2^{m-6}}$	I^*_{m+2}; III
N1	$2p^2\sqrt{\frac{2^m-1}{p}}$	$2^m p^3$	$-2^{2m+6}p^9$	$\frac{-(2^{m-2}-1)^3}{2^{2m-12}}$	I^*_{2m-4}; III*
N2	$-2^2p^2\sqrt{\frac{2^m-1}{p}}$	-2^2p^3	$2^{m+12}p^9$	$\frac{(2^{m+2}-1)^3}{2^{m-6}}$	I^*_{m+2}; III*
N1′	$-2p^2\sqrt{\frac{2^m-1}{p}}$	$2^m p^3$	$-2^{2m+6}p^9$	$\frac{-(2^{m-2}-1)^3}{2^{2m-12}}$	I^*_{2m-4}; III*
N2′	$2^2p^2\sqrt{\frac{2^m-1}{p}}$	-2^2p^3	$2^{m+12}p^9$	$\frac{(2^{m+2}-1)^3}{2^{m-6}}$	I^*_{m+2}; III*

$|T_2| = 2$ *for all these curves.*

10. *there exists $m \geq 2$ such that $\frac{2^m+1}{p}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
O1	$2p\sqrt{\frac{2^m+1}{p}}$	$2^m p$	2	$2^{2m+6}p^3$	$\frac{(2^{m-2}-1)^3}{2^{2m-12}}$	I^*_{2m-4}; III
O2	$-2^2p\sqrt{\frac{2^m+1}{p}}$	2^2p	2	$2^{m+12}p^3$	$\frac{(2^{m+2}+1)^3}{2^{m-6}}$	I^*_{m+2}; III
O1′	$-2p\sqrt{\frac{2^m+1}{p}}$	$2^m p$	2	$2^{2m+6}p^3$	$\frac{(2^{m-2}-1)^3}{2^{2m-12}}$	I^*_{2m-4}; III
O2′	$2^2p\sqrt{\frac{2^m+1}{p}}$	2^2p	2	$2^{m+12}p^3$	$\frac{(2^{m+2}+1)^3}{2^{m-6}}$	I^*_{m+2}; III
P1	$2p^2\sqrt{\frac{2^m+1}{p}}$	$2^m p^3$	2	$2^{2m+6}p^9$	$\frac{(2^{m-2}-1)^3}{2^{2m-12}}$	I^*_{2m-4}; III*
P2	$-2^2p^2\sqrt{\frac{2^m+1}{p}}$	2^2p^3	2	$2^{m+12}p^9$	$\frac{(2^{m+2}+1)^3}{2^{m-6}}$	I^*_{m+2}; III*
P1′	$-2p^2\sqrt{\frac{2^m+1}{p}}$	$2^m p^3$	2	$2^{2m+6}p^9$	$\frac{(2^{m-2}-1)^3}{2^{2m-12}}$	I^*_{2m-4}; III*
P2′	$2^2p^2\sqrt{\frac{2^m+1}{p}}$	2^2p^3	2	$2^{m+12}p^9$	$\frac{(2^{m+2}+1)^3}{2^{m-6}}$	I^*_{m+2}; III*

Theorem 6.8 *The elliptic curves $E/\mathbb{Q}$ of conductor $128p^2$ with a rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *$p = 13$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves in the table in Appendix C.*
2. *p is a prime ≥ 5 and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
A1	$2p$	$2p^2$	2	-2^8p^6	2^7	III; I_0^*
A2	-2^2p	-2^2p^2	2	$2^{13}p^6$	$2^5 7^3$	I_2^*; I_0^*
A1′	$-2p$	$2p^2$	2	-2^8p^6	2^7	III; I_0^*
A2′	2^2p	-2^2p^2	2	$2^{13}p^6$	$2^5 7^3$	I_2^*; I_0^*
B1	$2p$	$-p^2$	2	2^7p^6	$2^5 7^3$	III; I_0^*
B2	-2^2p	2^3p^2	2	$-2^{14}p^6$	2^7	I_2^*; I_0^*
B1′	$-2p$	$-p^2$	2	2^7p^6	$2^5 7^3$	III; I_0^*
B2′	2^2p	2^3p^2	2	$-2^{14}p^6$	2^7	I_2^*; I_0^*

3. $2p-1$ *is a square,* $p \equiv 1 \pmod 4$, $p \neq 13$ *and* E *is* $\mathbb{Q}$*-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
C1	$2p\sqrt{2p-1}$	$2p^3$	2	-2^8p^8	$\frac{-128(p-2)^3}{p^2}$	III; I_2^*
C2	$-2^2p\sqrt{2p-1}$	-2^2p^2	2	$2^{13}p^7$	$\frac{32(8p-1)^3}{p}$	I_2^*; I_1^*
C1′	$-2p\sqrt{2p-1}$	$2p^3$	2	-2^8p^8	$\frac{-256(p-2)^3}{p^2}$	III; I_2^*
C2′	$2^2p\sqrt{2p-1}$	-2^2p^2	2	$2^{13}p^7$	$\frac{32(8p-1)^3}{p}$	I_2^*; I_1^*
D1	$2p\sqrt{2p-1}$	$-p^2$	2	2^7p^7	$\frac{32(8p-1)^3}{p}$	II; I_1^*
D2	$-2^2p\sqrt{2p-1}$	2^3p^3	2	$-2^{14}p^8$	$\frac{-128(p-2)^3}{p^2}$	III*; I_2^*
D1′	$-2p\sqrt{2p-1}$	$-p^2$	2	2^7p^7	$\frac{32(8p-1)^3}{p}$	II; I_1^*
D2′	$2^2p\sqrt{2p-1}$	2^3p^3	2	$-2^{14}p^8$	$\frac{-128(p-2)^3}{p^2}$	III*; I_2^*

4. $2p^2-1$ *is a square,* $p \equiv 1 \pmod 4$, *and* E *is* $\mathbb{Q}$*-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
E1	$2p\sqrt{2p^2-1}$	$2p^4$	2	-2^8p^{10}	$\frac{-128(p^2-2)^3}{p^4}$	III; I_4^*
E2	$-2^2p\sqrt{2p^2-1}$	-2^2p^2	2	$2^{13}p^8$	$\frac{32(8p^2-1)^3}{p^2}$	I_2^*; I_2^*
E1′	$-2p\sqrt{2p^2-1}$	$2p^4$	2	-2^8p^{10}	$\frac{-128(p^2-2)^3}{p^4}$	III; I_4^*
E2′	$2^2p\sqrt{2p^2-1}$	-2^2p^2	2	$2^{13}p^8$	$\frac{32(8p^2-1)^3}{p^2}$	I_2^*; I_2^*
F1	$2p\sqrt{2p^2-1}$	$-p^2$	2	2^7p^8	$\frac{32(8p^2-1)^3}{p^2}$	II; I_2^*
F2	$-2^2p\sqrt{2p^2-1}$	2^3p^4	2	$-2^{14}p^{10}$	$\frac{-128(p^2-2)^3}{p^4}$	III*; I_4^*
F1′	$-2p\sqrt{2p^2-1}$	$-p^2$	2	2^7p^8	$\frac{32(8p^2-1)^3}{p^2}$	II; I_2^*
F2′	$2^2p\sqrt{2p^2-1}$	2^3p^4	2	$-2^{14}p^{10}$	$\frac{-128(p^2-2)^3}{p^4}$	III*; I_4^*

5. *$p-2$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
G1	$2p\sqrt{p-2}$	p^3	2	-2^7p^8	$\frac{-32(p-8)^3}{p^2}$	II; I_2^*
G2	$-2^2p\sqrt{p-2}$	-2^3p^2	2	$2^{14}p^7$	$\frac{128(2p-1)^3}{p}$	III^*; I_1^*
G1′	$-2p\sqrt{p-2}$	p^3	2	-2^7p^8	$\frac{-32(p-8)^3}{p^2}$	II; I_2^*
G2′	$2^2p\sqrt{p-2}$	-2^3p^2	2	$2^{14}p^7$	$\frac{128(2p-1)^3}{p}$	III^*; I_1^*
H1	$2p\sqrt{p-2}$	$-2p^2$	2	2^8p^7	$\frac{128(2p-1)^3}{p}$	III; I_1^*
H2	$-2^2p\sqrt{p-2}$	2^2p^3	2	$-2^{13}p^8$	$\frac{-32(p-8)^3}{p^2}$	I_2^*; I_2^*
H1′	$-2p\sqrt{p-2}$	$-2p^2$	2	2^8p^7	$\frac{128(2p-1)^3}{p}$	III; I_1^*
H2′	$2^2p\sqrt{p-2}$	2^2p^3	2	$-2^{13}p^8$	$\frac{-32(p-8)^3}{p^2}$	I_2^*; I_2^*

6. *p^n+2 is a square for some integer $n\geq 1$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
I1	$2p\sqrt{p^n+2}$	p^{n+2}	2	2^7p^{2n+6}	$\frac{32(p^n+8)^3}{p^{2n}}$	II; I_{2n}^*
I2	$-2^2p\sqrt{p^n+2}$	2^3p^2		$2^{14}p^{n+6}$	$\frac{128(2p^n+1)^3}{p^n}$	III^*; I_n^*
I1′	$-2p\sqrt{p^n+2}$	p^{n+2}	2	2^7p^{2n+6}	$\frac{32(p^n+8)^3}{p^{2n}}$	II; I_{2n}^*
I2′	$2^2p\sqrt{p^n+2}$	2^3p^2		$2^{14}p^{n+6}$	$\frac{128(2p^n+1)^3}{p^n}$	III^*; I_n^*
J1	$2p\sqrt{p^n+2}$	$2p^2$		2^8p^{n+6}	$\frac{128(2p^n+1)^3}{p^n}$	III; I_n^*
J2	$-2^2p\sqrt{p^n+2}$	2^2p^{n+2}	2	$2^{13}p^{2n+6}$	$\frac{32(p^n+8)^3}{p^{2n}}$	I_2^*; I_{2n}^*
J1′	$-2p\sqrt{p^n+2}$	$2p^2$		2^8p^{n+6}	$\frac{128(2p^n+1)^3}{p^n}$	III; I_n^*
J2′	$2^2p\sqrt{p^n+2}$	2^2p^{n+2}	2	$2^{13}p^{2n+6}$	$\frac{32(p^n+8)^3}{p^{2n}}$	I_2^*; I_{2n}^*

Theorem 6.9 *The elliptic curves $E/\mathbb{Q}$ of conductor $256p^2$ with a rational point of order 2 are the ones such that one of the following conditions is satisfied:*

1. *$p=23$ and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves in the table in Appendix C.*

2. *p is a prime ≥ 5 and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\|T_2\|$	Δ	*j-invariant*	*Kodaira*
A1	0	$2p$	2	-2^9p^3	1728	$\mathrm{III};\mathrm{III}$
A2	0	-2^3p	2	$2^{15}p^3$	1728	$\mathrm{III}^*;\mathrm{III}$
B1	0	$-2p$	2	2^9p^3	1728	$\mathrm{III};\mathrm{III}$
B2	0	2^3p	2	$-2^{15}p^3$	1728	$\mathrm{III}^*;\mathrm{III}$
C1	0	$2p^2$	2	-2^9p^6	1728	$\mathrm{III};\mathrm{I}_0^*$
C2	0	-2^3p^2	2	$2^{15}p^6$	1728	$\mathrm{III}^*;\mathrm{I}_0^*$
D1	0	$-2p^2$	2	2^9p^6	1728	$\mathrm{III};\mathrm{I}_0^*$
D2	0	2^3p^2	2	$-2^{15}p^6$	1728	$\mathrm{III}^*;\mathrm{I}_0^*$
E1	0	$2p^3$	2	-2^9p^9	1728	$\mathrm{III};\mathrm{III}^*$
E2	0	-2^3p^3	2	$2^{15}p^9$	1728	$\mathrm{III}^*;\mathrm{III}^*$
F1	0	$-2p^3$	2	2^9p^9	1728	$\mathrm{III};\mathrm{III}^*$
F2	0	2^3p^3	2	$-2^{15}p^9$	1728	$\mathrm{III}^*;\mathrm{III}^*$
G1	2^2p	$2p^2$	2	2^9p^6	2^65^3	$\mathrm{III};\mathrm{I}_0^*$
G2	-2^3p	2^3p^2	2	$2^{15}p^6$	2^65^3	$\mathrm{III}^*;\mathrm{I}_0^*$
G1′	-2^2p	$2p^2$	2	2^9p^6	2^65^3	$\mathrm{III};\mathrm{I}_0^*$
G2′	2^3p	2^3p^2	2	$2^{15}p^6$	2^65^3	$\mathrm{III}^*;\mathrm{I}_0^*$

3. *$\frac{p-1}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\|T_2\|$	Δ	*j-invariant*	*Kodaira*
H1	$2^2p\sqrt{\frac{p-1}{2}}$	$2p^3$	2	-2^9p^8	$\frac{-64(p-4)^3}{p^2}$	$\mathrm{III};\mathrm{I}_2^*$
H2	$-2^3p\sqrt{\frac{p-1}{2}}$	-2^3p^2	2	$2^{15}p^7$	$\frac{64(4p-1)^3}{p}$	$\mathrm{III}^*;\mathrm{I}_1^*$
H1′	$-2^2p\sqrt{\frac{p-1}{2}}$	$2p^3$	2	-2^9p^8	$\frac{-64(p-4)^3}{p^2}$	$\mathrm{III};\mathrm{I}_2^*$
H2′	$2^3p\sqrt{\frac{p-1}{2}}$	-2^3p^2	2	$2^{15}p^7$	$\frac{64(4p-1)^3}{p}$	$\mathrm{III}^*;\mathrm{I}_1^*$
I1	$2^2p\sqrt{\frac{p-1}{2}}$	$-2p^2$	2	2^9p^7	$\frac{64(4p-1)^3}{p}$	$\mathrm{III};\mathrm{I}_1^*$
I2	$-2^3p\sqrt{\frac{p-1}{2}}$	2^3p^3	2	$-2^{15}p^8$	$\frac{-64(p-4)^3}{p^2}$	$\mathrm{III}^*;\mathrm{I}_2^*$
I1′	$-2^2p\sqrt{\frac{p-1}{2}}$	$-2p^2$	2	2^9p^7	$\frac{64(4p-1)^3}{p}$	$\mathrm{III};\mathrm{I}_1^*$
I2′	$2^3p\sqrt{\frac{p-1}{2}}$	2^3p^3	2	$-2^{15}p^8$	$\frac{-64(p-4)^3}{p^2}$	$\mathrm{III}^*;\mathrm{I}_2^*$

4. *$\frac{p^2-1}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
J1	$2^2p\sqrt{\frac{p^2-1}{2}}$	$2p^4$	2	-2^9p^{10}	$\frac{64(p^2-4)^3}{p^4}$	III; I_4^*
J2	$-2^3p\sqrt{\frac{p^2-1}{2}}$	-2^3p^2	2	$2^{15}p^8$	$\frac{64(4p^2-1)^3}{p^2}$	III*; I_2^*
J1′	$-2^2p\sqrt{\frac{p^2-1}{2}}$	$2p^4$	2	-2^9p^{10}	$\frac{64(p^2-4)^3}{p^4}$	III; I_4^*
J2′	$2^3p\sqrt{\frac{p^2-1}{2}}$	-2^3p^2	2	$2^{15}p^8$	$\frac{64(4p^2-1)^3}{p^2}$	III*; I_2^*
K1	$2^2p\sqrt{\frac{p^2-1}{2}}$	$-2p^2$	2	2^9p^8	$\frac{64(4p^2-1)^3}{p^2}$	III; I_2^*
K2	$-2^3p\sqrt{\frac{p^2-1}{2}}$	2^3p^4	2	$-2^{15}p^{10}$	$\frac{64(p^2-4)^3}{p^4}$	III*; I_4^*
K1′	$-2^2p\sqrt{\frac{p^2-1}{2}}$	$-2p^2$	2	2^9p^8	$\frac{64(4p^2-1)^3}{p^2}$	III; I_2^*
K2′	$2^3p\sqrt{\frac{p^2-1}{2}}$	2^3p^4	2	$-2^{15}p^{10}$	$\frac{64(p^2-4)^3}{p^4}$	III*; I_4^*

5. *$\frac{p+1}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
L1	$2^2p\sqrt{\frac{p+1}{2}}$	$2p^3$	2	2^9p^8	$\frac{64(p+4)^3}{p^2}$	III; I_2^*
L2	$-2^3p\sqrt{\frac{p+1}{2}}$	2^3p^2	2	$2^{15}p^7$	$\frac{64(4p+1)^3}{p}$	III*; I_1^*
L1′	$-2^2p\sqrt{\frac{p+1}{2}}$	$2p^3$	2	2^9p^8	$\frac{64(p+4)^3}{p^2}$	III; I_2^*
L2′	$2^3p\sqrt{\frac{p+1}{2}}$	2^3p^2	2	$2^{15}p^7$	$\frac{64(4p+1)^3}{p}$	III*; I_1^*
M1	$2^2p\sqrt{\frac{p+1}{2}}$	$2p^2$	2	2^9p^7	$\frac{64(4p+1)^3}{p}$	III; I_1^*
M2	$-2^3p\sqrt{\frac{p+1}{2}}$	2^3p^3	2	$2^{15}p^8$	$\frac{64(p+4)^3}{p^2}$	III*; I_2^*
M1′	$-2^2p\sqrt{\frac{p+1}{2}}$	$2p^2$	2	2^9p^7	$\frac{64(4p+1)^3}{p}$	III; I_1^*
M2′	$2^3p\sqrt{\frac{p+1}{2}}$	2^3p^3	2	$2^{15}p^8$	$\frac{64(p+4)^3}{p^2}$	III*; I_2^*

6. *$\frac{p^2+1}{2}$ is a square and E is $\mathbb{Q}$-isomorphic to one of the elliptic curves:*

	a_2	a_4	$\lvert T_2\rvert$	Δ	*j-invariant*	*Kodaira*
N1	$2^2 p\sqrt{\frac{p^2+1}{2}}$	$2p^4$	2	$2^9 p^{10}$	$\frac{64(p^2+4)^3}{p^4}$	III; I_4^*
N2	$-2^3 p\sqrt{\frac{p^2+1}{2}}$	$2^3 p^2$	2	$2^{15} p^8$	$\frac{64(4p^2+1)^3}{p^2}$	III*; I_2^*
N1′	$-2^2 p\sqrt{\frac{p^2+1}{2}}$	$2p^4$	2	$2^9 p^{10}$	$\frac{64(p^2+4)^3}{p^4}$	III; I_4^*
N2′	$2^3 p\sqrt{\frac{p^2+1}{2}}$	$2^3 p^2$	2	$2^{15} p^8$	$\frac{64(4p^2+1)^3}{p^2}$	III*; I_2^*
O1	$2^2 p\sqrt{\frac{p^2+1}{2}}$	$2p^2$	2	$2^9 p^8$	$\frac{64(4p^2+1)^3}{p^2}$	III; I_2^*
O2	$-2^3 p\sqrt{\frac{p^2+1}{2}}$	$2^3 p^4$	2	$2^{15} p^{10}$	$\frac{64(p^2+4)^3}{p^4}$	III*; I_4^*
O1′	$-2^2 p\sqrt{\frac{p^2+1}{2}}$	$2p^2$	2	$2^9 p^8$	$\frac{64(4p^2+1)^3}{p^2}$	III; I_2^*
O2′	$2^3 p\sqrt{\frac{p^2+1}{2}}$	$2^3 p^4$	2	$2^{15} p^{10}$	$\frac{64(p^2+4)^3}{p^4}$	III*; I_4^*

In Chapter 8 we will be interested in knowing, up to isogeny, the elliptic curves with conductor of the form $32p^2$ or $256p^2$, and their j-invariants. We have the following corollaries to Theorems 6.6 and 6.9.

Corollary 6.10 *Suppose $p \geq 5$ is prime and that $E/\mathbb{Q}$ is an elliptic curve with a rational 2-torsion point and conductor $32p^2$. Then E is isogenous over $\mathbb{Q}$ to a curve of the form*

$$y^2 = x^3 + a_2 x^2 + a_4 x$$

with coefficients given in the following table.

p	a_2	a_4	*j-invariant*
any	0	$-p^2$	1728
any	0	$(-1)^{(p+1)/2}p$	1728
any	0	$(-1)^{(p+1)/2}p^3$	1728
7	± 7	$2 \cdot 7^2$	$8000/7$
7	± 7	$2 \cdot 7$	-2^6
7	$\pm 7^2$	$2 \cdot 7^3$	-2^6
$s^2+1,\ s \in \mathbb{Z}$	$2ps$	$-p^2$	$\frac{64(4p-1)^3}{p}$
$s^2+8,\ s \in \mathbb{Z}$	ps	$-2p^2$	$\frac{64(p-2)^3}{p}$
$s^2-8,\ s \in \mathbb{Z}$	ps	$2p^2$	$\frac{64(p+2)^3}{p}$

Corollary 6.11 *Suppose $p \geq 5$ is prime and that $E/\mathbb{Q}$ is an elliptic curve with a rational 2-torsion point and conductor $256p^2$. Then E is isogenous over $\mathbb{Q}$ to a curve of the form*

$$y^2 = x^3 + a_2x^2 + a_4x$$

with coefficients given in the following table.

p	a_2	a_4	*j-invariant*
any	0	$\pm 2p$	1728
any	0	$\pm 2p^2$	1728
any	0	$\pm 2p^3$	1728
any	$\pm 4p$	$2p^2$	$2^6 5^3$
23	$\pm 2^3 \cdot 23 \cdot 39$	$2 \cdot 23^5$	$\frac{2^6 3^3 4057^3}{23^6}$
23	$\pm 2^4 \cdot 23 \cdot 39$	$2^3 \cdot 23^5$	$\frac{2^6 3^3 4057^3}{23^6}$
$2s^2+1,\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^3$	$\frac{-64(p-4)^3}{p^2}$
$2s^2+1,\ s \in \mathbb{Z}$	$\pm 4ps$	$-2p^2$	$\frac{64(4p-1)^3}{p}$
$\sqrt{2s^2+1},\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^4$	$\frac{64(p^2-4)^3}{p^4}$
$\sqrt{2s^2+1},\ s \in \mathbb{Z}$	$\pm 4ps$	$-2p^2$	$\frac{64(4p^2-1)^3}{p^2}$
$2s^2-1,\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^3$	$\frac{64(p+4)^3}{p^2}$
$2s^2-1,\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^2$	$\frac{64(4p+1)^3}{p}$
$\sqrt{2s^2-1},\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^4$	$\frac{64(p^2+4)^3}{p^4}$
$\sqrt{2s^2-1},\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^2$	$\frac{64(4p^2+1)^3}{p^2}$

6.2 The Proof

We will only sketch the proof of Theorem 6.2, it should be clear from this how the proofs of the remaining theorems follow from their counterparts in Section 3.1.1 and the Diophantine lemmata of Chapter 4.

Let E be an elliptic curve over $\mathbb{Q}$ with a rational 2-torsion point and conductor $N = 2p^2$ for a fixed prime $p \geq 5$. Then E is $\mathbb{Q}$-isomorphic to one of the curves in Theorem 3.2 and p satisfies one of the corresponding Diophantine equations:

1) $d^2 = 2^m p^n + 1$,

2) $d^2 = 2^m + p^n$,

3) $d^2 = 2^m - p^n$,
4) $d^2 = p^n - 2^m$,
5) $pd^2 = 2^m + 1$,
6) $pd^2 = 2^m - 1$,
with $n \geq 0$ and $m \geq 7$.

Applying the Diophantine lemmata from Chapter 4, the solutions of these are respectively as follows:

1) $(p, d, n) = (2^{m-2} + 1, 2p - 1, 1)$ and $(p, d, n) = (2^{m-2} - 1, 2p + 1, 1)$,
2) $(p, d, m, n) = (17, 71, 7, 3)$, $(p, d, n) = (2^{m-2} - 1, p + 2, 2)$, and solutions with $n = 1$,
3) $(p, d, m, n) = (7, 13, 9, 3)$, and solutions with $n = 1$,
4) $(p, d, n) = (2^{m-2} + 1, p - 2, 2)$, and solutions with $n = 1$.
5) $\frac{2^m+1}{p}$ is a square,
6) $\frac{2^m-1}{p}$ is a square.

Thus, p must satisfy one of these conditions. Suppose p satisfies the first condition in 1, that is $p = 2^{m-2}+1$, $d = 2p-1$, and $n = 1$. Then E is $\mathbb{Q}$-isomorphic to one of

$$y^2 = x^3 + p(2p-1)x^2 + 2^{m-2}p^3x,$$
$$y^2 = x^3 - 2p(2p-1)x^2 + p^2x,$$

by part (1) of Theorem 3.2 (neither curve is minimal at 2). The minimal models of these curves can be computed using Corollary 2.2:

$$y^2 + xy = x^3 + \frac{p(2p-1)-1}{4}x^2 + \frac{p^3(p-1)}{16}x,$$
$$y^2 + xy = x^3 + \frac{p(2p-1)-1}{4}x^2 + \frac{-p^3(p-1)}{4}x + \frac{-p^4(p-1)(2p-1)}{16}.$$

Thus E is isomorphic to either A1 or A2 in Theorem 6.2.

Suppose that p satisfies the first condition in 4, that is, $p = 2^{m-2} + 1$, $d = p - 2$, and $n = 2$. Then a similar argument shows that E is isomorphic to either B1 or B2 in Theorem 6.2.

Similarly, one can verify the rest of Theorem 6.2 by considering p of each form in 1 through 6 listed above.

This completes the sketch of the proof for these tables.

Chapter 7

On the Classification of Elliptic Curves over $\mathbb{Q}$ with 2-torsion and conductor $2^\alpha 3^2 p$

A more appropriate title for this chapter would be "Classification *of primes* for which there exist elliptic curves over $\mathbb{Q}$ with 2-torsion and conductor $2^\alpha 3^2 p$ with $\alpha \in \{1, 2, 3\}$", since it is the collection of primes we will be studying, not the curves themselves. The tables in Section 3.2 provide a classification of elliptic curves of conductor $2^\alpha 3^2 p$ in which the prime p must satisfy one of a list of Diophantine equations. In this chapter, we use the lemmata of Chapter 4 to resolve all the Diophantine equations which occurred. Hence, we can list, rather explicitly, all the primes that can occur. In Chapter 9, we will be interested in the primes for which there are no elliptic curves of conductor $2^\alpha 3^2 p$, with $\alpha \in \{1, 2, 3\}$. Our main focus here will be to determine properties of this set of primes. We will show that for all primes $p \equiv 317$ or $1757 \pmod{2040}$ there are no elliptic curves with 2-torsion and conductor $2^\alpha 3^2 p$ with $\alpha \in \{1, 2, 3\}$.

7.1 Statement of Results

Theorem 7.1 *The primes p for which there exists an elliptic curve $E/\mathbb{Q}$ of conductor $18p$, and having at least one rational point of order 2, satisfy one of the following:*

1. $p \in \{5, 7, 11, 17, 19, 23, 73\}$;
2. $p = 2^{m-2}3^\ell \pm 1$ *with* $m \geq 7$, $\ell \geq 0$;
3. $p = \frac{2^{m-2}+1}{3^\ell}$ *with* $m \geq 7$, $\ell \geq 1$;

4. $p = 3^\ell + 2^{m-2}$ *with* $m \geq 7$, $\ell \geq 0$;
5. $p = 3^\ell - 2^{m-2}$ *with* $m \geq 7$, $\ell \geq 0$;
6. $p = 2^{m-2} - 3^\ell$ *with* $m \geq 7$, $\ell \geq 0$;
7. $p = d^2 + 2^m 3^\ell$ *with* $m \geq 7$ *and* $\ell \geq 0$;
8. $p = d^2 - 2^m 3^\ell$ *with* $m \geq 7$ *and* $\ell \geq 0$;
9. $p = 2^m 3^\ell - d^2$ *with* $m \geq 7$ *and* $\ell \geq 0$;
10. $p = \frac{d^2+2^m}{3^\ell}$ *with* $m \geq 7$, $\ell \geq 1$;
11. $p = 3d^2 + 2^m$ *with* $m \geq 7$;
12. $p = 3d^2 - 2^m$ *with* $m \geq 7$;
13. $p = 2^m - 3d^2$ *with* $m \geq 7$;

Theorem 7.2 *The primes p for which there exists an elliptic curve $E/\mathbb{Q}$ of conductor $36p$, and having at least one rational point of order 2, satisfy one of the following:*

1. $p \in \{5, 13\}$;
2. $p^n = d^2 + 4 \cdot 3^\ell$ *with* $\ell \geq 0$ *even,* $n = 1$ *or* $P_{\min}(n) \geq 7$;
3. $p^n = d^2 - 4 \cdot 3^\ell$ *with* $\ell \geq 1$ *odd,* $n = 1$ *or* $P_{\min}(n) \geq 7$;
4. $p^n = 4 \cdot 3^\ell - d^2$ *with* $\ell \geq 1$ *odd,* $n = 1$ *or* $P_{\min}(n) \geq 7$;
5. $p^n = \frac{d^2+3^\ell}{4}$ *with* $\ell \geq 1$ *odd,* $n = 1$ *or* $P_{\min}(n) \geq 7$, $p \equiv -1 \pmod 4$;
6. $4p^n = 3d^2 + 1$ *with* $n \in \{1, 2\}$ *and* $p^n \equiv 1 \pmod 4$;
7. $p = 3d^2 - 4$;

Theorem 7.3 *The primes p for which there exists an elliptic curve $E/\mathbb{Q}$ of conductor $72p$, and having at least one rational point of order 2, satisfy one of the following:*

1. $p \in \{5, 7, 13, 23, 29, 31, 47, 67, 73, 193, 1153\}$;
2. $p = \frac{3^\ell+1}{4}$ *with* ℓ *odd;*

3. $p^n = d^2 + 4 \cdot 3^\ell$ *with* $\ell \geq 1$ *odd,* $n = 1$ *or* $P_{\min}(n) \geq 7$*;*
4. $p^n = d^2 - 4 \cdot 3^\ell$ *with* $\ell \geq 0$ *even,* $n = 1$ *or* $P_{\min}(n) \geq 7$*;*
5. $p^n = 4 \cdot 3^\ell - d^2$ *with* $\ell \geq 0$ *even,* $n = 1$ *or* $P_{\min}(n) \geq 7$*;*
6. $p = 2^{m-2}3^\ell \pm 1$ *with* $m \in \{4, 5\}$*,* $\ell \geq 0$*;*
7. $p^n = d^2 + 2^m \cdot 3^\ell$ *with* $m \in \{4, 5\}$*,* $\ell \geq 0$*,* $n = 1$ *or* $P_{\min}(n) \geq 7$*;*
8. $p^n = d^2 - 2^m \cdot 3^\ell$ *with* $m \in \{4, 5\}$*,* $\ell \geq 0$*,* $n = 1$ *or* $P_{\min}(n) \geq 7$*;*
9. $p^n = 2^m \cdot 3^\ell - d^2$ *with* $m \in \{4, 5\}$*,* $\ell \geq 0$*,* $n = 1$ *or* $P_{\min}(n) \geq 7$*;*
10. $p^n = \frac{d^2+3^\ell}{4}$ *with* ℓ *odd,* $p \equiv 1 \pmod{12}$*,* $n = 1$ *or* $P_{\min}(n) \geq 7$*;*
11. $p = 3^\ell \pm 4$ *with* $\ell \geq 0$*;*
12. $p = 3^\ell \pm 8$ *with* $\ell \geq 0$*;*
13. $p = \frac{d^2+2^m}{3^\ell}$ *with* $m \in \{4, 5\}$ *and* ℓ *odd;*
14. $p^n = \frac{d^2+32}{3^\ell}$ *with* ℓ *odd,* $n = 1$ *or* $P_{\min}(n) \geq 7$*;*
15. $p = \frac{3d^2+1}{4}$*;*
16. $p^2 = \frac{3d^2+1}{4}$*;*
17. $p = 3d^2 - 2^m$ *with* $m \in \{4, 5\}$*;*
18. $p = 3d^2 + 2^m$ *with* $m \in \{2, 4, 5\}$.

Corollary 7.4 *Let* $p \geq 5$ *be a prime.*

1. *If there exists an elliptic curve over* $\mathbb{Q}$ *with* 2*-torsion and conductor* $18p$ *then one of the following must hold:* $p = 5$*,* $p \not\equiv 2 \pmod 3$*,* $p \not\equiv 2 \pmod 5$*,* $p \not\equiv 5 \pmod 8$*, or* $p \not\equiv 6$ *and* $11 \pmod{17}$*.*
2. *If there exists an elliptic curve over* $\mathbb{Q}$ *with* 2*-torsion and conductor* $36p$ *then one of the following must hold:* $p = 5$*,* $p \not\equiv 2 \pmod 3$*, or* $p \not\equiv 1$ *and* $5 \pmod 8$*.*

3. *If there exists an elliptic curve over $\mathbb{Q}$ with 2-torsion and conductor $72p$ then one of the following must hold: $p = 5$, $p = 29$, $p \not\equiv 2 \pmod 3$, or $p \not\equiv 5 \pmod 8$.*

It follows that there are no elliptic curves over $\mathbb{Q}$ with 2-torsion and conductor $2^\alpha 9p$, where $\alpha \in \{1, 2, 3\}$, for p satisfying $p \equiv 317$ or $1757 \pmod{2040}$ (i.e. $p \equiv 5 \pmod 8$, $p \equiv 2 \pmod 3$, $p \equiv 2 \pmod 5$, and $p \equiv 6$ or $11 \pmod{17}$).

By Dirichlet's theorem on primes in arithmetic progression, we have that there are infinitely many primes p for which there are no elliptic curves over $\mathbb{Q}$ with 2-torsion and conductor $2^\alpha 9p$, with $\alpha \in \{1, 2, 3\}$; since primes congruent to 317 or 1757 modulo 2040 have this property. Though this list is infinite, it misses a lot of primes with the property. Indeed, a quick search through Cremona's tables of elliptic curves up to conductor 130000 reveals the following list of the first few primes:

$$197, 317, 439, 557, 653, 677, 701, 773, 797, 821, 1013, 1039,$$
$$1061, 1109, 1231, 1277, 1279, 1289, 1301, 1399, 1447, 1471, 1493$$
$$1613, 1637, 1663, 1709, 1733.$$

Let $\mathcal{S}$ denote set of primes which satisfy one of the forms in the statements of Theorems 7.1, 7.2, and 7.3. We would like to show that $\mathcal{S}$ has density zero in the set of all primes. By this we mean, if $\#\mathcal{S}(X)$ is the number of primes in $\mathcal{S}$ less than X then

$$\lim_{X \to \infty} \frac{\#\mathcal{S}(X)}{\pi(X)} = 0,$$

where $\pi(X)$ is the number of all primes less than X. Determining the density of primes of the form $p = \frac{d^2+2^m}{3^\ell}$ is somewhat problematic. So, let $\mathcal{S}'$ denote set of primes which satisfy one of the forms in the statements of Theorems 7.1, 7.2, and 7.3, except $p^n = \frac{d^2+2^m}{3^\ell}$. Also, let $\mathcal{S}'(X) = \{p \in \mathcal{S}' : p \leq X\}$. We prove the following.

Lemma 7.5

$$\lim_{X \to \infty} \frac{\#\mathcal{S}'(X)}{\pi(X)} = 0.$$

7.2 The Proofs

7.2.1 Proof of Theorem 7.1

We proceed through the cases of Theorem 7.1 (with $b = 2$) and use the lemmata of Chapter 4 to resolve the Diophantine equations that arise. Notice that in all cases we are only concerned with solutions to the Diophantine equations with $m \geq 7$. In what follows, by "solvable", we mean there are solutions for which $m \geq 7$, $\ell \geq 0$ and $n \geq 1$

1) According to Lemma 4.7 if $d^2 = 2^m 3^\ell p^n + 1$ is solvable then the prime p is of one of the following forms

$$p = 2^{m-2}3^\ell \pm 1, \;\; p = \frac{2^{m-2}+1}{3^\ell}, \text{ or } p = 17.$$

2) If $d^2 = 2^m 3^\ell + p^n$ is solvable then the prime p is of one of the following forms (see Lemma 4.9):

$$d^2 - 2^m 3^\ell, \;\; 2^{m-2}3^\ell - 1, \;\; 3^\ell - 2^{m-2}, \;\; 2^{m-2} - 3^\ell, \;\; 5, \;\; 7, \;\; 17, \text{ or } 73.$$

3) If $d^2 = 2^m 3^\ell - p^n$ is solvable then the prime p is of one of the following forms (see Lemma 4.9):

$$7, \;\; 23, \text{ or } 2^m 3^\ell - d^2.$$

4) If $d^2 = 2^m p^n + 3^\ell$ is solvable then the prime p is of one of the following forms (see Lemma 4.8):

$$2^{m-2} \pm 3^{\ell/2}, \text{ or } 5.$$

5) If $d^2 = 2^m + 3^\ell p^n$ is solvable then the prime p is of one of the following forms (see Lemma 4.10):

$$\frac{2^{m/2+1}+1}{3^\ell}, \;\; 3^\ell \pm 2^{m/2+1}, \;\; d^2 - 2^m, \;\; 7, \;\; 2^{m-2} - 1, \text{ or } 17.$$

6) If $d^2 = 2^m - 3^\ell p^n$ is solvable then the prime p is of one of the following forms (see Lemma 4.10):

$$2^{m/2+1} - 3^\ell, \;\; 2^m - d^2, \;\; 5, \text{ or } 7.$$

7) If $d^2 = 3^\ell p^n - 2^m$ is solvable then the prime p is of one of the following forms (see lemma 4.10):

$$\frac{2^{m+1}+1}{3^{\ell/2}},\ 11,\ 17,\ 19, \text{ or } \frac{d^2+2^m}{3^\ell}.$$

8) If $d^2 = 3^\ell - 2^m p^n$ is solvable then the prime p is of one of the following forms (see Lemma 4.8):

$$3^{\ell/2} - 2^{m-2}, \text{ or } 7.$$

9) If $d^2 = p^n - 2^m 3^\ell$ is solvable then the prime p is of one of the following forms (see Lemma 4.9):

$$2^{m-2}3^\ell + 1,\ 3^\ell + 2^{m-2},\ 17, \text{ or } 2^m 3^\ell + d^2.$$

10) If $3d^2 = 2^m + p^n$ is solvable then the prime p is of one of the following forms (see Lemma 4.11):

$$11, \text{ or } \ 3d^2 - 2^m.$$

11) If $3d^2 = 2^m - p^n$ is solvable then the prime p is of one of the following forms (see Lemma 4.11):

$$5, \text{ or } 2^m - 3d^2.$$

12) If $3d^2 = p^n - 2^m$ is solvable then the prime p is of the form $3d^2 + 2^m$ (see Lemma 4.11).

This proves Theorem 7.1.

7.2.2 Proof of Theorem 7.2

Again, we proceed through the cases of Theorem 7.2 (with $b = 2$) and use the lemmata of Chapter 4 to resolve the Diophantine equations that arise. In all cases, we are only concerned with solutions to the Diophantine equations with $m = 2$. In what follows, by "solvable", we mean there are solutions for which $\ell \geq 0$ and $n \geq 1$

1) If $d^2 = 4 \cdot 3^\ell + p^n$ is solvable then the prime p is of one of the following forms (see Lemma 4.9):

$$13,\ \ d^2 - 4 \cdot 3^\ell,$$

or $p^n = d^2 - 4 \cdot 3^\ell$ with $P_{\min}(n) \geq 7$.

2) If $d^2 = 4 \cdot 3^\ell - p^n$ is solvable then $n = 1$ or $P_{\min}(n) \geq 7$ (see Lemma 4.9).

3) If $d^2 = 4p^n - 3^\ell$ is solvable then $n = 1$ or $P_{\min}(n) \geq 7$ (see Lemma 4.8) and $p \equiv -1 \pmod 4$.

4) If $d^2 = p^n - 4 \cdot 3^\ell$ is solvable then either $p = 5$, $n = 1$ or $P_{\min}(n) \geq 7$ (see Lemma 4.9).

5) If $3d^2 = 4p^n - 1$ is solvable then $n \in \{1, 2\}$ (see Lemma 4.11).

6) If $3d^2 = p^n + 4$ is solvable then $n = 1$ so $p = 3d^2 - 4$ (see Lemma 4.11).

This proves Theorem 7.2.

7.2.3 Proof of Theorem 7.3

Again, we proceed through the cases of Theorem 7.3 (with $b = 2$) and use the Diophantine lemmata. In all cases, we are only concerned with solutions to the Diophantine equations with $m = 2, 4, 5$. So, by "solvable", we mean there are solutions for which $m \in \{4, 5\}$, $\ell \geq 0$ and $n \geq 1$

1) If $d^2 = 2^m 3^\ell p^n + 1$ is solvable then the prime p is of one of the following forms (see Lemma 4.7):

$$2^{m-2}3^\ell \pm 1, \quad \frac{3^\ell + 1}{4}, \text{ or } 5.$$

2) If $d^2 = 4 \cdot 3^\ell + p^n$ is solvable with ℓ even then the prime p is of the form $p^n = d^2 - 4 \cdot 3^\ell$ with $n = 1$ or $P_{\min}(n) \geq 7$ (see Lemma 4.9).

3) If $d^2 = 2^m 3^\ell + p^n$ is solvable then the prime p is of one of the following forms (see Lemma 4.9):

$$d^2 - 2^m 3^\ell, \quad 2^{m-2}3^\ell - 1, \quad 3^\ell - 2^{m-2}, \quad 2^{m-2} - 3^\ell.$$

or $p^n = d^2 - 2^m 3^\ell$ with $P_{\min}(n) \geq 7$.

4) If $d^2 = 4 \cdot 3^\ell - p^n$ is solvable with ℓ even then $n = 1$ or $P_{\min}(n) \geq 7$ (see Lemma 4.9).

5) If $d^2 = 2^m 3^\ell - p^n$ is solvable then one of the following must hold: $p = 47$, $n = 1$ or $P_{\min}(n) \geq 7$ (see Lemma 4.9) .

6) If $d^2 = 2^m p^n + 3^\ell$ is solvable then the prime p is of one of the following forms (see Lemma 4.9):

$$\frac{3^{\ell/2} + 1}{4}, \quad 2^{m-2} + 3^{\ell/2}, \quad 5, \text{ or } 7.$$

7) If $d^2 = 4p^n - 3^\ell$ with $p \equiv 1 \pmod 4$ is solvable then the prime p is of the form $\frac{3^\ell+1}{4}$ or $n = 1$ or $P_{\min}(n) \geq 7$ (see Lemma 4.8).

8) If $d^2 = 4 + 3^\ell p^n$ is solvable then the prime p is of one of the following forms (see Lemma 4.10):

$$5 \text{ or } \frac{3^\ell \pm 1}{4}.$$

9) If $d^2 = 2^m + 3^\ell p^n$ is solvable then the prime p is of one of the following forms (see Lemma 4.10):

$$d^2 - 32, \;\; 3^\ell \pm 8, \text{ or } 7.$$

10) If $d^2 = 2^m - 3^\ell p^n$ is solvable then the prime p is of one of 5, 7, 23, or 31.

11) If $d^2 = 3^\ell p^n - 2^m$ is solvable then the prime p is of one of the following forms (see Lemma 4.10):

$$\frac{2^{m-1}+1}{3^{\ell/2}}, \;\; 5, \;\; 67,$$

or $n = 1$ or $P_{\min}(n) \geq 7$.

12) If $d^2 = 3^\ell - 2^m p^n$ is solvable then the prime p is of the form $3^{\ell/2} - 2^{m-2}$ (see Lemma 4.8).

13) If $d^2 = 4p^n - 3^\ell$, with ℓ odd, is solvable then $p = 13$ or $n = 1$ or $P_{\min}(n) \geq 7$ (see Lemma 4.8).

14) If $d^2 = p^n - 2^m 3^\ell$ is solvable then the prime p is of one of the following forms (see Lemma 4.9):

$$2^{m-2}3^\ell + 1, \;\; 3^\ell + 2^{m-2}, \;\; 72, \;\; 193, \;\; 1153, \;\; 5,$$

or $n = 1$ or $P_{\min}(n) \geq 7$.

15) If $3d^2 = 2^m + p^n$ is solvable then $n = 1$ and so $p = 3d^2 - 2^m$ (see Lemma 4.11).

16) If $3d^2 = 2^m + p^n$ is solvable p is either 5, 13 or 29 (see Lemma 4.11).

17) If $3d^2 = 4p^n - 1$ is solvable then $n \in \{1, 2\}$ so $p = \frac{3d^2+1}{4}$ or $p^2 = \frac{3d^2+1}{4}$ (see Lemma 4.11).

18) If $3d^2 = p^n - 4$ is solvable then $n = 1$ so $p = 3d^2 + 4$ (see Lemma 4.11).

19) If $3d^2 = p^n - 2^m$ is solvable then $n = 1$ so $p = 3d^2 + 16$ or $p = 3d^2 + 32$ (see Lemma 4.11).

This proves Theorem 7.3.

7.2.4 Proof of Corollary 7.4

We show that all the primes appearing in Theorems 7.1, 7.2 and 7.3 satisfy at least one of

$$p \not\equiv 5 \pmod 8, \;\; p \not\equiv 2 \pmod 3, \;\; p \not\equiv 2 \pmod 5, \text{ or } p \not\equiv 6 \text{ and } 11 \pmod{17} \tag{7.1}$$

This will prove the corollary.

Theorem 7.1: Certainly the primes in (1) satisfy (7.1). Primes of the form (2) satisfy $p \equiv \pm 1 \pmod 8$ and primes of the form (3), (4) or (5) satisfy $p \equiv 1$ or $3 \pmod 8$. Primes of the form (7) or (8) satisfy $p \equiv 1 \pmod 8$ and primes of the form (9) satisfy $p \equiv -1 \pmod 8$. Primes of the form (10) satisfy $p \equiv 1$ or $3 \pmod 8$ and primes of the form (11) or (12) satisfy satisfy $p \equiv 3 \pmod 8$. All that remains is to consider primes of the form (6) and (13) and show they satisfy at least one of the congruences in 7.1.

Suppose p is a prime of the form $p = 2^{m-2} - 3^\ell$ with $m \geq 7$ and $\ell \geq 1$. If m and ℓ are both even then p is a difference of squares from which we find $p = 7$. If m is even and ℓ is odd then $p \equiv 1 \pmod 3$ and $p \equiv 1 \pmod 4$. If m is odd and ℓ is even then $p \equiv 2 \pmod 3$ and $p \equiv -1 \pmod 4$. If m and ℓ both odd then $p \equiv 2 \pmod 3$ and $p \equiv 5 \pmod 8$ so we need to consider the congruence class of p modulo 5, which is as follows:

$$\begin{aligned}
&\text{if } m-2 \equiv 1 \pmod 4, \ell \equiv 1 \pmod 4 \text{ then } p \equiv 2-3 \equiv -1 \pmod 5;\\
&\text{if } m-2 \equiv 1 \pmod 4, \ell \equiv 3 \pmod 4 \text{ then } p \equiv 2-2 \equiv 0 \pmod 5;\\
&\text{if } m-2 \equiv 3 \pmod 4, \ell \equiv 1 \pmod 4 \text{ then } p \equiv 3-3 \equiv 0 \pmod 5;\\
&\text{if } m-2 \equiv 3 \pmod 4, \ell \equiv 3 \pmod 4 \text{ then } p \equiv 3-2 \equiv 1 \pmod 5.
\end{aligned}$$

Thus, p of the form (6) satisfies one of the congruences in 7.1.

Suppose p is a prime of the form $p = 2^m - 3d^2$ with $m \geq 7$. Modulo 3 we have

$$p \equiv \begin{cases} 1 \pmod 3 & \text{if } m \text{ is even,} \\ 2 \pmod 3 & \text{if } m \text{ is odd.} \end{cases}$$

So, assume m is odd. In this case we have

$$p \equiv \begin{cases} 3 \pmod 5 & \text{if } m \equiv 3 \pmod 4 \text{ and } d^2 \equiv 0 \pmod 5, \\ 0 \pmod 5 & \text{if } m \equiv 3 \pmod 4 \text{ and } d^2 \equiv 1 \pmod 5, \\ 0 \pmod 5 & \text{if } m \equiv 3 \pmod 4 \text{ and } d^2 \equiv 4 \pmod 5, \\ 2 \pmod 5 & \text{if } m \equiv 1 \pmod 4 \text{ and } d^2 \equiv 0 \pmod 5, \\ 4 \pmod 5 & \text{if } m \equiv 1 \pmod 4 \text{ and } d^2 \equiv 1 \pmod 5, \\ 4 \pmod 5 & \text{if } m \equiv 1 \pmod 4 \text{ and } d^2 \equiv 4 \pmod 5, \end{cases}$$

Thus, the only trouble seems to occur when $m \equiv 1 \pmod 4$ and $5 \mid d$, In this case the prime is of the form

$$p = 2^m - 75k^2 \quad \text{with } m \equiv 1 \pmod 4. \tag{7.2}$$

Some primes of this form are as follows

$$4517, 6317, 7517, 8117, 91397, 103997, 109397, 1760477,$$

$$1818077, 1994477, 2042477, 33197357, 536675837.$$

This is not even close to being a complete list of such primes up to 54×10^7 however we chose this collection of primes since their reductions hit every congruence class modulo 7, 11 and 13. This means, to characterize such primes locally, we have to go as far as 17. We will show for p of the form (7.2) that $p \not\equiv 6 \pmod{17}$.

In the multiplicative group $U(\mathbb{Z}/17\mathbb{Z})$ the element 2 is of order 8, and the quadratic residues are $\{0, 1, 2, 4, 8, 9, 13, 15, 16\}$. Since $m \equiv 1 \pmod 4$ and 2 has order 8 in $U(\mathbb{Z}/17\mathbb{Z})$, we consider the two case, $m \equiv 1 \pmod 8$ and $m \equiv 5 \pmod 8$, separately. Considering each possible quadratic residue in turn we have

$$p = 2^m - 75k^2 \equiv \begin{cases} 2, 12, 5, 8, 14, 7, 13, 16, \text{ or } 9 \pmod{17} & \text{if } m \equiv 1 \pmod 8, \\ 15, 8, 1, 4, 10, 3, 9, 12, \text{ or } 5 \pmod{17} & \text{if } m \equiv 5 \pmod 8, \end{cases}$$

Thus, for $p = 2^m - 3d^2$ with $m \equiv 1 \pmod 4$ and $5 \mid d$ we have $p \not\equiv 6$ and $11 \pmod{17}$.

This proves the corollary for the primes appearing in Theorem 7.1.

Theorem 7.2: If p is of the form (2), (3) or (5) then $p \equiv 1 \pmod 3$. If p is of the form (4) then $p \equiv 3 \pmod 8$. If p is of the form (6) then $p \equiv 1 \pmod 3$; for $n = 1$ this is clear, whereas for $n = 2$ we factor as $(2p+1)(2p-1) = 3d^2$ to obtain $4p = 3d_1^2 + d_2^2 \equiv 1 \pmod 3$, where $d - d_1 d_2$. Finally, if p is of the form (7) then $p \equiv -1 \pmod 8$. Therefore, the curves of conductor $36p$ have $p = 5$ or $p \equiv 1 \pmod 3$ or $p \equiv -1$ or $3 \pmod 8$.

Theorem 7.3: It is easy to check that the result holds for primes in (1). If p is of the form (2), (3), (4), (10), (15) or (16) then $p \equiv 1 \pmod 3$. If p is of the form (5), (13), (14), (17) or (18) then $p \equiv -1 \pmod 4$. If p is of the form (7) or (8) then $p \equiv 1 \pmod 8$. If p is of the form (6) then if $\ell = 0$ we have $p = 5$ or 7, else if $\ell \geq 1$ then $p \equiv 1 \pmod 3$ or $p \equiv -1 \pmod 4$ depending on whether the sign is positive or negative. If p is of the form (9) then $p \equiv -1 \pmod 8$. If p is of the form (11) then $p \equiv 1 \pmod 3$ if the sign is positive, whereas if the sign is negative then $p \equiv -1 \pmod 4$ for ℓ odd and $p = 5$ or 17 for ℓ even. Finally, If p is of the form (12) then $p \equiv 1$ or $3 \pmod 8$. Therefore, the curves of conductor $2^3 3^2 p$ satisfy one of the following $p = 5$, $p = 29$, $p \equiv 1 \pmod 3$, or $p \equiv \pm 1$ or $3 \pmod 8$.

7.2.5 Proof of Lemma 7.5

We list the primes appearing in (7.1), (7.2), and (7.3) (except $p^n = \frac{d^2+2^m}{3^\ell}$) in the following table. Unless otherwise stated $\ell \geq 0$.

p	conditions	p	conditions
$2^{m-2}3^\ell \pm 1$	$m = 4, 5$ or ≥ 7	$\pm(d^2 - 4 \cdot 3^\ell)$	ℓ odd
$\frac{2^{m-2}+1}{3^\ell}$	$m = 5$ or ≥ 7	$p^n = \pm(d^2 - 4 \cdot 3^\ell)$	$n = 1$ or $P_{\min}(n) \geq 7$, ℓ even
$\pm(2^{m-2} - 3^\ell)$	$m = 4, 5$ or ≥ 7, $\ell \geq 4$	$p^n = d^2 + 4 \cdot 3^\ell$	$n = 1$ or $P_{\min}(n) \geq 7$
$2^{m-2} + 3^\ell$	$m = 4, 5$ or ≥ 7	$p^n = \frac{d^2+3^\ell}{4}$	$n = 1$ or $P_{\min}(n) \geq 7$, ℓ odd
$\pm(d^2 - 2^m 3^\ell)$	$m \geq 7$	$p^n = \frac{3d^2+1}{4}$	$n = 1$ or 2
$d^2 + 2^m 3^\ell$	$m \geq 7$	$p^n = d^2 \pm 2^m \cdot 3^\ell$	$n = 1$ or $P_{\min}(n) \geq 7$ $m = 4, 5$
$\pm(3d^2 - 2^m)$	$m = 4, 5$, or ≥ 7	$p^n = 2^m 3^\ell - d^2$	$n = 1$ or $P_{\min}(n) \geq 7$ $m = 4, 5$
$3d^2 + 2^m$	$m = 2, 4, 5$, or ≥ 7		
$\frac{3^\ell+1}{4}$	ℓ odd		
$3d^2 - 4$			

We are interested in counting the number of primes of each of these forms up to X. First we observe that for the forms in the second column there are only finitely many primes satisfying the conditions with $P_{\min}(n) \geq 7$. Indeed, if p, ℓ, m, n, d satisfy one of the equations then Shorey and Tijdeman ([68], page 180) implies that n is bounded by a constant, and Darmon and Granville ([27], Theorem 2) implies there are only finitely many solutions for p, ℓ, m, n, d.

From now on, we only consider the case when $n = 1$. This just ignores some finite (density zero) collection of primes. Also, we will just bound the number of integers of each form listed in the table. This will then bound the number of primes as well. If $\eta(X)$ is an upper bound on the number of integers up to X satisfying one of the forms in the table then we want to show $\eta(X)$ is "little-Oh" of $\pi(X)$; denoted $\eta(X) = o(\pi(X))$. Here $\pi(X)$ denotes the number of primes up to X and $\eta(X) = o(\pi(X))$ means $\lim_{X\to\infty} \frac{\eta(X)}{\pi(X)} = 0$.

1) If $2^{m-2}3^\ell \pm 1 \leq X$ then $m, \ell \leq c \log X$ for a fixed constant c (i.e. $c = 2$ works). So there are at most $\eta_1(X) = c^2 \log^2 X = o(\pi(X))$ such integers.

2) If $\frac{2^{m-2}+1}{3^\ell}$ is an integer then $2^{m-2} \equiv -1 \pmod{3^\ell}$. It follows that the order of 2 modulo 3^ℓ, which is $2 \cdot 3^{\ell-1}$, must divide $2(m-2)$. Thus, $3^{\ell-1} | m-2$, hence $\ell \leq c \log m$ for a fixed constant c. Now if $\frac{2^{m-2}+1}{3^\ell} \leq X$ then $m \leq c_1 \log^2 X$ for

some constant c_1. The number of integers of this form is bounded by $\eta_2(X) = (c_1 \log X)(c \log(c_1 \log X)) = o(\pi(X))$.

3) If $\pm(2^{m-2} - 3^\ell)$ is an integer such that $|2^{m-2} - 3^\ell| \leq X$, it follows from a result of Ellison that $m \leq c \log X$ for some fixed constant c. Thus,

$$\ell \leq \begin{cases} \dfrac{\log(X + 2^{c \log X})}{\log 3} & \text{if } 2^{m-2} - 3^\ell \leq 0 \\ c_2 \log X & \text{if } 2^{m-2} - 3^\ell \geq 0 \end{cases},$$

for some fixed constant c_2. Therefore, the number of primes of this form up to X is bounded above by

$$\eta_3(X) \leq \begin{cases} c \log X \dfrac{\log(X + 2^{c \log X})}{\log 3} & \text{if } 2^{m-2} - 3^\ell \leq 0, \\ c_3 \log^2 X & \text{if } 2^{m-2} - 3^\ell \geq 0, \end{cases}$$

where C_3 is some fixed constant. Thus, $\eta_3(X) = o(\pi(X))$.

4) If $2^{m-2} + 3^\ell \leq X$ then $m, \ell \leq c \log X$ for some fixed constant c. Thus, the number of primes of this form up to X is $\eta_4(X) \leq c^2 \log^2 X = o(\pi(X))$.

5) Consider the set of primes of the form $p = |d^2 - 2^m 3^\ell|$ up to X. If m and ℓ are even then factor to obtain

$$p = |d + 2^{m/2} 3^{\ell/2}| \cdot |d - 2^{m/2} 3^{\ell/2}|.$$

It follows that $p = d + 2^{m/2} 3^{\ell/2}$ and $1 = |d - 2^{m/2} 3^{\ell/2}|$. Eliminate d to obtain $p = 2^{m/2+1} 3^{\ell/2} \pm 1$. Thus, $m, \ell \leq c \log X$ for some constant c, and the number of primes of this form is $o(\pi(X))$.

Now suppose m odd and ℓ even; $m = 2m_0 + 1$, $\ell = 2\ell_0$. Factoring over $\mathbb{Z}[\sqrt{2}]$ gives

$$p = |d - 2^{m_0} 3^{\ell_0} \sqrt{2}||d + 2^{m_0} 3^{\ell_0} \sqrt{2}| \leq X.$$

Let $\epsilon = |\sqrt{2} - \frac{d}{2^{m_0} 3^{\ell_0}}|$ and $F = |d + 2^{m_0} 3^{\ell_0} \sqrt{2}|$. The equation can be written as

$$2^{m_0} 3^{\ell_0} \epsilon F \leq X. \tag{7.3}$$

According to Ridout [62], ϵ cannot be too small,

$$\epsilon = \left| \sqrt{2} - \frac{d}{2^{m_0} 3^{\ell_0}} \right| \tilde{\geq} \frac{1}{(2^{m_0} 3^{\ell_0})^{1+\delta}},$$

for any $\delta > 0$, where $\tilde{\geq}$ means "except for finitely many m_0 and n_0" (independent of X). From (7.3) it follows that

$$\frac{F}{(2^{m_0}3^{\ell_0})^\delta} \tilde{\leq} X,$$

that is,

$$\left| \frac{d}{(2^{m_0}3^{\ell_0})^\delta} + \sqrt{2}(2^{m_0}3^{\ell_0})^{1-\delta} \right| \tilde{\leq} X.$$

This implies

$$(2^{m_0}3^{\ell_0})^{1-\delta} \tilde{\leq} X,$$

and so,

$$2^{m_0}3^{\ell_0} \tilde{\leq} X^{1+\delta_1},$$

where δ_1 satisfies $(1-\delta)(1+\delta_1) = 1$. Therefore,

$$2^m 3^\ell \tilde{\leq} X^{2+\delta_2}$$

where $\delta_2 = 2\delta_1$, whence

$$m, \ell \leq c \log X$$

for some fixed constant c.

It now remains to bound d as a function of X. For this, we consider two cases: (i) $2^m 3^\ell \leq X^{2-\delta_2}$, (ii) $X^{2-\delta_2} \leq 2^m 3^\ell \leq X^{2+\delta_2}$. In the first case, it follows directly from $|d^2 - 2^m 3^\ell| \leq X$ that

$$d < cX^{1-\delta_2/2}.$$

In the second case, if d is large, say $d \geq d_0 := [\sqrt{2^m 3^\ell}] + 1$, write $d = d_0 + k$. Then $|d^2 - 2^m 3^\ell| \leq X$ becomes

$$|d_0^2 - 2^m 3^\ell + 2d_0 k + k^2| \leq X,$$

from which it follows that

$$2d_0 k + k^2 \leq X.$$

But $2d_0 \geq X^{1-\delta_2/2}$ so $k \leq X^{\delta_2/2}$. Thus, the number of primes of the form $|d^2 - 2^m 3^\ell|$ up to X is bounded above by

$$\max(X^{\delta_2/2} \log^2 X, X^{1-\delta_2/2} \log^2 X = o(\pi(X)).$$

A similar argument works in the case when m is even, ℓ is odd, and in the case when both m and ℓ are odd. Here, we would apply Ridout's Theorem for the algebraic numbers $\sqrt{3}$ and $\sqrt{6}$ to get the same bound on m and ℓ as above.

6) If $d^2 + 2^m 3^\ell \leq X$ then $m, \ell \leq c \log X$ and $d \leq \sqrt{X}$ thus the number of primes of this form, $\eta_6(X)$, satisfies

$$\eta_6(X) \leq c\sqrt{X} \log^2 X = o(\pi(X)).$$

7) A similar argument as to the one used in (5) shows that the number of primes of the form $3d^2 \pm 2^m$, up to X, is of order $o(\pi(X))$.

8) If $3d^2 + 2^m \leq X$ then $m \leq c_1 \log X$ and $d \leq c_2\sqrt{X}$, for some fixed constants c_1 and c_2, thus the number of primes of this form, $\eta_8(X)$, satisfies

$$\eta_8(X) \leq c\sqrt{X} \log^2 X = o(\pi(X)).$$

9) If $\frac{3^\ell + 1}{4} \leq X$ then $\ell \leq c \log X$ hence the number of such primes is of order $o(\pi(X))$.

10) The number of primes of the form $3d^2 - 4$ up to X is bounded by $c\sqrt{X}$ and hence of order $o(\pi(X))$.

11) The argument in (5) shows that the number of primes of the form $|d^2 - 4 \cdot 3^\ell|$ is of order $o(\pi(X))$.

For the rest of the forms in the table we can assume that $n = 1$, as we stated at the beginning of the proof. It is then easy to see that the number primes satisfying these conditions are of order $o(\pi(X))$, since may forms reduce to the ones considered above.

This completes the proof of Lemma 7.5.

Chapter 8

On the equation $x^n + y^n = 2^\alpha p z^2$

In this chapter, we show, if p is prime, that the equation $x^n + y^n = 2pz^2$ has no solutions in coprime integers x and y with $|xy| \geq 1$ and $n > p^{132p^2}$, and if $p \neq 7$, the equation $x^n + y^n = pz^2$ has no solutions in coprime integers x and y with $|xy| \geq 1$, z even, and $n > p^{12p^2}$. A modified version of the contents of this chapter has been published [4].

8.1 Introduction

Inspired by the work of Wiles [Wi95] and subsequently that of Breuil, Conrad, Diamond and Taylor [BCDT01], there has been a great amount of research centered around applying techniques from modular forms and Galois representations to Diophantine equations of the form

$$Ax^p + By^q = Cz^r, \tag{8.1}$$

for p, q and r positive integers with $1/p + 1/q + 1/r < 1$.

We briefly outlined in Section 1.2 some of the more notable works in this area. The reader is directed to [45] for a survey,

In this chapter we study the insolubility of

$$x^n + y^n = 2^\alpha p z^2, \tag{8.2}$$

in coprime integers (x, y, z), for $\alpha \in \{0, 1\}$. We use the approach of [BVY04], though here we will need a classification of elliptic curves over $\mathbb{Q}$ with rational 2-torsion and conductor $2^\alpha p^2$. In the case when $p = 2$ or 3 it is shown in [BS04] that the only solution in nonzero pairwise coprime integers (x, y, z) is

$(p, \alpha, x, y, z, n) = (2, 0, 3, -1, \pm 11, 5)$. Thus, in this chapter, we may take p to be a prime ≥ 5.

Our main results are as follows:

Theorem 8.1 *If n an odd prime and $p \geq 5$ a prime ($p \neq 7$), then the Diophantine equation*

$$x^n + y^n = pz^2$$

has no solutions in coprime integers x, y and z with $|xy| > 1$, z even, and $n > p^{12p^2}$.

Theorem 8.2 *If n an odd prime and $p \geq 5$ a prime then the Diophantine equation*

$$x^n + y^n = 2pz^2$$

has no solutions in coprime integers x, y and z with $|xy| > 1$ and $n > p^{132p^2}$.

An immediate corollary of these theorems is:

Corollary 8.3 *If $p \geq 5$ is a prime, then*

i) if $p \neq 7$ the Diophantine equation

$$x^n + y^n = pz^2$$

has at most finitely many solutions in integers x, y, z, α, and n with x and y coprime, $|xy| > 1$, z even and n divisible by an odd prime.

ii) the Diophantine equation

$$x^n + y^n = 2pz^2$$

at most finitely many solutions in integers x, y, z, α, and n with x and y coprime, $|xy| > 1$ and n divisible by an odd prime.

8.2 Elliptic Curves

We always assume that n is an odd prime and (a, b, c) is an integral solution to (8.2) where $\alpha \in \{0, 1\}$, $|ab| > 1$. In the case that $\alpha = 0$ we further assume

that $c \equiv 0 \pmod 2$. As in [5] we associate to the solution (a, b, c) an elliptic curve

$$E_\alpha(a, b, c) : Y^2 = X^3 + 2^{\alpha+1} cpX^2 + 2^\alpha pb^n X.$$

The following lemma, which follows from [BS04] Lemma 2.1 and corollary 2.2, summarizes some useful facts about these curves.

Lemma 8.4 *Let $\alpha = 0$ or 1.*

(a) *The discriminant $\Delta(E)$ of the curve $E = E_\alpha(a, b, c)$ is given by*

$$\Delta(E) = 2^{3\alpha+6} p^3 (ab^2)^n.$$

(b) *The conductor $N(E)$ of the curve $E = E_\alpha(a, b, c)$ is given by*

$$N(E) = 2^{3\alpha+5} p^2 \prod_{q|ab} q.$$

In particular, E has multiplicative reduction at each odd prime p dividing ab.

(c) *The curve $E_\alpha(a, b, c)$ has a $\mathbb{Q}$-rational point of order 2, namely $(0, 0)$.*

(d) *The curve $E_\alpha(a, b, c)$ obtains good reduction over $\mathbb{Q}(\sqrt[4]{2^\alpha p})$ at all primes ideals dividing p. Over any quadratic field K, the curve $E_\alpha(a, b, c)$ has bad reduction at all prime ideals dividing p.*

(e) *If $n \geq 7$ is prime and ab is divisible by an odd prime q, then the j-invariant $j(E)$ of the curve $E = E_\alpha(a, b, c)$ satisfies*

$$ord_q(j(E)) < 0.$$

In particular, if $ab \neq \pm 1$ then $E_\alpha(a, b, c)$ does not have complex multiplication.

8.3 Outline of the Proof of the main theorems

To the elliptic curve $E_\alpha(a, b, c)$ we will associate a weight 2 cuspidal newform f of level $32p^2$ (if $\alpha = 0$) or $256p^2$ (if $\alpha = 1$). This is done in section 8.4. Let $\{c_i\}_{i=1}^\infty$ be the Fourier coefficients of f and K_f their field of definition. We will refer to $[K_f : \mathbb{Q}]$ as the *dimension* of f.

If f has dimension ≥ 2 then $c_\ell \notin \mathbb{Q}$ for some ℓ. We will see that n must divide $Norm_{K_f/\mathbb{Q}}(c_\ell - a_\ell)$, for some $a_\ell \in \mathbb{Z}$ such that $|a_\ell| \leq \ell + 1$ (Proposition

8.6). This gives a bound on n in terms of ℓ. The question then arises: How small can ℓ be? That is, how far must we go to find a coefficient c_i which reveals f is not of dimension 1? This is answered by a proposition of Kraus (see Proposition 8.11), from which we derive our *big* bound on n in the main theorem.

Now suppose f is of dimension 1, that is $c_i \in \mathbb{Z}$ for all i. We again have that n must divide $Norm_{K_f/\mathbb{Q}}(c_i - a_i)$. It may happen that c_i and a_i are equal from which we derive no information on n. However, the a_i are all even so in the case that one of the c_i's is odd, say c_ℓ, we are able to obtain a bound on n in terms of ℓ. Again, the question arises of how small ℓ can be. This question is answered by another proposition of Kraus (see Proposition 8.12). The bound on n we receive in this case is much smaller than the one we obtained above. The only case that remains now is when all the coefficients c_i are even rational integers. In this case f corresponds to an elliptic curve F over $\mathbb{Q}$ with rational 2-torsion and conductor $32p^2$ or $256p^2$. By Lemma 8.4 (d) $E_\alpha(a, b, c)$ has potentially good reduction at p, we will see (Proposition 8.7) that this implies F has potentially good reduction at p, i.e. p does not divide the denominator of $j(F)$. Also, by Lemma 8.4 (e) $E_\alpha(a, b, c)$ does not have CM, we will see (Proposition 8.7) that if F has CM then we obtain a bound on n of 13. Thus, if F is an elliptic curve over $\mathbb{Q}$ with rational 2-torsion, conductor $32p^2$ or $256p^2$, potentially good reduction at p and without CM we will not be able to derive any information on n. The question then arises; Are there any such elliptic curves? This question is answered Section 8.6.

8.4 Galois Representations and Modular Forms

In this section we describe how to associate to the elliptic curve $E_\alpha(a, b, c)$ a weight 2 modular form.

Let $E = E_\alpha(a, b, c)$ for some primitive solution (a, b, c) to (8.2). We associate to the elliptic curves E a Galois representation

$$\rho_n^E : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_n),$$

the representation of $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the n-torsion points $E[n]$ of the elliptic curve E. If $n \geq 7$ and $ab \neq 1$ then ρ_n^E is absolutely irreducible (see [BS04] Corollary 3.1).

Let $\overline{\mathbb{F}_n}$ be an algebraic closure of the finite field $\mathbb{F}_n$ and ν be any prime of $\overline{\mathbb{Q}}$ extending n. To a holomorphic newform f of weight $k \geq 1$ and level N, we associate a continuous, semisimple representation

$$\rho_{f,\nu} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_n)$$

unramified outside of Nn and satisfying, if $f(z) = \sum_{n=1}^{\infty} c_n q^n$ for $q := e^{2\pi i z}$,

$$\mathrm{trace}\rho_{f,\nu}(\mathrm{Frob}_p) \equiv c_p \pmod{\nu}$$

for all p coprime to Nn. Here, Frob_p is a Frobenius element at the prime p.

If the representation ρ_n^E, after extending scalars to $\overline{\mathbb{F}_n}$, is equivalent to $\rho_{f,\nu}$, for some newform f, then we say that ρ_n^E is modular, arising from f.

The next lemma follows from [5] Lemma 3.3.

Lemma 8.5 *Suppose that $n \geq 7$ is a prime and that ρ_n^E is associated to a primitive solution (a, b, c) to (8.2) with $ab \neq \pm 1$. Put*

$$N_n(E) = \begin{cases} 32p^2 & \alpha = 0, \\ 256p^2 & \alpha = 1. \end{cases}$$

The representation ρ_n^E arises from a cuspidal newform of weight 2, level $N_n(E)$, and trivial Nebentypus character.

This lemma says that we can associate to the elliptic curve $E = E_\alpha(a, b, c)$ a weight 2 modular form of level $32p^2$ (if $\alpha = 0$) or $256p^2$ (if $\alpha = 1$).

8.5 Useful Propositions

In this section we collect together some results concerning the newforms of level $N_n(E)$ from which our representation ρ_n^E can arise. The proofs of these propositions can be found in [5]. The first proposition gives a relationship between n and the coefficients of the newform. We will use this result to obtain the bounds on n in the main theorem.

Proposition 8.6 *Suppose $n \geq 7$ is a prime and $E = E_i(a, b, c)$ is a curve associated to a primitive solution of (8.2) with $ab \neq \pm 1$. Suppose further that*

$$f = \sum_{m=1}^{\infty} c_m q^m \quad (q := e^{2\pi i z})$$

is a newform of weight 2 and level $N_n(E)$ giving rise to ρ_n^E and that K_f is a number field containing the Fourier coefficients of f. If q is a prime, coprime to $2pn$, then n divides one of either

$$Norm_{K_f/\mathbb{Q}}\,(c_q \pm (q+1))$$

or

$$Norm_{K_f/\mathbb{Q}}(c_q \pm 2r),$$

for some integer $r \leq \sqrt{q}$.

In the case when the space of cuspforms of level $N_n(E)$ contains newforms associated to elliptic curves with rational 2-torsion we will find the following result useful.

Proposition 8.7 *Suppose $n \neq p$ is an odd prime and $E = E_\alpha(a,b,c)$ is a curve associated to a primitive solution of (8.2). Suppose also that E' is another elliptic curve defined over $\mathbb{Q}$ such that $\rho_n^E \cong \rho_n^{E'}$. Then the denominator of the j-invariant $j(E')$ is not divisible by p.*

Finally, in the case when the space of cuspforms of level $N_n(E)$ contains newforms associated to elliptic curves with rational 2-torsion and CM we will need the following result.

Proposition 8.8 *Suppose $n \geq 7$ is a prime and $E = E_i(a,b,c)$ is a curve associated to a primitive solution of (8.2) with $ab \neq \pm 1$. Suppose that ρ_n^E arises from a newform having CM by an imaginary quadratic field K. Then one of the following holds:*

(a) *$ab = \pm 2^r$, $r > 0$, $2 \nmid ABC$ and 2 splits in K.*

(b) *$n = 7$ or 13, n splits in K and either $E(K)$ has infinite order for all elliptic curves of conductor $2n$ or $ab = \pm 2^r 3^s$ with $s > 0$ and 3 ramifies in K.*

8.6 Elliptic curves with rational 2-torsion

It is possible that the modular form associated to $E = E_\alpha(a,b,c)$ has rational integer coefficients in which case the results of the previous section will not help in eliminating the existence of such a form. In this case however, the modular form must correspond to an isogeny class of elliptic curves over $\mathbb{Q}$ with 2-torsion and conductor equal to the level of the modular form: $32p^2$

or $256p^2$. We use the classification of such elliptic curves found in Chapter 6. We restate the relevant results (Corollaries 6.10 and 6.11) of Chapter 6 in the following two propositions.

Proposition 8.9 *Suppose $p \geq 5$ is prime and that $E/\mathbb{Q}$ is an elliptic curve with a rational 2-torsion point and conductor $32p^2$. Then E is isogenous over $\mathbb{Q}$ to a curve of the form*

$$y^2 = x^3 + a_2x^2 + a_4x$$

with coefficients given in the following table.

p	a_2	a_4	*j-invariant*
any	0	$-p^2$	1728
any	0	$(-1)^{(p+1)/2}p$	1728
any	0	$(-1)^{(p+1)/2}p^3$	1728
7	± 7	$2 \cdot 7^2$	$8000/7$
7	± 7	$2 \cdot 7$	-2^6
7	$\pm 7^2$	$2 \cdot 7^3$	-2^6
$s^2 + 1,\ s \in \mathbb{Z}$	$2ps$	$-p^2$	$\frac{64(4p-1)^3}{p}$
$s^2 + 8,\ s \in \mathbb{Z}$	ps	$-2p^2$	$\frac{64(p-2)^3}{p}$
$s^2 - 8,\ s \in \mathbb{Z}$	ps	$2p^2$	$\frac{64(p+2)^3}{p}$

Proposition 8.10 *Suppose $p \geq 5$ is prime and that $E/\mathbb{Q}$ is an elliptic curve with a rational 2-torsion point and conductor $256p^2$. Then E is isogenous over $\mathbb{Q}$ to a curve of the form*

$$y^2 = x^3 + a_2x^2 + a_4x$$

with coefficients given in the following table.

p	a_2	a_4	*j-invariant*
any	0	$\pm 2p$	1728
any	0	$\pm 2p^2$	1728
any	0	$\pm 2p^3$	1728
any	$\pm 4p$	$2p^2$	$2^6 5^3$
23	$\pm 2^3 \cdot 23 \cdot 39$	$2 \cdot 23^5$	$\frac{2^6 3^3 4057^3}{23^6}$
23	$\pm 2^4 \cdot 23 \cdot 39$	$2^3 \cdot 23^5$	$\frac{2^6 3^3 4057^3}{23^6}$
$2s^2+1,\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^3$	$\frac{-64(p-4)^3}{p^2}$
$2s^2+1,\ s \in \mathbb{Z}$	$\pm 4ps$	$-2p^2$	$\frac{64(4p-1)^3}{p}$
$\sqrt{2s^2+1},\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^4$	$\frac{64(p^2-4)^3}{p^4}$
$\sqrt{2s^2+1},\ s \in \mathbb{Z}$	$\pm 4ps$	$-2p^2$	$\frac{64(4p^2-1)^3}{p^2}$
$2s^2-1,\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^3$	$\frac{64(p+4)^3}{p^2}$
$2s^2-1,\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^2$	$\frac{64(4p+1)^3}{p}$
$\sqrt{2s^2-1},\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^4$	$\frac{64(p^2+4)^3}{p^4}$
$\sqrt{2s^2-1},\ s \in \mathbb{Z}$	$\pm 4ps$	$2p^2$	$\frac{64(4p^2+1)^3}{p^2}$

The main feature of these propositions we will use is that an elliptic curve $E/\mathbb{Q}$ with rational 2-torsion and conductor $32p^2$ or $256p^2$ either has CM or p dividing the denominator of $j(E)$, with one exception: there are curves of conductor $32p^2$ when $p = 7$ without CM and potentially good reduction at p, namely

$$y^2 = x^3 \pm 7x^2 + 14x \text{ and } y^2 = x^3 \pm 49x^2 + 686x.$$

It is the presence of these curves which prevents us from extending the results of Theorem 8.1 to include $p = 7$.

8.7 Theorems 8.1 and 8.2

To prove Theorems 8.1 and 8.2, we will combine Propositions 8.9 and 8.10 with a result of Kraus (Lemma 1 of [43]) and the proposition of Appendice II of Kraus and Oesterlé [46] (regarding this last assertion, note the comments in the Appendice of [43]). We define

$$\mu(N) = N \prod_{l|N} \left(1 + \frac{1}{l}\right),$$

where the product is over prime l.

Proposition 8.11 *(Kraus) Let N be a positive integer and $f = \sum_{n\geq 1} c_n q^n$ be a weight 2, level N newform, normalized so that $c_1 = 1$. Suppose that for every prime p with $(p, N) = 1$ and $p \leq \mu(N)/6$ we have $c_p \in \mathbb{Z}$. Then we may conclude that $c_n \in \mathbb{Z}$ for all $n \geq 1$.*

Proposition 8.12 *(Kraus and Oesterlé) Let k be a positive integer, χ a Dirichlet character of conductor N and $f = \sum_{n\geq 0} c_n q^n$ be a modular form of weight k, character χ for $\Gamma_0(N)$, with $c_n \in \mathbb{Z}$. Let p be a rational prime. If $c_n \equiv 0 \pmod{p}$ for all $n \leq \mu(N)k/12$, then $c_n \equiv 0 \pmod{p}$ for all n.*

We now proceed with the proofs of Theorems 8.1 and 8.2; in each case, from Lemma 8.5, we may assume the existence of a weight 2, level N cuspidal newform f (with trivial character), where

$$N \in \left\{32p^2, 256p^2\right\}.$$

If f has at least one Fourier coefficient that is not a rational integer, then, from Proposition 8.11, there is a prime l coprime to $2p$ with

$$l \leq \begin{cases} 8p(p+1) & \text{if } N = 32p^2, \\ 64p(p+1) & \text{if } N = 256p^2. \end{cases} \tag{8.3}$$

such that $c_l \notin \mathbb{Z}$. It follows from Proposition 8.6 that n divides $\mathrm{Norm}_{K_f/\mathbb{Q}}(c_l - a_l)$, where a_l is the lth Fourier coefficient corresponding to the Frey curve $E(a, b, c)$. Since $a_l \in \mathbb{Z}$ (whereby $a_l \neq c_l$), and l is coprime to $2p$, the Weil bounds; $|c_\ell| \leq 2\sqrt{\ell}$, $|a_\ell| \leq \ell + 1$, imply that

$$n \leq \left(l + 1 + 2\sqrt{l}\right)^{[K_f:\mathbb{Q}]} = \left(\sqrt{l} + 1\right)^{2[K_f:\mathbb{Q}]}, \tag{8.4}$$

where, as previously, K_f denotes the field of definition for the Fourier coefficients of the form f. Next, we note that $[K_f : \mathbb{Q}] \leq g_0^+(N)$ where $g_0^+(N)$ denotes the dimension (as a $\mathbb{C}$-vector space) of the space of cuspidal, weight 2, level N newforms. Applying Theorem 2 of Martin [49] we have

$$g_0^+(32p^2) \leq \frac{32p^2 + 1}{12} \leq 3p^2,$$

and

$$g_0^+(256p^2) \leq \frac{256p^2+1}{12} \leq 22p^2.$$

Combining these with inequalities (8.3) and (8.4), we may therefore conclude that

$$n \leq \begin{cases} \left(\sqrt{8p(p+1)}+1\right)^{6p^2} & \text{if } N = 32p^2, \\ \left(\sqrt{64p(p+1)}+1\right)^{44p^2} & \text{if } N = 256p^2. \end{cases} \tag{8.5}$$

It follows, after routine calculation, that

$$n \leq \begin{cases} p^{12p^2} & \text{if } N = 32p^2, \\ p^{132p^2} & \text{if } N = 256p^2. \end{cases}$$

where these inequalities are a consequence of (8.5) for $p \geq 5$.

It remains, then, to consider the case when the form f has rational integer Fourier coefficients c_n for all $n \geq 1$. In such a situation, f corresponds to an isogeny class of elliptic curves over $\mathbb{Q}$ with conductor N. Define

$$f^* = \sum_{n\geq 1,(n,2p)=1} c_n q^n \quad \text{and} \quad g^* = \sum_{n\geq 1,(n,2p)=1} \sigma_1(n) q^n,$$

where $\sigma_1(n)$ is the usual sum of divisors function; i.e. $\sigma_1(n) = \sum_{d|n} d$. Lemma 4.6.5 of Miyake [Mi:1989] ensures that f^* and g^* are weight 2 modular forms of level dividing $512p^3$. Applying Proposition 8.12 (at the prime 2) to $f^* - g^*$ and using the fact that $\sigma(l) = l + 1$, for all primes l one of the following necessarily occurs :

(i) There exists a prime l, coprime to $2p$, satisfying $l \leq 128p^2(p+1)$ and $c_l \equiv 1 \pmod 2$.

(ii) $c_l \equiv 0 \pmod 2$ for all prime l coprime to $2p$.

In the former case, since n divides the (nonzero) integer $c_l - a_l$, we obtain the inequality

$$n \leq l + 1 + 2\sqrt{l} \leq 128p^2(p+1) + 1 + 16p\sqrt{p+1} < p^{2p}, \tag{8.6}$$

where the last inequality is valid for $p \geq 5$. In the latter situation, there necessarily exists a curve, say F, in the given isogeny class, with a rational 2-torsion

point. Propositions 8.9 and 8.10 then immediately imply Theorems 8.1 and 8.2. Regarding Theorem 8.1, where $N = 32p^2$, we may apply Proposition 8.9 to conclude that, for $p \neq 7$, F has j-invariant whose denominator is divisible by p or CM by an order in $\mathbb{Q}(\sqrt{-1})$. In the former case, we get a contradiction with Proposition 8.7, thus the latter case must hold, from which it follows from Proposition 8.8 that $n \leq 13$ (note, part (a) of Proposition cannot hold in this case since we are assuming $c \equiv 0 \pmod 2$ and a, b, c pairwise coprime). Regarding Theorem 8.2, where $N = 256p^2$, we apply Proposition 8.10 to conclude that F has j-invariant whose denominator is divisible by p or CM by an order in $\mathbb{Q}(\sqrt{-1})$ or $\mathbb{Q}(\sqrt{-2})$. In the former case, we again get a contradiction with Proposition 8.7, thus the latter case must hold, from which it follows from Proposition 8.8 that $n \leq 13$. Combining these observations with (8.6) and the inequalities following (8.5) completes the proofs of Theorems 8.1 and 8.2.

Corollary 8.3 is an easy consequence of Theorems 8.1 and 8.2, after applying a result of Darmon and Granville [DG95] (which implies, for fixed values of $n \geq 4$ and α, that the equation $x^n + y^n = 2^\alpha pz^2$ has at most finitely many solutions in coprime, nonzero integers x, y and z.

8.8 Concluding Remarks

In case $p \in \{2, 3, 5\}$, equation 8.2 is solved completely in [5], for $n \geq 4$. Further, the equation

$$x^n + y^n = 7z^2$$

with x, y and z coprime nonzero integers, may, as in e.g. Kraus [38], be treated for *fixed* values for n. We will not undertake this here.

Chapter 9
On the equation $x^3 + y^3 = \pm p^m z^n$

In this chapter we restrict our attention to determining primes p for which $x^3 + y^3 = \pm p^m z^n$ can be shown to be unsolvable in integers (x, y, z) for all suitable large primes n.

9.1 Introduction

Let T denote the set of primes p for which there are no elliptic curves over $\mathbb{Q}$ with rational 2-torsion and conductor in $\{18p, 36p, 72p\}$. We have already seen in Chapter 7 that T is infinite, in fact it contains all primes p satisfying $p \equiv 317$ or $1757 \pmod{2040}$ (see Corollary 7.4). It is believed that T contains all primes except for a set of density zero. Corollary 7.5 is the most we can prove in this direction. The first few elements of T are

$$197, 317, 439, 557, 653, 677, 701, 773, 797, 821, 1013, 1039,$$
$$1061, 1109, 1231, 1277, 1279, 1289, 1301, 1399, 1447, 1471, 1493$$
$$1613, 1637, 1663, 1709, 1733.$$

In this chapter we prove the following.

Theorem 9.1 *Let $p \in T$ and $m \geq 1$ an integer. Then the equation*

$$x^3 + y^3 = \pm p^m z^n \tag{9.1}$$

has no solutions in coprime nonzero integers x, y and z, and prime n satisfying $n \geq p^{8p}$ and $n \nmid m$.

We remark that in the case that $n \mid m$ the equation can be written as $x^3 + y^3 = z^n$. Kraus has treated these equations in [44]. So, in what follows, we will assume $n \nmid m$.

As an almost immediate consequence of this theorem, we have:

Corollary 9.2 *Let $p \in T$. Then equation (9.1) has at most finitely many solutions in coprime nonzero integers x, y and z, and integers $m \geq 1$, $n \geq 5$ with $n \nmid m$.*

9.2 Frey Curve

Let p be a prime number ≥ 5, n a prime ≥ 7 and m a positive integer. We consider a proper, nontrivial solution (a, b, c) of the equation $a^3 + b^3 = \pm p^m c^n$, i.e. pgcd$(a, b, pc) = 1$ [1]. We suppose, without loss of generality, that the following conditions are satisfied:

$$ac \text{ is even, and } b \equiv \begin{cases} -1 \pmod 4 & \text{if } c \text{ is even,} \\ 1 \pmod 4 & \text{if } c \text{ is odd.} \end{cases} \tag{9.2}$$

Darmon and Granville [27] associate to the triple (a, b, c) an elliptic curve defined over $\mathbb{Q}$. It is, up to $\mathbb{Q}$-isomorphism, the elliptic curve that we denote $E_{a,b}$, with equation

$$y^2 = x^3 + 3abx + b^3 - a^3, \tag{9.3}$$

which has a point of order 2; $(a-b, 0)$. The standard invariants $c_4(a, b), c_6(a, b)$ and $\Delta(a, b)$ associated with the equation 9.3 are the following:

$$\begin{cases} c_4(a, b) = -2^4 3^2 ab \\ c_6(a, b) = 2^5 3^3 (a^3 - b^3) \\ \Delta(a, b) = -2^4 3^3 p^{2m} c^{2n} \end{cases} \tag{9.4}$$

We determine the conductor $N_{E_{a,b}}$ of $E_{a,b}$. We designate by $\mathcal{R}$ the product of the prime numbers distinct from 2, 3, and p that divide c, which is to say the largest squarefree integer prime to $6p$ which divides c. Given an integer k and a prime number l, we denote by $v_l(k)$ the exponent of l in the decomposition of k into prime factors.

[1] pgcd denotes the pairwise gcd.

Lemma 9.3 *We have (under conditions (9.2) on a, b, and c)*

$$N_{E_{a,b}} = \begin{cases} 2 \cdot 3^2 p\mathcal{R} & \text{if } c \text{ even, } b \equiv -1 \pmod 4, \\ 2^3 3^2 p\mathcal{R} & \text{if } c \text{ odd, } v_2(a) = 1 \text{ and } b \equiv 1 \pmod 4, \\ 2^2 3^2 p\mathcal{R} & \text{if } c \text{ odd, } v_2(a) \geq 2 \text{ and } b \equiv 1 \pmod 4. \end{cases}$$

Proof. We will use Theorems 2.1, 2.3, and 2.4 to compute $v_\ell(N_{E_{a,b}})$ for all primes l. To do this we first need to move the point of order 2 to $(0, 0)$. Applying the change of variables

$$x = X + (a - b), \;\; y = Y,$$

the curve $E_{a,b}$ is $\mathbb{Q}$-isomorphic to

$$E_{a,b}: \;\; Y^2 = X^3 + 3(a-b)X^2 + 3(a^2 - ab + b^2)X. \tag{9.5}$$

The invariants of this model are still as in (9.4).

1) Let l be a prime number ≥ 5 which divides pc. As the integers a, b and pc are prime to each other we have $l \nmid a - b$ and equation (9.5) is minimal at l. On the other hand, if l is a prime number ≥ 5 and is prime to pc then $v_l(\Delta(a, b)) = 0$ and again equation (9.5) is minimal at l. It follows from Theorem 2.4 that

$$v_l(N_{E_{a,b}}) = \begin{cases} 1 & \text{if } \ell \text{ divides } pc, \\ 0 & \text{if } \ell \text{ does not divide } pc. \end{cases} \tag{9.6}$$

2) We determine the exponent of 2 in $N_{E_{a,b}}$.

2.1) Suppose that c is even. In this case ab is odd, because $\gcd(a, b, pc) = 1$. We have $\pm p^m c^n = (a + b)(a^2 - ab + b^2)$ and the number $a^2 - ab + b^2$ is odd. As n is ≥ 5, we have

$$a + b \equiv 0 \pmod{32}.$$

As a and b are odd, it follows that 4 does not divide $a - b$. Therefore

$$\begin{cases} v_2(3(a-b)) = v_2(a-b) = 1, \\ v_2(3(a^2 - ab + b^2)) = 0. \end{cases}$$

Thus, from Theorem 2.1, the value of $v_2(N_{E(a,b)})$ depends on the congruence class of $3(a - b)$ modulo 8 (note $v_2(\Delta) \geq 4 + 2n \geq 14$). It follows from $a + b \equiv$

$0 \pmod{32}$, $a - b \equiv 2 \pmod 4$ and the assumption $b \equiv -1 \pmod 4$ (see 9.2) that $a - b \equiv 2 \pmod 8$, hence

$$3(a - b) \equiv 6 \pmod 8.$$

So, from theorem 2.1, $v_2(N_{E_{a,b}}) = 1$.
2.2) Suppose that c is odd. It follows from condition (9.2) that a is even and $b \equiv 1 \pmod 4$. We therefore have

$$\begin{cases} v_2(3(a-b)) = 0, \\ v_2(3(a^2 - ab + b^2)) = 0, \end{cases}$$

thus, from Theorem 2.1 the value of $v_2(N_{E(a,b)})$ depends on the congruence classes of $3(a - b)$ and $3(a^2 - ab + b^2)$ modulo 4. Since $b \equiv 1 \pmod 4$ then

$$3(a-b) \equiv \begin{cases} 1 \pmod 4 & \text{if } a \equiv 0 \pmod 4, \\ -1 \pmod 4 & \text{if } a \equiv 2 \pmod 4, \end{cases}$$

and

$$3(a^2 - ab + b^2) \equiv \begin{cases} -1 \pmod 4 & \text{if } a \equiv 0 \pmod 4, \\ 1 \pmod 4 & \text{if } a \equiv 2 \pmod 4. \end{cases}$$

It follows from Theorem 2.1 that

$$v_2(N_{E_{a,b}}) = \begin{cases} 2 & \text{if } a \equiv 0 \pmod 4, \\ 3 & \text{if } a \equiv 2 \pmod 4. \end{cases}$$

3) We now determine the exponent of 3 in $N_{E_{a,b}}$.
3.1) Suppose that 3 divides c. Under this hypothesis 3 does not divide ab. From the equality $a^3 + b^3 = p^m c^n$ we have $a \equiv -b \pmod 3$ and 3 does not divide $a - b$ or $a^3 - b^3$. It follows that 3 divides $a^2 - ab + b^2$. Therefore $v_3(3(a - b)) = 1$ and $v_3(3(a^2 - ab + b^2)) \geq 2$. The Néron type of $E_{a,b}$ at 3 is then I_v^* with $v = 2nv_3(c) - 3$ and $v_3(N_{E_{a,b}}) = 2$ by Theorem 2.3.
3.2) Suppose that 3 divides ab. We have in this case 3 does not divide $a - b$ or $a^2 - ab + b^2$ since $\gcd(a, b) = 1$. Therefore $v_3(3(a - b)) = 1$ and $v_3(3(a^2 - ab + b^2)) = 1$. The Néron type of $E_{a,b}$ at 3 is thus III and again $v_3(N_{E_{a,b}}) = 2$ by Theorem 2.3.

3.3) Suppose that 3 does not divide abc. As 3 does not divide pc, we have from the equality $a^3 + b^3 = p^m c^n$ that $a \equiv b \pmod 3$ and so $a - b \equiv 0 \pmod 3$ and 3 does not divide $a^2 - ab + b^2$. Thus $v_3(3(a-b)) \geq 2$ and $v_3(3(a^2 - ab + b^2)) = 1$. The Néron type of $E_{a,b}$ at 3 is thus III, and we have again $v_3(N_{E_{a,b}}) = 2$. This completes the proof of Lemma 9.3. □

9.3 The Modular Galois Representation $\rho_n^{a,b}$

Let $\overline{\mathbb{Q}}$ be an algebraic closure of $\mathbb{Q}$ and $E_{a,b}[n]$ the subgroup of n-torsion points of $E_{a,b}(\overline{\mathbb{Q}})$. $E_{a,b}[n]$ is a vector space of dimension 2 over $\mathbb{Z}/n\mathbb{Z}$ on which the Galois group $\mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ acts naturally. We denote the corresponding mod n Galois representation on $E_{a,b}[n]$ by

$$\rho_n^{a,b} : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{F}_n).$$

Let k and $N(\rho_n^{a,b})$ denote the weight and conductor of $\rho_n^{a,b}$ respectively, which are defined by Serre in [64].

Lemma 9.4 *1.* $k = 2$.

2. $$N(\rho_n^{a,b}) = \begin{cases} 18p & \text{if } c \text{ even, } b \equiv -1 \pmod 4, \\ 36p & \text{if } c \text{ odd, } v_2(a) \geq 2 \text{ and } b \equiv 1 \pmod 4, \\ 72p & \text{if } c \text{ odd, } v_2(a) = 1 \text{ and } b \equiv 1 \pmod 4. \end{cases}$$

3. The representation $\rho_n^{a,b}$ is irreducible.

Proof. 1) Recall $n \neq p$ by assumption. If $n \nmid c$ then $E_{a,b}$ has good reduction at p. Otherwise, $E_{a,b}$ has multiplicative reduction at n and the exponent of n in the minimal discriminant is a multiple of n. From which the above assertion follows, see ([64], P. 191, Proposition 5).

2) Let q be a prime distinct from p and n. The curve $E_{a,b}$ has multiplicative reduction at q (Lemma 9.3) and the exponent of q in the minimal discriminant of $E_{a,b}$ is a multiple of n (see 9.4). This assertion then follows as a direct consequence of Lemma 9.3 and a proposition of Kraus [42]; see also ([64], p. 120).

3) Suppose $\rho_n^{a,b}$ is reducible. Since $E_{a,b}$ has a point of order 2 there exists a subgroup of $E_{a,b}(\mathbb{Q})$ of order 2 stable under Galois $G(\overline{\mathbb{Q}}/\mathbb{Q})$.

If $n \geq 11$ then the modular curve $Y_0(2n)$ does not have any $\mathbb{Q}$-rational points (see [39] which uses the results of [50]), from which the lemma follows.

Suppose $n = 7$. The modular curve $Y_0(14)$ is the elliptic curve $14a1$ in the table of [26]. It follows that $Y_0(14)$ has a rational point of order 2 and so there corresponds two $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over $\mathbb{Q}$ with j invariants -15^3 and 255^3, respectively. These are precisely the curves $49a1$ and $49a2$ in the tables of [26], each of which contains a subgroup of order 14 stable under Galois. Since $E_{a,b}$ has j-invariant

$$j = \frac{6912(ab)^3}{p^{2m}c^{2n}}$$

the lemma follows. □

Given an integer $N \geq 1$ we let $S_2(\Gamma_0(N))$ denote the $\mathbb{C}$-vector space of cuspidal modular forms of weight 2 for the congruence subgroup $\Gamma_0(N)$. Denote by $S_2^+(N)$ the subspace of newforms of $S_2(\Gamma_0(N))$, and $g_0^+(N)$ its dimension as a $\mathbb{C}$-vector space. See [49] for an explicit determination of $g_0^+(N)$.

Since the representation $\rho_n^{a,b}$ is irreducible of weight 2 and $E_{a,b}$ is modular (by the extraordinary work of Breuil, Conrad, Diamond, Taylor, and Wiles: [80], [77], [8]) there exists a newform $f \in S_2^+(N(\rho_n^{a,b}))$ whose Taylor expansion is

$$t \mapsto g + \sum_{n \geq 2} a_n(f) q^n \text{ where } q = e^{2\pi t}$$

and a place $\mathcal{B}$ of $\overline{\mathbb{Q}}$ of residual characteristic n such that for all prime numbers l which do not divide $nN_{E_{a,b}}$ one has

$$a_l(f) \equiv a_l(E_{a,b}) \text{ (mod } \mathcal{B}).$$

It follows that

$$n \mid \mathrm{Norm}_{K_f/\mathbb{Q}}(a_l(f) - a_l(E_{a,b})), \tag{9.7}$$

where K_f denotes the field of definition of the coefficients.

9.4 Proof of Theorem 9.1

We now proceed with the proof of Theorem 9.1. Let us suppose that f is a weight 2, level N cuspidal newform (with trivial character), where

$$N \in \{18p, 36p, 72p\},$$

corresponding, as in Section 9.3, to a nontrivial solution to equation (9.1). From Theorem 3 of [43], we may suppose that f has rational integer Fourier coefficients, provided $n \geq p^{4p}$ (in case $N = 18p$ or $36p$) or $n \geq p^{8p}$ (in case $N = 72p$). This follows from 9.7 and applying Theorem 1 of [49] to obtain

$$g_0^+(N) \leq \begin{cases} p & \text{if } N = 18p, 36p \\ 5p/4 & \text{if } N = 72p. \end{cases}$$

To finish the proof of Theorem 9.1 we will combine the results of Chapter 7 with the Proposition of Kraus and Oesterlé, see Proposition 8.12.

Since the form f has rational integer Fourier coefficients $a_m(f)$ for all $m \geq 1$, f corresponds to an isogeny class of elliptic curves over $\mathbb{Q}$ with conductor $N = 18p$, $32p$, or $72p$. Define f^* and g^* as in section 8.7, though this time they are both weight 2 cusp forms with level dividing $2^4 3^3 p^2$. Applying the Proposition of Kraus and Oesterlé to $f^* - g^*$, and using $\sigma(l) = l + 1$, for all primes l one of the following necessarily occurs:

(i) There exists a prime l, coprime to $6p$, satisfying $l \leq 144p(p+1)$ and $a_l(f) \equiv 1 \pmod 2$.

(ii) $a_l(f) \equiv 0 \pmod 2$ for all prime l coprime to $6p$.

In the former case, since n divides the (nonzero) integer $a_l(f) - a_l(E_{a,b})$ we obtain the inequality

$$n \leq l + 1 + 2\sqrt{l} \leq 144p(p+1) + 1 + 24\sqrt{p(p+1)} < p^p,$$

where the last inequality is valid for $p \geq 5$. In the latter case, there exists and elliptic curve F, in the given isogeny class, with a rational 2-torsion point. That is, F is an elliptic curves over $\mathbb{Q}$ with 2-torsion and conductor $18p$, $36p$ or $72p$. It follows that $p \notin T$. Therefore, for $p \in T$ such an F cannot exist, hence

$n \leq p^{4p}$ (if $N = 18p$ or $36p$) or $n \leq p^{8p}$ (if $N = 72p$). This completes the proof of Theorem 9.1.

Corollary 9.2 is an easy consequence of Theorem 9.1, after applying a result of Darmon and Granville [27] (which implies, for fixed values of $n \geq 4$ and m, that the equation $x^3 + y^3 = \pm p^m z^n$ has at most finitely many solutions in coprime, nonzero integers x, y and z).

Bibliography

[1] M. Bauer and M. A. Bennett. Applications of the hypergeometric method to the generalized Ramanujen-Nagell equation. *The Ramanujan J.*, 6:209–270, 2002.

[2] M. A. Bennett. Pillai's conjecture revisited. *J. Number Theory*, 98(2):228–235, 2003.

[3] M. A. Bennett. Products of consecutive integers. *Bull. London Math. Soc.*, 36(5):683–694, 2004.

[4] M. A. Bennett and J. Mulholland. On the diophantine equation $x^n + y^n = 2^\alpha p z^2$. *C. R. Math. Rep. Acad. Sci. Canada*, 28(1):6–11, 2006.

[5] M. A. Bennett and C. Skinner. Ternary diophantine equations via galois representations and modular forms. *Canad. J. Math.*, 56:24–54, 2004.

[6] M. A. Bennett, V. Vatsal, and S. Yazdani. Ternary Diophantine equations of signature $(p, p, 3)$. *Compos. Math.*, 140(6):1399–1416, 2004.

[7] M. A. Bennett and G. Walsh. The Diophantine equation $b^2X^4 - dY^2 = 1$. *Proc. Amer. Math. Soc.*, 127(12):3481–3491, 1999.

[8] Christophe Breuil, Brian Conrad, Fred Diamond, and Richard Taylor. On the modularity of elliptic curves over $\mathbf{Q}$: wild 3-adic exercises. *J. Amer. Math. Soc.*, 14(4):843–939 (electronic), 2001.

[9] N. Bruin. Chabauty methods using covers of curves of geus 2. Report no. W99-15, University of Leiden., 1999.

[10] N. Bruin. *Chabauty methods and covering techniques applied to generalized Fermat equations*, volume 133 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 2002.

[11] N. Bruin. Chabauty methods using elliptic curves. *J. Reine Angew. Math.*, 562:27–49, 2003.

[12] N. Bruin. Personal communication. SFU, 2006.

[13] N. Bruin. Some ternary diophantine equations of signature $(n, n, 2)$. to appear in Discovering Mathematics with Magma, W. Bosma, J. Cannon (eds). (Springer), 2006.

[14] D. G. Cantor. Computing in the Jacobian of a hyperelliptic curve. *Math. Comp.*, 48(177):95–101, 1987.

[15] J. W. S. Cassels and E. V. Flynn. *Prolegomena to a middlebrow arithmetic of curves of genus* 2, volume 230 of *London Mathematical Society Lecture Note Series*. Cambridge University Press, Cambridge, 1996.

[16] C. Chabauty. Sur les points rationnels des courbes algébriques de genre supérieur à l'unité. *C. R. Acad. Sci. Paris*, 212:882–885, 1941.

[17] F. Coghlan. *Elliptic Curves with conductor* 2^a3^b. PhD thesis, Univ. Manchester, 1967.

[18] J. H. E. Cohn. The Diophantine equations $x^3 = Ny^2 \pm 1$. *Quart. J. Math. Oxford Ser. (2)*, 42(165):27–30, 1991.

[19] J. H. E. Cohn. The Diophantine equation $x^2+2^k = y^n$. *Arch. Math. (Basel)*, 59(4):341–344, 1992.

[20] J. H. E. Cohn. The Diophantine equation $x^2 + 3 = y^n$. *Glasgow Math. J.*, 35(2):203–206, 1993.

[21] J. H. E. Cohn. The Diophantine equation $x^2 + C = y^n$. *Acta Arith.*, 65(4):367–381, 1993.

[22] J. H. E. Cohn. The Diophantine equation $x^4 - Dy^2 = 1$. II. *Acta Arith.*, 78(4):401–403, 1997.

[23] J. H. E. Cohn. The Diophantine equation $x^4 + 1 = Dy^2$. *Math. Comp.*, 66(219):1347–1351, 1997.

[24] J. H. E. Cohn. The Diophantine equation $d^2x^4 + 1 = Dy^2$. *Q. J. Math.*, 51(2):183–184, 2000.

[25] R. F. Coleman. Effective Chabauty. *Duke Math. J.*, 52(3):765–770, 1985.

[26] J. E. Cremona. *Algorithms for modular elliptic curves*. Cambridge University Press, Cambridge, 1997.

[27] H. Darmon and A. Granville. On the equations $z^m = F(x, y)$ and $Ax^p + By^q = Cz^r$. *Bull. London Math. Soc.*, 27(6):513–543, 1995.

[28] H. Darmon and L. Merel. Winding quotients and some variants of Fermat's last theorem. *J. Reine Angew. Math.*, 490:81–100, 1997.

[29] S. David. Minorations de formes linéaires de logarithmes elliptiques. *Mém. Soc. Math. France (N.S.)*, 1(62):iv+143, 1995.

[30] B. M. M. de Weger. *Algorithms for Diophantine equations*, volume 65 of *CWI Tract*. Stichting Mathematisch Centrum Centrum voor Wiskunde en Informatica, Amsterdam, 1989.

[31] E. V. Flynn. Coverings of curves of genus 2. In *Algorithmic number theory (Leiden, 2000)*, volume 1838 of *Lecture Notes in Comput. Sci.*, pages 65–84. Springer, Berlin, 2000.

[32] J. Gebel, E. Herrmann, A. Pethö, and H. G. Zimmer. Computing all S-integral points on elliptic curves. *Math. Proc. Cambridge Philos. Soc.*, 127(3):383–402, 1999.

[33] J. Gebel, A. Pethö, and H. G. Zimmer. Computing S-integral points on elliptic curves. In *Algorithmic number theory (Talence, 1996)*, volume 1122 of *Lecture Notes in Comput. Sci.*, pages 157–171. Springer, Berlin, 1996.

[34] T. Hadano. On the conductor of an elliptic curve with a rational point of order 2. *Nagoya Math. J.*, 53:199–210, 1974.

[35] T. Hadano. Elliptic curves with a rational point of finite order. *Manuscripta Math.*, 39(1):49–79, 1982.

[36] W. Ivorra. Sur les équations $x^p + 2^\beta y^p = z^2$ et $x^p + 2^\beta y^p = 2z^2$. *Acta Arith.*, 108(4):327–338, 2003.

[37] W. Ivorra. Courbes elliptiques sur $\mathbb{Q}$, ayant un point d'ordre 2 rationnel sur $\mathbb{Q}$, de conducteur $2^N p$. *Dissertationes Math. (Rozprawy Mat.)*, 429:55, 2004.

[38] W. Ivorra and A. Kraus. Quelques résultats sur les équations $ax^p + by^p = cz^2$. *Canad. J. Math.*, 58(1):115–153, 2006.

[39] M. A. Kenku. On the number of **Q**-isomorphism classes of elliptic curves in each **Q**-isogeny class. *J. Number Theory*, 15(2):199–202, 1982.

[40] A. W. Knapp. *Elliptic curves*, volume 40 of *Mathematical Notes*. Princeton University Press, Princeton, NJ, 1992.

[41] A. Kraus. Sur les équations $a^p + b^p + 15c^p = 0$ et $a^p + 3b^p + 5c^p = 0$. *C. R. Acad. Sci. Paris Sér. I Math.*, 322(9):809–812, 1996.

[42] A. Kraus. Détermination du poids et due conducteur associés aux représentations des points de p-torsion d'une courbe elliptique. *Dissertationes Math. (Rozprawy Mat.)*, 364:39, 1997.

[43] A. Kraus. Majorations effectives pour l'équation de Fermat généralisée. *Canad. J. Math.*, 49(6):1139–1161, 1997.

[44] A. Kraus. Sur l'équation $a^3 + b^3 = c^p$. *Experiment. Math.*, 7(1):1–13, 1998.

[45] A. Kraus. On the equation $x^p + y^q = z^r$: a survey. *Ramanujan J.*, 3(3):315–333, 1999.

[46] A. Kraus and J. Oesterlé. Sur une question de B. Mazur. *Math. Ann.*, 293(2):259–275, 1992.

[47] W. Ljunggren. Ein Satz über die diophantische Gleichung $Ax^2 - By^4 = C$ $(C = 1, 2, 4)$. In *Tolfte Skandinaviska Matematikerkongressen, Lund, 1953*, pages 188–194. Lunds Universitets Matematiska Inst., Lund, 1954.

[48] W. Ljunggren. On the diophantine equation $Ax^4 - By^2 = C$ $(C = 1,\ 4)$. *Math. Scand.*, 21:149–158 (1969), 1967.

[49] G. Martin. Dimensions of the spaces of cusp forms and newforms on $\Gamma_0(N)$ and $\Gamma_1(N)$. *J. Number Theory*, 112(2):298–331, 2005.

[50] B. Mazur. Modular curves and the Eisenstein ideal. *Inst. Hautes Études Sci. Publ. Math.*, 47:33–186 (1978), 1977.

[51] B. Mazur. Rational isogenies of prime degree (with an appendix by D. Goldfeld). *Invent. Math.*, 44(2):129–162, 1978.

[52] P. Mihăilescu. Primary cyclotomic units and a proof of Catalan's conjecture. *J. Reine Angew. Math.*, 572:167–195, 2004.

[53] I. Miyawaki. Elliptic curves of prime power conductor with $\mathbf{Q}$-rational points of finite order. *Osaka J. Math.*, 10:309–323, 1973.

[54] T. Nagell. Contributions to the theory of a category of Diophantine equations of the second degree with two unknowns. *Nova Acta Soc. Sci. Upsal. (4)*, 16(2):38, 1955.

[55] A. P. Ogg. Abelian curves of 2-power conductor. *Proc. Cambridge Philos. Soc.*, 62:143–148, 1966.

[56] A. P. Ogg. Abelian curves of small conductor. *J. Reine Angew. Math.*, 226:204–215, 1967.

[57] I. Papadopoulos. Sur la classification de Néron des courbes elliptiques en caractéristique résiduelle 2 et 3. *J. Number Theory*, 44(2):119–152, 1993.

[58] B. Poonen. Computing torsion points on curves. *Experiment. Math.*, 10(3):449–465, 2001.

[59] B. Poonen, E. Schaefer, and M. Stoll. Twists of $x(7)$ and primitive solutions to $x^2 + y^3 = z^7$. preprint, 2005.

[60] G. Rémond and F. Urfels. Approximation diophantienne de logarithmes elliptiques p-adiques. *J. Number Theory*, 57(1):133–169, 1996.

[61] K. A. Ribet. On the equation $a^p + 2^\alpha b^p + c^p = 0$. *Acta Arith.*, 79(1):7–16, 1997.

[62] D. Ridout. Rational approximations to algebraic numbers. *Mathematika*, 4:125–131, 1957.

[63] J. P. Serre. Propriétés galoisiennes des points d'ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[64] J. P. Serre. Sur les représentations modulaires de degré 2 de $\mathrm{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. *Duke Math. J.*, 54(1):179–230, 1987.

[65] J. P. Serre. Travaux de Wiles (et Taylor, ...). I. *Astérisque*, 1(237):Exp. No. 803, 5, 319–332, 1996.

[66] B. Setzer. Elliptic curves of prime conductor. *J. London Math. Soc. (2)*, 10:367–378, 1975.

[67] I. R. Shafarevich. *Basic algebraic geometry. 1*. Springer-Verlag, Berlin, 1994.

[68] T. N. Shorey and R. Tijdeman. *Exponential Diophantine equations*, volume 87 of *Cambridge Tracts in Mathematics*. Cambridge University Press, Cambridge, 1986.

[69] J. H. Silverman. *The arithmetic of elliptic curves*, volume 106 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1986.

[70] J. H. Silverman. *Advanced topics in the arithmetic of elliptic curves*, volume 151 of *Graduate Texts in Mathematics*. Springer-Verlag, New York, 1994.

[71] N. P. Smart. *The algorithmic resolution of Diophantine equations*, volume 41 of *London Mathematical Society Student Texts*. Cambridge University Press, Cambridge, 1998.

[72] M. Stoll. On the arithmetic of the curves $y^2 = x^l + A$. II. *J. Number Theory*, 93(2):183–206, 2002.

[73] M. Stoll. Data tables for the curves $y^2 = x^5 \pm 2^a 3^b$. Personal communication, 2005.

[74] M. Stoll. Independence of rational points on twists of a given curve. arXiv:math.NT/0603557 v1 23 Mar 2006, 2006.

[75] M. Stoll. On the number of rational squares at a fixed distance from a fifth power. arXiv:math.NT/0604425 v1 19 Apr 2006, 2006.

[76] J. Tate. Algorithm for determining the type of a singular fiber in an elliptic pencil. In *Modular functions of one variable, IV (Proc. Internat. Summer School, Univ. Antwerp, Antwerp, 1972)*, pages 33–52. Lecture Notes in Math., Vol. 476. Springer, Berlin, 1975.

[77] Richard Taylor and Andrew Wiles. Ring-theoretic properties of certain Hecke algebras. *Ann. of Math. (2)*, 141(3):553–572, 1995.

[78] J. Vélu. Courbes elliptiques sur $\mathbf{Q}$ ayant bonne réduction en dehors de $\{11\}$. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A73–A75, 1971.

[79] J. Vélu. Isogénies entre courbes elliptiques. *C. R. Acad. Sci. Paris Sér. A-B*, 273:A238–A241, 1971.

[80] A. Wiles. Modular elliptic curves and Fermat's last theorem. *Ann. of Math. (2)*, 141(3):443–551, 1995.

Appendix A

On the $\mathbb{Q}$-Isomorphism Classes of Elliptic Curves with 2-Torsion and Conductor $2^\alpha 3^\beta p^\delta$

In this appendix, we provide the proof of the main lemmata used in our classification of elliptic curves. In particular, we will give a list of elliptic curves which contains a representative for each $\mathbb{Q}$-isomorphism class of curves containing 2 torsion and having conductor of the form $2^\alpha 3^\beta p^\delta$.

Let E be an elliptic curve over $\mathbb{Q}$ of conductor $2^M 3^L p^N$, with $0 \leq M \leq 8$ and $0 \leq L, N \leq 2$, and having at least one rational point of order 2. We may assume that E is given by a model of the form

$$y^2 = x^3 + ax^2 + bx,$$

where a and b are integers both divisible by p iff $N = 2$, both divisible by 3 iff $L = 2$, and a, b have no other common odd divisors (see results of Chapter 2). We may also assume that this model is minimal outside of 2. From the hypothesis on the conductor of E there exist three natural numbers α, β and δ such that

$$b^2(a^2 - 4b) = \pm 2^\alpha 3^\beta p^\delta \tag{A.1}$$

We have $b \neq 0$ and the only possible divisors of b are 2, 3 and p. We consider the two cases: (i) $b > 0$, (ii) $b < 0$. The first case is treated in Section A.1 and the second in A.2.

A.1 $b > 0$

Lemma A.1 *Suppose $b > 0$. Then there exists an integer d, and non-negative integers m, ℓ, and n satisfying one of the equations in the first column and E is $\mathbb{Q}$-*

isomorphic to the corresponding curve in the second column, for some $r_1, r_2, r_3 \in \{0, 1\}$; except in cases 1 through 9, where if $m = 1$ then $r_1 \in \{1, 2\}$.

		$y^2 = x^3 + a_2x^2 + a_4x$	
	Diophantine Equation	a_2	a_4
1	$d^2 - 2^m3^\ell p^n = \pm 1$	$2^{r_1}3^{r_2}p^{r_3}d$	$2^{m+2r_1-2}3^{\ell+2r_2}p^{n+2r_3}$
2	$d^2 - 2^m3^\ell = \pm p^n$	$2^{r_1}3^{r_2}p^{r_3}d$	$2^{m+2r_1-2}3^{\ell+2r_2}p^{2r_3}$
3	$d^2 - 2^m p^n = \pm 3^\ell$	$2^{r_1}3^{r_2}p^{r_3}d$	$2^{m+2r_1-2}3^{2r_2}p^{n+2r_3}$
4	$d^2 - 2^m = \pm 3^\ell p^n$	$2^{r_1}3^{r_2}p^{r_3}d$	$2^{m+2r_1-2}3^{2r_2}p^{2r_3}$
5	$pd^2 - 2^m3^\ell = \pm 1$	$2^{r_1}3^{r_2}p^{r_3+1}d$	$2^{m+2r_1-2}3^{\ell+2r_2}p^{2r_3+1}$
6	$pd^2 - 2^m = \pm 3^\ell$	$2^{r_1}3^{r_2}p^{r_3+1}d$	$2^{m+2r_1-2}3^{2r_2}p^{2r_3+1}$
7	$3d^2 - 2^m p^n = \pm 1$	$2^{r_1}3^{r_2+1}p^{r_3}d$	$2^{m+2r_1-2}3^{2r_2+1}p^{n+2r_3}$
8	$3d^2 - 2^m = \pm p^n$	$2^{r_1}3^{r_2+1}p^{r_3}d$	$2^{m+2r_1-2}3^{2r_2+1}p^{2r_3}$
9	$3pd^2 - 2^m = \pm 1$	$2^{r_1}3^{r_2+1}p^{r_3+1}d$	$2^{m+2r_1-2}3^{2r_2+1}p^{2r_3+1}$
10	$d^2 - 3^\ell p^n = \pm 2^m$	$2^{r_1+1}3^{r_2}p^{r_3}d$	$2^{2r_1}3^{\ell+2r_2}p^{n+2r_3}$
11	$d^2 - 3^\ell = \pm 2^m p^n$	$2^{r_1+1}3^{r_2}p^{r_3}d$	$2^{2r_1}3^{\ell+2r_2}p^{2r_3}$
12	$d^2 - p^n = \pm 2^m 3^\ell$	$2^{r_1+1}3^{r_2}p^{r_3}d$	$2^{2r_1}3^{2r_2}p^{n+2r_3}$
13	$d^2 - 1 = \pm 2^m 3^\ell p^n$	$2^{r_1+1}3^{r_2}p^{r_3}d$	$2^{2r_1}3^{2r_2}p^{2r_3}$
14	$pd^2 - 3^\ell = \pm 2^m$	$2^{r_1+1}3^{r_2}p^{r_3+1}d$	$2^{2r_1}3^{\ell+2r_2}p^{2r_3+1}$
15	$pd^2 - 1 = \pm 2^m 3^\ell$	$2^{r_1+1}3^{r_2}p^{r_3+1}d$	$2^{2r_1}3^{2r_2}p^{2r_3+1}$
16	$3d^2 - p^n = \pm 2^m$	$2^{r_1+1}3^{r_2+1}p^{r_3}d$	$2^{2r_1}3^{2r_2+1}p^{n+2r_3}$
17	$3d^2 - 1 = \pm 2^m p^n$	$2^{r_1+1}3^{r_2+1}p^{r_3}d$	$2^{2r_1}3^{2r_2+1}p^{2r_3}$
18	$3pd^2 - 1 = \pm 2^m$	$2^{r_1+1}3^{r_2+1}p^{r_3+1}d$	$2^{2r_1}3^{2r_2+1}p^{2r_3+1}$
19	$2d^2 - 3^\ell p^n = \pm 1$	$2^{r_1+2}3^{r_2}p^{r_3}d$	$2^{2r_1+1}3^{\ell+2r_2}p^{n+2r_3}$
20	$2d^2 - 3^\ell = \pm p^n$	$2^{r_1+2}3^{r_2}p^{r_3}d$	$2^{2r_1+1}3^{\ell+2r_2}p^{2r_3}$
21	$2d^2 - p^n = \pm 3^\ell$	$2^{r_1+2}3^{r_2}p^{r_3}d$	$2^{2r_1+1}3^{2r_2}p^{n+2r_3}$
22	$2d^2 - 1 = \pm 3^\ell p^n$	$2^{r_1+2}3^{r_2}p^{r_3}d$	$2^{2r_1+1}3^{2r_2}p^{2r_3}$
23	$2pd^2 - 3^\ell = \pm 1$	$2^{r_1+2}3^{r_2}p^{r_3+1}d$	$2^{2r_1+1}3^{\ell+2r_2}p^{2r_3+1}$
24	$2pd^2 - 1 = \pm 3^\ell$	$2^{r_1+2}3^{r_2}p^{r_3+1}d$	$2^{2r_1+1}3^{2r_2}p^{2r_3+1}$
25	$6d^2 - p^n = \pm 1$	$2^{r_1+2}3^{r_2+1}p^{r_3}d$	$2^{2r_1+1}3^{2r_2+1}p^{n+2r_3}$
26	$6d^2 - 1 = \pm p^n$	$2^{r_1+2}3^{r_2+1}p^{r_3}d$	$2^{2r_1+1}3^{2r_2+1}p^{2r_3}$
27	$6pd^2 - 1 = \pm 1$	$2^{r_1+2}3^{r_2+1}p^{r_3+1}d$	$2^{2r_1+1}3^{2r_2+1}p^{2r_3+1}$

Remark. To avoid trivial redundancies in the list above we are free to make the following convention: m,ℓ and n may be zero if they appear on the right-hand side of the Diophantine equation, otherwise they must be ≥ 1.

A warning to the reader. The following proof is tedious and very repetitive. We have included all the details only for the purpose of completeness.

For those interested in getting an idea of the flavor of the proof, we suggest only reading a few cases.

Proof. It follows from (A.1) that the only possible divisors of b are 2, 3 and p. Thus, there exist integers i, j and k such that

$$b = 2^i 3^j p^k, \text{ and } 0 \leq 2i \leq \alpha,\ 0 \leq 2j \leq \beta,\ 0 \leq 2k \leq \delta.$$

We obtain from (A.1)

$$a^2 - 2^{i+2} 3^j p^k = \pm 2^{\alpha-2i} 3^{\beta-2j} p^{\delta-2k} \tag{A.2}$$

In what follows we consider the following twenty-seven cases:
1) $i+2 > \alpha-2i,\ j > \beta-2j,\ k > \delta-2k$,
2) $i+2 > \alpha-2i,\ j > \beta-2j,\ k < \delta-2k$,
3) $i+2 > \alpha-2i,\ j > \beta-2j,\ k = \delta-2k$,
4) $i+2 > \alpha-2i,\ j < \beta-2j,\ k > \delta-2k$,
5) $i+2 > \alpha-2i,\ j < \beta-2j,\ k < \delta-2k$,
6) $i+2 > \alpha-2i,\ j < \beta-2j,\ k = \delta-2k$,
7) $i+2 > \alpha-2i,\ j = \beta-2j,\ k > \delta-2k$,
8) $i+2 > \alpha-2i,\ j = \beta-2j,\ k < \delta-2k$,
9) $i+2 > \alpha-2i,\ j = \beta-2j,\ k = \delta-2k$,
10) $i+2 < \alpha-2i,\ j > \beta-2j,\ k > \delta-2k$,
11) $i+2 < \alpha-2i,\ j > \beta-2j,\ k < \delta-2k$,
12) $i+2 < \alpha-2i,\ j > \beta-2j,\ k = \delta-2k$,
13) $i+2 < \alpha-2i,\ j < \beta-2j,\ k > \delta-2k$,
14) $i+2 < \alpha-2i,\ j < \beta-2j,\ k < \delta-2k$,
15) $i+2 < \alpha-2i,\ j < \beta-2j,\ k = \delta-2k$,
16) $i+2 < \alpha-2i,\ j = \beta-2j,\ k > \delta-2k$,
17) $i+2 < \alpha-2i,\ j = \beta-2j,\ k < \delta-2k$,
18) $i+2 < \alpha-2i,\ j = \beta-2j,\ k = \delta-2k$,
19) $i+2 = \alpha-2i,\ j > \beta-2j,\ k > \delta-2k$,
20) $i+2 = \alpha-2i,\ j > \beta-2j,\ k < \delta-2k$,
21) $i+2 = \alpha-2i,\ j > \beta-2j,\ k = \delta-2k$,
22) $i+2 = \alpha-2i,\ j < \beta-2j,\ k > \delta-2k$,
23) $i+2 = \alpha-2i,\ j < \beta-2j,\ k < \delta-2k$,
24) $i+2 = \alpha-2i,\ j < \beta-2j,\ k = \delta-2k$,
25) $i+2 = \alpha-2i,\ j = \beta-2j,\ k > \delta-2k$,

26) $i+2=\alpha-2i$, $j=\beta-2j$, $k<\delta-2k$,
27) $i+2=\alpha-2i$, $j=\beta-2j$, $k=\delta-2k$.

1. We have $i+2>\alpha-2i$, $j>\beta-2j$ and $k>\delta-2k$. In this case $v_2(a^2)=\alpha-2i$, $v_3(a^2)=\beta-2j$ and $v_p(a^2)=\delta-2k$ so α, β, and δ are even. Therefore, $v_2(a)=\frac{\alpha}{2}-i$, $v_3(a)=\frac{\beta}{2}-j$, and $v_p(a)=\frac{\delta}{2}-k$. Let

$$u=\frac{a}{2^{\frac{\alpha}{2}-i}3^{\frac{\beta}{2}-j}p^{\frac{\delta}{2}-k}}$$

so (A.2) becomes

$$u^2-2^{3i-\alpha+2}3^{3j-\beta}p^{3k-\delta}=\pm 1,$$

with $3i-\alpha+2\geq 1$, $3j-\beta\geq 1$ and $3k-\delta\geq 1$.

Let

$$d=u,\ m=3i-\alpha+2,\ \ell=3j-\beta,\ n=3k-\delta,$$

then (d,m,ℓ,n,p) is a solution to

$$d^2-2^m3^\ell p^n=\pm 1,$$

with $m,\ell,n\geq 1$. The model for E can be written

$$y^2=x^3+2^{\frac{\alpha}{2}-i}3^{\frac{\beta}{2}-j}p^{\frac{\delta}{2}-k}dx^2+2^i3^jp^kx.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{\alpha}{2}-i=2q_1+r_1,\quad \frac{\beta}{2}-j=2q_2+r_2,\quad \frac{\delta}{2}-k=2q_3+r_3,$$

with $r_1,r_2,r_3\in\{0,1\}$. There are two cases to consider:

1.i) We have $(m,r_1)=(1,0)$. Putting

$$X=\frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y=\frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2=X^3+2^23^{r_2}p^{r_3}dX^2+2^33^{\ell+2r_2}p^{n+2r_3}X$$

which is the curve in case 1 of the lemma with $r_1=2$.

1.ii) We have $(m, r_1) > (1, 0)$[1]. Putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1}3^{r_2}p^{r_3}dX^2 + 2^{m+2r_1-2}3^{\ell+2r_2}p^{n+2r_3}X$$

which is the curve in case 1 of the lemma with $r_1 = 0$ or 1.

2. We have $i + 2 > \alpha - 2i$, $j > \beta - 2j$ and $k < \delta - 2k$. In this case $v_2(a^2) = \alpha - 2i$, $v_3(a^2) = \beta - 2j$ and $v_p(a^2) = k$ so α, β, and k are even. Therefore, $v_2(a) = \frac{\alpha}{2} - i$, $v_3(a) = \frac{\beta}{2} - j$, and $v_p(a) = \frac{k}{2}$. Let

$$u = \frac{a}{2^{\frac{\alpha}{2}-i}3^{\frac{\beta}{2}-j}p^{\frac{k}{2}}}$$

so (A.2) becomes

$$u^2 - 2^{3i-\alpha+2}3^{3j-\beta} = \pm p^{\delta-3k},$$

with $3i - \alpha + 2 \geq 1$, $3j - \beta \geq 1$ and $\delta - 3k \geq 1$.

Let

$$d = u,\ m = 3i - \alpha + 2,\ \ell = 3j - \beta,\ n = \delta - 3k,$$

then (d, m, ℓ, n, p) is a solution to

$$d^2 - 2^m 3^\ell = \pm p^n,$$

with $m, \ell, n \geq 1$. The the model for E can be written

$$y^2 = x^3 + 2^{\frac{\alpha}{2}-i}3^{\frac{\beta}{2}-j}p^{\frac{k}{2}}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{\alpha}{2} - i = 2q_1 + r_1, \quad \frac{\beta}{2} - j = 2q_2 + r_2, \quad \frac{k}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. There are, again, two cases to consider:

2.i) We have $(m, r_1) = (1, 0)$. Putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

[1]Lexicographic order.

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2} p^{r_3} dX^2 + 2^3 3^{\ell+2r_2} p^{2r_3} X$$

which is the curve in case 2 of the lemma with $r_1 = 2$.

2.ii) We have $(m, r_1) > (1, 0)$. Putting

$$X = \frac{x}{2^{2q_1} 3^{2q_2} p^{2q_3}},\ Y = \frac{y}{2^{3q_1} 3^{3q_2} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1} 3^{r_2} p^{r_3} dX^2 + 2^{m+2r_1-2} 3^{\ell+2r_2} p^{2r_3} X$$

which is the curve in case 2 of the lemma with $r_1 = 0$ or 1.

3. We have $i+2 > \alpha-2i$, $j > \beta-2j$ and $k = \delta-2k$. In this case $v_2(a^2) = \alpha-2i$, $v_3(a^2) = \beta-2j$ so α and β are even. Therefore, $v_2(a) = \frac{\alpha}{2} - i$, $v_3(a) = \frac{\beta}{2} - j$. Also, $v_p(a^2) \geq k = \delta - 2k$ so $v_p(a^2) \geq \frac{k+\epsilon_3}{2}$ where ϵ_3 denotes the residue of k modulo 2. Let

$$u = \frac{a}{2^{\frac{\alpha}{2}-i} 3^{\frac{\beta}{2}-j} p^{\frac{k+\epsilon_3}{2}}}$$

so (A.2) becomes

$$p^{\epsilon_3} u^2 - 2^{3i-\alpha+2} 3^{3j-\beta} = \pm 1,$$

with $3i - \alpha + 2 \geq 1$ and $3j - \beta \geq 1$. Let

$$d = u,\ m = 3i - \alpha + 2,\ \ell = 3j - \beta,$$

then (d, m, ℓ) is a solution to

$$p^{\epsilon_3} d^2 - 2^m 3^\ell = \pm 1,$$

with $m, \ell \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{\alpha}{2}-i} 3^{\frac{\beta}{2}-j} p^{\frac{k+\epsilon_3}{2}} dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{\alpha}{2} - i = 2q_1 + r_1, \quad \frac{\beta}{2} - j = 2q_2 + r_2, \quad \frac{k}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider:

3.1) Suppose $\epsilon_3 = 0$.

3.1.i) If $(m, r_1) = (1, 0)$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2} p^{r_3} dX^2 + 2^3 3^{\ell+2r_2} p^{2r_3} X$$

which is the curve in case 2 of the lemma with $n = 0$ and $r_1 = 2$.

3.1.ii) If $(m, r_1) > (1, 0)$, then putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1} 3^{r_2} p^{r_3} dX^2 + 2^{m+2r_1-2} 3^{\ell+2r_2} p^{2r_3} X$$

which is the curve in case 2 of the lemma with $n = 0$ and $r_1 = 0$ or 1.

3.2) Suppose $\epsilon_3 = 1$.

3.2.i) If $(m, r_1) = (1, 0)$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2} p^{2-r_3} dX^2 + 2^3 3^{\ell+2r_2} p^{3-2r_3} X$$

which is the curve in case 5 of the lemma with $r_1 = 2$ and $r_3 = 1 - r_3$.

3.2.ii) We have $(m, r_1) > (1, 0)$ and $r_3 = 0$. Putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1} 3^{r_2} p^{2-r_3} dX^2 + 2^{m+2r_1-2} 3^{\ell+2r_2} p^{3-2r_3} X$$

which is the curve in case 5 of the lemma with $r_1 = 0$ or 1 and $r_3 = 1 - r_3$.

4. We have $i+2 > \alpha - 2i$, $j < \beta - 2j$ and $k > \delta - 2k$. In this case $v_2(a^2) = \alpha - 2i$, $v_3(a^2) = j$ and $v_p(a^2) = \delta - 2k$ so α, j, and δ are even. Therefore, $v_2(a) = \frac{\alpha}{2} - i$, $v_3(a) = \frac{j}{2}$, and $v_p(a) = \frac{\delta}{2} - k$. Let

$$u = \frac{a}{2^{\frac{\alpha}{2}-i}3^{\frac{j}{2}}p^{\frac{\delta}{2}-k}}$$

so (A.2) becomes

$$u^2 - 2^{3i-\alpha+2}p^{3k-\delta} = \pm 3^{\beta-3j},$$

with $3i - \alpha + 2 \geq 1$, $\beta - 3j \geq 1$ and $3k - \delta \geq 1$.

Let

$$d = u,\ m = 3i - \alpha + 2,\ \ell = \beta - 3j,\ n = 3k - \delta,$$

then (d, m, ℓ, n, p) is a solution to

$$d^2 - 2^m p^n = \pm 3^\ell,$$

with $m, \ell, n \geq 1$. The the model for E can be written

$$y^2 = x^3 + 2^{\frac{\alpha}{2}-i}3^{\frac{j}{2}}p^{\frac{\delta}{2}-k}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{\alpha}{2} - i = 2q_1 + r_1, \quad \frac{j}{2} = 2q_2 + r_2, \quad \frac{\delta}{2} - k = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. There are, again, two cases to consider:

4.i) We have $(m, r_1) = (1, 0)$. Putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2} p^{r_3} dX^2 + 2^3 3^{2r_2} p^{n+2r_3} X$$

which is the curve in case 3 of the lemma with $r_1 = 2$.

4.ii) We have $(m, r_1) > (1, 0)$. Putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1}3^{r_2}p^{r_3}dX^2 + 2^{m+2r_1-2}3^{2r_2}p^{n+2r_3}X$$

which is the curve in case 3 of the lemma with $r_1 = 0$ or 1.

5. We have $i+2 > \alpha-2i$, $j < \beta-2j$ and $k < \delta-2k$. In this case $v_2(a^2) = \alpha-2i$, $v_3(a^2) = j$ and $v_p(a^2) = k$ so α, j, and k are even. Therefore, $v_2(a) = \frac{\alpha}{2} - i$, $v_3(a) = \frac{j}{2}$, and $v_p(a) = \frac{k}{2}$. Let

$$u = \frac{a}{2^{\frac{\alpha}{2}-i}3^{\frac{j}{2}}p^{\frac{k}{2}}}$$

so (A.2) becomes

$$u^2 - 2^{3i-\alpha+2} = \pm 3^{\beta-3j}p^{\delta-3k},$$

with $3i - \alpha + 2 \geq 1$, $\beta - 3j \geq 1$ and $\delta - 3k \geq 1$.

Let

$$d = u,\ m = 3i - \alpha + 2,\ \ell = \beta - 3j,\ n = \delta - 3k,$$

then (d, m, ℓ, n, p) is a solution to

$$d^2 - 2^m = \pm 3^{\ell}p^n,$$

with $m, \ell, n \geq 1$. The the model for E can be written

$$y^2 = x^3 + 2^{\frac{\alpha}{2}-i}3^{\frac{j}{2}}p^{\frac{k}{2}}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{\alpha}{2} - i = 2q_1 + r_1, \quad \frac{j}{2} = 2q_2 + r_2, \quad \frac{k}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. There are, again, two cases to consider:

5.i) We have $(m, r_1) = (1, 0)$. Putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2}p^{r_3}dX^2 + 2^3 3^{2r_2}p^{2r_3}X$$

which is the curve in case 4 of the lemma with $r_1 = 2$.

5.ii) We have $(m, r_1) > (1, 0)$. Putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1}3^{r_2}p^{r_3}dX^2 + 2^{m+2r_1-2}3^{2r_2}p^{2r_3}X$$

which is the curve in case 4 of the lemma with $r_1 = 0$ or 1.

6. We have $i + 2 > \alpha - 2i$, $j < \beta - 2j$ and $k = \delta - 2k$. In this case $v_2(a^2) = \alpha - 2i$ and $v_3(a^2) = j$ so α and j are even. Therefore, $v_2(a) = \frac{\alpha}{2} - i$ and $v_3(a) = \frac{j}{2}$. Also, $v_p(a^2) \geq k = \delta - 2k$ so $v_p(a) \geq \frac{k+\epsilon_3}{2}$ where ϵ_3 denotes the residue of k modulo 2. Let

$$u = \frac{a}{2^{\frac{\alpha}{2}-i}3^{\frac{j}{2}}p^{\frac{k+\epsilon_3}{2}}}$$

so (A.2) becomes

$$p^{\epsilon_3}u^2 - 2^{3i-\alpha+2} = \pm 3^{\beta-3j},$$

with $3i - \alpha + 2 \geq 1$ and $\beta - 3j \geq 1$. Let

$$d = u,\ m = 3i - \alpha + 2,\ \ell = \beta - 3j,$$

then (d, m, ℓ, p) is a solution to

$$p^{\epsilon_3}d^2 - 2^m = \pm 3^{\ell},$$

with $m, \ell \geq 1$, and the model for E can be written

$$y^2 = x^3 + 2^{\frac{\alpha}{2}-i}3^{\frac{j}{2}}p^{\frac{k+\epsilon_3}{2}}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{\alpha}{2} - i = 2q_1 + r_1,\quad \frac{j}{2} = 2q_2 + r_2,\quad \frac{k+\epsilon_3}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider:

6.1) Suppose $\epsilon_3 = 0$.

6.1.i) If $(m, r_1) = (1, 0)$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2} p^{r_3} dX^2 + 2^3 3^{2r_2} p^{2r_3} X$$

which is the curve in case 4 of the lemma with $n = 0$ and $r_1 = 2$.

6.1.ii) If $(m, r_1) > (1, 0)$, then putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1} 3^{r_2} p^{r_3} dX^2 + 2^{m+2r_1-2} 3^{2r_2} p^{2r_3} X$$

which is the curve in case 4 of the lemma with $n = 0$ and $r_1 = 0$ or 1.

6.2) Suppose $\epsilon_3 = 1$.

6.2.i) If $(m, r_1) = (1, 0)$ and $r_3 = 0$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2(q_3-1)}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3(q_3-1)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2} p^2 dX^2 + 2^3 3^{2r_2} p^3 X$$

which is the curve in case 6 of the lemma with $r_1 = 2$ and $r_3 = 1$.

6.2.ii) If $(m, r_1) = (1, 0)$ and $r_3 = 1$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2} p dX^2 + 2^3 3^{2r_2} p X$$

which is the curve in case 6 of the lemma with $r_1 = 2$, $r_3 = 0$.

6.2.iii) If $(m, r_1) > (1, 0)$ and $r_3 = 0$, then putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2(q_3-1)}},\ Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3(q_3-1)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1}3^{r_2}p^2dX^2 + 2^{m+2r_1-2}3^{2r_2}p^3X$$

which is the curve in case 6 of the lemma with $r_1 = 0$ or 1 and $r_3 = 1$.

6.2.iv) If $(m, r_1) > (1, 0)$ and $r_3 = 0$, then putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1}3^{r_2}pdX^2 + 2^{m+2r_1-2}3^{2r_2}pX$$

which is the curve in case 6 of the lemma with $r_1 = 0$ or 1 and $r_3 = 0$.

7. We have $i + 2 > \alpha - 2i$, $j = \beta - 2j$ and $k > \delta - 2k$. In this case $v_2(a^2) = \alpha - 2i$, and $v_p(a^2) = \delta - 2k$ so α and δ are even. Therefore, $v_2(a) = \frac{\alpha}{2} - i$ and $v_p(a) = \frac{\delta}{2} - k$. Also, $v_3(a^2) \geq j = \beta - 2j$ so $v_3(a) \geq \frac{j+\epsilon_2}{2}$ where ϵ_2 denotes the residue of j modulo 2. Let

$$u = \frac{a}{2^{\frac{\alpha}{2}-i}3^{\frac{j+\epsilon_2}{2}}p^{\frac{\delta}{2}-k}}$$

so (A.2) becomes

$$3^{\epsilon_2}u^2 - 2^{3i-\alpha+2}p^{3k-\delta} = \pm 1,$$

with $3i - \alpha + 2 \geq 1$ and $3k - \delta \geq 1$. Let

$$d = u,\ m = 3i - \alpha + 2,\ n = 3k - \delta,$$

then (d, m, n, p) is a solution to

$$d^2 - 2^m p^n = \pm 1,$$

with $m, n \geq 1$, and the model for E can be written

$$y^2 = x^3 + 2^{\frac{\alpha}{2}-i}3^{\frac{j+\epsilon_2}{2}}p^{\frac{\delta}{2}-k}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{\alpha}{2} - i = 2q_1 + r_1,\quad \frac{j+\epsilon_2}{2} = 2q_2 + r_2,\quad \frac{\delta}{2} - k = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider:

7.1) Suppose $\epsilon_2 = 0$.

7.1.i) If $(m, r_1) = (1, 0)$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2} p^{r_3} dX^2 + 2^3 3^{2r_2} p^{n+2r_3} X$$

which is the curve in case 3 of the lemma with $\ell = 0$ and $r_1 = 2$.

7.1.ii) If $(m, r_1) > (1, 0)$, then putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1} 3^{r_2} p^{r_3} dX^2 + 2^{m+2r_1-2} 3^{2r_2} p^{n+2r_3} X$$

which is the curve in case 3 of the lemma with $\ell = 0$ and $r_1 = 0$ or 1.

7.2) Suppose $\epsilon_2 = 1$.

7.2.i) If $(m, r_1) = (1, 0)$ and $r_2 = 0$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2(q_2-1)}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3(q_2-1)}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^2 p^{r_3} dX^2 + 2^3 3^3 p^{n+2r_3} X$$

which is the curve in case 7 of the lemma with $r_1 = 2$ and $r_2 = 1$.

7.2.ii) If $(m, r_1) = (1, 0)$ and $r_2 = 1$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3 p^{r_3} dX^2 + 2^3 3 p^{n+2r_3} X$$

which is the curve in case 7 of the lemma with $r_1 = 2$, $r_2 = 0$.

7.2.iii) If $(m, r_1) > (1, 0)$ and $r_2 = 0$, then putting

$$X = \frac{x}{2^{2q_1}3^{2(q_2-1)}p^{2q_3}},\ Y = \frac{y}{2^{3q_1}3^{3(q_2-1)}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1}3^2p^{r_3}dX^2 + 2^{m+2r_1-2}3^3p^{n+2r_3}X$$

which is the curve in case 7 of the lemma with $r_1 = 0$ or 1 and $r_2 = 1$.

7.2.iv) If $(m, r_1) > (1, 0)$ and $r_2 = 1$, then putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1}3p^{r_3}dX^2 + 2^{m+2r_1-2}3p^{n+2r_3}X$$

which is the curve in case 7 of the lemma with $r_1 = 0$ or 1 and $r_2 = 0$.

8. We have $i + 2 > \alpha - 2i$, $j = \beta - 2j$ and $k < \delta - 2k$. In this case $v_2(a^2) = \alpha - 2i$, and $v_p(a^2) = k$ so α and k are even. Therefore, $v_2(a) = \frac{\alpha}{2} - i$ and $v_p(a) = \frac{k}{2}$. Also, $v_3(a^2) \geq j = \beta - 2j$ so $v_3(a^2) \geq \frac{j+\epsilon_2}{2}$ where ϵ_2 denotes the residue of j modulo 2. Let

$$u = \frac{a}{2^{\frac{\alpha}{2}-i}3^{\frac{j+\epsilon_2}{2}}p^{\frac{k}{2}}}$$

so (A.2) becomes

$$3^{\epsilon_2}u^2 - 2^{3i-\alpha+2} = \pm p^{\delta-3k},$$

with $3i - \alpha + 2 \geq 1$ and $\delta - 3k \geq 1$. Let

$$d = u,\ m = 3i - \alpha + 2,\ n = \delta - 3k,$$

then (d, m, n, p) is a solution to

$$d^2 - 2^m = \pm p^n,$$

with $m, n \geq 1$ and the model for E can be written

$$y^2 = x^3 + 2^{\frac{\alpha}{2}-i}3^{\frac{j}{2}}p^{\frac{k}{2}}dx^2 + 2^i3^jp^kx.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{\alpha}{2} - i = 2q_1 + r_1, \quad \frac{j}{2} = 2q_2 + r_2, \quad \frac{k}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider:

8.1) Suppose $\epsilon_2 = 0$.

8.1.i) If $(m, r_1) = (1, 0)$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}}, \; Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2} p^{r_3} dX^2 + 2^3 3^{2r_2} p^{2r_3} X$$

which is the curve in case 4 of the lemma with $\ell = 0$ and $r_1 = 2$.

8.1.ii) If $(m, r_1) > (1, 0)$, then putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2q_3}}, \; Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1} 3^{r_2} p^{r_3} dX^2 + 2^{m+2r_1-2} 3^{2r_2} p^{2r_3} X$$

which is the curve in case 4 of the lemma with $\ell = 0$ and $r_1 = 0$ or 1.

8.2) Suppose $\epsilon_2 = 1$.

8.2.i) If $(m, r_1) = (1, 0)$ and $r_2 = 0$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2(q_2-1)}p^{2q_3}}, \; Y = \frac{y}{2^{3(q_1-1)}3^{3(q_2-1)}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^2 p^{r_3} dX^2 + 2^3 3^3 p^{2r_3} X$$

which is the curve in case 8 of the lemma with $r_1 = 2$ and $r_2 = 1$.

8.2.ii) If $(m, r_1) = (1, 0)$ and $r_2 = 1$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}}, \; Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3 p^{r_3} d X^2 + 2^3 3 p^{2r_3} X$$

which is the curve in case 8 of the lemma with $r_1 = 2$, $r_2 = 0$.

8.2.iii) If $(m, r_1) > (1, 0)$ and $r_2 = 0$, then putting

$$X = \frac{x}{2^{2q_1} 3^{2(q_2-1)} p^{2q_3}},\ Y = \frac{y}{2^{3q_1} 3^{3(q_2-1)} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1} 3^2 p^{r_3} d X^2 + 2^{m+2r_1-2} 3^3 p^{2r_3} X$$

which is the curve in case 8 of the lemma with $r_1 = 0$ or 1 and $r_2 = 1$.

8.2.iv) If $(m, r_1) > (1, 0)$ and $r_2 = 1$,then putting

$$X = \frac{x}{2^{2q_1} 3^{2q_2} p^{2q_3}},\ Y = \frac{y}{2^{3q_1} 3^{3q_2} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1} 3 p^{r_3} d X^2 + 2^{m+2r_1-2} 3 p^{2r_3} X$$

which is the curve in case 8 of the lemma with $r_1 = 0$ or 1 and $r_2 = 0$.

9. We have $i + 2 > \alpha - 2i$, $j = \beta - 2j$ and $k = \delta - 2k$. In this case $v_2(a^2) = \alpha - 2i$, so α is even. Therefore $v_2(a) = \frac{\alpha}{2} - i$. Also, $v_3(a^2) \geq j = \beta - 2j$ and $v_p(a^2) \geq k = \delta - 2k$ so $v_3(a) \geq \frac{j+\epsilon_2}{2}$ and $v_p(a) \geq \frac{k+\epsilon_3}{2}$ where ϵ_2 denotes the residue of j modulo 2 and ϵ_3 denotes the residue of k modulo 2. Let

$$u = \frac{a}{2^{\frac{\alpha}{2}-i} 3^{\frac{j+\epsilon_2}{2}} p^{\frac{k+\epsilon_3}{2}}}$$

so (A.2) becomes

$$3^{\epsilon_2} p^{\epsilon_3} u^2 - 2^{3i-\alpha+2} = \pm 1,$$

with $3i - \alpha + 2 \geq 1$. Let

$$d = u,\ m = 3i - \alpha + 2,$$

then (d, m) is a solution to

$$3^{\epsilon_2} p^{\epsilon_3} d^2 - 2^m = \pm 1,$$

with $m, n \geq 1$, and the model for E can be written

$$y^2 = x^3 + 2^{\frac{\alpha}{2}-i} 3^{\frac{j+\epsilon_2}{2}} p^{\frac{k+\epsilon_3}{2}} dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{\alpha}{2} - i = 2q_1 + r_1, \quad \frac{j+\epsilon_2}{2} = 2q_2 + r_2, \quad \frac{k+\epsilon_3}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have four cases to consider:

9.1) Suppose $\epsilon_2 = 0$ and $\epsilon_3 = 0$.

9.1.i) If $(m, r_1) = (1, 0)$, then putting

$$X = \frac{x}{2^{2(q_1-1)} 3^{2q_2} p^{2q_3}}, \; Y = \frac{y}{2^{3(q_1-1)} 3^{3q_2} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2} p^{r_3} dX^2 + 2^3 3^{2r_2} p^{2r_3} X$$

which is the curve in case 4 of the lemma with $\ell = 0$, $n = 0$ and $r_1 = 2$.

9.1.ii) If $(m, r_1) > (1, 0)$, then putting

$$X = \frac{x}{2^{2q_1} 3^{2q_2} p^{2q_3}}, \; Y = \frac{y}{2^{3q_1} 3^{3q_2} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1} 3^{r_2} p^{r_3} dX^2 + 2^{m+2r_1-2} 3^{2r_2} p^{2r_3} X$$

which is the curve in case 4 of the lemma with $\ell = 0$, $n = 0$ and $r_1 = 0$ or 1.

9.2) Suppose $\epsilon_2 = 0$ and $\epsilon_3 = 1$.

9.2.i) If $(m, r_1) = (1, 0)$, then putting

$$X = \frac{x}{2^{2(q_1-1)} 3^{2q_2} p^{2(q_3-1+r_3)}}, \; Y = \frac{y}{2^{3(q_1-1)} 3^{3q_2} p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{r_2} p^{2-r_3} dX^2 + 2^3 3^{2r_2} p^{3-2r_3} X$$

which is the curve in case 6 of the lemma with $\ell = 0$, $r_1 = 2$ and $r_3 = 1 - r_3$.

9.2.ii) If $(m, r_1) > (1, 0)$, then putting

$$X = \frac{x}{2^{2q_1}3^{2q_2}p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3q_1}3^{3q_2}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^2dX^2 + 2^{m+2-2r_1}3^{2r_2}p^{3-2r_3}X$$

which is the curve in case 6 of the lemma with $\ell = 0$, $r_1 = 0$ or 1 and $r_3 = 1-r_3$.

9.3) Suppose $\epsilon_2 = 1$ and $\epsilon_3 = 0$.

9.3.i) If $(m, r_1) = (1, 0)$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2(q_2-1+r_2)}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3(q_2-1+r_2)}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{2-r_2}p^{r_3}dX^2 + 2^3 3^{3-2r_2}p^{2r_3}X$$

which is the curve in case 8 of the lemma with $n = 0$, $r_1 = 2$ and $r_2 = 1 - r_2$.

9.3.ii) If $(m, r_1) > (1, 0)$, then putting

$$X = \frac{x}{2^{2q_1}3^{2(q_2-1+r_2)}p^{2q_3}},\ Y = \frac{y}{2^{3q_1}3^{3(q_2-1+r_2)}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{2-r_2}p^{r_3}dX^2 + 2^{m+2-2r_1}3^{3-2r_2}p^{2r_3}X$$

which is the curve in case 8 of the lemma with $n = 0$, $r_1 = 0$ or 1 and $r_2 = 1 - r_2$.

9.4) Suppose $\epsilon_2 = 1$ and $\epsilon_3 = 1$.

9.4.i) If $(m, r_1) = (1, 0)$, then putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2(q_2-1+r_2)}p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3(q_2-1+r_2)}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^2 3^{2-r_2}p^{2-r_3}dX^2 + 2^3 3^{3-2r_2}p^{3-2r_3}X$$

which is the curve in case 9 of the lemma with $r_1 = 2$, $r_2 = 1 - r_2$ and $r_3 = 1 - r_3$.

9.4.ii) If $(m, r_1) > (1, 0)$, then putting

$$X = \frac{x}{2^{2q_1}3^{2(q_2-1+r_2)}p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3q_1}3^{3(q_2-1+r_2)}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{2-r_2}p^{2-r_3}dX^2 + 2^{m+2-2r_1}3^{3-2r_2}p^{3-2r_3}X$$

which is the curve in case 9 of the lemma with $r_1 = 0$ or 1, $r_2 = 1 - r_2$ and $r_3 = 1 - r_3$.

10. We have $i + 2 < \alpha - 2i$, $j > \beta - 2j$ and $k > \delta - 2k$. In this case $v_2(a^2) = i + 2$, $v_3(a^2) = \beta - 2j$ and $v_p(a^2) = \delta - 2k$ so i, β, and δ are even. Therefore, $v_2(a) = \frac{i}{2} + 1$, $v_3(a) = \frac{\beta}{2} - j$, and $v_p(a) = \frac{\delta}{2} - k$. Let

$$u = \frac{a}{2^{\frac{i}{2}+1}3^{\frac{\beta}{2}-j}p^{\frac{\delta}{2}-k}}$$

so (A.2) becomes

$$u^2 - 3^{3j-\beta}p^{3k-\delta} = \pm 2^{\alpha-3i-2},$$

with $\alpha - 3i - 2 \geq 1$, $3j - \beta \geq 1$ and $3k - \delta \geq 1$. Let

$$d = u,\ m = \alpha - 3i - 2,\ \ell = 3j - \beta,\ n = 3k - \delta,$$

then (d, m, ℓ, n, p) is a solution to

$$d^2 - 3^\ell p^n = \pm 2^m,$$

with $m, \ell, n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i}{2}+1}3^{\frac{\beta}{2}-j}p^{\frac{\delta}{2}-k}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i}{2} + 1 = 2q_1 + r_1,\quad \frac{\beta}{2} - j = 2q_2 + r_2,\quad \frac{\delta}{2} - k = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{\ell+2r_2}p^{n+2r_3}X$$

which is the curve in case 10 of the lemma with $r_1 = 1 - r_1$.

11. We have $i + 2 < \alpha - 2i$, $j > \beta - 2j$ and $k < \delta - 2k$. In this case $v_2(a^2) = i+2$, $v_3(a^2) = \beta-2j$ and $v_p(a^2) = k$ so i, β, and k are even. Therefore, $v_2(a) = \frac{i}{2} + 1$, $v_3(a) = \frac{\beta}{2} - j$, and $v_p(a) = \frac{k}{2}$. Let

$$u = \frac{a}{2^{\frac{i}{2}+1}3^{\frac{\beta}{2}-j}p^{\frac{k}{2}}}$$

so (A.2) becomes

$$u^2 - 3^{3j-\beta} = \pm 2^{\alpha-3i-2}p^{\delta-3k},$$

with $\alpha - 3i - 2 \geq 1$, $3j - \beta \geq 1$ and $\delta - 3k \geq 1$. Let

$$d = u,\ m = \alpha - 3i - 2,\ \ell = 3j - \beta,\ n = \delta - 3k,$$

then (d, m, ℓ, n, p) is a solution to

$$d^2 - 3^\ell = \pm 2^m p^n,$$

with $m, \ell, n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i}{2}+1}3^{\frac{\beta}{2}-j}p^{\frac{k}{2}}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i}{2} + 1 = 2q_1 + r_1, \quad \frac{\beta}{2} - j = 2q_2 + r_2, \quad \frac{k}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{\ell+2r_2}p^{2r_3}X$$

which is the curve in case 11 of the lemma with $r_1 = 1 - r_1$.

12. We have $i+2 < \alpha - 2i$, $j > \beta - 2j$ and $k = \delta - 2k$. In this case $v_2(a^2) = i+2$, $v_3(a^2) = \beta - 2j$ so i and β are even. Therefore, $v_2(a) = \frac{i}{2}+1$, $v_3(a) = \frac{\beta}{2} - j$. Also, $v_p(a^2) \geq k = \delta - 2k$ so $v_p(a) \geq \frac{k+\epsilon_3}{2}$ where ϵ_3 denotes the residue of k modulo 2. Let

$$u = \frac{a}{2^{\frac{i}{2}+1}3^{\frac{\beta}{2}-j}p^{\frac{k+\epsilon_3}{2}}}$$

so (A.2) becomes

$$p^{\epsilon_3}u^2 - 3^{3j-\beta} = \pm 2^{\alpha-3i-2},$$

with $\alpha - 3i - 2 \geq 1$ and $3j - \beta \geq 1$. Let

$$d = u,\ m = \alpha - 3i - 2,\ \ell = 3j - \beta,$$

then (d, m, ℓ) is a solution to

$$p^{\epsilon_3}d^2 - 3^{\ell} = \pm 2^m,$$

with $m, \ell \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i}{2}+1}3^{\frac{\beta}{2}-j}p^{\frac{k+\epsilon_3}{2}}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i}{2} + 1 = 2q_1 + r_1, \quad \frac{\beta}{2} - j = 2q_2 + r_2, \quad \frac{k+\epsilon_3}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider:

12.1) Suppose $\epsilon_3 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{\ell+2r_2}p^{2r_3}X$$

which is the curve in case 11 of the lemma with $n = 0$ and $r_1 = 1 - r_1$.

12.2) Suppose $\epsilon_3 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{2-r_3}dX^2 + 2^{2-2r_1}3^{\ell+2r_2}p^{3-2r_3}X$$

which is the curve in case 14 of the lemma with $r_1 = 1 - r_1$ and $r_3 = 1 - r_3$.

13. We have $i + 2 < \alpha - 2i$, $j < \beta - 2j$ and $k > \delta - 2k$. In this case $v_2(a^2) = i+2$, $v_3(a^2) = j$ and $v_p(a^2) = \delta - 2k$ so i, j, and δ are even. Therefore, $v_2(a) = \frac{i}{2} + 1$, $v_3(a) = \frac{j}{2}$, and $v_p(a) = \frac{\delta}{2} - k$. Let

$$u = \frac{a}{2^{\frac{i}{2}+1}3^{\frac{j}{2}}p^{\frac{\delta}{2}-k}}$$

so (A.2) becomes

$$u^2 - p^{3k-\delta} = \pm 2^{\alpha-3i-2}3^{\beta-3j},$$

with $\alpha - 3i - 2 \geq 1$, $\beta - 3j \geq 1$ and $3k - \delta \geq 1$. Let

$$d = u,\ m = \alpha - 3i - 2,\ \ell = \beta - 3j = \ell,\ n = 3k - \delta,$$

then (d, m, ℓ, n, p) is a solution to

$$d^2 - p^n = \pm 2^m 3^\ell,$$

with $m, \ell, n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i}{2}+1}3^{\frac{j}{2}}p^{\frac{\delta}{2}-k}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i}{2} + 1 = 2q_1 + r_1, \quad \frac{j}{2} = 2q_2 + r_2, \quad \frac{\delta}{2} - k = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{2r_2}p^{n+2r_3}X$$

which is the curve in case 12 of the lemma with $r_1 = 1 - r_1$.

14. We have $i+2 < \alpha - 2i$, $j < \beta - 2j$ and $k < \delta - 2k$. In this case $v_2(a^2) = i+2$, $v_3(a^2) = j$ and $v_p(a^2) = k$ so i, j, and k are even. Therefore, $v_2(a) = \frac{i}{2}+1$, $v_3(a) = \frac{j}{2}$, and $v_p(a) = \frac{k}{2}$. Let

$$u = \frac{a}{2^{\frac{i}{2}+1}3^{\frac{j}{2}}p^{\frac{k}{2}}}$$

so (A.2) becomes

$$u^2 - 1 = \pm 2^{\alpha-3i-2}3^{\beta-3j}p^{\delta-3k},$$

with $\alpha - 3i - 2 \geq 1$, $\beta - 3j \geq 1$ and $\delta - 3k \geq 1$. Let

$$d = u,\ m = \alpha - 3i - 2,\ \ell = \beta - 3j,\ n = \delta - 3k,$$

then (d, m, ℓ, n, p) is a solution to

$$d^2 - 1 = \pm 2^m 3^\ell p^n,$$

with $m, \ell, n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i}{2}+1}3^{\frac{j}{2}}p^{\frac{k}{2}}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i}{2} + 1 = 2q_1 + r_1, \quad \frac{j}{2} = 2q_2 + r_2, \quad \frac{k}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{2r_2}p^{2r_3}X$$

which is the curve in case 13 of the lemma with $r_1 = 1 - r_1$.

15. We have $i+2 < \alpha - 2i$, $j < \beta - 2j$ and $k = \delta - 2k$. In this case $v_2(a^2) = i+2$ and $v_3(a^2) = j$ so i and j are even. Therefore, $v_2(a) = \frac{i}{2}+1$ and $v_3(a) = \frac{j}{2}$. Also, $v_p(a^2) \geq k = \delta - 2k$ so $v_p(a) \geq \frac{k+\epsilon_3}{2}$ where ϵ_3 denotes the residue of k modulo 2. Let

$$u = \frac{a}{2^{\frac{i}{2}+1}3^{\frac{j}{2}}p^{\frac{k+\epsilon_3}{2}}}$$

so (A.2) becomes

$$p^{\epsilon_3}u^2 - 1 = \pm 2^{\alpha-3i-2}3^{\beta-3j},$$

with $\alpha - 3i - 2 \geq 1$ and $\beta - 3j \geq 1$. Let

$$d = u,\ m = \alpha - 3i - 2,\ \ell = \beta - 3j,$$

then (d, m, ℓ) is a solution to

$$p^{\epsilon_3}d^2 - 1 = \pm 2^m 3^\ell,$$

with $m, \ell \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i}{2}+1}3^{\frac{j}{2}}p^{\frac{k}{2}}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i}{2} + 1 = 2q_1 + r_1, \quad \frac{j}{2} = 2q_2 + r_2, \quad \frac{k+\epsilon_3}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider.

15.1) Suppose $\epsilon_3 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{2r_2}p^{2r_3}X$$

which is the curve in case 13 of the lemma with $n = 0$ and $r_1 = 1 - r_1$.

15.2) Suppose $\epsilon_3 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{2-r_3}dX^2 + 2^{2-2r_1}3^{2r_2}p^{3-2r_3}X$$

which is the curve in case 15 of the lemma with $r_1 = 1 - r_1$ and $r_3 = 1 - r_3$.

16. We have $i + 2 < \alpha - 2i$, $j = \beta - 2j$ and $k > \delta - 2k$. In this case $v_2(a^2) = i+2$, and $v_p(a^2) = \delta - 2k$ so i and δ are even. Therefore, $v_2(a) = \frac{i}{2} + 1$

and $v_p(a) = \frac{\delta}{2} - k$. Also, $v_3(a^2) \geq j = \beta - 2j$ so $v_3(a^2) \geq \frac{j+\epsilon_2}{2}$ where ϵ_2 denotes the residue of j modulo 2. Let

$$u = \frac{a}{2^{\frac{i}{2}+1} 3^{\frac{j+\epsilon_2}{2}} p^{\frac{\delta}{2}-k}}$$

so (A.2) becomes

$$3^{\epsilon_2} u^2 - p^{3k-\delta} = \pm 2^{\alpha-3i-2},$$

with $\alpha - 3i - 2 \geq 1$ and $3k - \delta \geq 1$. Let

$$d = u,\ m = \alpha - 3i - 2,\ n = 3k - \delta,$$

then (d, m, n, p) is a solution to

$$3^{\epsilon_2} d^2 - p^n = \pm 2^m,$$

with $m, n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i}{2}+1} 3^{\frac{j+\epsilon_2}{2}} p^{\frac{\delta}{2}-k} dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i}{2} + 1 = 2q_1 + r_1, \quad \frac{j+\epsilon_2}{2} = 2q_2 + r_2, \quad \frac{\delta}{2} - k = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider.

16.1) Suppose $\epsilon_2 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)} 3^{2q_2} p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)} 3^{3q_2} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1} 3^{r_2} p^{r_3} dX^2 + 2^{2-2r_1} 3^{2r_2} p^{n+2r_3} X$$

which is the curve in case 12 of the lemma with $\ell = 0$ and $r_1 = 1 - r_1$.

16.2) Suppose $\epsilon_2 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)} 3^{2(q_2-1+r_2)} p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)} 3^{3(q_2-1+r_2)} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1} 3^{2-r_2} p^{r_3} dX^2 + 2^{2-2r_1} 3^{3-2r_2} p^{n+2r_3} X$$

which is the curve in case 16 of the lemma with $r_1 = 1 - r_1$ and $r_2 = 1 - r_2$.

17. We have $i + 2 < \alpha - 2i$, $j = \beta - 2j$ and $k < \delta - 2k$. In this case $v_2(a^2) = i+2$, and $v_p(a^2) = k$ so i and k are even. Therefore, $v_2(a) = \frac{i}{2}+1$ and $v_p(a) = \frac{k}{2}$. Also, $v_3(a^2) \geq j = \beta - 2j$ so $v_3(a^2) \geq \frac{j+\epsilon_2}{2}$ where ϵ_2 is the residue of j modulo 2. Let

$$u = \frac{a}{2^{\frac{i}{2}+1}3^{\frac{j+\epsilon_2}{2}}p^{\frac{k}{2}}}$$

so (A.2) becomes

$$3^{\epsilon_2}u^2 - 1 = \pm 2^{\alpha-3i-2}p^{\delta-3k},$$

with $\alpha - 3i - 2 \geq 1$ and $\delta - 3k \geq 1$. Let

$$d = u,\ m = \alpha - 3i - 2,\ n = \delta - 3k,$$

then (d, m, n, p) is a solution to

$$3^{\epsilon_2}d^2 - 1 = \pm 2^m p^n,$$

with $m, n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i}{2}+1}3^{\frac{j+\epsilon_2}{2}}p^{\frac{k}{2}}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i}{2} + 1 = 2q_1 + r_1, \quad \frac{j+\epsilon_2}{2} = 2q_2 + r_2, \quad \frac{k}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider.

17.1) Suppose $\epsilon_2 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{2r_2}p^{2r_3}X$$

which is the curve in case 13 of the lemma with $\ell = 0$ and $r_1 = 1 - r_1$.

17.2) Suppose $\epsilon_2 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2(q_2-1+r_2)}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3(q_2-1+r_2)}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{2-r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{3-2r_2}p^{2r_3}X$$

which is the curve in case 17 of the lemma with $r_1 = 1 - r_1$ and $r_2 = 1 - r_2$.

18. We have $i + 2 < \alpha - 2i$, $j = \beta - 2j$ and $k = \delta - 2k$. In this case $v_2(a^2) = i + 2$, so i is even. Therefore $v_2(a) = \frac{i}{2} + 1$. Also, $v_3(a^2) \geq j = \beta - 2j$ and $v_p(a^2) \geq k = \delta - 2k$ so $v_3(a) \geq \frac{j+\epsilon_2}{2}$ and $v_p(a) \geq \frac{k+\epsilon_3}{2}$ where ϵ_2 denotes the residue of j modulo 2 and ϵ_3 denotes the residue of k modulo 2. Let

$$u = \frac{a}{2^{\frac{i}{2}+1}3^{\frac{j+\epsilon_2}{2}}p^{\frac{k+\epsilon_3}{2}}}$$

so (A.2) becomes

$$3^{\epsilon_2}p^{\epsilon_3}u^2 - 1 = \pm 2^{\alpha-3i-2},$$

with $\alpha - 3i - 2 \geq 1$. Let

$$d = u,\ m = \alpha - 3i - 2,$$

then (d, m) is a solution to

$$3^{\epsilon_2}p^{\epsilon_3}d^2 - 1 = \pm 2^m,$$

with $m, n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i}{2}+1}3^{\frac{j+\epsilon_2}{2}}p^{\frac{k+\epsilon_3}{2}}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i}{2} + 1 = 2q_1 + r_1, \quad \frac{j+\epsilon_2}{2} = 2q_2 + r_2, \quad \frac{k+\epsilon_3}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. There are four cases to consider.

18.1) Suppose $\epsilon_2 = 0$ and $\epsilon_3 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{2r_2}p^{2r_3}X$$

which is the curve in case 13 of the lemma with $\ell = 0$, $n = 0$ and $r_1 = 1 - r_1$.

18.2) Suppose $\epsilon_2 = 0$ and $\epsilon_3 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{2-r_3}dX^2 + 2^{2-2r_1}3^{2r_2}p^{3-2r_3}X$$

which is the curve in case 15 of the lemma with $\ell = 0$, $r_1 = 1 - r_1$ and $r_3 = 1 - r_3$.

18.3) Suppose $\epsilon_2 = 1$ and $\epsilon_3 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2(q_2-1+r_2)}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3(q_2-1+r_2)}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{2-r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{3-2r_2}p^{2r_3}X$$

which is the curve in case 17 of the lemma with $n = 0$, $r_1 = 1 - r_1$ and $r_2 = 1 - r_2$.

18.4) Suppose $\epsilon_2 = 1$ and $\epsilon_3 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2(q_2-1+r_2)}p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3(q_2-1+r_2)}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_!}3^{2-r_2}p^{2-r_3}dX^2 + 2^{2-2r_1}3^{3-2r_2}p^{3-2r_3}X$$

which is the curve in case 18 of the lemma with $r_1 = 1 - r_1$, $r_2 = 1 - r_2$ and $r_3 = 1 - r_3$.

19. We have $i + 2 = \alpha - 2i$, $j > \beta - 2j$ and $k > \delta - 2k$. In this case $v_3(a^2) = \beta - 2j$ and $v_p(a^2) = \delta - 2k$ so β, and δ are even. Therefore, $v_3(a) = \frac{\beta}{2} - j$ and $v_p(a) = \frac{\delta}{2} - k$. Also, $v_2(a^2) =\geq i + 2 = \alpha - 2i$ so $v_2(a) =\geq \frac{i+\epsilon_1}{2} + 1$ where ϵ_1 is the residue of i modulo 2. Let

$$u = \frac{a}{2^{\frac{i+\epsilon_1}{2}+1}3^{\frac{\beta}{2}-j}p^{\frac{\delta}{2}-k}}$$

so (A.2) becomes

$$2^{\epsilon_1}u^2 - 3^{3j-\beta}p^{3k-\delta} = \pm 1,$$

with $3j - \beta \geq 1$ and $3k - \delta \geq 1$. Let

$$d = u,\ \ell = 3j - \beta = \ell,\ n = 3k - \delta,$$

then (d, ℓ, n, p) is a solution to

$$2^{\epsilon_1}d^2 - 3^{\ell}p^n = \pm 1,$$

with $\ell, n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i+\epsilon_1}{2}+1}3^{\frac{\beta}{2}-j}p^{\frac{\delta}{2}-k}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i+\epsilon_1}{2} + 1 = 2q_1 + r_1, \quad \frac{\beta}{2} - j = 2q_2 + r_2, \quad \frac{\delta}{2} - k = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider.

19.1) Suppose $\epsilon_1 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{\ell+2r_2}p^{n+2r_3}X$$

which is the curve in case 10 of the lemma with $m = 0$ and $r_1 = 1 - r_1$.

19.2) Suppose $\epsilon_1 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1+2}3^{r_2}p^{r_3}dX^2 + 2^{2r_1+1}3^{\ell+2r_2}p^{n+2r_3}X$$

which is the curve in case 19 of the lemma.

20. We have $i + 2 = \alpha - 2i$, $j > \beta - 2j$ and $k < \delta - 2k$. In this case $v_3(a^2) = \beta - 2j$ and $v_p(a^2) = k$ so β, and k are even. Therefore, $v_3(a) = \frac{\beta}{2} - j$,

and $v_p(a) = \frac{k}{2}$. Also, $v_2(a^2) =\geq i+2 = \alpha - 2i$ so $v_2(a) =\geq \frac{i+\epsilon_1}{2} + 1$ where ϵ_1 is the residue of i modulo 2. Let

$$u = \frac{a}{2^{\frac{i+\epsilon_1}{2}+1} 3^{\frac{\beta}{2}-j} p^{\frac{k}{2}}}$$

so (A.2) becomes

$$2^{\epsilon_1} u^2 - 3^{3j-\beta} = \pm p^{\delta - 3k},$$

with $3j - \beta \geq 1$ and $\delta - 3k \geq 1$. Let

$$d = u,\ \ell = 3j - \beta,\ n = \delta - 3k,$$

then (d, ℓ, n, p) is a solution to

$$2^{\epsilon_1} d^2 - 3^{\ell} = \pm p^n,$$

with $\ell, n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i+\epsilon_1}{2}+1} 3^{\frac{\beta}{2}-j} p^{\frac{k}{2}} dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i+\epsilon_1}{2} + 1 = 2q_1 + r_1, \quad \frac{\beta}{2} - j = 2q_2 + r_2, \quad \frac{k}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider.

20.1) Suppose $\epsilon_1 = 0$. Putting

$$X = \frac{x}{2^{2(q_1 - 1 + r_1)} 3^{2q_2} p^{2q_3}},\ Y = \frac{y}{2^{3(q_1 - 1 + r_1)} 3^{3q_2} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1} 3^{r_2} p^{r_3} dX^2 + 2^{2-2r_1} 3^{\ell + 2r_2} p^{2r_3} X$$

which is the curve in case 11 of the lemma with $m = 0$ and $r_1 = 1 - r_1$.

20.2) Suppose $\epsilon_1 = 0$. Putting

$$X = \frac{x}{2^{2(q_1 - 1)} 3^{2q_2} p^{2q_3}},\ Y = \frac{y}{2^{3(q_1 - 1)} 3^{3q_2} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1 + 2} 3^{r_2} p^{r_3} dX^2 + 2^{2r_1 + 1} 3^{\ell + 2r_2} p^{2r_3} X$$

which is the curve in case 20 of the lemma.

21. We have $i+2=\alpha-2i$, $j>\beta-2j$ and $k=\delta-2k$. In this case $v_3(a^2)=\beta-2j$ so β is even. Therefore, $v_3(a)=\frac{\beta}{2}-j$. Also, $v_2(a^2)\geq i+2=\alpha-2i$ and $v_p(a^2)\geq k=\delta-2k$ so let ϵ_1 and ϵ_3 denote the residues of i and k modulo 2, respectively. Then $v_2(a)\geq\frac{i+\epsilon_1}{2}+1$ and $v_p(a)\geq\frac{k+\epsilon_3}{2}$. Let

$$u=\frac{a}{2^{\frac{i+\epsilon_1}{2}+1}3^{\frac{\beta}{2}-j}p^{\frac{k+\epsilon_3}{2}}}$$

so (A.2) becomes

$$2^{\epsilon_1}p^{\epsilon_2}u^2-3^{3j-\beta}=\pm1,$$

with $3j-\beta\geq1$. Let

$$d=u,\ \ell=3j-\beta,$$

then (d,m,ℓ) is a solution to

$$2^{\epsilon_1}p^{\epsilon_2}d^2-3^{\ell}=\pm1,$$

with $\ell\geq1$. The model for E can be written

$$y^2=x^3+2^{\frac{i+\epsilon_1}{2}+1}3^{\frac{\beta}{2}-j}p^{\frac{k+\epsilon_3}{2}}dx^2+2^i3^jp^kx.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i+\epsilon_1}{2}+1=2q_1+r_1,\quad\frac{\beta}{2}-j=2q_2+r_2,\quad\frac{k+\epsilon_3}{2}=2q_3+r_3,$$

with $r_1,r_2,r_3\in\{0,1\}$. We have four cases to consider:

21.1) Suppose $\epsilon_1=0$ and $\epsilon_3=0$. Putting

$$X=\frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y=\frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2=X^3+2^{2-r_1}3^{r_2}p^{r_3}dX^2+2^{2-2r_1}3^{\ell+2r_2}p^{2r_3}X$$

which is the curve in case 11 of the lemma with $m=0$, $n=0$ and $r_1=1-r_1$.

21.2) Suppose $\epsilon_1=0$ and $\epsilon_3=1$. Putting

$$X=\frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2(q_3-1+r_3)}},\ Y=\frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{2-r_3}dX^2 + 2^{2-2r_1}3^{\ell+2r_2}p^{3-2r_3}X$$

which is the curve in case 14 of the lemma with $m = 0$, $r_1 = 1 - r_1$ and $r_3 = 1 - r_3$.

21.3) Suppose $\epsilon_1 = 1$ and $\epsilon_3 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1+2}3^{r_2}p^{r_3}dX^2 + 2^{2r_1+1}3^{\ell+2r_2}p^{2r_3}X$$

which is the curve in case 20 of the lemma with $n = 0$.

21.4) Suppose $\epsilon_1 = 1$ and $\epsilon_3 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1+2}3^{r_2}p^{2-r_3}dX^2 + 2^{2r_1+1}3^{\ell+2r_2}p^{3-2r_3}X$$

which is the curve in case 23 of the lemma with $r_3 = 1 - r_3$.

22. We have $i + 2 = \alpha - 2i$, $j < \beta - 2j$ and $k > \delta - 2k$. In this case $v_3(a^2) = j$ and $v_p(a^2) = \delta - 2k$ so j, and δ are even. Therefore, $v_3(a) = \frac{j}{2}$ and $v_p(a) = \frac{\delta}{2} - k$. Also, $v_2(a^2) =\geq i + 2 = \alpha - 2i$ so $v_2(a) =\geq \frac{i+\epsilon_1}{2} + 1$ where ϵ_1 is the residue of i modulo 2. Let

$$u = \frac{a}{2^{\frac{i+\epsilon_1}{2}+1}3^{\frac{j}{2}}p^{\frac{\delta}{2}-k}}$$

so (A.2) becomes

$$2^{\epsilon_1}u^2 - p^{3k-\delta} = \pm 3^{\beta-3j},$$

with $\beta - 3j \geq 1$ and $3k - \delta \geq 1$. Let

$$d = u,\ \ell = \beta - 3j,\ n = 3k - \delta,$$

then (d, ℓ, n, p) is a solution to

$$2^{\epsilon_1} d^2 - p^n = \pm 3^\ell,$$

with $\ell, n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i+\epsilon_1}{2}+1} 3^{\frac{j}{2}} p^{\frac{\delta}{2}-k} dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i+\epsilon_1}{2} + 1 = 2q_1 + r_1, \quad \frac{j}{2} = 2q_2 + r_2, \quad \frac{\delta}{2} - k = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider.

22.1) Suppose $\epsilon_1 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)} 3^{2q_2} p^{2q_3}}, \; Y = \frac{y}{2^{3(q_1-1+r_1)} 3^{3q_2} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1} 3^{r_2} p^{r_3} dX^2 + 2^{2-2r_1} 3^{2r_2} p^{n+2r_3} X$$

which is the curve in case 12 of the lemma with $m = 0$ and $r_1 = 1 - r_1$.

22.2) Suppose $\epsilon_1 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1)} 3^{2q_2} p^{2q_3}}, \; Y = \frac{y}{2^{3(q_1-1)} 3^{3q_2} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1+2} 3^{r_2} p^{r_3} dX^2 + 2^{2r_1+1} 3^{2r_2} p^{n+2r_3} X$$

which is the curve in case 21 of the lemma.

23. We have $i+2 = \alpha - 2i$, $j < \beta - 2j$ and $k > \delta - 2k$. In this case $v_3(a^2) = j$ and $v_p(a^2) = k$ so j, and k are even. Therefore, $v_3(a) = \frac{j}{2}$ and $v_p(a) = \frac{k}{2}$. Also, $v_2(a^2) =\geq i + 2 = \alpha - 2i$ so $v_2(a) =\geq \frac{i+\epsilon_1}{2} + 1$ where ϵ_1 is the residue of i modulo 2. Let

$$u = \frac{a}{2^{\frac{i+\epsilon_1}{2}+1} 3^{\frac{j}{2}} p^{\frac{k}{2}}}$$

so (A.2) becomes

$$2^{\epsilon_1} u^2 - 1 = \pm 3^{\beta-3j} p^{\delta-3k},$$

with $\beta - 3j \geq 1$ and $\delta - 3k \geq 1$. Let

$$d = u,\ \ell = \beta - 3j,\ n = \delta - 3k,$$

then (d, ℓ, n, p) is a solution to

$$2^{\epsilon_1} d^2 - 1 = \pm 3^{\ell} p^n,$$

with $\ell, n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i+\epsilon_1}{2}+1} 3^{\frac{j}{2}} p^{\frac{k}{2}} dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i+\epsilon_1}{2} + 1 = 2q_1 + r_1, \quad \frac{j}{2} = 2q_2 + r_2, \quad \frac{k}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have two cases to consider:

23.1) Suppose $\epsilon_1 = 0$. Putting

$$X = \frac{x}{2^{2(q_1 - 1 + r_1)} 3^{2q_2} p^{2q_3}},\ Y = \frac{y}{2^{3(q_1 - 1 + r_1)} 3^{3q_2} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1} 3^{r_2} p^{r_3} dX^2 + 2^{2-2r_1} 3^{2r_2} p^{2r_3} X$$

which is the curve in case 13 of the lemma with $m = 0$ and $r_1 = 1 - r_1$.

23.2) Suppose $\epsilon_1 = 0$. This is impossible since there are no solutions to the equation $2d^2 - 1 = \pm 3^{\ell} p^n$ with $\ell \geq 1$ due to a local obstruction at 3.

24. We have $i + 2 = \alpha - 2i$, $j < \beta - 2j$ and $k = \delta - 2k$. In this case $v_3(a^2) = j$ so j is even. Therefore, $v_3(a) = \frac{j}{2}$. Also, $v_2(a^2) \geq i + 2 = \alpha - 2i$ and $v_p(a^2) \geq k = \delta - 2k$ so let ϵ_1 and ϵ_3 denote the residues of i and k modulo 2, respectively. Then $v_2(a) \geq \frac{i+\epsilon_1}{2} + 1$ and $v_p(a) \geq \frac{k+\epsilon_3}{2}$. Let

$$u = \frac{a}{2^{\frac{i+\epsilon_1}{2}+1} 3^{\frac{j}{2}} p^{\frac{k+\epsilon_3}{2}}}$$

so (A.2) becomes

$$2^{\epsilon_1} p^{\epsilon_2} u^2 - 1 = \pm 3^{\beta - 3j},$$

with $\beta - 3j \geq 1$. Let

$$d = u,\ \ell = \beta - 3j,$$

then (d, ℓ) is a solution to

$$2^{\epsilon_1} p^{\epsilon_2} d^2 - 1 = \pm 3^{\ell},$$

with $\ell \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i+\epsilon_1}{2}+1} 3^{\frac{j}{2}} p^{\frac{k+\epsilon_3}{2}} dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i+\epsilon_1}{2} + 1 = 2q_1 + r_1, \quad \frac{j}{2} = 2q_2 + r_2, \quad \frac{k+\epsilon_3}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have four cases to consider:

24.1) Suppose $\epsilon_1 = 0$ and $\epsilon_3 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)} 3^{2q_2} p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)} 3^{3q_2} p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1} 3^{r_2} p^{r_3} dX^2 + 2^{2-2r_1} 3^{2r_2} p^{2r_3} X$$

which is the curve in case 13 of the lemma with $m = 0$, $n = 0$ and $r_1 = 1 - r_1$.

24.2) Suppose $\epsilon_1 = 0$ and $\epsilon_3 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)} 3^{2q_2} p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3(q_1-1+r_1)} 3^{3q_2} p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1} 3^{r_2} p^{2-r_3} dX^2 + 2^{2-2r_1} 3^{2r_2} p^{3-2r_3} X$$

which is the curve in case 15 of the lemma with $m = 0$, $r_1 = 1 - r_1$ and $r_3 = 1 - r_3$.

24.3) Suppose $\epsilon_1 = 1$ and $\epsilon_3 = 0$. This is impossible since there are no solutions to the equation $2d^2 - 1 = \pm 3^{\ell}$, with $\ell \geq 1$, due to a local obstruction at 3.

24.4) Suppose $\epsilon_1 = 1$ and $\epsilon_3 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2(q_3-1+r_3)}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3(q_3-1+r_3)}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1+2}3^{r_2}p^{2-r_3}dX^2 + 2^{2r_1+1}3^{2r_2}p^{3-2r_3}X$$

which is the curve in case 24 of the lemma with $r_3 = 1 - r_3$.

25. We have $i + 2 = \alpha - 2i$, $j = \beta - 2j$ and $k > \delta - 2k$. In this case $v_p(a^2) = \delta - 2k$ so δ is even. Therefore, $v_p(a) = \frac{\delta}{2} - k$. Also, $v_2(a^2) \geq i + 2 = \alpha - 2i$ and $v_3(a^2) \geq j = \beta - 2j$ so let ϵ_1 and ϵ_2 denote the residues of i and j modulo 2, respectively. Then $v_2(a) \geq \frac{i+\epsilon_1}{2} + 1$ and $v_3(a) \geq \frac{j+\epsilon_2}{2}$. Let

$$u = \frac{a}{2^{\frac{i+\epsilon_1}{2}+1}3^{\frac{j+\epsilon_2}{2}}p^{\frac{\delta}{2}-k}}$$

so (A.2) becomes

$$2^{\epsilon_1}3^{\epsilon_2}u^2 - p^{3k-\delta} = \pm 1,$$

with $3k - \delta \geq 1$. Let

$$d = u,\ n = 3k - \delta,$$

then (d, n, p) is a solution to

$$2^{\epsilon_1}3^{\epsilon_2}d^2 - p^n = \pm 1,$$

with $n \geq 1$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i+\epsilon_1}{2}+1}3^{\frac{j+\epsilon_2}{2}}p^{\frac{\delta}{2}-k}dx^2 + 2^i3^jp^kx.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i+\epsilon_1}{2} + 1 = 2q_1 + r_1,\quad \frac{j+\epsilon_2}{2} - j = 2q_2 + r_2,\quad \frac{\delta}{2} - k = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have four cases to consider:

25.1) Suppose $\epsilon_1 = 0$ and $\epsilon_2 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{2r_2}p^{n+2r_3}X$$

which is the curve in case 12 of the lemma with $m = 0$, $\ell = 0$ and $r_1 = 1 - r_1$.

25.2) Suppose $\epsilon_1 = 0$ and $\epsilon_2 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2(q_2-1+r_2)}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3(q_2-1+r_2)}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{2-r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{3-2r_2}p^{n+2r_3}X$$

which is the curve in case 16 of the lemma with $m = 0$, $r_1 = 1 - r_1$ and $r_2 = 1 - r_2$.

25.3) Suppose $\epsilon_1 = 1$ and $\epsilon_2 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1+2}3^{r_2}p^{r_3}dX^2 + 2^{2r_1+1}3^{2r_2}p^{n+2r_3}X$$

which is the curve in case 21 of the lemma with $\ell = 0$.

25.4) Suppose $\epsilon_1 = 1$ and $\epsilon_2 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2(q_2-1+r_2)}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3(q_2-1+r_2)}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1+2}3^{2-r_2}p^{r_3}dX^2 + 2^{2r_1+1}3^{3-2r_2}p^{n+2r_3}X$$

which is the curve in case 25 of the lemma with $r_2 = 1 - r_2$.

26. We have $i + 2 = \alpha - 2i$, $j = \beta - 2j$ and $k < \delta - 2k$. In this case $v_p(a^2) = k$ so k is even. Therefore, $v_p(a) = \frac{k}{2}$. Also, $v_2(a^2) \geq i + 2 = \alpha - 2i$ and $v_3(a^2) \geq j = \beta - 2j$ so let ϵ_1 and ϵ_2 denote the residues of i and j modulo 2, respectively. Then $v_2(a) \geq \frac{i+\epsilon_1}{2} + 1$ and $v_3(a) \geq \frac{j+\epsilon_2}{2}$. Let

$$u = \frac{a}{2^{\frac{i+\epsilon_1}{2}+1}3^{\frac{j+\epsilon_2}{2}}p^{\frac{k}{2}}}$$

so (A.2) becomes

$$2^{\epsilon_1}3^{\epsilon_2}u^2 - 1 = \pm p^{\delta-3k},$$

with $\delta - 3k \geq 1$.

Suppose that (d, n, p) is a solution to

$$2^{\epsilon_1}3^{\epsilon_2}d^2 - 1 = \pm p^n,$$

with $n \geq 1$. Then we may write

$$u = d,\ \delta - 3k = n.$$

Then the model for E can be written

$$y^2 = x^3 + 2^{\frac{i+\epsilon_1}{2}+1}3^{\frac{j+\epsilon_2}{2}}p^{\frac{k}{2}}dx^2 + 2^i 3^j p^k x.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i+\epsilon_1}{2} + 1 = 2q_1 + r_1, \quad \frac{j+\epsilon_2}{2} - j = 2q_2 + r_2, \quad \frac{k}{2} = 2q_3 + r_3,$$

with $r_1, r_2, r_3 \in \{0, 1\}$. We have four cases to consider:

26.1) Suppose $\epsilon_1 = 0$ and $\epsilon_2 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{2r_2}p^{2r_3}X$$

which is the curve in case 13 of the lemma with $m = 0$, $\ell = 0$ and $r_1 = 1 - r_1$.

26.2) Suppose $\epsilon_1 = 0$ and $\epsilon_2 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1+r_1)}3^{2(q_2-1+r_2)}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1+r_1)}3^{3(q_2-1+r_2)}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{2-r_1}3^{2-r_2}p^{r_3}dX^2 + 2^{2-2r_1}3^{3-2r_2}p^{2r_3}X$$

which is the curve in case 17 of the lemma with $m = 0$, $r_1 = 1 - r_1$ and $r_2 = 1 - r_2$.

26.3) Suppose $\epsilon_1 = 1$ and $\epsilon_2 = 0$. Putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1+2}3^{r_2}p^{r_3}dX^2 + 2^{2r_1+1}3^{2r_2}p^{2r_3}X$$

which is the curve in case 22 of the lemma with $\ell = 0$.

26.4) Suppose $\epsilon_1 = 1$ and $\epsilon_2 = 1$. Putting

$$X = \frac{x}{2^{2(q_1-1)}3^{2(q_2-1+r_2)}p^{2q_3}},\ Y = \frac{y}{2^{3(q_1-1)}3^{3(q_2-1+r_2)}p^{3q_3}},$$

we obtain the new model for E

$$Y^2 = X^3 + 2^{r_1+2}3^{2-r_2}p^{r_3}dX^2 + 2^{2r_1+1}3^{3-2r_2}p^{2r_3}X$$

which is the curve in case 26 of the lemma with $r_2 = 1 - r_2$.

27. We have $i + 2 = \alpha - 2i$, $j = \beta - 2j$ and $k = \delta - 2k$. In this case $v_2(a^2) \geq i + 2 = \alpha - 2i$, $v_3(a^2) \geq j = \beta - 2j$ and $v_p(a^2) \geq k = \delta - 2k$. Let ϵ_1, ϵ_2 and ϵ_3 denote the residues of i, j and k modulo 2, respectively. Then $v_2(a) \geq \frac{i+\epsilon_1}{2} + 1$, $v_3(a) \geq \frac{j+\epsilon_2}{2}$ and $v_p(a) \geq \frac{k+\epsilon_3}{2}$. Let

$$u = \frac{a}{2^{\frac{i+\epsilon_1}{2}+1}3^{\frac{j+\epsilon_2}{2}}p^{\frac{k+\epsilon_3}{2}}}$$

so (A.2) becomes

$$2^{\epsilon_1}3^{\epsilon_2}p^{\epsilon_3}u^2 - 1 = \pm 1.$$

Clearly $u = 0$ is a solution to this equation and this leads to the curve

$$y^2 = x^3 + 2^r3^sp^tx,$$

where $r, s, t \in \{0, 1, 2, 3\}$, which appears in one of the cases 13, 15, 17, 18, 22, 24, 26, 27 of the lemma with $d = 0$.

The only other solution to $2^{\epsilon_1}3^{\epsilon_2}p^{\epsilon_3}u^2 - 1 = \pm 1$ has $u = 1$ and $(\epsilon_1, \epsilon_2, \epsilon_3) = (1, 0, 0)$. The model for E can be written

$$y^2 = x^3 + 2^{\frac{i+1}{2}+1}3^{\frac{j}{2}}p^{\frac{k}{2}}x^2 + 2^i3^jp^kx.$$

There exist six integers r_1, q_1, r_2, q_2, r_3, and q_3 such that

$$\frac{i+\epsilon_1}{2}+1=2q_1+r_1,\quad \frac{j}{2}=2q_2+r_2,\quad \frac{k}{2}=2q_3+r_3,$$

with $r_1, r_2, r_3 \in \{0,1\}$. Putting

$$X=\frac{x}{2^{2(q_1-1)}3^{2q_2}p^{2q_3}},\ Y=\frac{y}{2^{3(q_1-1)}3^{3q_2}p^{3q_3}},$$

we obtain the new model for E

$$Y^2=X^3+2^{r_1+2}3^{r_2}p^{r_3}dX^2+2^{2r_1+1}3^{2r_2}p^{2r_3}X$$

which is the curve in case 22 of the lemma with $\ell=0$ and $n=0$.

This completes the proof of the lemma.

□

A.2 $b<0$

Lemma A.2 *Suppose $b<0$. Then there exists an integer d, and non-negative integers m, ℓ, and n satisfying one of the equations in the first column and E is $\mathbb{Q}$-isomorphic to the corresponding curve in the second column, for some $r_1, r_2, r_3 \in \{0,1\}$; except in cases 2 to 8, where if $m=1$ then $r_1 \in \{1,2\}$.*

	Diophantine Equation	$y^2 = x^3 + a_2x^2 + a_4x$	
		a_2	a_4
2	$d^2 + 2^m3^\ell = p^n$	$2^{r_1}3^{r_2}p^{r_3}d$	$-2^{m+2r_1-2}3^{\ell+2r_2}p^{2r_3}$
3	$d^2 + 2^mp^n = 3^\ell$	$2^{r_1}3^{r_2}p^{r_3}d$	$-2^{m+2r_1-2}3^{2r_2}p^{n+2r_3}$
4	$d^2 + 2^m = 3^\ell p^n$	$2^{r_1}3^{r_2}p^{r_3}d$	$-2^{m+2r_1-2}3^{2r_2}p^{2r_3}$
6	$pd^2 + 2^m = 3^\ell$	$2^{r_1}3^{r_2}p^{r_3+1}d$	$-2^{m+2r_1-2}3^{2r_2}p^{2r_3+1}$
8	$3d^2 + 2^m = p^n$	$2^{r_1}3^{r_2+1}p^{r_3}d$	$-2^{m+2r_1-2}3^{2r_2+1}p^{2r_3}$
10	$d^2 + 3^\ell p^n = 2^m$	$2^{r_1+1}3^{r_2}p^{r_3}d$	$-2^{2r_1}3^{\ell+2r_2}p^{n+2r_3}$
11	$d^2 + 3^\ell = 2^mp^n$	$2^{r_1+1}3^{r_2}p^{r_3}d$	$-2^{2r_1}3^{\ell+2r_2}p^{2r_3}$
12	$d^2 + p^n = 2^m3^\ell$	$2^{r_1+1}3^{r_2}p^{r_3}d$	$-2^{2r_1}3^{2r_2}p^{n+2r_3}$
13	$d^2 + 1 = 2^m3^\ell p^n$	$2^{r_1+1}3^{r_2}p^{r_3}d$	$-2^{2r_1}3^{2r_2}p^{2r_3}$
14	$pd^2 + 3^\ell = 2^m$	$2^{r_1+1}3^{r_2}p^{r_3+1}d$	$-2^{2r_1}3^{\ell+2r_2}p^{2r_3+1}$
15	$pd^2 + 1 = 2^m3^\ell$	$2^{r_1+1}3^{r_2}p^{r_3+1}d$	$-2^{2r_1}3^{2r_2}p^{2r_3+1}$
16	$3d^2 + p^n = 2^m$	$2^{r_1+1}3^{r_2+1}p^{r_3}d$	$-2^{2r_1}3^{2r_2+1}p^{n+2r_3}$
17	$3d^2 + 1 = 2^mp^n$	$2^{r_1+1}3^{r_2+1}p^{r_3}d$	$-2^{2r_1}3^{2r_2+1}p^{2r_3}$
18	$3pd^2 + 1 = 2^m$	$2^{r_1+1}3^{r_2+1}p^{r_3+1}d$	$-2^{2r_1}3^{2r_2+1}p^{2r_3+1}$
20	$2d^2 + 3^\ell = p^n$	$2^{r_1+2}3^{r_2}p^{r_3}d$	$-2^{2r_1+1}3^{\ell+2r_2}p^{2r_3}$
21	$2d^2 + p^n = 3^\ell$	$2^{r_1+2}3^{r_2}p^{r_3}d$	$-2^{2r_1+1}3^{2r_2}p^{n+2r_3}$
22	$2d^2 + 1 = 3^\ell p^n$	$2^{r_1+2}3^{r_2}p^{r_3}d$	$-2^{2r_1+1}3^{2r_2}p^{2r_3}$
24	$2pd^2 + 1 = 3^\ell$	$2^{r_1+2}3^{r_2}p^{r_3+1}d$	$-2^{2r_1+1}3^{2r_2}p^{2r_3+1}$
26	$6d^2 + 1 = p^n$	$2^{r_1+2}3^{r_2+1}p^{r_3}d$	$-2^{2r_1+1}3^{2r_2+1}p^{2r_3}$
27	$6pd^2 + 1 = 1$	$2^{r_1+2}3^{r_2+1}p^{r_3+1}d$	$-2^{2r_1+1}3^{2r_2+1}p^{2r_3+1}$

The proof of this lemma is entirely analogous to that of lemma A.1. The only change that needs to be made is that b, i.e. a_4, is now negative, and the minus sign on the right-hand side of the Diophantine equations changes to a plus sign. We've kept the numbering of rows in the table the same as the previous lemma. This allows one to see the analogy between the two lemmata. Of course, some of the rows don't appear, say for example, the row analogous to row 1. This row would have equation $d^2+2^m3^\ell p^n = 1$, but this has no solutions except with $d = m = n = \ell = 0$, and the corresponding curve is already contained in row 2.

Appendix B
Tables of S-integral Points on Elliptic Curves.

In this section, we present tables listing all the S-integral points on curves of the form $y^2 = x^3 \pm 2^a 3^b$, where $S = \{2, 3, \infty\}$. These results are used in the proofs of the Diophantine lemmata of Chapter 4 (in the case when 3 divides n). For the reader interested in a very brief account of the theory behind computing S-integral points on elliptic curves, we sketch this in the the first two sections. The tables are presented in Section B.3.

B.1 S-integral points on Elliptic Curves

Let S be a finite set of primes (places) including the place at infinity; $S = \{p_1, \ldots, p_{s-1}, \infty\}$. The set of *S-integers* of $\mathbb{Q}$ is

$$\mathbb{Z}_S := \{x \in \mathbb{Q} : |x|_p \leq 1 \text{ for all } p \notin S\},$$

where, for p finite, the $|x|_p$'s are the usual (normalized) p-adic absolute values of $\mathbb{Q}$, and for p infinite, $|x|_\infty$ is the usual archimedean absolute value of $\mathbb{Q}$. In other words, a rational number is an S-integer if the only primes in its denominator are those in S.

Let E be the elliptic curve over $\mathbb{Q}$ given by the following equation, in long Weierstrass form,

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6,$$

$a_i \in \mathbb{Z}$. The set of *integral points* of $E(\mathbb{Q})$ is

$$E(\mathbb{Z}) = \{P \in E(\mathbb{Q}) : x(P) \in \mathbb{Z}\}$$

and the set of *S-integral points* of $E(\mathbb{Q})$ is

$$E(\mathbb{Z}_S) = \{P \in E(\mathbb{Q}) : x(P) \in \mathbb{Z}_S\}.$$

The fact that $x(P) \in \mathbb{Z}$ (resp. $\mathbb{Z}_S$) implies $y(P) \in \mathbb{Z}$ (resp. $\mathbb{Z}_S$), provided $y(P) \in \mathbb{Q}$, is straightforward to check using the equation defining E.

Siegel proved in 1929 that the number of integral points on an elliptic curve over a number field is finite and Mahler generalized this result to S-integral points in 1934 (see [Sil:1989]). However, the methods they used to prove these results were not effective, which means that they did not yield an algorithm to find all of the points.

In 1968, Baker gave an effective upper bound on the size of integral points, based on his work on linear forms in complex logarithms, thus, theoretically, producing an algorithm to find all integral points. In some cases, this led to the complete determination of sets of solutions to a given elliptic Diophantine equation. However, the bounds one obtains using Baker's work are usually astronomical, typically at least of size 10^{20} or so, which makes naive searching for all points impossible. In his thesis [dW:1989], de Weger developed a technique using lattice basis reduction (LLL algorithm) to reduce the bounds obtained from Baker's work. This resulted in an algorithm to find integral points on elliptic curves which works well in practice (though, one needs to deal with computations in various complicated number fields).

This method does not make use of the underlying group structure of the elliptic curve. That, combined with the need to consider complicated number fields, led Lang and Zagier to suggest a way to work directly on the elliptic curve. Moreover, this new approach can be generalized to apply to S-integral points as well. We discuss this approach in the next section.

B.2 Computing S-integral points on Elliptic Curves

Let $S = \{p_1, \ldots, p_{s-1}, \infty\}$ and consider the Mordell-Weil group $E(\mathbb{Q})$ of the elliptic curve

$$E : y^2 = x^3 + ax + b,$$

over $\mathbb{Q}$. Recall that $E(\mathbb{Q})$ is a finitely generated abelian group so it can be written as

$$E(\mathbb{Q}) \cong E(\mathbb{Q})_{tors} \times \mathbb{Z}^r,$$

where $E(\mathbb{Q})_{tors}$ is the (finite) torsion subgroup of $E(\mathbb{Q})$ and r the *rank* of $E(\mathbb{Q})$. The method of Lang and Zagier requires that we know generators for $E(\mathbb{Q})$, so, let $P_1, \ldots, P_r$ be generators for the free part $E(\mathbb{Q})$. Every rational point $P \in E(\mathbb{Q})$ has a unique representation

$$P = T + \sum_{i=1}^{r} n_i P_i,$$

where $n_i \in \mathbb{Z}$ and $T \in E(\mathbb{Q})_{tors}$. In the case when P is an S-integral point we want to show

$$N := max\{|n_i|\} \leq N_2$$

for an effectively computable constant N_2 depending only on E and S. Thus, all S-integral points on $E(\mathbb{Q})$ are contained in the finite set

$$\{T + \sum_{i=1}^{r} n_i P_i : 0 \leq |n_i| \leq N, T \in E(\mathbb{Q})_{tors}\},$$

and can be determined, provided N_2 is small enough.

We briefly sketch the details involved in finding the upper bound N_2. For all the details the reader should consult [GPZ:1996]. Let $P = (x, y) \in E(\mathbb{Q})$ be an S-integral points and choose $p \in S$ such that $|x|_p = max\{|x|_q : q \in S\}$. It is straightforward to show

$$\frac{1}{{|x|_p}^{1/2}} \leq C_2 e^{-C_3 N^2} \tag{B.1}$$

for effectively computable constants C_2 and C_3 which depend only on a, b, $\#S$, and the generators P_i. Obtaining a lower bound on $|x|_p^{-1/2}$ together with (B.1) would then give and upper bound on N. If the upper bound on N is quite large then an application of de Weger reduction could bring this bound down to a more manageable level. In practice this is usually the case.

Lower bounds on $|x|_p^{-1/2}$ are obtained by estimating a linear form in elliptic logarithms. In the case when $p = \infty$ such estimates were done by David [Da:1995]. In the case when $p = p_i \in S$, estimates for lower bounds of p-adic elliptic logarithms in general are not known. However, if the rank of $E(\mathbb{Q})$ is at most 2 then such a bound was obtained by Rémond and Urfels [RU:1996]. Gebel, Pethö and Zimmer [GPZ:1996] applied these lower bounds to find all S-integeral points on Mordell's curves $y^2 = x^3 + k$, with $|k| \leq 10^4$, and rank at most 2. Their algorithms were implemented in the SIMATH package, and have since made their way into the MAGMA package. We will use MAGMA to generate the tables in the next section.

B.3 Tables of S-integral points on the curves $y^2 = x^3 \pm 2^a 3^b$

For $S = \{2, 3, \infty\}$, the following tables list the S-integer points on curves of the form $y^2 = x^3 \pm 2^a 3^b$. It is easy to check all these curves have rank ≤ 2. The points were found using the MAGMA package. If (x_0, y_0) is a point on the curve then so is $(x_0, -y_0)$, thus, in the tables, we list only the points with non-negative y coordinate. These curves always contain the point at infinity, ∞, so, it suffices to list only the finite points in the tables. Values (a, b) are left absent from the table if there are no finite S-integral points on the curve.

$y^2 = x^3 + 2^a 3^b$		
a	b	S-integral points $\setminus\{\infty\}$
0	0	$(2,3), (0,1), (-1,0)$
0	1	$(1,2), (-23/16, 11/64)$
0	2	$(0,3), (-2,1), (3,6), (6,15), (40,253), (-15/16, 183/64)$
0	3	$(-3,0)$
0	4	$(0,9)$
1	0	$(-1,1), (17/4, 71/8)$
1	2	$(7,19)$
1	3	$(3,9), (-15/4, 9/8), (19/9, 215/27), (5745/16, 435447/64)$
1	5	$(-5,19)$
2	0	$(0,2)$
2	1	$(-2,2), (13,47)$
2	2	$(0,6), (4,10), (12,42), (-3,3), (105/4, 1077/8)$
2	3	$(6,18), (-3,9), (-2,10), (33/4, 207/8), (366, 7002)$
2	4	$(0,18)$
3	0	$(-2,0), (2,4), (1,3), (-7/4, 13/8), (46, 3121)$
3	1	$(-2,4), (25/4, 131/8), (8158, 736844), (1,5), (10/9, 136/271),$ $(10,32), (-23/9, 73/27), (478/81, 11044/729), (505/256, 23053/4096)$
3	2	$(-2,8), (73/16, 827/64)$
3	3	$(-6,0)$
3	5	$(-2,44)$
4	0	$(0,4)$
4	1	$(1,7)$
4	2	$(0,12)$
4	4	$(0,36), (-8,28), (9,45), (72,612)$
5	2	$(1,17)$
5	5	$(-47/9, 2359/27)$

Table B.1: S-integral points on $y^2 = x^3 + 2^a 3^b$

$y^2 = x^3 - 2^a 3^b$		
a	b	S-integral points $\setminus\{\infty\}$
0	0	$(1, 0)$
0	3	$(3, 0)$
0	4	$(13, 46)$
0	5	$(7, 10)$
1	0	$(3, 5)$
1	2	$(3, 3), (57/4, 429/8)$
1	3	$(7, 17)$
2	0	$(2, 2), (5, 11), (106/9, 1090/27)$
2	4	$(10, 26)$
2	5	$(13, 35)$
3	0	$(2, 0)$
3	2	$(6, 12), (33/4, 177/8), (1942/9, 85580/27)$
3	3	$(6, 0), (10, 28), (33, 189)$
3	4	$(18, 72), (153/16, 963/64), (657/4, 16839/8), (9, 9),$ $(22, 100), (1809, 76941), (54, 396), (97, 955)$
3	5	$(70, 584)$
4	1	$(4, 4), (28, 148), (73/9, 595/27)$
4	3	$(12, 36)$
4	4	$(193, 2681)$
5	2	$(9, 21)$
5	5	$(1153, 39151)$

Table B.2: S-integral points on $y^2 = x^3 - 2^a 3^b$

Appendix C

Tables of $\mathbb{Q}$-Isomorphism Classes of Curves of Conductor $2^\alpha p^2$ with Small p.

In the theorems of Chapter 6, we classified curves up to primes p which satisfied some family of Diophantine equations. There were some extraneous small primes and corresponding curves that did not fit into any family and we referred to the tables in this appendix for a list those extra curves.

Let me emphasize that the following tables list the EXTRA curves that are not contained in the tables of Chapter 6, they do NOT list all the curves of the indicated conductor.

In these tables a_2 and a_4 are the coefficients of the curves as we have found them (by applying the Diophantine lemmata to the tables of Chapter 3 Section 3.1). The minimal model of the curve is also included as 5-tuple of coefficients $(a_1', a_2', a_3', a_4', a_6')$. It is sufficient to include just the minimal model in the table but we thought we should include the a_2 and a_4 for the sake of the reader who wishes to verify these results.

Conductor: $N = 2p^2$				
p	a_2	a_4	j-invariant	minimal model
7	$-7 \cdot 13$	$2^7 7^2$	$\frac{5^3 43^3}{2^6 7^3}$	$1, 1, 0, 220, 2192$
7	$2 \cdot 7 \cdot 13$	-7^5	$\frac{5^3 11^3 31^3}{2^3 7^6}$	$1, 1, 0, -1740, 22184$
17	$2 \cdot 17 \cdot 71$	17^5	$\frac{5^6 7^3 31^3}{2 \cdot 17^6}$	$1, 1, 1, -32663, -1583717$
17	$-17 \cdot 71$	$2^5 17^3$	$\frac{5^3 23^3 43^3}{2^2 \cdot 17^3}$	$1, 1, 1, -29773, -1989473$

Table C.1: Extraneous curves of conductor $2p^2$.

Conductor: $N = 2^2 p^2$				
p	a_2	a_4	j-invariant	minimal model
5	$2 \cdot 5 \cdot 11$	5^5	$\frac{-2^4 109^3}{5^6}$	$0, -1, 0, -908, -15688$
5	$-5 \cdot 11$	-5^2	$\frac{2^{14} 31^3}{5^3}$	$0, -1, 0, -1033, -12438$

Table C.2: Extraneous curves of conductor $2^2 p^2$.

Conductor: $N = 2^3p^2$				
p	a_2	a_4	j-invariant	minimal model
5	$5 \cdot 9$	$2^2 \cdot 5^3$	$\frac{2^4 3^3 7^3}{5^2}$	$0, 0, 0, -175, -750$
5	$-2 \cdot 5 \cdot 9$	5^2	$\frac{2^2 3^3 107^3}{5}$	$0, 0, 0, -2675, -53250$
5	$2 \cdot 5 \cdot 3$	5^4	$\frac{2^2 3^3 13^3}{5^4}$	$0, 0, 0, 325, -4250$
5	$5 \cdot 3$	5^2	$\frac{2^1 13^3}{5}$	$0, 0, 0, -50, 125$
5	-5	5	2^{11}	$0, 1, 0, -3, -2$
5	-5^2	5^3	2^{11}	$0, -1, 0, -83, -88$
5	$2 \cdot 5$	5	$2^4 17^3$	$0, 1, 0, -28, 48$
5	$2 \cdot 5^2$	5^3	$2^4 17^3$	$0, -1, 0, -708, 7412$
7	$7 \cdot 15$	$2^3 \cdot 7^3$	$\frac{2^2 3^3 19^3}{7^2}$	$0, 0, 0, -931, -10290$
7	$-2 \cdot 7 \cdot 15$	7^2	$\frac{2 \cdot 3^3 13^3 23^3}{7}$	$0, 0, 0, -14651, -682570$
7	$2 \cdot 7 \cdot 9$	7^4	$\frac{23^3 59^3}{7^4}$	$0, 0, 0, -2891, 47334$
7	$7 \cdot 3$	$2^2 \cdot 7^2$	$\frac{2^4 3^3}{7}$	$0, 0, 0, 49, -686$
7	$-7 \cdot 5$	$2^3 \cdot 7^2$	$\frac{-2^2}{7}$	$0, 1, 0, -16, 1392$
7	$2 \cdot 7 \cdot 5$	-7^3	$\frac{2 \cdot 11^6}{7^2}$	$0, 1, 0, -1976, 32752$
17	17	$2^2 \cdot 17$	$2^4 5^3$	$0, -1, 0, -28, -12$
17	17^2	$2^2 \cdot 17^3$	$2^4 5^3$	$0, 1, 0, -8188, -107904$
17	$-2 \cdot 17$	17	$2^2 5^3 13^3$	$0, -1, 0, -368, -2596$
17	$-2 \cdot 17^2$	17^3	$2^2 5^3 13^3$	$0, 1, 0, -106448, -13392656$
23	$23 \cdot 3$	$2^3 \cdot 23^2$	$\frac{2^2 3^3 5^3}{23}$	$0, 0, 0, 2645, -73002$
23	$-2 \cdot 23 \cdot 3$	-23^3	$\frac{2 \cdot 3^3 5^3 7^3}{23^2}$	$0, 0, 0, -18515, -754354$
31	-31	$2^3 \cdot 31^2$	$\frac{2^2 23^3}{31}$	$0, -1, 0, 7368, 74780$
31	$2 \cdot 31$	-31^3	$\frac{2 \cdot 97^3}{31^2}$	$0, -1, 0, -31072, 643692$
31	-31	$2^3 \cdot 31$	$-2^2 7^3$	$0, -1, 0, -72, 380$
31	31^2	$2^3 \cdot 31^3$	$-2^2 7^3$	$0, 1, 0, -69512, -10626560$
31	$2 \cdot 31$	-31	$2 \cdot 127^3$	$0, -1, 0, -1312, 18732$
31	$-2 \cdot 31^2$	-31^3	$2 \cdot 127^3$	$0, 1, 0, -1261152, -545434592$

Table C.3: Extraneous curves of conductor 2^3p^2.

Conductor: $N = 2^4p^2$				
p	a_2	a_4	j-invariant	minimal model
5	$-5 \cdot 9$	$2^2 \cdot 5^3$	$\frac{2^4 3^3 7^3}{5^2}$	$0, 0, 0, -175, 750$
5	$2 \cdot 5 \cdot 9$	5^2	$\frac{2^2 3^3 107^3}{5}$	$0, 0, 0, -2675, 53250$
5	$-2 \cdot 5 \cdot 11$	5^5	$\frac{-2^4 109^3}{5^6}$	$0, 1, 0, -908, 15688$
5	$5 \cdot 11$	-5^2	$\frac{2^{14} 31^3}{5^3}$	$0, 1, 0, -1033, 12438$
5	$-2 \cdot 5 \cdot 3$	5^4	$\frac{2^2 3^3 13^3}{5^4}$	$0, 0, 0, 325, 4250$
5	$-5 \cdot 3$	5^2	$\frac{2^1 13^3}{5}$	$0, 0, 0, -50, -125$
5	5	5	2^{11}	$0, -1, 0, -3, 2$
5	5^2	5^3	2^{11}	$0, 1, 0, -83, 88$
5	$-2 \cdot 5$	5	$2^4 17^3$	$0, -1, 0, -28, -48$
5	$-2 \cdot 5^2$	5^3	$2^4 17^3$	$0, 1, 0, -708, -7412$
7	$7 \cdot 13$	$2^7 \cdot 7^2$	$\frac{5^3 43^3}{2^6 \cdot 7^3}$	$0, 1, 0, 3512, -133260$
7	$-2 \cdot 7 \cdot 13$	-7^5	$\frac{5^3 11^3 31^3}{2^3 \cdot 7^6}$	$0, 1, 0, -27848, -1475468$
7	$-7 \cdot 3$	$2^2 \cdot 7^2$	$\frac{2^4 3^3}{7}$	$0, 0, 0, 46, 686$
7	$7 \cdot 5$	$2^3 \cdot 7^2$	$\frac{-2^2}{7}$	$0, -1, 0, -16, -1392$
7	$-2 \cdot 7 \cdot 5$	-7^3	$\frac{2 \cdot 11^6}{7^2}$	$0, -1, 0, -1976, -32752$
7	$-7 \cdot 3$	$2^4 \cdot 7$	$-3^3 5^3$	$0, 0, 0, -35, 98$
7	$7^2 \cdot 3$	$2^4 \cdot 7^3$	$-3^3 5^3$	$0, 0, 0, -1715, -33614$
7	$2 \cdot 7 \cdot 3$	-7	$3^3 5^3 17^3$	$0, 0, 0, -595, 5586$
7	$-2 \cdot 7^2 \cdot 3$	-7^3	$3^3 5^3 17^3$	$0, 0, 0, -29155, -1915998$
17	$-2 \cdot 17 \cdot 71$	17^5	$\frac{5^6 7^3 31^3}{2 \cdot 17^6}$	$0, 1, 0, -522608, 100312660$
17	$17 \cdot 71$	$2^5 \cdot 17^2$	$\frac{5^3 23^3 43^3}{2^2 \cdot 17^3}$	$0, 1, 0, -476368, 126373524$
17	$-17 \cdot 9$	$2^4 \cdot 17^2$	$\frac{3^3 11^3}{17}$	$0, 0, 0, -3179, -29478$
17	-17	$2^2 \cdot 17$	$2^4 5^3$	$0, 1, 0, -28, 12$
17	-17^2	$2^2 \cdot 17^3$	$2^4 5^3$	$0, -1, 0, -8188, 107904$
17	$2 \cdot 17$	17	$2^2 5^3 13^3$	$0, 1, 0, -368, 2596$
17	$2 \cdot 17^2$	17^3	$2^2 5^3 13^3$	$0, -1, 0, -106448, 13392656$
23	$-23 \cdot 3$	$2^3 \cdot 23^2$	$\frac{2^2 3^3 5^3}{23}$	$0, 0, 0, 2645, 73002$
23	$2 \cdot 23 \cdot 3$	-23^3	$\frac{2 \cdot 3^3 5^3 7^3}{23^2}$	$0, 0, 0, -18515, 754354$
31	31	$2^3 \cdot 31^2$	$\frac{2^2 23^3}{31}$	$0, 1, 0, 7368, -74780$
31	$-2 \cdot 31$	-31^3	$\frac{2 \cdot 97^3}{31^2}$	$0, 1, 0, -31072, -643692$
31	31	$2^3 \cdot 31$	$-2^2 7^3$	$0, 1, 0, -72, -380$
31	-31^2	$2^3 \cdot 31^3$	$-2^2 7^3$	$0, -1, 0, -69512, 10626560$
31	$-2 \cdot 31$	-31	$2 \cdot 127^3$	$0, 1, 0, -1312, -18732$
31	$2 \cdot 31^2$	-31^3	$2 \cdot 127^3$	$0, -1, 0, -1261152, 545434592$

Table C.4: Extraneous curves of conductor 2^4p^2.

Conductor: $N = 2^5p^2$				
p	a_2	a_4	j-invariant	minimal model
7	7	$2 \cdot 7^2$	$\frac{2^6 5^3}{7}$	$0, 1, 0, 82, -176$
7	-7	$2 \cdot 7^2$	$\frac{2^6 5^3}{7}$	$0, -1, 0, 82, 176$
7	$2 \cdot 7$	-7^3	$\frac{2^3 5^6}{7^2}$	$0, -1, 0, -408, 1940$
7	$-2 \cdot 7$	-7^3	$\frac{2^3 5^6}{7^2}$	$0, 1, 0, -408, -1940$
7	7	$2 \cdot 7$	-2^6	$0, 1, 0, -2, -8$
7	-7	$2 \cdot 7$	-2^6	$0, -1, 0, -2, 8$
7	7^2	$2 \cdot 7^3$	-2^6	$0, 1, 0, -114, -2528$
7	-7^2	$2 \cdot 7^3$	-2^6	$0, -1, 0, -114, 2528$
7	$2 \cdot 7$	-7	$2^3 31^3$	$0, -1, 0, -72, 260$
7	$-2 \cdot 7$	-7	$2^3 31^3$	$0, 1, 0, -72, -260$
7	$2 \cdot 7^2$	-7^3	$2^3 31^3$	$0, -1, 0, -3544, 82104$
7	$-2 \cdot 7^2$	-7^3	$2^3 31^3$	$0, 1, 0, -3544, -82104$

Table C.5: Extraneous curves of conductor 2^5p^2.

Conductor: $N = 2^6p^2$				
p	a_2	a_4	j-invariant	minimal model
5	$2 \cdot 5 \cdot 9$	$2^4 5^3$	$\frac{2^4 3^3 7^3}{5^2}$	$0, 0, 0, -700, -6000$
5	$-2 \cdot 5 \cdot 9$	$2^4 5^3$	$\frac{2^4 3^3 7^3}{5^2}$	$0, 0, 0, -700, 6000$
5	$2^2 \cdot 5 \cdot 9$	$2^2 5^2$	$\frac{2^2 3^3 107^3}{5}$	$0, 0, 0, -10700, 426000$
5	$-2^2 \cdot 5 \cdot 9$	$2^2 5^2$	$\frac{2^2 3^3 107^3}{5}$	$0, 0, 0, -10700, -426000$
5	$2^2 \cdot 5 \cdot 11$	$2^2 5^5$	$\frac{-2^4 109^3}{5^6}$	$0, 1, 0, -3633, -129137$
5	$-2^2 \cdot 5 \cdot 11$	$2^2 5^5$	$\frac{-2^4 109^3}{5^6}$	$0, -1, 0, -3633, 129137$
5	$2 \cdot 5 \cdot 11$	$-2^2 5^2$	$\frac{2^{14} 31^3}{5^3}$	$0, -1, 0, -4133, 103637$
5	$-2 \cdot 5 \cdot 11$	$-2^2 5^2$	$\frac{2^{14} 31^3}{5^3}$	$0, 1, 0, -4133, -103637$
5	$2^2 \cdot 5 \cdot 3$	$2^2 5^4$	$\frac{2^2 3^3 13^3}{5^4}$	$0, 0, 0, 1300, -34000$
5	$-2^2 \cdot 5 \cdot 3$	$2^2 5^4$	$\frac{2^2 3^3 13^3}{5^4}$	$0, 0, 0, 1300, 34000$
5	$2 \cdot 5 \cdot 3$	$-2^4 5^2$	$\frac{2^4 3^3 7^3}{5^2}$	$0, 0, 0, -700, 6000$
5	$2 \cdot 5 \cdot 3$	$-2^4 5^2$	$\frac{2^4 3^3 7^3}{5^2}$	$0, 0, 0, -700, -6000$
7	$2 \cdot 7 \cdot 13$	$2^9 7^2$	$\frac{5^3 43^3}{2^6 7^3}$	$0, -1, 0, 14047, -1080127$
7	$-2 \cdot 7 \cdot 13$	$2^9 7^2$	$\frac{5^3 43^3}{2^6 7^3}$	$0, 1, 0, 14047, 1080127$
7	$2^2 \cdot 7 \cdot 13$	$-2^2 7^5$	$\frac{5^3 11^3 31^3}{2^3 7^6}$	$0, 1, 0, -111393, 11692351$
7	$-2^2 \cdot 7 \cdot 13$	$-2^2 7^5$	$\frac{5^3 11^3 31^3}{2^3 7^6}$	$0, -1, 0, -111393, -11692351$
17	$2^2 \cdot 17 \cdot 71$	$2^2 17^5$	$\frac{5^6 7^3 31^3}{2 \cdot 17^6}$	$0, 1, 0, -2090433, -804591713$
17	$-2^2 \cdot 17 \cdot 71$	$2^2 17^5$	$\frac{5^6 7^3 31^3}{2 \cdot 17^6}$	$0, -1, 0, -2090433, 804591713$
17	$2 \cdot 17 \cdot 71$	$2^7 17^2$	$\frac{5^3 23^3 43^3}{2^2 \cdot 17^3}$	$0, -1, 0, -1905473, 1012893665$
17	$-2 \cdot 17 \cdot 71$	$2^7 17^2$	$\frac{5^3 23^3 43^3}{2^2 \cdot 17^3}$	$0, 1, 0, -1905473, -1012893665$

Table C.6: Extraneous curves of conductor 2^6p^2.

Conductor: $N = 2^7p^2$				
p	a_2	a_4	j-invariant	minimal model
13	$2 \cdot 13 \cdot 5$	$2 \cdot 13^3$	$\frac{-2^7 11^3}{13^2}$	$0, 1, 0, -1239, -28079$
13	$-2 \cdot 13 \cdot 5$	$2 \cdot 13^3$	$\frac{-2^7 11^3}{13^2}$	$0, -1, 0, -1239, 28079$
13	$2^2 13 \cdot 5$	$2^3 13^3$	$\frac{-2^7 11^3}{13^2}$	$0, -1, 0, -4957, -219675$
13	$-2^2 13 \cdot 5$	$2^3 13^3$	$\frac{-2^7 11^3}{13^2}$	$0, 1, 0, -4957, 219675$
13	$2 \cdot 13 \cdot 5$	-13^2	$\frac{2^5 103^3}{13}$	$0, 1, 0, -5802, 168130$
13	$-2 \cdot 13 \cdot 5$	-13^2	$\frac{2^5 103^3}{13}$	$0, -1, 0, -5802, -168130$
13	$2^2 13 \cdot 5$	$-2^2 13^2$	$\frac{2^5 103^3}{13}$	$0, -1, 0, -23209, 1368249$
13	$-2^2 13 \cdot 5$	$-2^2 13^2$	$\frac{2^5 103^3}{13}$	$0, 1, 0, -23209, -1368249$
13	$2 \cdot 13 \cdot 239$	$2 \cdot 13^6$	$\frac{-2^7 28559^3}{13^8}$	$0, 1, 0, -3217647, -2223146015$
13	$-2 \cdot 13 \cdot 239$	$2 \cdot 13^6$	$\frac{-2^7 28559^3}{13^8}$	$0, -1, 0, -3217647, 2223146015$
13	$2^2 13 \cdot 239$	$2^3 13^6$	$\frac{-2^7 28559^3}{13^8}$	$0, -1, 0, -12870589, -17772297531$
13	$-2^2 13 \cdot 239$	$2^3 13^6$	$\frac{-2^7 28559^3}{13^8}$	$0, -1, 0, -12870589, 17772297531$
13	$2 \cdot 13 \cdot 239$	-13^2	$\frac{2^5 7^6 4663^3}{13^4}$	$0, 1, 0, -12871434, 17769846862$
13	$-2 \cdot 13 \cdot 239$	-13^2	$\frac{2^5 7^6 4663^3}{13^4}$	$0, -1, 0, -12871434, -17769846862$
13	$2^2 13 \cdot 239$	$-2^2 13^2$	$\frac{2^5 7^6 4663^3}{13^4}$	$0, -1, 0, -51485737, 142210260633$
13	$-2^2 13 \cdot 239$	$-2^2 13^2$	$\frac{2^5 7^6 4663^3}{13^4}$	$0, 1, 0, -51485737, -142210260633$

Table C.7: Extraneous curves of conductor 2^7p^2.

Conductor: $N = 2^8p^2$				
p	a_2	a_4	j-invariant	minimal model
23	$2^3 \cdot 23 \cdot 39$	$2 \cdot 23^5$	$\frac{2^6 3^3 4057^3}{23^6}$	$0, 0, 0, -4292306, -3419024336$
23	$-2^3 \cdot 23 \cdot 39$	$2 \cdot 23^5$	$\frac{2^6 3^3 4057^3}{23^6}$	$0, 0, 0, -4292306, 3419024336$
23	$2^4 \cdot 23 \cdot 39$	$2^3 23^5$	$\frac{2^6 3^3 4057^3}{23^6}$	$0, 0, 0, -17169224, -27352194688$
23	$-2^4 \cdot 23 \cdot 39$	$2^3 23^5$	$\frac{2^6 3^3 4057^3}{23^6}$	$0, 0, 0, -17169224, 27352194688$
23	$2^3 \cdot 23 \cdot 39$	$2 \cdot 23^2$	$\frac{2^6 3^3 16223^3}{23^3}$	$0, 0, 0, -17163934, 27369909840$
23	$-2^3 \cdot 23 \cdot 39$	$2 \cdot 23^2$	$\frac{2^6 3^3 16223^3}{23^3}$	$0, 0, 0, -17163934, -27369909840$
23	$2^4 \cdot 23 \cdot 39$	$2^3 23^2$	$\frac{2^6 3^3 16223^3}{23^3}$	$0, 0, 0, -68655736, 218959278720$
23	$-2^4 \cdot 23 \cdot 39$	$2^3 23^2$	$\frac{2^6 3^3 16223^3}{23^3}$	$0, 0, 0, -68655736, -218959278720$

Table C.8: Extraneous curves of conductor 2^8p^2.