Journal of Number Theory 184 (2018) 473–484

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

Divisibility on the sequence of perfect squares minus one: The gap principle

Tsz Ho Chan[a], Stephen Choi[b,1], Peter Cho-Ho Lam[b,*]

[a] Department of Mathematical Sciences, University of Memphis, Memphis, TN 38152, USA

[b] Department of Mathematics, Simon Fraser University, Burnaby BC, V5A 1S6, Canada

ARTICLE INFO

Article history:
Received 13 June 2017
Received in revised form 20 July 2017
Accepted 13 August 2017
Available online 21 September 2017
Communicated by S.J. Miller

MSC:
primary 11B05

Keywords:
Gap principle
Pell's equations
Quadratic congruence

ABSTRACT

In this paper, we consider a gap principle when $a^2 - 1|b^2 - 1|c^2 - 1$ with $1 < a < b < c$. As a byproduct, we are led to determine the complete set of pairs of positive integers $1 \leq u \leq v \leq x$ such that $u|v^2 - 1$ and $v|u^2 - 1$ and the diophantine equation $u^2 + v^2 - 1 = muv$. We also generalize our main theorems to the polynomial $f(n) = A(n + B)^2 + C$.

1. Introduction and main results

In a previous paper [1], the first author studied the sequence of numbers $f(n) = n^2(n^2 + 1)$ and asked

[*] Corresponding author.
E-mail addresses: thchan6174@gmail.com (T.H. Chan), schoia@sfu.ca (S. Choi), chohol@sfu.ca (P.C.-H. Lam).
[1] Research supported by NSERC, grant number 611312.

https://doi.org/10.1016/j.jnt.2017.08.032

Question 1. Suppose $a^2(a^2+1)$ divides $b^2(b^2+1)$ with $a<b$. Must it be true that there is some gap between a and b? More precisely, is it true that $b > a^{1+\lambda}$ for some small $\lambda > 0$?

He managed to prove a gap principle with some additional requirements, namely

Theorem 1. *Suppose $a^2(a^2+1)$ divides $b^2(b^2+1)$ with $a<b$, $(a^2, b^2+1) = a^2/(a^2,b^2)$ and $(a^2+1, b^2) = b^2/(a^2,b^2)$. Then*

$$\frac{b}{a} \gg \frac{(\log a)^{1/8}}{(\log\log a)^{12}}.$$

One can also ask the same question for any polynomial with integral coefficients. Here we formulate the question more precisely:

Definition 1. Let n be a positive integer and $f(x)$ be a polynomial with integral coefficients. Consider the set of all positive integers $a_0 < a_1 < a_2 < ... < a_n$ such that $f(a_i)$ divides $f(a_{i+1})$ for $0 \le i \le n-1$. We say that $f(x)$ satisfies the **gap principle of order** n if $\lim a_n/a_0 = \infty$ as $a_0 \to \infty$.

Note that the set of all such $(a_0, a_1, ..., a_n)$ is always infinite since

$$f(a+f(a)) \equiv 0 \pmod{f(a)}.$$

If $f(x)$ satisfies the gap principle of some order n, it will also satisfy the gap principle of any larger order. Therefore we can also make the following definition:

Definition 2. Let $f(x)$ be a polynomial with integral coefficients. We define the **gap order** of $f(x)$ to be the smallest positive integer n such that $f(x)$ satisfies the gap principle of order n. If such n does not exist, we say that $f(x)$ **does not satisfy the gap principle**.

If we can remove the conditions $(a^2, b^2+1) = a^2/(a^2,b^2)$ and $(a^2+1, b^2) = b^2/(a^2,b^2)$ in Theorem 1, then we would have shown that $f(x) = x^2(x^2+1)$ satisfies the gap principle of order 1 and hence $f(x)$ has gap order 1. On the other hand, there are polynomials that do not satisfy the gap principle of any order. For example when $f(x) = x^m$ where $m \in \mathbb{N}$, we can choose $a_i = 2^i a_0$ for all i. Consequently $a_n/a_0 = 2^n$ and this does not approach to infinity when a_0 does.

Another example is $f(x) = ax + b$ where $a, b \in \mathbb{Z}$. If a_i is chosen, we can choose $a_i < a_{i+1} \le a_i + f(a_i)$ so that it satisfies the congruence

$$f(a_{i+1}) \equiv 0 \pmod{f(a_i)}.$$

This implies $a_{i+1} < (a+2)a_i$ for sufficiently large a_i and hence $f(x)$ does not satisfy the gap principle. Inspired by these examples, we make the following conjecture:

Conjecture 1. *If the degree of $f(x)$ is at least 2 and $f(x)$ does not satisfy the gap principle, then it must take the form $f(x) = A(x+B)^m$ for some $A, B \in \mathbb{Q}$ and $m \in \mathbb{N}$.*

In this paper, we are going to focus on the sequence $f(n) = n^2 - 1$. Of course, by the theory of Pell's equations, there are infinitely many solutions to $b^2 - 1 = 2(a^2 - 1)$. Therefore $x^2 - 1$ does not satisfy the gap principle of order 1. However, if

$$a^2 - 1 | b^2 - 1 | c^2 - 1,$$

we expect there is some gap between a and c. In our argument we need to study the special case $a^2 - 1 | b^2 - 1$ where their quotient is a perfect square. That is

$$b^2 - 1 = d^2(a^2 - 1)$$

for some integer $d > 1$. To this, we have the following gap result:

Theorem 2. *Suppose $a^2 - 1 | b^2 - 1$ with $b > a \geq 1$ and $b^2 - 1 = d^2(a^2 - 1)$ for some $d \geq 3$. Then $d \geq (2(b+1))^{1/2}$. Moreover, the bound is best possible and it occurs in the special case when $d = 2a$ and $b = 2a^2 - 1$. With this special case aside, then we have*

$$\frac{(d+1)^{1/2}(d-2)}{2} \geq b$$

and, again, this bound is best possible. Note that this bound implies $d \geq (2b)^{2/3}$.

With this theorem, we have

Theorem 3. *If $a^2 - 1 | b^2 - 1 | c^2 - 1$ with $1 < a < b < c$, then*

$$\frac{c}{a} \gg \frac{(\log c)^{1/6}}{(\log \log c)^{5/6}}.$$

In other words, $x^2 - 1$ satisfies the gap principle of order 2 and hence $x^2 - 1$ has gap order 2. However, one expects more to be true, namely

Conjecture 2. *There exists a small positive constant λ such that if $a^2 - 1 | b^2 - 1 | c^2 - 1$ with $1 < a < b < c$, then $c > a^{1+\lambda}$.*

In the proof of Theorem 2, we encounter the diophantine equation

$$u^2 + v^2 - 1 = muv$$

with positive integers m, u and v. We have determined all the solutions:

Theorem 4. *For positive integers m and $1 \le u \le v$, the diophantine equation*

$$u^2 + v^2 - 1 = muv$$

has solutions

$$\begin{array}{ll} (1) & u = v = m = 1 \\ (2) & m = 2, v = u + 1 \\ (3) & m \ge 3, (u, v) = F^n(1, m) \text{ for } n = 0, 1, 2, \ldots \end{array}$$

where

$$F(x, y) = (y, my - x)$$

and $F^0(x, y) = (x, y)$, $F^n(x, y) = F(F^{n-1}(x, y))$ for $n \ge 1$.

As a corollary, we have the following interesting result on the number of pairs of positive integers (u, v) with $u|v^2 - 1$ and $v|u^2 - 1$.

Corollary 1. *For $x \ge 1$,*

$$|\{1 \le u \le v \le x : \ u|v^2 - 1 \text{ and } v|u^2 - 1\}| = 2x + x^{1/2} + O(x^{1/3}).$$

In principle, one can get all the lower order terms by working out explicitly the iterations of $F^n(1, m)$ in Theorem 3.

The paper is organized as follows. First, we prove Theorem 4 which lays down the foundation. Then we use it to prove Corollary 1 and Theorem 2. Finally, we use Theorem 2 to finish off Theorem 3. In fact, we will prove some more general versions of Theorem 2 and 3 for the polynomial $f(n) = A(n + B)^2 + C$ in Section 4 and 5 respectively.

Some notations. The symbol $a|b$ means that a divides b. The notations $f(x) = O(g(x))$, $f(x) \ll g(x)$ and $g(x) \gg f(x)$ are all equivalent to $|f(x)| \le Cg(x)$ for some constant $C > 0$. Finally $f(x) = O_\lambda(g(x))$, $f(x) \ll_\lambda g(x)$ or $g(x) \gg_\lambda f(x)$ mean that the implicit constant C may depend on λ. Also, for a set S, $|S|$ stands for its cardinality.

2. Proof of Theorem 4

Consider the diophantine equation

$$u^2 + v^2 - 1 = muv \tag{1}$$

with positive integers m and $1 \le u \le v$.

If $m = 1$, then $u^2 - uv + v^2 = 1$ and $(u - v)^2 + uv = 1$ which has the only solution $u = 1 = v$.

If $m = 2$, then $(u - v)^2 = 1$ which gives $v = u + 1$ as $u \leq v$.

If $u = 1$, then (1) gives $v = m$. From now on, we assume that $m > 2$ and $u > 1$. Rewrite (1) into a quadratic equation in v:

$$v^2 - (mu)v + (u^2 - 1) = 0$$

and let v' be the other solution to this quadratic equation. Then we have

$$v + v' = mu \tag{2}$$

and

$$vv' = u^2 - 1. \tag{3}$$

From (2) we know that v' is an integer. And then (3) tells us that $u > v' \geq 0$ since $v \geq u$. Therefore, if $u > 1$, then we have $v' = (u^2 - 1)/v > 0$ and we obtain a new solution (v', u) of (1) with $v' < u$. Let $G(u, v) := (mu - v, u)$. With this descent we can keep producing "smaller" solutions (u, v) to (1) with $u < v$.

Based on the above, let $F(u, v) := (v, mv - u)$ and

$$S(m) := \{(u, v) : u^2 + v^2 - 1 = muv, 1 \leq u \leq v\}.$$

Then if $(u, v) \in S(m)$, then we claim that $F(u, v) = (v, mv - u) \in S(m)$ have strictly larger value in the second coordinate of (u, v), i.e. $v < mv - u$. Indeed, clearly $(x, y) = (v, mv - u)$ satisfies the equation $x^2 + y^2 - 1 = mxy$ and $x = v > 0$. Also $mv - u > v$ because $m > 2$ and $u \leq v$. This proves the claim.

Starting from a solution $(u, v) = (1, m)$, we get a sequence of solutions

$$T(m) := \{(1, m), F(1, m), F^2(1, m), F^3(1, m), ...\}.$$

Now we claim that $T(m)$ contains all the solutions (u, v) with $1 \leq u \leq v$, i.e., $S(m) = T(m)$.

Clearly, $T(m) \subseteq S(m)$. If (u, v) is any solution to (1) with $0 < u < v$, the descent $G(u, v) = (mu - v, u)$ cannot go on forever and must stop at some point. That must be $u = 1$ and $v = m$ since if $u > 1$, $G(u, v)$ is still a "smaller" solution. Thus there is an N such that $G^N(u, v) = (1, m)$. But F and G are inverse of each other, so $(u, v) = F^N(1, m)$. Hence (u, v) belongs to $T(m)$ and this implies $S(m) = T(m)$. This shows that $T(m)$ contains all the solutions (u, v) with $1 \leq u \leq v$ and finishes the proof of Theorem 3.

3. Proof of Corollary 1

Let

$$M := |\{1 \leq u \leq v \leq x : \ u|v^2 - 1 \text{ and } v|u^2 - 1\}|.$$

Note that $uv|u^2+v^2-1 \Leftrightarrow u|v^2-1$ and $v|u^2-1$. If $u|v^2-1$ and $v|u^2-1$, we must have $(u,v)=1$ which gives $uv|u^2+v^2-1$. On the other hand if $uv|u^2+v^2-1$, then $u|u^2+v^2-1$ and hence $u|v^2-1$. Similarly $v|u^2=1$. Thus it suffices to study the equation

$$u^2+v^2-1 = muv \text{ for some positive integer } m.$$

From Theorem 4, the case $m=1$ gives us one solution and the case $m=2$ gives us $x+O(1)$ solutions. When $m \geq 3$, we define $(u_n, v_n) = F^n(1,m)$ for $n \geq 0$. Note that

$$v_{n+1} = mv_n - u_n \geq (m-1)v_n.$$

Since $v_0 = m$, by induction we have $v_n > (m-1)^{n+1}$.

With this estimate we are ready to estimate $|M|$. For $n=0$, we have $u_0=1$ and $v_0=m$ which contributes $x+O(1)$ solutions to M. For $n=1$, we have $u_1=m$ and $v_1=m^2-1$ which contributes $x^{1/2}+O(1)$ solutions to M. Summarizing the above,

$$2x+x^{1/2}+O(1) \leq |M| \leq 2x+x^{1/2}+O(1)+\sum_{2\leq n\leq \log_2 x} \sum_{\substack{m\geq 3 \\ (m-1)^{n+1}\leq x}} 1 = 2x+x^{1/2}+O(x^{1/3})$$

which gives Corollary 1.

4. Proof of Theorem 2

In fact, we are going to prove a more general result.

Theorem 5. *Suppose A is a positive integer, B is any integer and C is a non-zero integer. Let $f(n) = A(n+B)^2+C$. Suppose $f(a)|f(b)$ with $f(b) = d^2 f(a)$ for some $b > a \geq 1-B$ and $d \geq 3$. Suppose $A+C \geq 0$ also. Then we have*

(i) *if $C < 0$, then*

$$\frac{2A(b+B)+(A-C)}{|C|} \leq d^2. \tag{4}$$

Moreover, the bound is best possible and it occurs in the special case when

$$d = \frac{Aa+\sqrt{A^2a^2+AC+C^2}}{|C|}$$

is a positive integer and $b = da-1$. With this special case aside, we have

$$(b+B) \leq \frac{|C|d^2-d+2C}{2\sqrt{A}\sqrt{d-C}} \tag{5}$$

and, again, this bound is best possible. The right hand side of (5) is positive since $d \geq 3$. Note that this bound implies $\left(\frac{2\sqrt{A}}{|C|}(b+B)\right)^{2/3} \leq d$.

(ii) *if $C > 0$, then*

$$\frac{(2A)(b+B)+(C-A)}{C} \leq d^2 \tag{6}$$

and, again, this bound is best possible.

Proof. Without loss of generality, we may assume $B = 0$.

Suppose $Ab^2 + C = d^2(Aa^2 + C)$ for some $b > a \geq 1$ and $d \geq 3$. Then

$$Ab^2 + C = A(da)^2 + Cd^2. \tag{7}$$

Let $da = b + k$. Clearly $k \neq 0$ otherwise we have $C = Cd^2$ which contradicts $d > 1$. If $C > 0$, then $Ab^2 = A(da)^2 + C(d^2-1) > A(da)^2$ and hence $b > da$ and $k < 0$. Similarly, if $C < 0$, then $k > 0$.

In view of (7), we have

$$A(da)^2 + Cd^2 = A(da-k)^2 + C = A(da)^2 - 2Adak + Ak^2 + C$$

which gives

$$Ak^2 + C(1-d^2) = 2Akda = 2Ak(b+k) = 2Akb + 2Ak^2. \tag{8}$$

Hence

$$-Ak^2 + C(1-d^2) = 2Akb. \tag{9}$$

Suppose $C < 0$. Then $k \geq 1$. Let

$$F(x) := \frac{-Ax^2 + C(1-d^2)}{x} = -Ax + \frac{C(1-d^2)}{x}, \quad x \geq 1.$$

Then $F'(x) = -A - C(1-d^2)/x^2 < 0$ for $d > 1$ and $x \geq 1$. So $F(x)$ is decreasing on $[1, \infty)$. So $F(k) \leq F(1) = -A + C(1-d^2)$. It follows that

$$b = \frac{-Ak^2 + C(1-d^2)}{2Ak} = \frac{F(k)}{2A} \leq \frac{F(1)}{2A} = \frac{-A + C(1-d^2)}{2A}.$$

This gives (4).

The equality holds only if $k = 1$. In this case $b = da - 1$. By (8), we have $A + C(1-d^2) = 2Ada$ and therefore

$$-Cd^2 - 2Aad + A + C = 0.$$

Treating it as a quadratic equation in d, we have

$$d = \frac{-Aa \pm \sqrt{A^2a^2 + AC + C^2}}{C}.$$

Since $d > 1$ and $C < 0$, we should take $-$ in the $\pm$ sign.

Conversely, suppose we have $d = (-Aa - \sqrt{A^2a^2 + AC + C^2})/C$ and $b = da - 1$. The definition of d implies $-Cd^2 + A + C = 2Aad$. Thus

$$\frac{2Ab + A - C}{|C|} = \frac{2Ada - A - C}{|C|} = d^2.$$

Furthermore,

$$\begin{aligned} d^2(Aa^2 + C) &= A(da)^2 + Cd^2 \\ &= A(b+1)^2 + Cd^2 \\ &= Ab^2 + C + 2Ab + A + C(d^2 - 1) \\ &= Ab^2 + C + 2A(da - 1) + A + C(d^2 - 1) \\ &= Ab^2 + C. \end{aligned}$$

To show that our bound is best possible, it remains to show that $A^2a^2 + AC + C^2$ can be a perfect square. To do this we only need to put $A + C = 0$.

Now suppose $k > 1$. Equation (8) implies $d|(Ak^2 + C)$. Since $Ak^2 + C > A + C \geq 0$, we have $d \leq Ak^2 + C$. Thus $k \geq ((d - C)/A)^{1/2}$. Hence

$$b = \frac{F(k)}{2A} \leq \frac{F\left(\sqrt{\frac{d-C}{A}}\right)}{2A} = \frac{-(d-C) + C(1-d^2)}{2A\sqrt{\frac{d-C}{A}}} = \frac{|C|d^2 - d + 2C}{2\sqrt{A}\sqrt{d-C}}.$$

This gives (5). Finally, $C < 0$ implies $d \geq \left(\frac{2\sqrt{A}b}{|C|}\right)^{2/3}$.

Next we need to show that the equality in (5) can be attained. For any even k, suppose A and C are odd such that $A + C \geq 3$ and $C^2 \equiv 1 \pmod{2Ak}$. Let $d := Ak^2 + C \geq 3$ so that $C \equiv d \pmod{2Ak}$ and $d^2 \equiv 1 \pmod{2Ak}$. It follows that

$$-Ak^2 + C(1 - d^2) \equiv 0 \pmod{2Ak}.$$

Let $a := \frac{1-Cd}{2Ak}$ and $b := \frac{-Ak^2+C(1-d^2)}{2Ak}$. Then $b = \frac{F(k)}{2A}$ with $k = \sqrt{\frac{d-C}{A}}$. It follows that $b > a \geq 1$ since

$$1 - Cd = 1 + |C|d \geq 1 + 3 = 4$$

and

$$b-a=\frac{1}{2Ak}(-Cd^2-d+2C-(1-Cd))=\frac{(d+1)(|C|(d-2)-1)}{2Ak}>0.$$

Moreover

$$da-k=\frac{d(1-Cd)-2Ak^2}{2Ak}=\frac{(Ak^2+C)-Cd^2-2Ak^2}{2Ak}=\frac{-Ak^2+C(1-d^2)}{2Ak}=b.$$

Therefore

$$\begin{aligned}d^2(Aa^2+C)&=A(da)^2+Cd^2\\&=A(b+k)^2+Cd^2\\&=Ab^2+C+2Abk+Ak^2+C(d^2-1)\\&=Ab^2+C+2Abk-2Abk\\&=Ab^2+C.\end{aligned}$$

This shows that the bound $b\le\frac{|C|d^2-d+2C}{2\sqrt{A}\sqrt{d-C}}$ is best possible.

Suppose $C>0$. Then $k<0$ and

$$b=\frac{-Ak^2+C(1-d^2)}{2Ak}=\frac{1}{2A}\left(\frac{Ak^2+C(d^2-1)}{|k|}\right)=\frac{G(|k|)}{2A}$$

where

$$G(x):=\frac{Ax^2+C(d^2-1)}{x}=Ax+\frac{C(d^2-1)}{x},\quad x\ge 1.$$

However, $G(x)$ is no long decreasing on $[1,\infty)$ because $C>0$. In fact,

$$G'(x)=A-\frac{C(d^2-1)}{x^2},G''(x)=\frac{2C(d^2-1)}{x^3}$$

and $G(x)$ is convex in $[1,\infty)$.

In view of (9), we have $C(1-d^2)\equiv 0 \pmod{Ak}$. So $|k|\le\frac{C(d^2-1)}{A}$. Since $k<0$, we have $1\le|k|\le\frac{C(d^2-1)}{A}$. It follows that

$$\begin{aligned}b=\frac{G(|k|)}{2A}&\le\max\left\{\frac{G(1)}{2A},\frac{G(C(d^2-1)/A)}{2A}\right\}\\&=\max\left\{\frac{A+C(d^2-1)}{2A},\frac{C(d^2-1)+A}{2A}\right\}=\frac{C(d^2-1)+A}{2A}.\end{aligned}$$

This gives (6).

To show that the equality can be attained, we suppose A and C are two positive odd integers. Let d be any positive even integer greater 3 such that $d^2 \equiv 1 \pmod{A}$. Since $A + C(d^2 - 1)$ is even, we have

$$A + C(d^2 - 1) \equiv 0 \pmod{2A}.$$

Let $b := \frac{A+C(d^2-1)}{2A}$. Hence $d^2 = \frac{2Ab+(C-A)}{C}$. Note that $\frac{d^2-1}{A}$ is odd and coprime to d, we can require our C to satisfy

$$C\left(\frac{d^2-1}{A}\right) \equiv 1 \pmod{2d}.$$

Then for sufficiently large C,

$$\frac{b-1}{d} = \frac{Cd^2 - A - C}{2Ad} = \frac{C\left(\frac{d^2-1}{A}\right) - 1}{2d}$$

is a positive integer. We define this to be a so that $da = b-1$ and $b > a \geq 1$. Consequently,

$$\begin{aligned} d^2(Aa^2 + C) &= Ab^2 + C - 2Ab + A + C(d^2 - 1) \\ &= Ab^2 + C - 2A \times \frac{A + C(d^2-1)}{2A} + A + C(d^2 - 1) \\ &= Ab^2 + C. \end{aligned}$$

This special case shows that the bound $\frac{2Ab+(C-A)}{C} \leq d^2$ cannot be improved. □

Theorem 2 follows from Theorem 5 with $A = 1$, $B = 0$ and $C = -1$.

5. Proof of Theorem 3

First, let us recall a result of Turk [2] on simultaneous Pell equations.

Theorem 6. *Let a, b, c, d be squarefree positive integers with $a \neq b$ and $c \neq d$ and let e and f be any integers. If $af = ce$ then we also assume that $abcd$ is not a perfect square. Then every positive integer solution of*

$$\begin{cases} ax^2 - by^2 = e \\ cx^2 - dz^2 = f \end{cases}$$

satisfies

$$\max(x, y, z) < e^{K\alpha^2(\log\alpha)^3\gamma\log\gamma}$$

where $\alpha = \max(a, b, c, d)$, $\beta = \max(|e|, |f|, 3)$, $\gamma = \max(\alpha \log \alpha, \log \beta)$ *and* K *is a large absolute constant.*

Again we prove the following more general theorem.

Theorem 7. *Suppose* A *is square-free positive integer, any integer* B *and* C *is a non-zero integer. Let* $f(n) = A(n+B)^2 + C$. *Suppose* $A + C \geq 0$ *also. Then if* $f(a)|f(b)|f(c)$ *with* $1 - B < a < b < c$, *then*

$$A' \left(\frac{A(c+B)^2 + C}{A(a+B)^2 + C} \right) \geq K \frac{(\log(c+B))^{1/6}}{(\log\log(c+B))^{5/6}},$$

for some absolute constant $K > 0$ *and* $A' := max\{|A|, |C|, 3\}$.

Proof. Again assume $B = 0$. Let $f(n) := An^2 + C$. Suppose $f(a)|f(b)|f(c)$ with $1 < a < b < c$. Say

$$Ac^2 + C = d(Aa^2 + C) \text{ and } Ac^2 + C = e(Ab^2 + C)$$

for some $2 \leq e < d$. Suppose $d = d_1 d_2^2$ and $e = e_1 e_2^2$ with d_1 and e_1 square-free. We may assume that $d_1 \neq 1$ and $e_1 \neq 1$ for otherwise the result follows from Theorem 5 immediately as $d = d_2^2$ or $e = e_2^2$. Hence, we have a pair of simultaneous Pell's equations

$$Ac^2 - d_1 A(d_2 a)^2 = C(d-1) \text{ and } Ac^2 - e_1 A(e_2 b)^2 = C(e-1).$$

As $d \neq e$, we can apply Theorem 6 with $\alpha \leq Ad, \beta \leq \max\{|C|d, 3\}, \gamma \leq \max\{Ad\log(Ad), \log(|C|d)\}$ and obtain

$$c < e^{K(A'd)^2(\log(A'd))^3(A'd\log(A'd))\log(A'd)}$$

for some absolute constant $K > 0$ and $A' = \max\{A, |C|, 3\}$. Let $x = A'd$ and take logarithm on both sides, we deduce that

$$\log c < Kx^3(\log x)^5.$$

If $x < (\log c)^{1/3}$, we have

$$A'd = x > K^{-1/3} \frac{(\log c)^{1/3}}{(\log((\log c)^{1/3}))^{5/3}} \geq K' \frac{(\log c)^{1/3}}{(\log\log c)^{5/3}} \tag{10}$$

for some absolute constant $K' > 0$. If $x \geq (\log c)^{1/3}$ then we have (10) with $K' = 1$. This gives Theorem 7 as $d = \frac{Ac^2+C}{Aa^2+C}$. □

References

[1] T.H. Chan, Common factors among pairs of consecutive integers, Int. J. Number Theory (2018), http://dx.doi.org/10.1142/S1793042118500525, in press.

[2] J. Turk, Almost powers in short intervals, Arch. Math. 43 (1984) 157–166.