GAP PRINCIPLE OF DIVISIBILITY SEQUENCES OF POLYNOMIALS

STEPHEN CHOI, PETER CHO-HO LAM, AND DANIEL TARNU

Abstract. Let $f \in \mathbb{Z}[x]$ and $\ell \in \mathbb{N}$. Consider the set of all $(a_0, a_1, \dots, a_\ell) \in \mathbb{N}^{\ell+1}$ with $a_i < a_{i+1}$ and $f(a_i) \mid f(a_{i+1})$ for all $0 \le i \le \ell - 1$. We say that f satisfies the gap principle of order ℓ if $\lim a_\ell / a_0 = \infty$ as $a_0 \to \infty$. We also define the gap order of $f(x)$ to be the smallest positive integer ℓ such that $f(x)$ satisfies the gap principle of order ℓ. If such ℓ does not exist, we say that $f(x)$ does not satisfy the gap principle. In this article, we prove a conjecture by Chan, Choi and Lam that $f(x)$ does not satisfy the gap principle if and only if $f(x)$ is in the form of $f(x) = A(Bx + C)^n$ for some $A, B, C \in \mathbb{Z}$. Moreover, we completely determine the gap order of any polynomial. We will show that if $f(x)$ is not in the form of $A(Bx + C)^n$, then $f(x)$ has gap order 2 if $f(x)$ is a quadratic polynomial or a power of a quadratic polynomial; and has gap order 1 otherwise.

1. Introduction

In [8], Erdős and Rosenfeld considered the differences between the divisors of a positive integer n. They exhibited infinitely many integers with four "small" differences and posed the question that any positive integer can have at most a bounded number of "small" differences. Specifically, they asked

Conjecture 1. Is there an absolute constant K, so that for every c, the number of divisors of n between $\sqrt{n} - c\sqrt[4]{n}$ and $\sqrt{n} + c\sqrt[4]{n}$ is at most K for $n > n_0(c)$?

They also mentioned a conjecture of Ruzsa which is a stronger question:

Conjecture 2. Given $\epsilon > 0$, is there a constant K_ϵ such that, for any positive integer n, the number of divisors of n between $n^{1/2} - n^{1/2-\epsilon}$ and $n^{1/2} + n^{1/2-\epsilon}$ is at most K_ϵ?

In [3], Chan proved the above conjecture of Erdős and Rosenfeld for perfect squares and made some progress towards Ruzsa's conjecture for perfect squares. In studying Conjecture 2 for the special form $n = N^4$, he considered the gap between a and b where $b^2(b^2 + 1) \mid a^2(a^2 + 1)$ and posed the following question in [4].

Question. 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 $\lambda > 0$?

Date: October 25, 2020.

2010 *Mathematics Subject Classification.* Primary 11B05, 11C08.

Key words and phrases. Gap principle, Pell's equations, Quadratic congruence.

Research supported by NSERC, grant number 611312.

For more progress about this question, we refer to [5].

One can also ask the same question for any polynomial with integral coefficients. In [6], the authors formulate the question more precisely:

Definition 1. *Let $f \in \mathbb{Z}[x]$ and $\ell \in \mathbb{N}$. Consider the set of all $(a_0, a_1, \ldots, a_\ell) \in \mathbb{N}^{\ell+1}$ with $a_i < a_{i+1}$ and $f(a_i) \mid f(a_{i+1})$ for all $0 \le i \le \ell - 1$. We say that f satisfies* **the gap principle of order** ℓ *if $\lim a_\ell / a_0 = \infty$ as $a_0 \to \infty$.*

In other words, f satisfies the gap principle of order ℓ if and only if for any sequence $\{\mathbf{a}_j\}_{j=1}^{\infty}$ of points in $\mathbb{N}^{\ell+1}$ with $\mathbf{a}_j := (a_{0j}, \ldots, a_{\ell j})$ such that $a_{ij} < a_{(i+1)j}$, $f(a_{ij}) | f(a_{(i+1)j})$ for all $0 \le i \le \ell - 1$ and $\lim\limits_{j\to\infty} a_{0j} = \infty$, we have

$$\lim_{j\to\infty} \frac{a_{\ell j}}{a_{0j}} = +\infty.$$

In view of this definition, the above question is asking if $f(x) = x^2(x^2+1)$ satisfies the gap principle of order 1, which is shown in Theorem 1 below (also see [5]). We believe that the study of the gap principle are useful in the study of variants of Conjectures 1 and 2 above.

We denote

$$S_f^\ell := \left\{(a_0, \ldots, a_\ell) \in \mathbb{N}^{\ell+1} : f(a_i) \mid f(a_{i+1}) \text{ and } a_i < a_{i+1} \text{ for all } 0 \le i \le \ell - 1\right\}.$$

Note that the set of all such $(a_0, a_1, \ldots, a_\ell)$ is always infinite since we have

$$f(a \pm f(a)) \equiv 0 \pmod{f(a)}, \ \textit{i.e.}, \ f(a) \mid f(a \pm f(a)), \quad \forall a \in \mathbb{N}$$

and $\max\{a + f(a), a - f(a)\} > a$ for sufficiently large a. Hence S_f^ℓ is always an infinite set.

If $f(x)$ satisfies the gap principle of some order ℓ, it will also satisfy the gap principle of any larger order.

Definition 2. *Let $f \in \mathbb{Z}[x]$. We define the* **gap order** *of $f(x)$ to be the smallest positive integer ℓ such that $f(x)$ satisfies the gap principle of order ℓ. If such ℓ does not exist, we say that $f(x)$* **does not satisfy the gap principle**.

As shown in [4] and [6], the polynomials $A(Bx + C)^n \in \mathbb{Z}[x]$ do not satisfy the gap principle and the polynomial $f(x) = x^2 - 1$ has gap order 2. For any integer $m \ge 1$, since $f(a) \mid f(b)$ if and only if $f(a)^m \mid f(b)^m$, so $f(x)$ satisfies the gap principle of order ℓ (or does not satisfy the gap principle) if and only if $f(x)^m$ satisfies the gap principle of order ℓ (or does not satisfy the gap principle). In [6], the authors make the following conjecture.

Conjecture 1 (Chan, Choi, Lam)**.** *Let $f(x) \in \mathbb{Z}[x]$ of degree $n \ge 0$. The polynomial $f(x)$ does not satisfy the gap principle if and only if $f(x)$ is in the form of $f(x) = A(Bx + C)^n$ for some $A, B, C \in \mathbb{Z}$.*

In this article, we will prove that this conjecture is true. Moreover, we completely determine the gap order of any polynomial. We will show the following theorems.

Theorem 1. *For any polynomial $f(x) \in \mathbb{Z}[x]$ such that $f(x) \ne A(Bx^2 + Cx + D)^n$, $f(x)$ satisfies the gap principle of order* 1.

Theorem 2. *All quadratic polynomials $f(x) = Ax^2 + Bx + C$ or powers of quadratic polynomials $f(x) = D(Ax^2 + Bx + C)^n$ such that $A, D \ne 0$ and $B^2 - 4AC \ne 0$ has gap order* 2.

In view of Theorems 1 and 2, any polynomials, not in Theorems 1 and 2, are in the form of $f(x) = A(Bx + C)^n$ for some $A, B, C \in \mathbb{Z}$ and this proves that Conjecture 1 is true.

2. Polynomials that satisfy the gap principle of order 1

If there is a sequence of pair of integers $\{(x_j, y_j)\}_{j=1}^{\infty}$ in S_f^1 such that $\lim_{j\to\infty} x_j = \infty$ and y_j/x_j is bounded, then $f(x)$ does not satisfy the gap principle of order 1. We show below the converse is also true.

Lemma 1. *A polynomial $f \in \mathbb{Z}[x]$ does not satisfy the gap principle of order 1 if and only if there is $N > 1$ such that the set*

$$S_N(f) := \left\{(x, y) \in \mathbb{N}^2 : f(x)|f(y), \quad 1 < y/x \le N\right\}$$

is infinite.

Proof. Suppose that f does not satisfy the gap principle of order 1. Then there exists a sequence $\{(x_j, y_j)\}_{j=1}^{\infty}$ in S_f^1 such that $\lim_{j\to\infty} x_j = \infty$ and

$$\lim_{j\to\infty} \frac{y_j}{x_j} < \infty.$$

So, there is a $N > 1$, such that $1 < y_j/x_j \le N$ for all $j \ge 1$. Hence $\{(x_j, y_j)\}_{j=1}^{\infty} \subseteq S_N(f)$ and $S_N(f)$ is infinite.

Suppose that $S_N(f)$ is infinite. Then there is a sequence $\{(x_j, y_j)\}_{j=1}^{\infty}$ of distinct points in $S_N(f)$. We claim that $\lim_{j\to\infty} x_j = \infty$. Indeed, if $\{x_j\}_{j=1}^{\infty}$ is bounded, then since $1 < y_j/x_j \le N$, so $\{y_j\}_{j=1}^{\infty}$ is also bounded. This contradicts the sequence $\{(x_j, y_j)\}_{j=1}^{\infty}$ of distinct points in S_N is infinite. Again since $1 < y_j/x_j \le N$, so $\limsup_{j\to\infty} y_j/x_j \le N < \infty$. Hence $f(x)$ does not satisfy the gap principle of order 1. □

The following is Theorem 1.1 in [1], found on P. 263.

Theorem 3 (Bilu and Tichy)**.** *The equation*

$$f(x) = g(y)$$

for non-constant polynomials $f, g \in \mathbb{Q}[x]$ has infinitely many rational solutions $(x, y) \in \mathbb{Q}^2$ with bounded denominator if and only if

$$f = \varphi \circ f_1 \circ \lambda$$
$$g = \varphi \circ g_1 \circ \mu$$

for some $\varphi \in \mathbb{Q}[x]$, linear polynomials $\lambda, \mu \in \mathbb{Q}[x]$, and (f_1, g_1) being one of the following standard pairs such that $f_1(x) = g_1(y)$ has infinitely many rational solutions with bounded denominator:

(1) *$(x^m, ax^r p(x)^m)$ or $(ax^r p(x)^m, x^m)$ where $0 \le r \le m$, $(r, m) = 1$, and $r + \deg(p) > 0$.*

(2) *$(x^2, (ax^2 + b)p(x)^2)$ or $((ax^2 + b)p(x)^2, x^2)$ for some $a, b \in \mathbb{Q}$ and $p \in \mathbb{Q}[x]$.*

(3) $(D_m(x, a^n), D_n(x, a^m))$, *where* $(n, m) = 1$, *and* D_m *is the* m*-th Dickson polynomial of degree* m, *defined by*

$$D_m(x + a/x, a) = x^m + (a/x)^m.$$

(4) $(a^{-m/2}D_m(x, a), -b^{-n/2}D_n(x, b))$, *where* $(n, m) = 2$.

(5) $((ax^2 - 1)^3, 3x^4 - 4x^3)$ *or* $(3x^4 - 4x^3, (ax^2 - 1)^3)$ *for some* $a \in \mathbb{Q}$.

Proof. This is Theorem 1.1 in [1]. □

We would like to show that if $g = kf$, $f(x)$ and $g(x)$ are not in the form of the composition above, then $f(y) = kf(x)$ has only finitely many integer solutions. The following lemma is needed to show that f satisfies the gap principle of order 1.

Lemma 2. *Let* $f \in \mathbb{Z}[x]$ *a polynomial such that* $f(x) \neq A(Bx^2 + Cx + D)^n$ *for* $A, B, C, D \in \mathbb{Z}$. *Let* k *be an integer* ≥ 2. *Then, the diophantine equation* $f(y) = kf(x)$ *has at most finitely many solutions* $(x, y) \in \mathbb{Z}^2$.

Proof. Let $f \in \mathbb{Z}[x]$ be a polynomial such that $f(x) \neq A(Bx^2 + Cx + D)^n$ where B may be zero. In view of Theorem 3, it suffices to show that

$$(f, kf) \neq (\varphi \circ f_1 \circ \lambda, \varphi \circ g_1 \circ \mu)$$

for $\varphi \in \mathbb{Q}[x]$, linear polynomials $\lambda, \mu \in \mathbb{Q}[x]$, and (f_1, g_1) being one of the standard pairs given in Theorem 3 because if $f(y) = kf(x)$ has only finitely many rational solutions with bounded denominator and hence it has only finitely many integer solutions $(x, y) \in \mathbb{N}^2$.

Suppose the contrary that there are $\varphi, f_1, g_1, \lambda, \mu \in \mathbb{Q}[x]$ such that

$$(f, kf) = (\varphi \circ f_1 \circ \lambda, \varphi \circ g_1 \circ \mu) \tag{1}$$

as above. We must have that $\deg(f_1) = \deg(g_1)$. So, for this reason, we can ignore the possibility that (f_1, g_1) is a standard pair of the fifth kind because they have different degrees. Also if (f_1, g_1) is a standard pair of the third kind, then $n = m = 1$ and $(f_1(x), g_1(x)) = (D_1(x, a), D_1(x, a)) = (x, x)$ which will be included in Case 1 below. Here $D_1(x, a) = x$. It remains to consider the standard pair of the first, second and fourth kinds.

Case 1 (first kind): Suppose that $(f_1, g_1) = (x^m, ax^r p(x)^m)$ is a standard pair of the first kind. Since $\deg(f_1) = \deg(g_1)$, we must have that either $r = 0, \deg(p) = 1$ (and hence $m = 1$ because of $(r, m) = 1$) or $r = m, \deg(p) = 0$ (and hence $r = m = 1$ because of $(r, m) = 1$). Hence $(r, m, \deg(p)) = (0, 1, 1)$ or $(1, 1, 0)$. In either cases, we have $f_1 \circ \lambda$ and $g_1 \circ \mu$ are linear polynomials. Suppose that

$$(f, kf) = (\varphi \circ \lambda_1, \varphi \circ \mu_1)$$

for some linear polynomials $\lambda_1, \mu_1 \in \mathbb{Q}[x]$. We can compose f and kf with λ_1^{-1} to get that $f(\lambda_1^{-1}(x)) = \varphi(x)$ and $kf(\lambda_1^{-1}(x)) = k\varphi(x) = \varphi(\mu_1(\lambda_1^{-1}(x)))$. For simplicity, we let $\nu(x) = \mu_1(\lambda_1^{-1}(x)) = cx + d \in \mathbb{Q}[x]$ such that

$$k\varphi = \varphi \circ \nu. \tag{2}$$

Note that the zeros of $k\varphi$ are exactly the zeros of φ and $\varphi \circ \nu$. Assume that φ has *distinct* zeros $\alpha_1, \alpha_2, \ldots, \alpha_\ell$ for some $\ell \geq 2$. We may not have $\nu(\alpha_i) = \nu(\alpha_j)$,but ν must permute the zeros $\alpha_1, \ldots, \alpha_\ell$. Let

$$\nu^r = \underbrace{\nu \circ \nu \circ \cdots \circ \nu}_{r \text{ of } \nu}.$$

Then, $\nu^{\ell!}(\alpha_i) = \alpha_i$ for all $1 \leq i \leq \ell$ and we have for $i \neq j$

$$\frac{\nu^{\ell!}(\alpha_i) - \nu^{\ell!}(\alpha_j)}{\alpha_i - \alpha_j} = \frac{\alpha_i - \alpha_j}{\alpha_i - \alpha_j} = 1. \tag{3}$$

Since $\nu(x) = cx + d$, so, if $c \neq 1$, then we have $\nu^j(\alpha_i) = c^j \alpha_i + d\left(\frac{c^j-1}{c-1}\right)$ for any $1 \leq j$ and $1 \leq i \leq \ell$. In view of (3), we have $c = \pm 1$. However, since $k\varphi = \varphi \circ \nu$, this implies that $k = \pm 1$ by comparing the leading coefficients. This contradicts our assumption that $k \geq 2$. So, we must have that φ has only one (repeated) zero, and is thus of the form $A(Cx + D)^n$ for some $A, C, D \in \mathbb{Q}$. Since $f(x) \in \mathbb{Z}[x]$, by considering the common denominators of A, C, D, we can assert that $A, C, D \in \mathbb{Z}$ which contradicts our assumption of f. Thus $(f_1, g_1) \neq (x^m, ax^r p(x)^m)$. Similarly, we can show that $(f_1, g_1) \neq (ax^r p(x)^m, x^m)$.

Case 2 (Second and fourth kinds): For (f_1, g_1) the standard pair of the second or fourth kinds, since $\deg(f_1) = \deg(g_1)$, both $f_1(x)$ and $g_1(x)$ are quadratic polynomials. We claim that

$$(f, kf) \neq (\varphi \circ f_1 \circ \lambda, \varphi \circ g_1 \circ \mu)$$

for any quadratic polynomials f_1 and g_1 in $\mathbb{Q}[x]$. We first find a linear polynomial $\lambda_1(x) \in \mathbb{Q}[x]$ such that $f_1 \circ \lambda \circ \lambda_1$ has no x term. So $f(\lambda_1(x)) = \varphi(a_1x^2 + b_1)$ for some $a_1, b_1 \in \mathbb{Q}$ and $a_1 \neq 0$. Then

$$kf(\lambda_1(x)) = k\varphi(a_1x^2 + b_1) = (\varphi \circ g_1 \circ \mu \circ \lambda_1)(x) = \varphi(a_2x^2 + b_2x + c_2)$$

for some $a_2, b_2, c_2 \in \mathbb{Q}$ and $a_2 \neq 0$ because $g_1 \circ \mu \circ \lambda_1$ is a quadratic polynomial. Since $\varphi(a_1x^2 + b_1)$ is an even function, so $b_2 = 0$. It follows that $k\varphi(a_1x^2 + b_1) = \varphi(a_2x^2 + c_2)$. By replacing x^2 by x, we have $k\varphi(a_1x + b_1) = \varphi(a_2x + c_2)$ and hence $k\varphi(x) = \varphi(\nu(x))$ where $\nu(x) = a_2a_1^{-1}x + (c_2 - a_2b_1a_1^{-1}) \in \mathbb{Q}[x]$, which goes back to (2) in Case 1 and can be treated in the same way as in Case 1. Therefore, $\varphi(x) = A(Cx + D)^n$ for some $A, C, D \in \mathbb{Q}$. Hence

$$f(x) = \varphi(a_1(\lambda_1^{-1}(x))^2 + b_1) = A(C(a_1(\lambda_1^{-1}(x))^2 + b_1) + D)^n = A(B'x^2 + C'x + D')^n$$

for some $A, B', C', D' \in \mathbb{Q}$ because $C(a_1(\lambda_1^{-1}(x))^2 + b_1) + D$ is a quadratic polynomial in $\mathbb{Q}[x]$. Since $f(x)$ has integer coefficients, so by considering the common denominators of A, B', C' and D', we can assert that $A, B', C', D' \in \mathbb{Z}$ and hence contradicts our assumption.

This completes the proof of the lemma. □

Proof of Theorem 1.

Let $f(x) \in \mathbb{Z}[x]$ be a polynomial such that $f(x) \neq A(Bx^2 + Cx + D)^n$. Without loss of generality, we may assume the leading coefficient of f is positive; otherwise, we replace f by $-f$. In view of Theorem 3 and Lemma 2, for any integer $k \geq 2$, the equation $f(y) = kf(x)$ has only finitely many integer solutions $(x, y) \in \mathbb{N}^2$. Therefore, the set

$$\{(x, y) \in \mathbb{N}^2 : f(y) = kf(x)\}$$

is finite.

We claim that $f(x)$ satisfies the gap principle of order 1. In view of Lemma 1, it suffices to show that for any $N > 1$, the set

$$S_N(f) = \{(x, y) \in \mathbb{N}^2 : f(x) \mid f(y), \quad 1 < y/x \le N\}$$

is finite.

Let $f(x) = a_m(x-\alpha_1)\cdots(x-\alpha_m)$ with $a_m > 0$ and $M = \max\{|\alpha_1|, |\alpha_2|, \dots |\alpha_m|\}$. For $x \ge 2M$, we have

$$\begin{aligned}
\left|\frac{f(y)}{f(x)}\right| &= \left|\frac{(y-\alpha_1)\cdots(y-\alpha_m)}{(x-\alpha_1)\cdots(x-\alpha_m)}\right| \\
&= \left|\frac{(y/x-\alpha_1/x)\cdots(y/x-\alpha_m/x)}{(1-\alpha_1/x)\cdots(1-\alpha_m/x)}\right| \\
&\le \frac{(y/x+|\alpha_1|/x)\cdots(y/x+|\alpha_m|/x)}{(1-|\alpha_1|/x)\cdots(1-|\alpha_m|/x)} \\
&\le \frac{(y/x+1/2)\cdots(y/x+1/2)}{(1-1/2)\cdots(1-1/2)} \\
&= 2^m(y/x+1/2)^m.
\end{aligned}$$

Hence, if $(x, y) \in S_N(f)$ and $x \ge 2M$, we have

$$|f(y)/f(x)| \le (2N+1)^m. \tag{4}$$

To obtain the finiteness of $S_N(f)$, we only need to consider sufficiently large $x > 0$. For sufficiently large $y > x \ge 2Mm$, we have

$$x^m \ge 2\frac{|a_{m-1}x^{m-1} + \cdots + a_1x + a_0|}{a_m} \quad \text{and} \quad y^m \ge 2\frac{|a_{m-1}y^{m-1} + \cdots + a_1y + a_0|}{a_m}.$$

As a result, we have $f(y) > f(x) > 0$ for $y > x \ge 2Mm$. Note that $f(x)$ is increasing on $[2Mm, \infty)$.

We now assume that $y > x \ge 2Mm$. Consider $f(x) \mid f(y)$. Then $f(y) = kf(x)$ for some positive integer $k \ge 2$. From (4), we have $k \le (2N+1)^m$. Since $\{(x, y) \in \mathbb{N} : f(y) = kf(x)\}$ is finite, so

$$\begin{aligned}
&\{(x, y) \in \mathbb{N}^2 : x \ge 2Mm,\ f(x) \mid f(y),\ 1 < y/x \le N\} \\
&\qquad\qquad \subseteq \bigcup_{2 \le k \le (2N+1)^m} \{(x, y) \in \mathbb{N}^2 : f(y) = kf(x)\}
\end{aligned}$$

is finite. Also, the set

$$\begin{aligned}
&\{(x, y) \in \mathbb{N}^2 : x < 2Mm,\ f(x) \mid f(y),\ 1 < y/x \le N\} \\
&\qquad\qquad \subseteq \{(x, y) \in \mathbb{N}^2 : x < 2Mm, y \le N2Mm\}
\end{aligned}$$

is also finite. Hence $S_N(f)$, which is the union of the above two subsets, is finite. This completes the proof of Theorem 1. $\square$

3. Quadratic Polynomials have gap order 2

In this section, we will show that all quadratic polynomials and all powers of quadratic polynomials, not in the form of $A(Bx+C)^n$, satisfy the gap principle of order 2. The following theorems extends Theorems 5 and 7 in [6] with similar proofs.

Theorem 4. *Let $f(x) = Ax^2 + Bx + C$ such that $A \neq 0$ and $\Delta := B^2 - 4AC \neq 0$. Suppose $f(a)|f(b)$ with $1 < a < b$ and $f(b) = d^2 f(a)$ for some $d > 1$. Then we have*

$$\frac{2|2Ab+B| - 1 + |\Delta|}{|\Delta|} \leq d^2. \tag{5}$$

Proof. We first note that

$$\begin{aligned} 4Af(x) &= (2Ax)^2 + 2B(2Ax) + 4(AC) \\ &= (2Ax+B)^2 - (B^2 - 4AC) = (2Ax+B)^2 - \Delta. \end{aligned} \tag{6}$$

Therefore, we consider the particular polynomials $g(x) := x^2 - \Delta$ so that $4Af(x) = g(2Ax+B)$. Let $\alpha := |2Aa+B|$ and $\beta := |2Ab+B|$. Then $f(b) = d^2 f(a)$ implies $g(\beta) = d^2 g(\alpha)$, i.e.

$$\beta^2 - \Delta = d^2(\alpha^2 - \Delta) = (d\alpha)^2 - d^2\Delta.$$

Let $d\alpha = \beta + k$. Clearly $k \neq 0$ otherwise we have $\Delta = \Delta d^2$ and hence $d = 1$. If $\Delta > 0$, then $\beta^2 = (d\alpha)^2 - \Delta(d^2-1) < (d\alpha)^2$ and hence $\beta < d\alpha$ and $k > 0$. Similarly, if $\Delta < 0$, then $k < 0$.

Now we have

$$(d\alpha)^2 - d^2\Delta = \beta^2 - \Delta = (d\alpha - k)^2 - \Delta = (d\alpha)^2 - 2d\alpha k + k^2 - \Delta$$

which gives

$$k^2 - \Delta(1-d^2) = 2kd\alpha = 2k(\beta+k) = 2k\beta + 2k^2. \tag{7}$$

Hence,

$$d^2 = \frac{k^2 + 2k\beta + \Delta}{\Delta}.$$

Suppose $\Delta > 0$. Then $k > 0$. Since k is an integer, we have $k \geq 1$. Therefore, we have

$$d^2 \geq \frac{1 + 2\beta + \Delta}{\Delta} > \frac{2\beta - 1 + |\Delta|}{|\Delta|}.$$

This proves (5) for $\Delta > 0$.

Suppose $\Delta < 0$. Then $k < 0$. In view of (7), we have $\Delta(1-d^2) \equiv 0 \pmod{k}$. So $|k| \leq |\Delta|(d^2-1)$. Therefore, we have $1 \leq |k| \leq |\Delta|(d^2-1)$. Also from (7), we have

$$\beta = \frac{-k^2 + \Delta(d^2-1)}{2k} = \frac{1}{2}\left(\frac{|k|^2 + |\Delta|(d^2-1)}{|k|}\right) = \frac{G(|k|)}{2}$$

where

$$G(x) := \frac{x^2 + |\Delta|(d^2-1)}{x} = x + \frac{|\Delta|(d^2-1)}{x}, \quad 1 \leq x \leq |\Delta|(d^2-1).$$

Since $G'(x) = 1 - \frac{|\Delta|(d^2-1)}{x^2}$ and $G''(x) = \frac{2|\Delta|(d^2-1)}{x^3} > 0$, so $G(x)$ is concave up on the interval $[1, |\Delta|(d^2-1)]$. Therefore,

$$G(|k|) \leq \max\{G(1), G(|\Delta|(d^2-1))\} = 1 + |\Delta|(d^2-1).$$

This implies that

$$\beta = \frac{G(|k|)}{2} \leq \frac{1+|\Delta|(d^2-1)}{2}.$$

Therefore,

$$\frac{2\beta - 1 + |\Delta|}{|\Delta|} \leq d^2.$$

This proves (5) for $\Delta < 0$. □

The following theorem gives an explicit lower bound, which tends to $+\infty$ when a tends to $+\infty$, for $f(c)/f(a)$ if $f(a)|f(b)|f(c)$ and $1 < a < b < c$.

Theorem 5. *Let $f(x) = Ax^2+Bx+C$ such that $A \neq 0$ and $\Delta \neq 0$. If $f(a)|f(b)|f(c)$ with $1 < a < b < c$, then*

$$\frac{f(c)}{f(a)} \gg \frac{(\log c)^{1/3}}{(\log\log c)^{5/3}}.$$

where the implicit positive constant depends only on A, B and C.

Proof. If $f(a)|f(b)|f(c)$ with $1 < a < b < c$, we write

$$f(c) = df(a) \text{ and } f(c) = ef(b)$$

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.

If $e_1 = 1$, then $f(c) = e_2^2 f(b)$. From Theorem 4, we have

$$\frac{f(c)}{f(a)} = \frac{f(c)}{f(b)}\frac{f(b)}{f(a)} \geq \frac{f(c)}{f(b)} = e_2^2 \geq \frac{2|2Ac+B| - 1 + |\Delta|}{|\Delta|} \gg c \gg \frac{(\log c)^{1/3}}{(\log\log c)^{5/3}}$$

where the implicit positive constant depends only on A, B and C. Similarly, if $d_1 = 1$, then $f(c) = d_2^2 f(a)$. By Theorem 4, we have

$$\frac{f(c)}{f(a)} = d_2^2 \gg c \gg \frac{(\log c)^{1/3}}{(\log\log c)^{5/3}}$$

where the implicit positive constant depends only on A, B and C.

We now assume that $d_1 \neq 1$ and $e_1 \neq 1$. As in (6), $f(c) = d_1 d_2^2 f(a)$ implies

$$(2Ac+B)^2 - d_1(d_2(2Aa+B))^2 = \Delta\left(1 - d_1 d_2^2\right).$$

Similarly, $f(c) = e_1 e_2^2 f(b)$ implies

$$(2Ac+B)^2 - e_1(e_2(2Ab+B))^2 = \Delta\left(1 - e_1 e_2^2\right).$$

Hence, we have a pair of simultaneous Pell's equations

$$\begin{cases} x^2 - d_1 y^2 = \Delta\,(1-d) \\ x^2 - e_1 z^2 = \Delta\,(1-e) \end{cases}$$

with positive integer solutions $x = |2Ac+B|, y = d_2|2Aa+B|$ and $z = e_2|2Ab+B|$. Now, since $e < d$,

$$\Delta\,(1-e) \neq \Delta\,(1-d)\,,$$

so the requirements of Theorem 6 in [6] (also see Proposition 3 in [9]) are satisfied. Applying Theorem 6 in [6] , we obtain

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

for some constants $A', K' > 0$ depending only on A, B and C . After some algebra, we have

$$\frac{f(c)}{f(a)} = d \gg \frac{(\log c)^{1/3}}{(\log\log c)^{5/3}}$$

where the implicit positive constant depends only on A, B and C. This proves Theorem 5. $\square$

Corollary 1. *All quadratic polynomials $f(x) = Ax^2+Bx+C$ or powers of quadratic polynomials $f(x) = D(Ax^2 + Bx + C)^n$ such that $A, D \neq 0$ and $\Delta = B^2 - 4AC \neq 0$ satisfy the gap principle of order* 2.

Proof. If $f(x) = Ax^2+Bx+C$, then the result follows readily from the last theorem and Definition 1. If $f(x) = D(Ax^2 + Bx + C)^n$, then $f(a) \mid f(b)$ if and only if $(Aa^2 + Ba + C) \mid (Ab^2 + Bb + C)$. Hence the result also follows from Theorem 5. $\square$

Lemma 3. *All quadratic polynomials $f(x) = Ax^2+Bx+C$ or powers of quadratic polynomials $f(x) = D(Ax^2 + Bx + C)^n$ such that $A, D \neq 0$ and $B^2 - 4AC \neq 0$ do not satisfy the gap principle of order* 1.

Proof. Without loss of generality, we assume $A > 0$. We first show that there are $a, b \in \mathbb{N}^2$ and a non-square integer $k > 1$ such that $f(b) = kf(a)$. In fact, for any positive integer $a > \frac{|B|}{2A} + \frac{|\Delta|}{4A}$, let $b = a + f(a)$. Then

$$f(a) = A\left(a + \frac{B}{2A}\right)^2 - \frac{B^2 - 4AC}{4A} = \frac{(Aa + B/2)^2}{A} - \frac{\Delta}{4A} > \frac{\Delta}{4A} - \frac{\Delta}{4A} = 0$$

because $Aa + B/2 \geq Aa - |B|/2 > |\Delta|/4 > 0$. So $b > a > 1$. Also we have

$$\begin{aligned}
k &= \frac{f(b)}{f(a)} = \frac{f(a + f(a))}{f(a)} \\
&= \frac{A(a + f(a))^2 + B(a + f(a)) + C}{f(a)} \\
&= \frac{Aa^2 + 2Aaf(a) + Af(a)^2 + Ba + Bf(a) + C}{f(a)} \\
&= \frac{f(a) + 2Aaf(a) + Af(a)^2 + Bf(a)}{f(a)} \\
&= 1 + 2Aa + B + Af(a) \\
&= 1 + 2Aa + B + A^2a^2 + BAa + AC \\
&= \left(Aa + \frac{B}{2} + 1\right)^2 - \frac{B^2 - 4AC}{4} \\
&= \left(Aa + \frac{B}{2} + 1\right)^2 - \frac{\Delta}{4}.
\end{aligned}$$

If $\Delta > 0$, then we claim that $(Aa + B/2 + 1/2)^2 < k < (Aa + B/2 + 1)^2$ and hence k cannot be the square of an integer. Indeed, $k = (Aa+B/2+1)^2 - |\Delta|/4 < (Aa + B/2 + 1)^2$ and

$$k = (Aa+B/2+1)^2 - |\Delta|/4 > (Aa+B/2+1)^2 - (Aa+B/2) > (aA+B/2+1/2)^2$$

because $Aa + B/2 > |\Delta|/4$.

If $\Delta < 0$, then $k = (Aa + B/2 + 1)^2 + |\Delta|/4 > (Aa + B/2 + 1)^2$ and $k = (Aa+B/2+1)^2+|\Delta|/4 < (Aa+B/2+1)^2+(Aa+B/2) < (aA+B/2+3/2)^2$ because $Aa + B/2 > |\Delta|/4$. So $(Aa + B/2 + 1)^2 < k < (aA + B/2 + 3/2)^2$ and hence k again cannot be the square of an integer.

We now fix a, b and k as above such that $f(b) = kf(a)$ with $1 < a < b$ and non-square $k > 1$. Consider the generalized Pell's equation

$$Y^2 = kX^2 - (k - 1)\Delta. \tag{8}$$

If $f(b) = kf(a)$, then we have $\frac{(2Ab+B)^2}{4} - \frac{\Delta}{4} = k\left(\frac{(2Aa+B)^2}{4} - \frac{\Delta}{4}\right)$ and hence

$$(2Ab + B)^2 - \Delta = k\,(2Aa + B)^2 - k\Delta.$$

Therefore, the equation (8) has solution $(X, Y) = (2Aa + B, 2Ab + B) \in \mathbb{N}^2$. It is well-known that for non-square positive integer k, there are infinitely many solutions $(s, t) \in \mathbb{N}^2$ of the Pell's equation

$$s^2 - kt^2 = 1 \tag{9}$$

with $1 \le t < s$. For any such solution $(s, t) \in \mathbb{N}^2$, $Y + \sqrt{k}X = ((2Ab + B) + \sqrt{k}(2Aa + B))(s + \sqrt{k}t)$ gives a solution (X, Y) of (8). In fact, we have

$$X = s(2Aa + B) + t(2Ab + B) = 2A(sa + tb) + (s + t)B$$

and

$$Y = s(2Ab + B) + kt(2Aa + B) = 2A(sb + kta) + (s + kt)B.$$

So $Y > X > B$ and

$$\begin{aligned}
Y^2 - kX^2 &= (s(2Ab + B) + kt(2Aa + B))^2 - k\,(s(2Aa + B) + t(2Ab + B))^2 \\
&= s^2(2Ab + B)^2 - kt^2(2Ab + B)^2 + k^2t^2(2Aa + B)^2 - ks^2(2Aa + B)^2 \\
&= (s^2 - kt^2)((2Ab + B)^2 - k(2Aa + B)^2) \\
&= -(k - 1)\Delta.
\end{aligned}$$

Hence,

$$\begin{aligned}
(x, y) &:= \left(\frac{X - B}{2A}, \frac{Y - B}{2A}\right) \\
&= \left(sa + tb + \frac{(s + t - 1)B}{2A}, sb + kta + \frac{(s + kt - 1)B}{2A}\right)
\end{aligned} \tag{10}$$

are solutions of $f(y) = kf(x)$. We claim that there are infinitely many solutions $(s, t) \in \mathbb{N}^2$ of (9) satisfying

$$s + t \equiv 1 \pmod{2A} \quad \text{and} \quad s + kt \equiv 1 \pmod{2A}. \tag{11}$$

Indeed, from the theory of Pell's equation, we know that if $(s_0, t_0) \in \mathbb{N}^2$ is the (fundamental) solution of (9) with the least value of $s_0 + t_0\sqrt{k}$, then the solutions $(s, t) \in \mathbb{Z}^2$ of (9) are precisely $s + t\sqrt{k} = (s_0 + t_0\sqrt{k})^\ell$ for all $\ell \in \mathbb{Z}$. Since

$$(s_1 + t_1\sqrt{k})(s_2 + t_2\sqrt{k}) = (s_1s_2 + t_1t_2k) + (s_1t_2 + s_2t_1)\sqrt{k},$$

we consider the cyclic group

$$G := \left\{(s, t) \in \mathbb{Z}^2 : s^2 - kt^2 = 1\right\} \cup \{(1, 0)\} =< (s_0, t_0) >$$

with the multiplication

$$(s_1, t_1) * (s_2, t_2) := (s_1s_2 + t_1t_2k, s_1t_2 + s_2t_1)$$

with the unity $(1,0)$. For any integer $m>1$, we let $\phi_m:\mathbb{Z}\to\mathbb{Z}/m\mathbb{Z}$ be the reduction map with $\phi_m(n)=\bar{n}$ for any integer n where $n\equiv\bar{n}\pmod{m}$ and $0\le\bar{n}\le m-1$. This map ϕ_m induces a group homomorphism from G to $(\mathbb{Z}/m\mathbb{Z})\times(\mathbb{Z}/m\mathbb{Z})$ by mapping $\phi_m(s,t)=(\bar{s},\bar{t})$. It then follows that the image of G under ϕ_m is a finite group. We denote by $g_k(m)$ the order of the image of G under ϕ_m. For further discussion on the value of $g_k(m)$, we refer to [2] and [7]. Hence, for any solution $(s,t)\in\mathbb{N}^2$ of (9), we have

$$\left(\phi_{2|A|}(s,t)\right)^{\ell g_k(2|A|)}=(\bar{1},\bar{0})$$

for any integer $\ell\ge 1$, or in other words, if $(s,t)\in\mathbb{N}^2$ of (9) are defined by

$$s+t\sqrt{k}=(s_0+t_0\sqrt{k})^{\ell g_k(2|A|)}$$

then $s\equiv 1\pmod{2|A|}$ and $t\equiv 0\pmod{2|A|}$ and hence condition (11) is satisfied. Therefore, there are infinitely many solutions $(s,t)\in\mathbb{N}^2$ of (9) satisfying (11) and this proves the claim. According to (10), these (s,t) give infinitely many solutions $(x,y)\in\mathbb{N}^2$ of $f(y)=kf(x)$ with $1<x<y$.

Since

$$\frac{|Y|}{|X|}=\frac{|2Ay+B|}{|2Ax+B|}=\left|\frac{y/x+B/(2Ax)}{1+B/(2Ax)}\right|\ge\frac{|y/x+B/(2Ax)|}{1+|B/(2Ax)|}\ge\frac{|y/x|-|B|/(2A)}{1+|B|/(2A)}$$

and

$$\frac{|Y^2|}{|X^2|}=\left|k-\frac{(k-1)\Delta}{X^2}\right|\le k+(k-1)|\Delta|,$$

so

$$1<y/x\le|B|/(2A)+(1+|B|/(2A))\sqrt{k+(k-1)|\Delta|}:=N.$$

Therefore, these infinitely many solutions $(x,y)\in\mathbb{N}^2$ of $f(y)=kf(x)$ belong to $S_N(f)$ in Lemma 1 and hence $S_N(f)$ is infinite and so $f(x)$ does not satisfy the gap principle of order 1.

Since $S_N(f)=S_N(f^n)$, so the case for the powers of quadratic polynomials follows from the case of quadratic polynomials and Lemma 1. $\square$

Theorem 2 readily follows from Corollary 1 and Lemma 3.

References

[1] Y. Bilu and R. Tichy, *The Diophantine equation $f(x)=g(y)$*, Acta Arith. **95** (2000), 261–288.

[2] J. Chahal and N. Priddis, *Some congruence properties of the Pell equation,* Ann. Sci. Math. Québec **35** (2011), no. 2, 175–184.

[3] T. H. Chan, *Factors of a perfect square,* Acta Arith. **163** (2014) no. 2, 141-143.

[4] T. H. Chan, *Common factors among pairs of consecutive integers,* Int. J. Number Theory **14** (2018), no.3, 871–880.

[5] T. H. Chan, *Gaps between divisible terms in $a^2(a^2+1)$,* Bulletin of the Australian Mathematical Society, **101** issue 3 (2020) , 396–400.

[6] T. H. Chan, S. Choi and P. C. Lam, *Divisibility on the sequence of perfect squares minus one: The gap principle*, Journal of Number Theory, **184** (2018), 473–484.

[7] S. Choi and D. Tarnu, *On the Quadratic Diophantine Equations in two variables,* (2020), to appear.

[8] P. Erdős and M. Rosenfeld, *The factor-difference set of integers,* Acta Arith. **79** (1997) no. 4, 353–359.

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

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, British Columbia V5A 1S6, Canada
E-mail address: schoia@sfu.ca

E-mail address: choholam@gmail.com

Department of Mathematics, Simon Fraser University, 8888 University Drive, Burnaby, British Columbia V5A 1S6, Canada
E-mail address: daniel_tarnu@sfu.ca