Bull. Aust. Math. Soc. **86** (2012), 389–404
doi:10.1017/S0004972712000202

THE LEAST COMMON MULTIPLE OF CONSECUTIVE TERMS IN A QUADRATIC PROGRESSION

GUOYOU QIAN, QIANRONG TAN and SHAOFANG HONG ✉

(Received 23 October 2011)

Abstract

Let k be any given positive integer. We define the arithmetic function g_k for any positive integer n by

$$g_k(n) := \frac{\prod_{i=0}^{k}((n+i)^2+1)}{\mathrm{lcm}_{0\le i\le k}\{(n+i)^2+1\}}.$$

We first show that g_k is periodic. Subsequently, we provide a detailed local analysis of the periodic function g_k, and determine its smallest period. We also obtain an asymptotic formula for $\log \mathrm{lcm}_{0\le i\le k}\{(n+i)^2+1\}$.

2010 *Mathematics subject classification*: primary 11B25; secondary 11N13, 11A05.

Keywords and phrases: quadratic progression, least common multiple, p-adic valuation, arithmetic function, smallest period.

1. Introduction and the main result

There are many beautiful and important theorems about arithmetic progressions in number theory, the two most famous examples being Dirichlet's theorem [12] and the Green–Tao theorem [6]. See [2, 15] for some other results. However, there are few renowned theorems but more conjectures about quadratic progressions, among which the sequence $\{n^2+1\}_{n\in\mathbb{N}}$ is best known. A famous conjecture [8] states that there are infinitely many primes of the form n^2+1. This seems to be extremely difficult to prove in the present state of knowledge. The best result is due to Iwaniec [13], who showed that there exist infinitely many integers n such that n^2+1 has at most two prime factors.

To investigate the arithmetic properties of a given sequence, studying the least common multiple of its consecutive terms seems quite natural. The least common multiple of consecutive integers was investigated by Chebyshev in the first significant

S. Hong was supported partially by National Science Foundation of China Grant #10971145 and by the PhD Programs Foundation of Ministry of Education of China Grant #20100181110073.

attempt to prove the prime number theorem in [3]. Since then, the topic of least common multiple of any given sequence of positive integers has become popular. Hanson [7] and Nair [14] respectively obtained the upper bound and lower bound of $\mathrm{lcm}_{1\le i\le n}\{i\}$. Bateman *et al.* [1] obtained an asymptotic estimate for the least common multiple of arithmetic progressions. Recently, Hong *et al.* [10] obtained an asymptotic estimate for the least common multiple of a sequence of products of linear polynomials.

In [4], Farhi investigated the least common multiple $\mathrm{lcm}_{0\le i\le k}\{n+i\}$ of finitely many consecutive integers by introducing the arithmetic function

$$\bar{g}_k(n) := \frac{\prod_{i=0}^{k}(n+i)}{\mathrm{lcm}_{0\le i\le k}\{n+i\}},$$

and also proved some arithmetic properties of $\mathrm{lcm}_{0\le i\le k}\{n+i\}$. Farhi showed that $\bar{g}_k$ is periodic and $k!$ is a period of it. Let $\bar{P}_k$ be the smallest period of $\bar{g}_k$. Then $\bar{P}_k \mid k!$. But Farhi did not determine the exact value of $\bar{P}_k$ in [4], so he posed the open problem of determining the smallest period $\bar{P}_k$. Hong and Yang [11] improved the period $k!$ to $\mathrm{lcm}_{1\le i\le k}\{i\}$ by showing that $\bar{g}_k(1) \mid \bar{g}_k(n)$ for any positive integer n. Moreover, they conjectured that $\mathrm{lcm}_{1\le i\le k+1}\{i\}/(k+1)$ divides $\bar{P}_k$ for all nonnegative integers k. Farhi and Kane [5] confirmed the Hong–Yang conjecture and determined the exact value of $\bar{P}_k$. Note that Farhi [4] also obtained the following nontrivial lower bound: $\mathrm{lcm}_{1\le i\le n}\{i^2+1\} \ge 0.32\cdot(1.442)^n$ (for all $n\ge 1$).

Let $\mathbb{Q}$ and $\mathbb{N}$ denote the field of rational numbers and the set of nonnegative integers. Define $\mathbb{N}^* := \mathbb{N}\setminus\{0\}$. Let $k, b\in\mathbb{N}$ and $a\in\mathbb{N}^*$. Recently, Hong and Qian [9] studied the least common multiple of finitely many consecutive terms in arithmetic progressions. Actually, they defined the arithmetic function $g_{k,a,b} : \mathbb{N}^* \longrightarrow \mathbb{N}^*$ by

$$g_{k,a,b}(n) = \frac{\prod_{i=0}^{k}(b+(n+i)a)}{\mathrm{lcm}_{0\le i\le k}\{b+(n+i)a\}}.$$

They proved that $g_{k,a,b}$ is periodic and determined the exact value of the smallest period of $g_{k,a,b}$.

In this paper, we are concerned with the least common multiple of consecutive terms in the quadratic sequence $\{n^2+1\}_{n\in\mathbb{N}}$. Let k be a positive integer. We define the arithmetic function g_k for any positive integer n by

$$g_k(n) := \frac{\prod_{i=0}^{k}((n+i)^2+1)}{\mathrm{lcm}_{0\le i\le k}\{(n+i)^2+1\}}.$$

One may naturally ask the following question: Is g_k periodic and, if so, what is the smallest period of g_k?

Suppose that g_k is periodic. Then we let P_k denote its smallest period. Now we can use P_k to give a formula for $\mathrm{lcm}_{0\le i\le k}\{(n+i)^2+1\}$ as follows: for any positive integer n,

$$\mathrm{lcm}_{0\le i\le k}\{(n+i)^2+1\} = \frac{\prod_{i=0}^{k}((n+i)^2+1)}{g_k(\langle n\rangle_{P_k})},$$

where $\langle n\rangle_{P_k}$ means the least positive integer congruent to n modulo P_k. Therefore, it is important to determine the exact value of P_k.

As usual, for any prime number p, we let v_p be the normalised p-adic valuation of $\mathbb{Q}$, that is, $v_p(a) = b$ if $p^b \parallel a$. We also let $\gcd(a, b)$ denote the greatest common divisor of any integers a and b. For any real number x, we denote by $\lfloor x\rfloor$ the largest integer no greater than x. For any positive integer k, we define

$$R_k := \mathrm{lcm}_{1\le i\le k}\{i(i^2+4)\}$$

and

$$Q_k := 2^{((-1)^k+1)/2}\cdot \frac{R_k}{2^{v_2(R_k)}\prod_{p\equiv 3 \pmod 4} p^{v_p(R_k)}}.$$

Evidently, $v_p(Q_k) = v_p(R_k)$ for any prime $p \equiv 1 \pmod 4$. We can now state the main result of this paper.

THEOREM 1.1. *Let k be a positive integer. Then the arithmetic function g_k is periodic, and its smallest period equals Q_k except that $v_p(k+1) \ge v_p(Q_k) \ge 1$ for at most one prime $p \equiv 1 \pmod 4$, in which case its smallest period is equal to $Q_k/p^{v_p(Q_k)}$.*

In Section 2, we first show that the arithmetic function g_k is periodic with R_k as a period of it by a well-known result of Hua. Then, with a little more effort, we show that Q_k is a period of g_k (see Theorem 2.5). Subsequently, in Section 3, we develop further p-adic analysis of the periodic function g_k, and determine the smallest period of g_k. In the final section, we give the proof of Theorem 1.1 and then provide an asymptotic formula for $\log \mathrm{lcm}_{0\le i\le k}\{(n+i)^2+1\}$.

2. Q_k is a period of g_k

In this section, we first prove that g_k is periodic by a theorem of Hua in [12]. We also arrive at a nontrivial period of g_k.

LEMMA 2.1. *The arithmetic function g_k is periodic, and R_k is a period of g_k.*

PROOF. For any positive integer n, using [12, Theorem 7.3] (see [12, p. 11]), we obtain that

$$g_k(n) = \prod_{r=1}^{k}\prod_{0\le i_0<\cdots<i_r\le k}(\gcd((n+i_0)^2+1,\ldots,(n+i_r)^2+1))^{(-1)^{r-1}}$$

and

$$g_k(n+R_k) = \prod_{r=1}^{k}\prod_{0\le i_0<\cdots<i_r\le k}(\gcd((n+R_k+i_0)^2+1,\ldots,(n+R_k+i_r)^2+1))^{(-1)^{r-1}}.$$

We claim that $g_k(n+R_k) = g_k(n)$. To show this claim, it suffices to prove that

$$\gcd((n+R_k+i)^2+1, (n+R_k+j)^2+1) = \gcd((n+i)^2+1, (n+j)^2+1)$$

https://doi.org/10.1017/S0004972712000202 Published online by Cambridge University Press

for any $0 \le i < j \le k$. Evidently

$$(2n + 3j - i)((n + i)^2 + 1) + (-2n + j - 3i)((n + j)^2 + 1) = (j - i)((j - i)^2 + 4).$$

Hence

$$\gcd((n + i)^2 + 1, (n + j)^2 + 1) \mid (j - i)((j - i)^2 + 4).$$

But $(j - i)((j - i)^2 + 4) \mid R_k$. So

$$\gcd((n + i)^2 + 1, (n + j)^2 + 1) \mid R_k. \tag{2.1}$$

We then derive that

$$\gcd((n + i)^2 + 1, (n + j)^2 + 1) \mid (n + i \pm R_k)^2 + 1$$

and

$$\gcd((n + i)^2 + 1, (n + j)^2 + 1) \mid (n + j \pm R_k)^2 + 1.$$

It follows that

$$\gcd((n + i)^2 + 1, (n + j)^2 + 1) \mid \gcd((n + R_k + i)^2 + 1, (n + R_k + j)^2 + 1)$$

and

$$\gcd((n + i)^2 + 1, (n + j)^2 + 1) \mid \gcd((n - R_k + i)^2 + 1, (n - R_k + j)^2 + 1). \tag{2.2}$$

Replacing n by $n + R_k$ in (2.2),

$$\gcd((n + R_k + i)^2 + 1, (n + R_k + j)^2 + 1) \mid \gcd((n + i)^2 + 1, (n + j)^2 + 1).$$

Therefore

$$\gcd((n + i)^2 + 1, (n + j)^2 + 1) = \gcd((n + i + R_k)^2 + 1, (n + j + R_k)^2 + 1)$$

for any positive integer n and any integers i, j with $0 \le i < j \le k$. The claim is proved. Thus g_k is periodic with R_k as its period. □

For any given prime p, define the arithmetic function $g_{p,k}$ for any positive integer n by $g_{p,k}(n) := v_p(g_k(n))$. Since g_k is a periodic function, $g_{p,k}$ is periodic for each prime p and P_k is a period of $g_{p,k}$. Let $P_{p,k}$ be the smallest period of $g_{p,k}$. Then we have the following result.

Lemma 2.2. *For any prime p, $P_{p,k}$ divides $p^{v_p(R_k)}$. Further,*

$$P_k = \prod_{p \mid R_k} P_{p,k}.$$

https://doi.org/10.1017/S0004972712000202 Published online by Cambridge University Press

Proof. First, we show that $p^{v_p(R_k)}$ is a period of $g_{p,k}$ for each prime p. For this purpose, it is sufficient to prove that

$$\begin{aligned} &v_p(\gcd((n+i+p^{v_p(R_k)})^2+1,(n+j+p^{v_p(R_k)})^2+1)) \\ &\quad = v_p(\gcd((n+i)^2+1,(n+j)^2+1)) \end{aligned} \tag{2.3}$$

for any given positive integer n and any two integers i, j with $0 \le i < j \le k$.

By (2.1), we obtain $v_p(\gcd((n+i)^2+1,(n+j)^2+1)) \le v_p(R_k)$. Hence

$$v_p((n+i)^2+1) \le v_p(R_k) \quad \text{or} \quad v_p((n+j)^2+1) \le v_p(R_k).$$

Therefore

$$v_p((n+i)^2+1) \le v_p((n+i \pm p^{v_p(R_k)})^2+1)$$

or

$$v_p((n+j)^2+1) \le v_p((n+j \pm p^{v_p(R_k)})^2+1).$$

So we obtain that

$$\begin{aligned} &v_p(\gcd((n+i)^2+1,(n+j)^2+1)) \\ &\quad = \min\{v_p((n+i)^2+1), v_p((n+j)^2+1)\} \\ &\quad \le \min\{v_p((n+i+p^{v_p(R_k)})^2+1), v_p((n+j+p^{v_p(R_k)})^2+1)\} \\ &\quad = v_p(\gcd((n+i+p^{v_p(R_k)})^2+1,(n+j+p^{v_p(R_k)})^2+1)) \end{aligned}$$

and

$$\begin{aligned} &v_p(\gcd((n+i)^2+1,(n+j)^2+1)) \\ &\quad \le v_p(\gcd((n+i-p^{v_p(R_k)})^2+1,(n+j-p^{v_p(R_k)})^2+1)). \end{aligned} \tag{2.4}$$

Replacing n by $n+p^{v_p(R_k)}$ in (2.4) gives us that

$$\begin{aligned} &v_p(\gcd((n+i+p^{v_p(R_k)})^2+1,(n+j+p^{v_p(R_k)})^2+1)) \\ &\quad \le v_p(\gcd((n+i)^2+1,(n+j)^2+1)). \end{aligned}$$

Therefore (2.3) is proved. It then follows that for any given prime p, we have $g_{p,k}(n) = g_{p,k}(n+p^{v_p(R_k)})$ for any positive integer n. That is, $p^{v_p(R_k)}$ is a period of $g_{p,k}$. Thus $P_{p,k} \mid p^{v_p(R_k)}$. This implies that $P_{p,k}$ are relatively prime for different prime numbers p and $P_{p,k} = 1$ for those primes $p \nmid R_k$. Hence $\prod_{\text{prime } q \mid R_k} P_{q,k} \mid P_k$ since $P_{q,k} \mid P_k$ for each prime q. Moreover, since $v_p(g_k(n + \prod_{\text{prime } q \mid R_k} P_{q,k})) = v_p(g_k(n))$ for each prime p and any positive integer n, it follows that $\prod_{p \mid R_k} P_{p,k}$ is a period of g_k, which implies that $P_k \mid \prod_{p \mid R_k} P_{p,k}$. Hence $P_k = \prod_{p \mid R_k} P_{p,k}$ as required. □

To determine the smallest period P_k of g_k, by Lemma 2.2 it is enough to determine the value of $P_{p,k}$ for all prime factors p of R_k. In the following, we treat some special cases, and show that Q_k is a period of g_k.

https://doi.org/10.1017/S0004972712000202 Published online by Cambridge University Press

Lemma 2.3. *We have* $P_{2,k} = 2^{((-1)^k+1)/2}$.

Proof. Clearly, for any even integer n, $v_2(n^2 + 1) = 0$. For any odd integer n, letting $n = 2m + 1$ gives us that

$$v_2(n^2 + 1) = v_2((2m + 1)^2 + 1) = v_2(4m(m + 1) + 2) = 1.$$

If $2 \nmid k$, then by direct computation, $v_2(g_k(n)) = (k - 1)/2$ for any positive integer n. Thus $P_{2,k} = 1$ if $2 \nmid k$.

If $2 \mid k$, then by direct computation,

$$v_2(g_k(n)) = \begin{cases} \dfrac{k}{2} & \text{if } n \text{ is odd,} \\ \dfrac{k}{2} - 1 & \text{if } n \text{ is even.} \end{cases}$$

That is, $v_2(g_k(n + 2)) = v_2(g_k(n))$ and $v_2(g_k(n + 1)) \neq v_2(g_k(n))$ for every positive integer n. Thus $P_{2,k} = 2$ if $2 \mid k$. So Lemma 2.3 is proved. □

Lemma 2.4. *If* $p \equiv 3 \pmod 4$, *then* $P_{p,k} = 1$.

Proof. It is a well-known fact that for any positive integer n, $n^2 + 1$ has no prime factor p of the form $p \equiv 3 \pmod 4$ (see, for example, [12]). Thus for any prime $p \equiv 3 \pmod 4$, we have $v_p(n^2 + 1) = 0$. It then follows that $g_{p,k}(n) = v_p(g_k(n)) = 0$. So $P_{p,k} = 1$ as desired. □

From the above three lemmas, we get the following result.

Theorem 2.5. *Let k be a positive integer. Then Q_k is a period of g_k.*

Proof. By Lemmas 2.2–2.4,

$$P_k = P_{2,k}\Big(\prod_{\substack{p\equiv 3 \pmod 4\\ p\mid R_k}} P_{p,k}\Big)\Big(\prod_{\substack{p\equiv 1 \pmod 4\\ p\mid R_k}} P_{p,k}\Big) = 2^{((-1)^k+1)/2} \prod_{\substack{p\equiv 1 \pmod 4\\ p\mid R_k}} P_{p,k}. \tag{2.5}$$

Since $P_{p,k}$ is a power of p for each prime p,

$$\prod_{p\mid R_k,\, p\equiv 1 \pmod 4} P_{p,k} \,\Big|\, \frac{R_k}{2^{v_2(R_k)} \prod_{p\equiv 3 \pmod 4} p^{v_p(R_k)}}.$$

Thus $P_k \mid Q_k$ and Q_k is a period of g_k. This completes the proof of Theorem 2.5. □

3. The case $p \equiv 1 \pmod 4$

By Theorem 2.5, Q_k is a period of g_k. In order to determine its smallest period, we need to develop more detailed p-adic analysis to treat the remaining case $p \equiv 1 \pmod 4$. Let

$$S_k(n) := \{n^2 + 1, (n + 1)^2 + 1, \ldots, (n + k)^2 + 1\}$$

be the set of any $k + 1$ consecutive terms in the quadratic progression $\{m^2 + 1\}_{m\in\mathbb{N}}$.

In what follows, we only need to treat the remaining case that $p \mid R_k$ and $p \equiv 1 \pmod 4$ by Theorem 2.5. First, it is known that for any prime $p \equiv 1 \pmod 4$, $x^2 + 1 \equiv 0 \pmod p$ has exactly two solutions in a complete residue system modulo p. It then follows immediately from Hensel's lemma that for any positive integer e, the congruence $x^2 + 1 \equiv 0 \pmod{p^e}$ has exactly two solutions in a complete residue system modulo p^e. In other words, we have the following result.

Lemma 3.1. *Let e and m be any given positive integers. If $p \equiv 1 \pmod 4$, then there exist exactly two terms divisible by p^e in any p^e consecutive terms of the quadratic progression $\{(m+i)^2 + 1\}_{i \in \mathbb{N}}$.*

Similarly, for all primes p with $p \equiv 1 \pmod 4$, we have by Hensel's lemma that the congruence $x^2 + 4 \equiv 0 \pmod{p^e}$ has exactly two solutions in the interval $[1, p^e]$. For any positive integer e, we define

$$X_{p^e} := \text{the smallest positive root of } x^2 + 4 \equiv 0 \pmod{p^e}.$$

Since X_{p^e} is the smallest positive root of $x^2 + 4 \equiv 0 \pmod{p^e}$ for any positive integer e, we have that $X_{p^e} \le X_{p^{e+1}}$ and $X_{p^e} < X_{p^{e+r}}$ for some positive integer r. Moreover, we have the following result.

Lemma 3.2. *For any prime $p \equiv 1 \pmod 4$ and any positive integer n, if $X_{p^e} \le k < X_{p^{e+1}}$ for some positive integer e, then there is at most one element divisible by p^{e+1} in $S_k(n)$.*

Proof. Suppose that there exist integers $n_0 > 0$ and $0 \le i_1 \le k$, $0 \le i_2 \le k$ $(i_1 \ne i_2)$ such that $(n_0 + i_1)^2 + 1 \equiv 0 \pmod{p^{e+1}}$ and $(n_0 + i_2)^2 + 1 \equiv 0 \pmod{p^{e+1}}$. Then $2(n_0 + i_1)$ and $2(n_0 + i_2)$ are both the solutions of the congruences $x^2 + 4 \equiv 0 \pmod{p^{e+1}}$. Since $2(n_0 + i_1) \not\equiv 2(n_0 + i_2) \pmod{p^{e+1}}$ for $0 \le i_1 \ne i_2 \le k < X_{p^{e+1}} < p^{e+1}$, we can assume that

$$2(n_0 + i_1) \equiv X_{p^{e+1}} \pmod{p^{e+1}} \quad \text{and} \quad 2(n_0 + i_2) \equiv -X_{p^{e+1}} \pmod{p^{e+1}}.$$

Then

$$2(n_0 + i_1) - 2(n_0 + i_2) \equiv 2(i_1 - i_2) \equiv 2X_{p^{e+1}} \pmod{p^{e+1}},$$

which implies that $i_1 - i_2 \equiv X_{p^{e+1}} \pmod{p^{e+1}}$. That is, $X_{p^{e+1}} + i_2 - i_1 \equiv 0 \pmod{p^{e+1}}$.

On the other hand, from the fact that

$$0 < X_{p^{e+1}} - k \le X_{p^{e+1}} + i_2 - i_1 \le X_{p^{e+1}} + k < 2X_{p^{e+1}} \le 2 \cdot \frac{p^{e+1} - 1}{2} < p^{e+1},$$

we deduce that $X_{p^{e+1}} + i_2 - i_1 \not\equiv 0 \pmod{p^{e+1}}$. This is a contradiction. Thus we obtain the desired result. □

For simplicity, we write $l := v_p(R_k)$. For all primes $p \equiv 1 \pmod 4$, since $v_p(\gcd(i, i^2 + 4)) = v_p(\gcd(i, 4)) = 0$,

$$l = \max_{1 \le i \le k}\{v_p(i(i^2 + 4))\} = \max_{1 \le i \le k}\{v_p(i^2 + 4), v_p(i)\} = \max\Big\{\max_{1 \le i \le k}\{v_p(i^2 + 4)\}, \max_{1 \le i \le k}\{v_p(i)\}\Big\}.$$

https://doi.org/10.1017/S0004972712000202 Published online by Cambridge University Press

Note that the congruence $x^2 + 4 \equiv 0 \pmod{p^{\max_{1\le i\le k}\{v_p(i)\}}}$ has exactly two solutions in the interval $[1, p^{\max_{1\le i\le k}\{v_p(i)\}}]$. It follows that there is an integer $i_0 \in [1, k]$ such that $v_p(i_0^2 + 4) \ge \max_{1\le i\le k}\{v_p(i)\}$, which implies that $\max_{1\le i\le k}\{v_p(i^2 + 4)\} \ge \max_{1\le i\le k}\{v_p(i)\}$. Hence

$$l = \max_{1\le i\le k}\{v_p(i^2 + 4)\}. \tag{3.1}$$

Then $j^2 + 4 \equiv 0 \pmod{p^l}$ for some $1 \le j \le k$ and $i^2 + 4 \not\equiv 0 \pmod{p^{l+1}}$ for all $1 \le i \le k$. By the definition of X_{p^l}, we have $k \ge j \ge X_{p^l}$ and $v_p(X_{p^l}^2 + 4) \ge l$. Since $k \ge X_{p^l}$, by (3.1) we have $v_p(X_{p^l}^2 + 4) \le l$. So

$$l = v_p(X_{p^l}^2 + 4).$$

We claim that $k < X_{p^{l+1}}$. Otherwise, $v_p(X_{p^{l+1}}^2 + 4) \le l$ by (3.1), which is impossible since $v_p(X_{p^{l+1}}^2 + 4) \ge l + 1$. The claim is proved. Therefore

$$X_{p^l} \le k < X_{p^{l+1}}. \tag{3.2}$$

Now, by (3.2) and Lemma 3.2, there is at most one element divisible by p^{l+1} in $S_k(n)$ for any positive integer n. It is easy to see that

$$\begin{aligned} g_{p,k}(n) &= \sum_{m\in S_k(n)} v_p(m) - \max_{m\in S_k(n)}\{v_p(m)\} \\ &= \sum_{e\ge 1} |S_k^{(e)}(n)| - \sum_{e\ge 1}(1 \text{ if } p^e \mid m \text{ for some } m \in S_k(n)) \\ &= \sum_{e\ge 1} \max\{0, |S_k^{(e)}(n)| - 1\}, \end{aligned} \tag{3.3}$$

where

$$S_k^{(e)}(n) := \{m \in S_k(n) : p^e \mid m\}. \tag{3.4}$$

Based on the above discussion, all the terms on the right-hand side of (3.3) are 0 if $e \ge l + 1$. Therefore by (3.3),

$$g_{p,k}(n) = \sum_{e=1}^{l} f_e(n) = \sum_{e=1}^{l-1} f_e(n) + f_l(n), \tag{3.5}$$

where $f_e(n) := \max\{0, |S_k^{(e)}(n)| - 1\}$. Evidently,

$$f_e(n) = |S_k^{(e)}(n)| - 1 \quad \text{if } |S_k^{(e)}(n)| > 1,$$

and 0 if $|S_k^{(e)}(n)| \le 1$.

Lemma 3.3. *There is at most one prime $p \equiv 1 \pmod 4$ such that $p \mid R_k$ and $v_p(k + 1) \ge v_p(R_k)$.*

https://doi.org/10.1017/S0004972712000202 Published online by Cambridge University Press

PROOF. Suppose that there are two distinct primes p and q congruent to 1 modulo 4 such that $v_p(k+1) \geq v_p(R_k) \geq 1$ and $v_q(k+1) \geq v_q(R_k) \geq 1$. Then

$$k+1 \geq p^{v_p(R_k)} q^{v_q(R_k)} \geq \max\{pq, p^{v_p(L_k)} q^{v_q(L_k)}\},$$

where $L_k := \mathrm{lcm}_{1\leq i\leq k}\{i\}$.

If $v_p(L_k) = 0$ or $v_q(L_k) = 0$, then $k+1 = p$ or q, which is impossible since $k+1 \geq pq$.

If $v_p(L_k) \geq 1$ and $v_q(L_k) \geq 1$, then

$$k+1 \geq p^{v_p(L_k)} q^{v_q(L_k)} > \min\{p^{v_p(L_k)+1}, q^{v_q(L_k)+1}\},$$

which implies that $k \geq \min\{p^{v_p(L_k)+1}, q^{v_q(L_k)+1}\}$. This is in contradiction to

$$p^{v_p(L_k)+1} = p^{\lfloor \log_p k\rfloor+1} \geq k+1 \quad \text{and} \quad q^{v_q(L_k)+1} \geq k+1.$$

Thus there is at most one prime $p \equiv 1 \pmod 4$ such that $v_p(k+1) \geq v_p(R_k) \geq 1$. Lemma 3.3 is proved. □

Now by providing p-adic analysis of (3.5) in detail, we get the following result.

LEMMA 3.4. *Let p be a prime satisfying $p \mid R_k$ and $p \equiv 1 \pmod 4$. Then $P_{p,k} = p^{v_p(R_k)}$ except that $v_p(k+1) \geq v_p(R_k)$, in which case $P_{p,k} = 1$.*

PROOF. We begin with the proof for the case $v_p(k+1) \geq v_p(R_k) = l$. For any given positive integer n, the set $\{(n+1)^2+1, \ldots, (n+k)^2+1\}$ is the intersection of $S_k(n)$ and $S_k(n+1)$. The distinct terms of $S_k(n)$ and $S_k(n+1)$ are n^2+1 and $(n+k+1)^2+1$, respectively. Therefore, to compare the number of terms divisible by p^e in the two sets $S_k(n)$ and $S_k(n+1)$ for each $e \in \{1, \ldots, l\}$, it suffices to compare the two terms n^2+1 and $(n+k+1)^2+1$. Since $v_p(k+1) \geq l$,

$$n^2+1 \equiv (n+k+1)^2+1 \pmod{p^e}$$

for each $1 \leq e \leq l$. Thus, for any positive integer n and each $e \in \{1, \ldots, l\}$, we have $|S_k^{(e)}(n)| = |S_k^{(e)}(n+1)|$, where $S_k^{(e)}(n)$ is defined in (3.4). Hence we deduce by (3.5) that $f_e(n) = f_e(n+1)$ for each $e \in \{1, \ldots, l\}$. Thus $g_{p,k}(n) = g_{p,k}(n+1)$ for any positive integer n. That is, $P_{p,k} = 1$ if $v_p(k+1) \geq v_p(R_k)$. So Lemma 3.4 is true if $v_p(k+1) \geq v_p(R_k) = l$.

In what follows, we let $v_p(k+1) < v_p(R_k) = l$. Since $v_p(k+1) < l$, we can suppose that $k+1 \equiv r \pmod{p^l}$ for some $1 \leq r \leq p^l - 1$. By the definition of X_{p^l}, we have $X_{p^l} \leq (p^l-1)/2$, so there exists a positive integer $v_0 \in [1, (p+1)/2]$ such that $(v_0-1)p^{l-1} \leq X_{p^l} < v_0 p^{l-1}$. For any positive integer n, $(n+i+v_0p^{l-1})^2+1 \equiv (n+i)^2+1 \pmod{p^e}$ for all integers $i \in \{0, 1, \ldots, k\}$ and $1 \leq e \leq l-1$. So $|S_k^{(e)}(n)| = |S_k^{(e)}(n+v_0p^{l-1})|$ for all integers $1 \leq e \leq l-1$. It then follows that

$$\sum_{e=1}^{l-1} f_e(n+v_0p^{l-1}) = \sum_{e=1}^{l-1} f_e(n).$$

https://doi.org/10.1017/S0004972712000202 Published online by Cambridge University Press

By Lemma 2.2, p^l is a period of $g_{p,k}$. We claim that there is a positive integer n_0 such that $f_l(n_0 + v_0 p^{l-1}) \le f_l(n_0) - 1$. It then follows from (3.5) and the claim that p^{l-1} is not a period of $g_{p,k}$ and this concludes the proof of Lemma 3.4 for the case $v_p(k+1) < v_p(R_k) = l$. Our final task is to prove the claim.

First, we note the fact that we can always find a positive integer x_0 with $x_0^2 + 1 \equiv 0 \pmod{p^l}$ such that either $(x_0 + X_{p^l})^2 + 1 \equiv 0 \pmod{p^l}$ or $(x_0 - X_{p^l})^2 + 1 \equiv 0 \pmod{p^l}$. Actually, for any root y_{p^l} of the congruence $x^2 + 1 \equiv 0 \pmod{p^l}$, it is obvious that $X_{p^l} \equiv 2y_{p^l}$ or $-2y_{p^l} \pmod{p^l}$. So if we choose a positive integer x_0 such that $2x_0 \equiv -X_{p^l} \pmod{p^l}$, then $x_0^2 + 1 \equiv 0 \pmod{p^l}$ and $(x_0 + X_{p^l})^2 + 1 \equiv x_0^2 + 1 + X_{p^l}^2 - X_{p^l} \cdot X_{p^l} \equiv 0 \pmod{p^l}$. On the other hand, if we choose x_0 such that $2x_0 \equiv X_{p^l} \pmod{p^l}$, then $x_0^2 + 1 \equiv 0 \pmod{p^l}$ and $(x_0 - X_{p^l})^2 + 1 \equiv 0 \pmod{p^l}$. We now divide the proof of the claim into the following two cases.

Case 1. $k \le v_0 p^{l-1}$. By the above discussion, we can choose an integer n_0 satisfying $n_0^2 + 1 \equiv 0 \pmod{p^l}$ and $(n_0 + X_{p^l})^2 + 1 \equiv 0 \pmod{p^l}$. In order to prove the claim in this case, it is sufficient to compare the number of terms divisible by p^l in the following two sets:

$$S_k(n_0) = \{n_0^2 + 1, \dots, (n_0 + X_{p^l})^2 + 1, \dots, (n_0 + k)^2 + 1\}$$

and

$$S_k(n_0 + v_0 p^{l-1}) = \{(n_0 + v_0 p^{l-1})^2 + 1, \dots, (n_0 + k + v_0 p^{l-1})^2 + 1\}.$$

Since $S_k(n_0)$ consists of $k+1$ terms and $k + 1 < p^l$, there are by Lemma 3.1 exactly two terms divisible by p^l in the set $S_k(n_0)$: $n_0^2 + 1$ and $(n_0 + X_{p^l})^2 + 1$. Therefore $f_l(n_0) = 1$.

We now consider the set $S_k(n_0 + v_0 p^{l-1})$. By Lemma 3.1, we know that the terms divisible by p^l in the quadratic progression $\{(n_0 + i)^2 + 1\}_{i \in \mathbb{N}}$ must be of the form $(n_0 + t_1 p^l)^2 + 1$ or $(n_0 + X_{p^l} + t_2 p^l)^2 + 1$, where $t_1, t_2 \in \mathbb{N}$. If $v_0 \le (p-1)/2$, then

$$X_{p^l} < v_0 p^{l-1} \le v_0 p^{l-1} + j \le v_0 p^{l-1} + k \le 2v_0 p^{l-1} \le (p-1)p^{l-1} < p^l \quad \text{for all } 0 \le j \le k.$$

Hence there is no term of the form $(n_0 + t_1 p^l)^2 + 1$ or $(n_0 + X_{p^l} + t_2 p^l)^2 + 1$ in the set $S_k(n_0 + v_0 p^{l-1})$, where $t_1, t_2 \in \mathbb{N}$. That is, $|S_k^{(l)}(n_0 + v_0 p^{l-1})| = 0$. Thus $f_l(n_0 + v_0 p^{l-1}) = 0$ if $v_0 \le (p-1)/2$. If $v_0 = (p+1)/2$, then for all $0 \le j \le k$,

$$X_{p^l} < v_0 p^{l-1} \le v_0 p^{l-1} + j \le v_0 p^{l-1} + k \le 2v_0 p^{l-1} \le p^l + p^{l-1} < p^l + X_{p^l}$$

and

$$k + v_0 p^{l-1} \ge X_{p^l} + v_0 p^{l-1} \ge (2v_0 + 1)p^{l-1} = p^l.$$

Hence there is no term of the form $(n_0 + X_{p^l} + t_2 p^l)^2 + 1$ in the set $S_k(n_0 + v_0 p^{l-1})$ while the term $(n_0 + p^l)^2 + 1$ is the only term divisible by p^l in the set $S_k(n_0 + v_0 p^{l-1})$. So $|S_k^{(l)}(n_0 + v_0 p^{l-1})| = 1$ and $f_l(n_0 + v_0 p^{l-1}) = 0$ if $v_0 = (p+1)/2$. Thus $f_l(n_0 + v_0 p^{l-1}) \le f_l(n_0) - 1$ as desired. The proof of the claim in this case is concluded.

Case 2. $k > v_0 p^{l-1}$. As in the proof of case 1, to prove the claim in this case, we need to choose a suitable n_0 and compare the number of terms divisible by p^l in the following two sets:

$$S_k(n_0) = \{n_0^2 + 1, \ldots, (n_0 + v_0 p^{l-1} - 1)^2 + 1, (n_0 + v_0 p^{l-1})^2 + 1, \ldots, (n_0 + k)^2 + 1\}$$

and

$$S_k(n_0 + v_0 p^{l-1}) = \{(n_0 + v_0 p^{l-1})^2 + 1, \ldots, (n_0 + k)^2 + 1, \\ (n_0 + k + 1)^2 + 1, \ldots, (n_0 + k + v_0 p^{l-1})^2 + 1\}.$$

Evidently, $\{(n_0 + v_0 p^{l-1})^2 + 1, \ldots, (n_0 + k)^2 + 1\}$ is the intersection of $S_k(n_0)$ and $S_k(n_0 + v_0 p^{l-1})$. So to compare $|S_k^{(l)}(n_0)|$ with $|S_k^{(l)}(n_0 + v_0 p^{l-1})|$, it is enough to compare the number of terms divisible by p^l in the set

$$\{n_0^2 + 1, \ldots, (n_0 + v_0 p^{l-1} - 1)^2 + 1\}$$

with the number of terms divisible by p^l in the set

$$\{(n_0 + k + 1)^2 + 1, \ldots, (n_0 + k + v_0 p^{l-1})^2 + 1\}.$$

Consider the following three subcases.

Subcase 2.1. $1 \le r \le p^l - v_0 p^{l-1}$. In this case, we choose the same n_0 as in case 1. Since $k + 1 \equiv r \pmod{p^l}$ and $1 \le r \le p^l - v_0 p^{l-1}$, we have $k + j \equiv r + j - 1 \pmod{p^l}$ and $1 \le r + j - 1 \le p^l - 1$ for all $1 \le j \le v_0 p^{l-1}$. Hence there is no term of the form $(n_0 + t_1 p^l)^2 + 1$ and at most one term of the form $(n_0 + (X_{p^l} + t_2 p^l))^2 + 1$ in the set $\{(n_0 + k + 1)^2 + 1, \ldots, (n_0 + (k + v_0 p^{l-1}))^2 + 1\}$, where $t_1, t_2 \in \mathbb{N}$. On the other hand, by Lemma 3.1 the terms $n_0^2 + 1$ and $(n_0 + X_{p^l})^2 + 1$ are the only two terms divisible by p^l in the set $\{n_0^2 + 1, \ldots, (n_0 + v_0 p^{l-1} - 1)^2 + 1\}$. Consequently,

$$|S_k^{(l)}(n_0 + v_0 p^{l-1})| \le |S_k^{(l)}(n_0)| - 1.$$

Thus $f_l(n_0 + v_0 p^{l-1}) \le f_l(n_0) - 1$ as required.

Subcase 2.2. $p^l - v_0 p^{l-1} < r \le p^l - 1$ and $1 \le v_0 \le (p-1)/2$. We can choose a suitable n_0 such that

$$(n_0 + v_0 p^{l-1} - 1)^2 + 1 \equiv 0 \pmod{p^l}$$

and

$$(n_0 + v_0 p^{l-1} - 1 - X_{p^l})^2 + 1 \equiv 0 \pmod{p^l}.$$

By Lemma 3.1, the terms divisible by p^l in the quadratic progression $\{(n_0 + i)^2 + 1\}_{i \in \mathbb{N}}$ must be of the form $(n_0 + v_0 p^{l-1} - 1 + t_1 p^l)^2 + 1$ or $(n_0 + v_0 p^{l-1} - 1 - X_{p^l} + t_2 p^l)^2 + 1$, where $t_1, t_2 \in \mathbb{N}$. Since $k + 1 \equiv r \pmod{p^l}$ and $p^l - v_0 p^{l-1} \le r \le p^l - 1$ with $1 \le v_0 \le (p-1)/2$, we have $k + j \equiv r + j - 1 \pmod{p^l}$ and

$$v_0 p^{l-1} + 1 < \frac{p+1}{2} p^{l-1} + 1 \le p^l - v_0 p^{l-1} + 1 \le r + j - 1 \le p^l + v_0 p^{l-1} - 2$$

https://doi.org/10.1017/S0004972712000202 Published online by Cambridge University Press

for all $1 \le j \le v_0 p^{l-1}$. Hence there is no term of the form $(n_0 + v_0 p^{l-1} - 1 + t_1 p^l)^2 + 1$ and at most one term of the form $(n_0 + v_0 p^{l-1} - 1 - X_{p^l} + t_2 p^l)^2 + 1$ in the set $\{(n_0 + k + 1)^2 + 1, \ldots, (n_0 + k + v_0 p^{l-1})^2 + 1\}$, where $t_1, t_2 \in \mathbb{N}$. Furthermore, the two terms $(n_0 + v_0 p^{l-1} - 1)^2 + 1$ and $(n_0 + v_0 p^{l-1} - 1 - X_{p^l})^2 + 1$ are the only two terms divisible by p^l in the set $\{n_0^2 + 1, \ldots, (n_0 + v_0 p^{l-1} - 1)^2 + 1\}$. Therefore, $|S_k^{(l)}(n_0 + v_0 p^{l-1})| \le |S_k^{(l)}(n_0)| - 1$. That is, $f_l(n_0 + v_0 p^{l-1}) \le f_l(n_0) - 1$ as desired.

Subcase 2.3. $p^l - v_0 p^{l-1} < r \le p^l - 1$ and $v_0 = (p+1)/2$. Then $((p-1)/2)p^{l-1} < r \le p^l - 1$. We partition the proof of this case into the following three subcases.

Subcase 2.3.1. $((p-1)/2)p^{l-1} < r \le X_{p^l}$. In this case, we pick a suitable n_0 such that

$$\Big(n_0 + \frac{p^{l-1} - 1}{2}\Big)^2 + 1 \equiv 0 \pmod{p^l}$$

and

$$\Big(n_0 + \frac{p^{l-1} - 1}{2} + X_{p^l}\Big)^2 + 1 \equiv 0 \pmod{p^l}.$$

By Lemma 3.1, terms divisible by p^l in the quadratic progression $\{(n_0 + i)^2 + 1\}_{i \in \mathbb{N}}$ must be of the form $(n_0 + (p^{l-1} - 1)/2 + t_1 p^l)^2 + 1$ or $(n_0 + (p^{l-1} - 1)/2 + X_{p^l} + t_2 p^l)^2 + 1$, where $t_1, t_2 \in \mathbb{N}$. Since $k + 1 \equiv r \pmod{p^l}$ and $((p-1)/2)p^{l-1} < r \le X_{p^l}$, we have for all $1 \le j \le v_0 p^{l-1}$ that $k + j \equiv r + j - 1 \pmod{p^l}$ and

$$\begin{aligned}\frac{p^{l-1} - 1}{2} < \frac{p-1}{2} p^{l-1} < r + j - 1 \le X_{p^l} + v_0 p^{l-1} - 1 &\le \frac{p^l - 1}{2} + v_0 p^{l-1} - 1 \\ &= p^l + \frac{p^{l-1} - 1}{2} - 1.\end{aligned}$$

Hence there is no term of the form $(n_0 + (p^{l-1} - 1)/2 + t_1 p^l)^2 + 1$ and at most one term of the form $(n_0 + (p^{l-1} - 1)/2 + X_{p^l} + t_2 p^l)^2 + 1$ in the set

$$\{(n_0 + k + 1)^2 + 1, \ldots, (n_0 + k + v_0 p^{l-1})^2 + 1\},$$

where $t_1, t_2 \in \mathbb{N}$. On the other hand, since

$$\frac{p^{l-1} - 1}{2} + X_{p^l} \le \frac{p^{l-1} - 1}{2} + \frac{p^l - 1}{2} \le \frac{p+1}{2} p^{l-1} - 1 = v_0 p^{l-1} - 1,$$

the terms $(n_0 + (p^{l-1} - 1)/2)^2 + 1$ and $(n_0 + (p^{l-1} - 1)/2 + X_{p^l})^2 + 1$ are just the only two terms divisible by p^l in the set $\{n_0^2 + 1, \ldots, (n_0 + v_0 p^{l-1} - 1)^2 + 1\}$. Therefore,

$$|S_k^{(l)}(n_0 + v_0 p^{l-1})| \le |S_k^{(l)}(n_0)| - 1.$$

Thus $f_l(n_0 + v_0 p^{l-1}) \le f_l(n_0) - 1$ as required.

https://doi.org/10.1017/S0004972712000202 Published online by Cambridge University Press

Subcase 2.3.2. $X_{p^l} < r \le v_0 p^{l-1}$. We choose the same n_0 as in case 1. Since

$$k+1 \equiv r \pmod{p^l} \quad \text{and} \quad (v_0-1)p^{l-1} \le X_{p^l} < r \le v_0 p^{l-1},$$

we have $k+j \equiv r+j-1 \pmod{p^l}$ and

$$X_{p^l} < r+j-1 \le p^l + p^{l-1} - 1 < p^l + X_{p^l} \quad \text{for all } 1 \le j \le v_0 p^{l-1}.$$

Thus there is no term of the form $(n_0 + X_{p^l} + t_1 p^l)^2 + 1$ and at most one term of the form $(n_0 + t_2 p^l)^2 + 1$ in the set $\{(n_0+k+1)^2+1, \ldots, (n_0+k+v_0 p^{l-1})^2+1\}$, where $t_1, t_2 \in \mathbb{N}$. Therefore $|S_k^{(l)}(n_0 + v_0 p^{l-1})| \le |S_k^{(l)}(n_0)| - 1$. That is, $f_l(n_0 + v_0 p^{l-1}) \le f_l(n_0) - 1$ as desired.

Subcase 2.3.3. $v_0 p^{l-1} < r \le p^l - 1$. Then we select the same integer n_0 as in subcase 2.2. Since

$$k+1 \equiv r \pmod{p^l} \quad \text{and} \quad v_0 p^{l-1} \le r \le p^l - 1,$$

we have $k+j \equiv r+j-1 \pmod{p^l}$ and

$$v_0 p^{l-1} < r+j-1 \le p^l + v_0 p^{l-1} - 2 \quad \text{for all } 1 \le j \le v_0 p^{l-1}.$$

Hence there is no term of the form $(n_0 + v_0 p^{l-1} - 1 + t_1 p^l)^2 + 1$ and at most one term of the form $(n_0 + v_0 p^{l-1} - 1 - X_{p^l} + t_2 p^l)^2 + 1$ in the set $\{(n_0+k+1)^2+1, \ldots, (n_0 + k + v_0 p^{l-1})^2 + 1\}$, where $t_1, t_2 \in \mathbb{Z}$. This implies that $|S_k^{(l)}(n_0 + v_0 p^{l-1})| \le |S_k^{(l)}(n_0)| - 1$. Thus $f_l(n_0 + v_0 p^{l-1}) \le f_l(n_0) - 1$ as required.

The claim is proved and so the proof of Lemma 3.4 is complete. □

4. Proof of Theorem 1.1 and application

Using the lemmas presented in previous sections, we are now in a position to prove Theorem 1.1.

Proof of Theorem 1.1. First, g_k is periodic by Lemma 2.1. By (2.5),

$$\begin{aligned} P_k &= 2^{((-1)^k+1)/2} \cdot \prod_{\substack{p \equiv 1 \pmod 4 \\ p \mid R_k}} P_{p,k} \\ &= 2^{((-1)^k+1)/2} \cdot \frac{R_k}{2^{v_2(R_k)} \prod_{p \equiv 3 \pmod 4} p^{v_p(R_k)}} \prod_{\substack{p \equiv 1 \pmod 4 \\ p \mid R_k}} \frac{P_{p,k}}{p^{v_p(R_k)}} \\ &= \frac{Q_k}{\prod_{\substack{p \equiv 1 \pmod 4 \\ p \mid R_k}} \frac{p^{v_p(R_k)}}{P_{p,k}}} := \frac{Q_k}{\Delta_k}. \end{aligned}$$

By Lemma 3.3, we know that there is at most one prime $p \equiv 1 \pmod 4$ such that $p \mid R_k$ and $v_p(k+1) \ge v_p(R_k)$.

https://doi.org/10.1017/S0004972712000202 Published online by Cambridge University Press

If there is exactly one prime $p \equiv 1 \pmod 4$ such that $p \mid R_k$ and $v_p(k+1) \geq v_p(R_k)$, then for such prime p, Lemma 3.4 tells us that $P_{p,k} = 1$. For all other primes $q \equiv 1 \pmod 4$ with $q \mid R_k$, we obtain by Lemma 3.4 that $P_{q,k} = q^{v_q(R_k)}$. In this case, $\Delta_k = p^{v_p(R_k)}$. Then $P_k = Q_k/p^{v_p(R_k)}$. Notice that $v_p(R_k) = v_p(Q_k)$ for such prime p. Hence $P_k = Q_k/p^{v_p(Q_k)}$ in this case.

If there is no prime $p \equiv 1 \pmod 4$ satisfying $p \mid R_k$ and $v_p(k+1) \geq v_p(R_k)$, then for all primes $q \equiv 1 \pmod 4$ with $q \mid R_k$, we have $P_{q,k} = q^{v_q(R_k)}$ and so $\Delta_k = 1$. Therefore $P_k = Q_k$ in this case. This completes the proof of Theorem 1.1. □

By Theorem 1.1, we can easily find infinitely many positive integers k such that $P_k = Q_k$ as the following two examples show.

Example 4.1. If $k + 1$ has no prime factors congruent to 1 modulo 4, then $P_k = Q_k$ by Theorem 1.1. For instance, if $k + 1$ equals 6^r with r a positive integer, or is a prime number congruent to 3 modulo 4, then $P_k = Q_k$.

Example 4.2. Let a and b be any two positive integers. If k is an integer having the form $k = 3^a 5^b - 1$, then $P_k = Q_k$. In fact, since $k = 3^a 5^b - 1 > (5^{b+1} - 1)/2$, the congruence $x^2 + 4 \equiv 0 \pmod{5^{b+1}}$ has at least one root modulo 5^{b+1} in the interval $[1, k]$. So

$$v_5(R_k) = v_5(\mathrm{lcm}_{1 \leq i \leq k}\{i(i^2+4)\}) \geq b + 1 > v_5(k+1) = b.$$

Then $P_k = Q_k$ by Theorem 1.1.

On the other hand, there are also infinitely many positive integers k such that P_k equals Q_k divided by a power of one prime $p \equiv 1 \pmod 4$. The following proposition gives us such example.

Proposition 4.3. *If $k + 1$ is a prime congruent to 1 modulo 4, then $P_k = Q_k/(k+1)$.*

Proof. For any integer $1 \leq i \leq k$, since $k + 1$ is a prime congruent to 1 modulo 4, implying that $k \geq 4$, we obtain $i^2 + 4 \leq k^2 + 4 < (k+1)^2$. Note that $k + 1$ is a prime. Hence $v_{k+1}(i^2 + 4) < 2$. Then, by (3.1),

$$v_{k+1}(R_k) = \max_{1 \leq i \leq k}\{v_{k+1}(i^2+4)\} < 2.$$

In addition, there is an integer $x \in [1, k]$ satisfying $x^2 + 4 \equiv 0 \pmod{k+1}$. In other words, $\max_{1 \leq i \leq k}\{v_{k+1}(i^2+4)\} \geq 1$. Thus

$$v_{k+1}(R_k) = \max_{1 \leq i \leq k}\{v_{k+1}(i^2+4)\} = 1 = v_{k+1}(k+1).$$

Then Proposition 4.3 follows immediately from Theorem 1.1. □

In concluding this paper, we give an interesting asymptotic formula as an application of Theorem 1.1.

https://doi.org/10.1017/S0004972712000202 Published online by Cambridge University Press

Proposition 4.4. *Let k be any given positive integer. Then the following asymptotic formula holds:*

$$\log \operatorname{lcm}_{0\le i\le k}\{(n+i)^2+1\} \sim 2(k+1)\log n \quad \textit{as } n\to\infty.$$

Proof. By Theorem 1.1, g_k is periodic. So for all positive integers n, $g_k(n) \le M := \max_{1\le m\le P_k}\{g_k(m)\}$. Hence

$$\log\Big(\prod_{i=0}^{k}((n+i)^2+1)\Big) - \log M \le \log \operatorname{lcm}_{0\le i\le k}\{(n+i)^2+1\} \le \log\Big(\prod_{i=0}^{k}((n+i)^2+1)\Big).$$

Since

$$\log\Big(\prod_{i=0}^{k}((n+i)^2+1)\Big) - \log M = 2(k+1)\log n + \sum_{i=0}^{k}\log\Big(1+\frac{2i}{n}+\frac{i^2+1}{n^2}\Big) - \log M,$$

it follows that

$$\lim_{n\to\infty}\frac{\log(\prod_{i=0}^{k}((n+i)^2+1)) - \log M}{2(k+1)\log n} = 1.$$

Note that

$$\lim_{n\to\infty}\frac{\log(\prod_{i=0}^{k}((n+i)^2+1))}{2(k+1)\log n} = 1.$$

Therefore

$$\lim_{n\to\infty}\frac{\log \operatorname{lcm}_{0\le i\le k}\{(n+i)^2+1\}}{2(k+1)\log n} = 1$$

as desired. The proof of Proposition 4.4 is complete. □

References

[1] P. Bateman, J. Kalb and A. Stenger, 'A limit involving least common multiples', *Amer. Math. Monthly* **109** (2002), 393–394.

[2] M. A. Bennett, N. Bruin, K. Győry and L. Hajdu, 'Powers from products of consecutive terms in arithmetic progression', *Proc. Lond. Math. Soc.* **92** (2006), 273–306.

[3] P. L. Chebyshev, 'Memoire sur les nombres premiers', *J. Math. Pures Appl.* **17** (1852), 366–390.

[4] B. Farhi, 'Nontrivial lower bounds for the least common multiple of some finite sequences of integers', *J. Number Theory* **125** (2007), 393–411.

[5] B. Farhi and D. Kane, 'New results on the least common multiple of consecutive integers', *Proc. Amer. Math. Soc.* **137** (2009), 1933–1939.

[6] B. Green and T. Tao, 'The primes contain arbitrarily long arithmetic progressions', *Ann. of Math.* (2) **167** (2008), 481–547.

[7] D. Hanson, 'On the product of the primes', *Canad. Math. Bull.* **15** (1972), 33–37.

[8] G. H. Hardy and J. E. Littlewood, 'Some problems of partitio numerorum III: On the expression of a number as a sum of primes', *Acta Math.* **44** (1923), 1–70.

[9] S. Hong and G. Qian, 'The least common multiple of consecutive arithmetic progression terms', *Proc. Edinb. Math. Soc.* **54** (2011), 431–441.

[10] S. Hong, G. Qian and Q. Tan, 'The least common multiple of a sequence of products of linear polynomials', *Acta Math. Hungar.*, **135** (2012), 160–167.

[11] S. Hong and Y. Yang, 'On the periodicity of an arithmetical function', *C.R. Acad. Sci. Paris Ser. I* **346** (2008), 717–721.
[12] L.-K. Hua, *Introduction to Number Theory* (Springer, Berlin, 1982).
[13] H. Iwaniec, 'Almost-primes represented by quadratic polynomials', *Invent. Math.* **47** (1978), 171–188.
[14] M. Nair, 'On Chebyshev-type inequalities for primes', *Amer. Math. Monthly* **89** (1982), 126–129.
[15] N. Saradha and T. N. Shorey, 'Almost squares in arithmetic progression', *Compositio Math.* **138** (2003), 73–111.

GUOYOU QIAN, Mathematical College, Sichuan University,
Chengdu 610064, PR China
e-mail: qiangy1230@gmail.com, qiangy1230@163.com

QIANRONG TAN, School of Computer Science and Technology,
Panzhihua University, Panzhihua 617000, PR China
e-mail: tqrmei6@126.com

SHAOFANG HONG, Yangtze Center of Mathematics, Sichuan University,
Chengdu 610064, PR China
e-mail: sfhong@scu.edu.cn, s-f.hong@tom.com, hongsf02@yahoo.com