EXTENDING A THEOREM OF PILLAI TO QUADRATIC SEQUENCES

Joshua Harrington
Department of Mathematics, Shippensburg University, Shippensburg, Pennsylvania
JSHarrington@ship.edu

Lenny Jones
Department of Mathematics, Shippensburg University, Shippensburg, Pennsylvania
lkjone@ship.edu

Received: 8/10/13, Revised: 1/5/14, Accepted: 4/9/14, Published: 6/15/15

Abstract

Let S be a sequence of integers, and let S_m be a list of exactly $m \geq 2$ consecutive terms of S. We say that S_m has property P_1 if there exists $x \in S_m$ such that $\gcd(x, y) = 1$ for all $y \in S_m$ with $y \neq x$. Define g_S to be the smallest integer m, if it exists, such that there exists S_m for which property P_1 fails to hold. Pillai investigated the particular sequence $S = [1, 2, 3, \ldots]$, and showed that $g_S = 17$ in this case. Other authors have extended this idea to arbitrary linear sequences and, more recently, to Lucas and Lehmer sequences. In this article, we extend this idea to quadratic sequences S whose nth term is $f(n)$, where $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ with $a > 0$. Among the results established is the determination of g_S when

- $f(x) = x^2 + bx + c$,
- $f(x) = 2^k x^2 + c$, except when $k = 2$ and $c = -17$, and
- $f(x) = ax^2 + bx + c$, when $b^2 - 4ac \in \{0, a^2, -q^k\}$, where q is an odd prime and $k \geq 1$.

1. Introduction

Let $\mathbb{N}_m$ denote a list of $m \geq 2$ consecutive positive integers. In an effort to prove that no product of two or more consecutive positive integers greater than 1 is ever a perfect power, Pillai [17, 18, 19, 20] investigated when $\mathbb{N}_m$ contains an element that is relatively prime to all other elements in $\mathbb{N}_m$. Saradha and Thangadurai [22] have subsequently refereed to this property as property P_1. Pillai showed that any list $\mathbb{N}_m$ with $m < 17$ has property P_1, and he conjectured that there exist infinitely many lists $\mathbb{N}_m$ that do not have property P_1 for each $m \geq 17$. Initially, Pillai was able to verify this conjecture for all $m \leq 430$, and later extend it to all $m \leq 12335$ [19]. The full conjecture was proven by Alfred Brauer [3], and shortly thereafter, Pillai himself [20] published a different proof. In actuality, a paper of Erdős [5] that predates Brauer's paper by 6 years also contains a proof. A simpler proof was given later by Evans [6], and more recently, Gassko [10] has given another proof. Since then, other authors have investigated various generalizations of these ideas. For example, Y. Caro [4], and later Saradha and Thangadurai [22], extended the notion of property P_1 in the following way. They say $\mathbb{N}_m$ has property P_d if there exists an element $x \in \mathbb{N}_m$ such that $\gcd(x, y) \leq d$ for all $y \in \mathbb{N}_m$ with $y \neq x$. Caro [4] proved that for any $d > 1$, there exist infinitely many lists $\mathbb{N}_m$ which do not have property P_d whenever m exceeds an effectively computable number $G(d)$. Denote by $g(d)$ the smallest integer such that there exists a set $\mathbb{N}_{g(d)}$ for which property P_d does not hold. Caro [4] also showed that $g(d) < 45d \log d$ and $G(d) < 54d \log d$. Using a combination of a computer search and more precise estimates for $\pi(x)$ due to Rosser and Schöenfeld [21], Saradha and Thangadurai [22] improved Caro's bounds for $g(d)$ and $G(d)$. Recently, Hajdu and Saradha [11] have investigated the following generalization of these notions. Given a non-empty set T of positive integers, they say $\mathbb{N}_m$ has property P_T if there exists $x \in \mathbb{N}_m$ such that $\gcd(x, y) \in T$ for all $y \in \mathbb{N}_m$ with $y \neq x$.

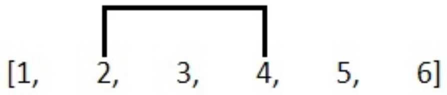
We are interested here in a slightly different generalization. Rather than change the property P_1, we change the list $\mathbb{N}_m$. This concept is not new and was first investigated by Evans [7], and later by Ohtomo and Tamari [16], when they changed the focus from sets of consecutive integers to sets of consecutive terms in an arithmetic progression. They showed that this problem in arithmetic progressions is equivalent to the original problem of Pillai. More recently, Hajdu and Szikszai [12] have investigated the original problem of Pillai when applied to sets of consecutive terms of Lucas and Lehmer sequences. For any sequence S of integers, let S_m be a list of exactly $m \geq 2$ consecutive terms of S. We define g_S to be the smallest integer m such that there exists S_m for which property P_1 fails to hold. It is easy to see that Pillai's original result applies immediately to sequences S whose nth term is n^2. That is, $g_S = 17$ for these sequences. This observation provides the motivation for the investigations in this article. Our focus is on the calculation of g_S for sequences S whose nth term is $f(n)$, where $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ with $a > 0$. Note that there is no loss of generality to restrict attention to $a > 0$. It turns out that g_S varies, depending on the values of a, b, c, and so we write $g(a, b, c)$, or simply g, instead of g_S. We remark that a number G_S (analogous to $G(1)$) can be defined in this situation, but we are not concerned with such calculations here. The main results in this article include the calculation of $g(1, b, c)$ for all $b, c \in \mathbb{Z}$, $g(a, 0, c)$ when $a = 2^k \geq 2$ (except $a = 4$ and $c = -17$), and $g(a, b, c)$ when $b^2 - 4ac \in \{0, a^2, -q^k\}$, where q is a prime and k is a positive integer. All computer calculations were done using Maple.

Throughout this article, we let $f(x) = ax^2 + bx + c \in \mathbb{Z}[x]$ with $a > 0$, and we let $\Delta := \Delta(f)$ denote the discriminant $b^2 - 4ac$ of $f(x)$. We define a sequence $S := S(f)$ of integers whose nth term is $f(n)$, and we let S_m denote a list of $m \geq 2$ consecutive terms of S. We let $\overline{m}$ denote the list $[1, 2, \ldots, m]$.

2. A General Combinatorial Problem

We now describe a combinatorial problem that, at first glance, might seem unrelated to the question of focus in this article. Let m be a fixed positive integer, and let H be a (possibly infinite) list of positive integers. We can use $\ell \in H$ to *cover* any two elements $u, v \in \overline{m}$ with $u < v$ and $v - u = \ell$. Borrowing some terminology from Gassko [10], we can think of this process of covering the integers u and v, as placing a *staple* of length ℓ above $\overline{m}$, so that the two ends of the staple are at locations u and v in $\overline{m}$. For example, if $m = 6$, a single staple of length 2 can be used to cover any particular two elements u and v in $\overline{m}$, where $(u, v) \in \{(1, 3), (2, 4), (3, 5), (4, 6)\}$. A visualization of this "stapling" is given in the following example, where we have chosen to cover the integers 2 and 4 in $\overline{6}$ with a staple of length 2.

Example 2.1. A staple of length 2 can be used to cover 2 and 4 in $\overline{6}$:



We impose the following restrictions on the process of using H to cover $\overline{m}$.

- Both ends of every staple used from H must cover only integers in $\overline{m}$.

  From the definition of what it means for $\ell \in H$ to cover the integers u and v in $\overline{m}$, it is clear that no $\ell \in H$ with $\ell > m - 1$ can be used. That is, staples of length greater than $m - 1$ would have at least one end of the staple "hanging over". Also, for example, if we want to cover $\overline{6}$, a staple of length 3 cannot be placed with its left end at location 5, since the right end of the staple would then be at location 8, which is not an element of $\overline{6}$.

- Staples can overlap, and two staples can even be used to cover the same element in $\overline{m}$.

  See Example 2.3 and Example 2.4.

- We cannot reuse a staple of length ℓ, unless ℓ actually appears more than once in the list H.

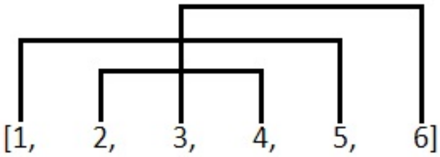
  In other words, if $H = [3, 3, 5]$, then we get to use a staple of length 3 twice, but a staple of length 5 only once.

We say that H *covers* $\overline{m}$ if staples of lengths from some sublist of H can be used to cover all the integers in $\overline{m}$. A natural question that arises is:

Question 2.2. Given a list H of positive integers, what is the smallest positive integer m, if it exists, such that H covers $\overline{m}$?

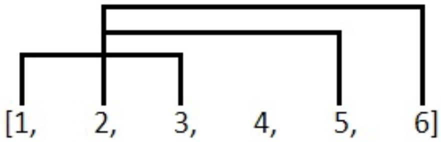
We believe that Question 2.2 is an interesting and difficult combinatorial question. The main reason for the difficulty of this problem is in determining when a particular list H actually covers $\overline{m}$. We do not know if there is some sort of general algorithm or criterion that can be used to determine whether H covers $\overline{m}$ or fails to cover $\overline{m}$. We illustrate some of the previously discussed ideas with the following examples.

Example 2.3. If $H = [2, 3, 4]$, then H can be used to cover $\overline{6}$ in the following way:



Observe that the placement of the staples in Example 2.3 to cover $\overline{6}$ is not unique. For example, the staple of length 2 can be used to cover the pair $(3, 5)$; the staple of length 3 can be used to cover the pair $(1, 4)$; and the staple of length 4 can be used to cover the pair $(2, 6)$. On the other hand, if we do not place the staples in certain positions, we could fail to cover $\overline{6}$. The following example illustrates this phenomenon.

Example 2.4. The following placement of the staples with staple lengths from $H = [2, 3, 4]$ results in not covering 4 in $\overline{6}$:



3. The Connection with Property P_1

In this section, we present the connection between the combinatorial problem described in Section 2 and property P_1 defined in Section 1. Given $f(x) = ax^2 + bx + c$, it is the main goal of this article to determine the smallest positive integer $g :=$

$g(a,b,c)$ for which there exists a positive integer n such that property P_1 fails for the list

$$S_g = [f(n), f(n+1), \ldots, f(n+g-1)].$$

Recall that Property P_1 fails for the list S_g if there does not exist $f(j) \in S_g$ such that $\gcd(f(j), f(i)) = 1$ for all $f(i) \in S_g$ with $i \neq j$. This implies, for any pair (i,j) with $n \leq i < j \leq n+g-1$, that there exists a prime p such that $\gcd(f(i), f(j)) \equiv 0 \pmod{p}$. To illustrate how the combinatorial problem described in Section 2 can be related to our polynomial problem, we give a hypothetical situation in the following example.

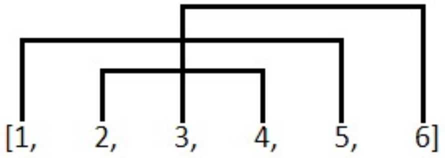
Example 3.1. Suppose, hypothetically, that $g := g(a,b,c) = 6$ and

$$S_g = [f(n), f(n+1), f(n+2), f(n+3), f(n+4), f(n+5)].$$

Suppose also that

$$\begin{aligned} &\gcd(f(n), f(n+4)) \equiv 0 \pmod{p_1}, \\ &\gcd(f(n+1), f(n+3)) \equiv 0 \pmod{p_2} \\ \text{and} \quad &\gcd(f(n+2), f(n+5)) \equiv 0 \pmod{p_3}. \end{aligned} \tag{3.1}$$

If we relabel the elements of S_g, replacing $f(n+j)$ with $j+1$, we can encapsulate the previous information using a slight modification of the diagram from Example 2.3 to incorporate the divisibility of the gcd's by the various primes in (3.1):



$$p_1 \quad p_2 \quad p_3 \quad p_2 \quad p_1 \quad p_3$$

Note that the staples in this diagram are redundant now since the location of the primes p_i gives us the same information. Hence, a further refinement of the diagram leads to

$$\begin{array}{cccccc} 1 & 2 & 3 & 4 & 5 & 6 \\ \hline p_1 & p_2 & p_3 & p_2 & p_1 & p_3 \end{array} \tag{3.2}$$

Remark 3.2. We will refer to a diagram such as (3.2) as a *scheme*.

Thus, the connection to the combinatorial problem from Section 2 has been somewhat established. However, there are still some loose ends. The question of main concern in this paper is not as general as Question 2.2. We are not handed some arbitrary list H of positive integers. The list H here of "allowable" or "useable" staple lengths is determined by the polynomial $f(x)$. The definition of "allowable" also varies in the literature from problem to problem. In [10], the elements of H must be prime numbers. In [11], the elements of H are not necessarily prime, but they must be unique and pairwise relatively prime. In this paper, the elements of H are not required to be prime, or even pairwise relatively prime, and repetitions are allowed. However, other restrictions imposed by the polynomial $f(x)$ do apply, and they are described in detail in Section 4. To calculate g and the actual lists S_g for which property P_1 fails to hold, we construct H according to these restrictions. These restrictions give us an associated list of primes that allow us to impose certain congruence conditions on the index n of the first element in the list S_g. If there exists a list H that covers $\overline{g}$, then, using the Chinese remainder theorem, we can calculate infinitely many such values of n.

4. The General Case $f(x) = ax^2 + bx + c$

Lemma 4.1. *Let p be a prime, and suppose that $f(n) \equiv 0 \pmod{p}$ for some $n \in \mathbb{Z}$. Let $r \in \mathbb{Z}$.*

1. *If $p = 2$, then $f(n+r) \equiv 0 \pmod{2}$ if and only if*

$$r \equiv 0 \pmod{2} \quad \textit{or} \quad a + b \equiv c \equiv 0 \pmod{2}.$$

2. *If $p > 2$ and $a \equiv 0 \pmod{p}$, then $f(n+r) \equiv 0 \pmod{p}$ if and only if*

$$r \equiv 0 \pmod{p} \quad \textit{or} \quad b \equiv c \equiv 0 \pmod{p}.$$

3. *If $p > 2$ and $a \not\equiv 0 \pmod{p}$. Then $f(n+r) \equiv 0 \pmod{p}$ if and only if*

$$r \equiv 0 \pmod{p} \quad \textit{or} \quad r \equiv a^{-1}z \pmod{p},$$

where $z^2 \equiv \Delta \pmod{p}$.

Proof. For any $r \in \mathbb{Z}$, observe that

$$f(n+r) = f(n) + r(ar + 2an + b). \tag{4.1}$$

Hence, since $f(n) \equiv 0 \pmod{p}$, we have from (4.1) that

$$f(n+r) \equiv 0 \pmod{p} \iff \left\{ \begin{array}{c} r \equiv 0 \pmod{p} \\ \text{or} \\ ar + 2an + b \equiv 0 \pmod{p} \end{array} \right. \tag{4.2}$$

Then (1) and (2) of the lemma follow easily from (4.2).

To see (3), first note that since $a \not\equiv 0 \pmod{p}$, $p > 2$ and $f(n) \equiv 0 \pmod{p}$, we have

$$n \equiv -(2a)^{-1}(b+z) \pmod{p},$$

where $z^2 \equiv d \pmod{p}$.

If $f(n+r) \equiv 0 \pmod{p}$ and $ar + 2an + b \equiv 0 \pmod{p}$ from (4.2), we see that

$$r \equiv -a^{-1}(2an+b) \equiv -a^{-1}\left(2a\left(-(2a)^{-1}(b+z)\right)+b\right) \equiv a^{-1}z \pmod{p}.$$

Conversely, if $r \equiv 0 \pmod{p}$, then $f(n+r) \equiv 0 \pmod{p}$ since $f(n) \equiv 0 \pmod{p}$. Also, if $r \equiv a^{-1}z \pmod{p}$, then since $f(n) \equiv 0 \pmod{p}$, we have from (4.1) that

$$\begin{aligned} f(n+r) &= f(n) + r(ar+2an+b) \\ &\equiv r(ar+2an+b) \pmod{p} \\ &\equiv a^{-1}z\left(a\left(a^{-1}z\right) + 2a\left(-(2a)^{-1}(z+b)\right) + b\right) \pmod{p} \\ &\equiv 0 \pmod{p}, \end{aligned}$$

which establishes (3) and completes the proof of the lemma. □

The calculation of the values of r in (3) of Lemma 4.1 is crucial to the results in this paper. These values are, in fact, elements of H, and Lemma 4.1 indicates the restrictions on r such that $r \in H$. One way to determine these values of r is to search for primes p for which $a \not\equiv 0 \pmod{p}$ and $\left(\frac{\Delta}{p}\right) \neq -1$, where $\left(\frac{\Delta}{p}\right)$ is the Legendre symbol of Δ with respect to p. Then $r \equiv a^{-1}z \pmod{p}$, where z is a square root of Δ modulo p. An equivalent approach is to examine the sequence $\{t_r\}$ defined by

$$t_r := \Delta - a^2r^2, \quad r = 1, 2, \ldots. \tag{4.3}$$

For a given r, if there exists a prime p such that $a \not\equiv 0 \pmod{p}$ and $t_r \equiv 0 \pmod{p}$, then r can be used in H. We denote the list of primes corresponding to the elements of H as $\mathcal{P}$. That is, if $r \in H$, then p appears in the corresponding location in $\mathcal{P}$.

There are two items to note. First, a prime p can appear at most twice in $\mathcal{P}$ since there are at most two distinct square roots of Δ modulo p, and hence at most two distinct values of r in this case. If there are two distinct values r_1 and r_2 of r arising from the square roots of Δ modulo p, then both r_1 and r_2 can be used as staple lengths in lieu of using the staple length p, provided the staples r_1 and r_2 are used consecutively. That is, if for some $n \in \mathbb{Z}$, we have $f(n) \equiv f(n+r_1) \equiv 0 \pmod{p}$, then we can use r_2 to get that $f(n+r_1+r_2) \equiv 0 \pmod{p}$, since

$$0 \equiv z_1 + z_2 \equiv ar_1 + ar_2 \pmod{p} \iff r_1 + r_2 \equiv 0 \pmod{p}. \tag{4.4}$$

A straightforward calculation shows condition (4.4) implies that the two congruences,

$$n \equiv -(2a)^{-1}(b+z_1) \pmod{p} \quad \text{and} \quad n + r_1 \equiv -(2a)^{-1}(b+z_2) \pmod{p},$$

for n arising from r_1 and r_2 are in fact the same congruence. Thus, we can use the Chinese remainder theorem to compute a value of n to generate a desired list S_g. The use of both r_1 and r_2 will be indicated in H by placing a hat over the pair of staple lengths. That is, if r_1 and r_2 are staple lengths corresponding to the same prime, and they are used with r_1 first (reading from left to right), then the pair $\widehat{r_1, r_2}$ would appear in H.

Secondly, we note that a given value of r can appear in H more than once, since it is possible that the calculation of r gives the same value for distinct primes p. This can happen, in fact, when t_r from (4.3) is divisible by more than one odd prime.

As indicated in Section 3, it will be convenient to use a diagram, which we call a *scheme*, to represent how the list H and the corresponding list of primes $\mathcal{P}$ are used to cover $\overline{g}$. Let $H = [r_1, r_2, \ldots, r_z]$ and $\mathcal{P} = [p_1, p_2, \ldots, p_z]$. Suppose that we use $r_i \in H$ to cover $u < v$ in $\overline{g}$. Then this information would appear in the scheme as follows:

$$\begin{array}{ccccccccc} 1 & 2 & \cdots & u & \cdots & v & \cdots & g \\ \hline * & * & \cdots & p_i & \cdots & p_i & \cdots & *. \end{array} \tag{4.5}$$

Note that for each prime $p_i \in \mathcal{P}$, the corresponding value $r_i \in H$ can be computed easily from (4.5). We point out that, in general, a scheme is not unique. Also, if p_i is found using (3) of Lemma 4.1, and $kr_i < m$ for some integer $k > 1$, then p_i divides the terms in the list S_g at locations $u - kr_i$ and $v + kr_i$.

The following lemmas are needed to establish our results. We use the sequence $\{t_r\}$ defined in (4.3).

Lemma 4.2. *If there exists a prime $p > 2$ such that $a \not\equiv 0 \pmod{p}$ and $t_1 \equiv 0 \pmod{p}$, then $g(a, b, c) = 2$.*

Proof. Let $n \equiv -(2a)^{-1}(a + b) \pmod{p}$. Then

$$\begin{aligned} f(n) &\equiv a\left(-(2a)^{-1}(a+b)\right)^2 + b(-(2a)^{-1}(a+b)) + c \pmod{p} \\ &\equiv -(4a)^{-1}(b^2 - 4ac - a^2) \pmod{p} \\ &\equiv -(4a)^{-1}t_1 \pmod{p} \\ &\equiv 0 \pmod{p}. \end{aligned}$$

Letting $z = a$ in (3) of Lemma 4.1, we conclude that modulo p, $f(x)$ has the two zeros n and $n + 1$. Hence, it follows that $g(a, b, c) = 2$. □

Corollary 4.3. *If $\Delta = a^2$, then $g(a, b, c) = 2$.*

Proof. Let $p > 2$ be any prime such that $p > a$. Then $a \not\equiv 0 \pmod{p}$ and

$$t_1 = \Delta - a^2 = 0 \equiv 0 \pmod{p}.$$

Thus, we see that the corollary is just a special case of Lemma 4.2. □

Remark 4.4. An alternate and somewhat more transparent proof of Lemma 4.2 can be given using the scheme notation with $H = [1]$ and $\mathcal{P} = [p]$. The scheme is then

$$\begin{array}{cc} 1 & 2 \\ \hline p & p. \end{array}$$

Thus, $g(a, b, c) = 2$.

Lemma 4.5. *If $a \equiv 1 \pmod 2$ and $\Delta \equiv 1 \pmod 8$, then $g(a, b, c) = 2$.*

Proof. Observe that $b \equiv 1 \pmod 2$ so that $b^2 \equiv 1 \pmod 8$. Thus,

$$0 \equiv \Delta - 1 \equiv -4ac \pmod 8,$$

and hence $c \equiv 0 \pmod 2$. Therefore, $a + b \equiv c \equiv 0 \pmod 2$ so that $f(1) \equiv 0 \pmod 2$. Letting $r = 1$ in (1) of Lemma 4.1, we conclude that $g(a, b, c) = 2$. □

Lemma 4.6. *There exists no $f(x)$ such that $g(a, b, c) = 3$.*

Proof. If $g(a, b, c) = 3$, then there exists a list $[f(n), f(n+1), f(n+2)]$ for which property P_1 fails to hold. Thus,

$$\text{either} \quad \gcd(f(n+1), f(n)) > 1 \quad \text{or} \quad \gcd(f(n+1), f(n+2)) > 1,$$

which implies that $g(a, b, c) = 2$. □

Lemma 4.7. *If $\Delta = 0$, then $g(a, b, c) = 17$.*

Proof. Since $\Delta = 0$, we can write $f(x) = (Ax + B)^2$, for some $A, B \in \mathbb{Z}$. Hence, the lemma follows from the original result of Pillai and its extension to arithmetic progressions. □

Lemma 4.8. *Suppose that $\gcd(a, b, c) = 1$ and either $a + b \equiv 1 \pmod 2$ or $c \equiv 1 \pmod 2$. Assume also that every odd prime divisor of t_1 divides a, and that there are distinct odd primes τ_2, τ_3 and τ_4 such that $t_i \equiv 0 \pmod{\tau_i}$ and $a \not\equiv 0 \pmod{\tau_i}$ for each i. Then $g(a, b, c) \in \{4, 5, 6\}$. Moreover,*

1. *If t_2 has an odd prime divisor $p \neq \tau_2$, then $g(a, b, c) = 4$.*

2. *If t_3 has an odd prime divisor $q \notin \{\tau_2, \tau_3\}$, and τ_2 is the only odd prime divisor of t_2, then $g(a, b, c) = 5$.*

3. *If τ_i is the only odd prime divisor of t_i for all i, then $g(a, b, c) = 6$.*

Proof. First note, by Lemma 4.1, that the hypotheses here imply that $r = 1$ cannot be used as a staple length, and hence $g(a, b, c) \neq 2$.

To prove *1.*, we use

$$H = [2, 2] \quad \text{and} \quad \mathcal{P} = [p, \tau_2],$$

from which we get the scheme

1	2	3	4
p	τ_2	p	τ_2.

Thus, $g(a, b, c) \leq 4$. By Lemma 4.6, $g(a, b, c) \neq 3$. Since $g(a, b, c) \neq 2$, it follows that $g(a, b, c) = 4$. Indeed, it is easy to see that this scheme is the only possible way to have $g(a, b, c) = 4$.

For *2.*, we use

$$H = [2, 3, 3] \quad \text{and} \quad \mathcal{P} = [\tau_2, q, \tau_3],$$

from which we construct the scheme

1	2	3	4	5
q	τ_3	τ_2	q	τ_3
τ_2				.

Thus, $g(a, b, c) \leq 5$. Since the staple length $r = 2$ cannot appear in H more than once, we see that $g(a, b, c) \neq 4$. By Lemma 4.6, $g(a, b, c) \neq 3$, and since $g(a, b, c) \neq 2$, we conclude that $g(a, b, c) = 5$.

Finally, for *3.*, we use

$$H = [2, 3, 4] \quad \text{and} \quad \mathcal{P} = [\tau_2, \tau_3, \tau_4],$$

from which we get the scheme

1	2	3	4	5	6
τ_4	τ_2	τ_3	τ_2	τ_4	τ_3.

Thus, $g(a, b, c) \leq 6$. As before, we see that $g(a, b, c) \not\leq 4$. Suppose that $g(a, b, c) = 5$, and let

$$V = [f(n), f(n+1), f(n+2), f(n+3), f(n+4)]$$

be a list for which property P_1 fails to hold. Since $g(a, b, c) \neq 2$, we have that

$$\gcd(f(n+1), f(n+2)) = \gcd(f(n+2), f(n+3)) = 1.$$

Hence, since $f(n+2)$ cannot be coprime to all other elements of V, there exists an odd prime β such that $a \not\equiv 0 \pmod{\beta}$ and either

$$f(n+2) \equiv f(n+4) \equiv 0 \pmod{\beta} \quad \text{or} \quad f(n+2) \equiv f(n) \equiv 0 \pmod{\beta}, \tag{4.6}$$

by (3) of Lemma 4.1. Suppose that

$$\gcd(f(n), f(n+2)) \equiv 0 \pmod{\beta}.$$

Now, if $\gcd(f(n+1), f(n+3)) > 1$, then, by (3) of Lemma 4.1, we have that

$$\gcd(f(n+1), f(n+3)) \equiv 0 \pmod{\beta}.$$

But then

$$\gcd(f(n+1), f(n+2)) \equiv 0 \pmod{\beta},$$

which contradicts the fact that $g(a, b, c) \neq 2$. Hence,

$$\gcd(f(n+1), f(n+3)) = 1.$$

Therefore, since $f(n+1)$ cannot be coprime to all other elements of V, it follows from (3) of Lemma 4.1 that there exists some odd prime γ such that $a \not\equiv 0 \pmod{\gamma}$ and

$$\gcd(f(n+1), f(n+4)) \equiv 0 \pmod{\gamma}.$$

Since $g(a, b, c) \neq 2$, we see that

$$\gcd(f(n+3), f(n+2)) = 1 = \gcd(f(n+3), f(n+4)).$$

Since $f(n+3)$ cannot be coprime to all other elements of V, we must have that

$$\text{either} \qquad \gcd(f(n+3), f(n)) > 1 \qquad \text{or} \qquad \gcd(f(n+3), f(n+1)) > 1.$$

However, again using (3) of Lemma 4.1, it follows that if $\gcd(f(n+3), f(n)) > 1$, then

$$\gcd(f(n+3), f(n)) \equiv 0 \pmod{\gamma},$$

which yields the contradiction that

$$\gcd(f(n+3), f(n+4)) \equiv 0 \pmod{\gamma}.$$

A similar contradiction occurs if $\gcd(f(n+3), f(n+1)) > 1$. Thus, we have shown that $f(n+3)$ is coprime to all other elements of V, which contradicts the assumption that property P_1 fails to hold for V. A similar argument shows that the assumption

$$f(n+2) \equiv f(n+4) \equiv 0 \pmod{\beta}$$

from (4.6) produces a contradiction as well, and hence $g(a, b, c) = 6$. □

Proposition 4.9. *Let a be an odd square-free integer, and suppose that $p > 2$ is a prime such that*

$$a \equiv 0 \pmod{p} \quad \text{and} \quad \Delta - a^2 \equiv 0 \pmod{p^2}. \tag{4.7}$$

Then $g(a, b, c) = 2$.

Proof. Conditions (4.7) imply that $a \equiv b \equiv c \equiv 0 \pmod{p}$. Hence, we immediately have that $g(a, b, c) = 2$. □

Corollary 4.10. *Let a be a fixed odd square-free integer and, for $n \in \mathbb{Z}$, define*

$$\mathcal{D}_n(a) := \left\{ f(x) \;\middle|\; \Delta = n \right\}.$$

Then there are at most finitely many $n \in \mathbb{Z}$ for which $\mathcal{D}_n(a)$ contains $f(x)$ with $g(a, b, c) > 2$.

Proof. If there exists an odd prime p with $a \not\equiv 0 \pmod{p}$ and $\Delta - a^2 \equiv 0 \pmod{p}$, then $g(a, b, c) = 2$ by Lemma 4.2. Suppose now that

$$\Delta - a^2 = 2^k p_1^{e_1} p_2^{e_2} \cdots p_t^{e_t},$$

where each p_i is an odd prime dividing a. If $g(a, b, c) \neq 2$, then Proposition 4.9 implies that each $e_i = 1$, and Lemma 4.5 implies that $k \leq 2$. Hence, there are only finitely many possibilities for Δ when $g(a, b, c) > 2$. □

5. The Case $f(x) = x^2 + bx + c$

The main result of this section is the following.

Theorem 5.1. *Let $f(x) = x^2 + bx + c$. Then*

$$g(1, b, c) = \begin{cases} 6 & \text{if } \Delta = -3 \\ 17 & \text{if } \Delta = 0 \\ 18 & \text{if } \Delta = 5 \\ 2 & \text{otherwise.} \end{cases}$$

Proof. We begin by showing that $g(1, b, c) = 2$ if and only if $\Delta \notin \{-3, 0, 5\}$. Suppose first that $\Delta \notin \{-3, 0, 5\}$. Note that

$$\Delta \equiv \begin{cases} 0 \pmod{4} & \text{if } b \equiv 0 \pmod{2} \\ 1 \pmod{4} & \text{if } b \equiv 1 \pmod{2}. \end{cases} \tag{5.1}$$

We know from Lemma 4.2 that if $\Delta - 1$ is divisible by any odd prime, then $g(1, b, c) = 2$. So suppose that $\Delta - 1 = \pm 2^k$ for some nonnegative integer k. It follows from Lemma 4.5 that $g(1, b, c) = 2$ if $k > 2$. If $k \leq 2$, then $\Delta \in \{-1, 2, 3\}$. However, this is impossible by (5.1). Hence, $g(1, b, c) = 2$.

Now suppose that $g(1, b, c) = 2$. Then there exists some prime p dividing $f(n)$ and $f(n + 1)$ for some integer n. Hence, by (3) of Lemma 4.1, we have $\Delta \equiv 1 \pmod{p}$. It follows that if $\Delta \in \{-3, 0, 5\}$, then $p = 2$ and $\Delta \in \{-3, 5\}$. However, by (1) of Lemma 4.1, if $p = 2$, then b is odd and c is even, which implies that $\Delta \equiv 1 \pmod 8$, and so $\Delta \notin \{-3, 5\}$. Therefore, $\Delta \notin \{-3, 0, 5\}$.

We consider next the three cases of $\Delta \in \{-3, 0, 5\}$. In the case of $\Delta = -3$, we can apply Lemma 4.8 to conclude that $g(1, b, c) = 6$. The case of $\Delta = 0$ is immediate from Lemma 4.7. So, suppose that $\Delta = 5$. We use

$$H = [\widehat{7,4}, 5, 6, 8, 9, 11, 12, 13, 14, 16]$$

$$\text{and} \quad \mathcal{P} = [11, 11, 5, 31, 59, 19, 29, 139, 41, 191, 251]$$

to construct the scheme

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
11	191	59	29	5	139	31	11	19	5	59	11	31	41	29	191	251	19
41																	139.
251																	

Hence, $g(1, b, c) \leq 18$. Although an argument similar to the arguments used in the proof of Lemma 4.8 can be used to show that $g(1, b, c) \not< 18$, we defer to a computer check in this situation because of the length of the argument. □

We illustrate in the following example how to use Theorem 5.1 to construct a list S_{18} for a particular $f(x)$ with $\Delta = 5$.

Example 5.2. Let $f(x) = x^2 + x - 1$. We use H and $\mathcal{P}$ as in the proof of Theorem 5.1 for $\Delta = 5$. We let $L[i]$ denote the position of the first appearance of the prime $\mathcal{P}[i]$ in the scheme, reading from left to right. For example, $L[11] = 1$ and $L[31] = 7$. Thus, $L = [1, 5, 7, 3, 9, 4, 6, 1, 2, 1]$. Then, according to (3) of Lemma 4.1, we use the Chinese remainder theorem to solve the system of congruences

$$n \equiv -\frac{1 + H[i]}{2} - L[i] - 1 \pmod{P[i]}$$

to get that the smallest positive integer solution is $n = 4332242442083508$. Thus, property P_1 fails to hold for the list

$$[f(n), f(n+1), \ldots, f(n+17)]\,.$$

6. The Case $f(x) = 2^k x^2 + c$

The case $k = 0$ has been addressed in Section 5, so we assume that $k \geq 1$. As before, our result depends on an analysis of the sequence $\{t_r\}$ given in (4.3). We see here that

$$t_r = \Delta - a^2 r^2 = \begin{cases} -4\left(2c + r^2\right) & \text{if } k = 1 \\ -2^{k+2}\left(c + 2^{k-2} r^2\right) & \text{if } k \geq 2. \end{cases} \tag{6.1}$$

The main theorem of this section is the following.

Theorem 6.1. *Let $f(x) = 2^k x^2 + c$, where $k \in \mathbb{Z}$ with $k \geq 1$. If $k \neq 2$, then $g(2^k, 0, c) = 2$. If $k = 2$, then, with the exception of $c = -17$, either $g(4, 0, c) \in \{2, 4, 5, 6\}$ or*

$$g(4,0,c) = \begin{cases} 15 & \textit{if } c = 7 \textit{ or } c = -3 \\ 18 & \textit{if } c = -5 \\ 8 & \textit{if } c = -65. \end{cases}$$

In addition, $g(4, 0, -17) \leq 35$.

Proof. First note that if $c \equiv 0 \pmod 2$, then $g(2^k, 0, c) = 2$. So, assume that $c \equiv 1 \pmod 2$. If $k = 1$ or $k > 2$, then we see from (6.1) that $\Delta - a^2$ has an odd prime divisor. Thus, $r = 1 \in H$, and by Lemma 4.1, we have that $g(2^k, 0, c) = 2$ in these cases.

Assume then that $k = 2$, so that $a = 4$, and consider first the case when $c > 0$. If $c \neq 2^z - 1$ for some integer $z \geq 1$, then $c + 1$ has an odd prime divisor, and again by Lemma 4.1, we have that $g(4, 0, c) = 2$. Thus, we can assume that $c = 2^z - 1$ for some integer $z \geq 1$, so that

$$t_r = -16\left(2^z - 1 + r^2\right).$$

Note that $r = 1 \notin H$ in this case. If all of the hypotheses of Lemma 4.8 are satisfied, then $g(4, 0, c) \in \{4, 5, 6\}$. So assume that there do not exist distinct odd primes τ_2, τ_3 and τ_4 such that $t_i \equiv 0 \pmod{\tau_i}$ for all $i \in \{2, 3, 4\}$. So, either some t_i is a power of 2 or not. It is straightforward to show that $t_i = 2^u$ for some integer $u \geq 1$ if and only if $i = z = 3$. Thus $c = 7$. Using $H = [2, 4, 6, 7, 8, 10, 12, 14]$ and $\mathcal{P} = [11, 23, 43, 7, 71, 107, 151, 29]$, we can construct the scheme

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
29	151	107	71	43	23	11	7	11	23	43	71	107	151	29
7														.

Thus, $g(4, 0, 7) = 15$ since it is easily verified that $g(4, 0, 7) < 15$ is impossible.

Another possible situation is that, for all $i \in \{2, 3, 4\}$, no t_i is a power of 2 and each t_i has a single odd prime divisor τ_i, but that two or three of the τ_i are the same. Suppose first that $\tau_2 = \tau_3$. Then $\tau_2 = 5$, and hence we see that $2^z + 3 = 5^u$ and $2^z + 8 = 5^v$. But subtracting these equations shows that this is impossible. Similarly, if $\tau_2 = \tau_4$, then $\tau_2 = 3$, which is also impossible; and finally, if $\tau_3 = \tau_4$, then $\tau_3 = 7$, which is again impossible. This completes the proof when $c > 0$.

Now we assume that $c < 0$. If $c \neq -(2^z + 1)$ for some integer $z \geq 1$, then $-c - 1$ has an odd prime divisor, and so by Lemma 4.1, we have that $g(4, 0, c) = 2$. Thus, we can assume that $c = -(2^z + 1)$ for some integer $z \geq 1$, so that

$$t_r = 16\left(2^z + 1 - r^2\right).$$

Note that $r = 1 \notin H$ in this case. As in the case of $c > 0$, if all of the hypotheses of Lemma 4.8 are satisfied, then $g(4, 0, c) \in \{4, 5, 6\}$. So assume that there do not exist distinct odd primes τ_2, τ_3 and τ_4 such that $t_i \equiv 0 \pmod{\tau_i}$ for all $i \in \{2,3,4\}$. This phenomenon can occur in several ways. Either $|t_i|$ is a power of 2 for some i or not. We see that $|t_2|$ is a power of 2 exactly when $z = 1$ or $z = 2$. Similarly, $|t_3|$ is a power of 2 exactly when $z = 2$ and $z = 4$, and $|t_4|$ can never be a power of 2. Other possibilities are when, for all $i \in \{2,3,4\}$, no t_i is a power of 2 and each t_i has a single odd prime divisor τ_i, but that two or three of the τ_i are the same. Observe that $\gcd(2^z - 3, 2^z - 15) = 1$ so that $\tau_2 \neq \tau_4$. If $\tau_2 = \tau_3$, then $\tau_2 = 5$ and we have that

$$2^z - 3 = 5^u \quad \text{and} \quad 2^z - 8 = 2^v \cdot 5^w, \tag{6.2}$$

for some positive integers u, v, w, z. To see that (6.2) is impossible, we subtract the equations to get

$$5 = 5^w \left(5^{u-w} - 2^v\right),$$

from which we conclude that $w = 1$ and $5^{u-1} - 2^v = 1$. By Mihăilescu's theorem (Catalan's conjecture) [15], the only solution is $u = v = 2$. But we see that this is impossible in (6.2). Now suppose that $\tau_3 = \tau_4$. Then $\tau_3 = 7$ and we have the two cases:

1. $2^z - 8 = 2^u \cdot 7^v$ and $2^z - 15 = 7^w$, or
2. $2^z - 8 = 2^u \cdot 7^v$ and $2^z - 15 = -7^w$, for some positive integers u, v, w, z.

An analysis of 1. similar to before gives that $w = 1$ and

$$1 = 2^u - 7^{w-1},$$

which, by Mihăilescu's theorem, has only the two solutions: $u = w = 1$, and $u = 3$ with $w = 2$. The first of these solutions is impossible in 1., but the second solution yields $z = 6$.

Subtracting the equations in 2. gives

$$7 = 2^u \cdot 7^v + 7^w,$$

which is clearly impossible.

To complete the proof of the theorem, we analyze these exceptional cases $z \in \{1, 2, 4, 6\}$ separately.

6.1. $z = 1$

In this case we use

$$H = [\widehat{4, 9}, 3, 5, 7, 8, 10, 11, 12, 13, 14]$$
$$\text{and} \quad \mathcal{P} = [13, 13, 3, 11, 23, 61, 97, 59, 47, 83, 193]$$

to construct the scheme

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15
97	13	23	11	3	13	61	3	11	23	97	59	47	83	13
59														
83														
47														.

Using a computer, we verify that $g(4,0,-3) \not< 15$. Hence, $g(4,0,-3) = 15$.

6.2. $z = 2$

In this case we use

$$H = [\widehat{4,7}, 5, 6, 8, 9, 11, 12, 13, 14, 16, 17]$$

$$\text{and} \quad \mathcal{P} = [11, 11, 5, 31, 59, 19, 29, 139, 41, 191, 251, 71]$$

to construct the scheme

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
139	191	59	11	5	31	20	11	19	5	59	31	139	41	11	191	71	19
41																	29
71																	

Using a computer, we verify that $g(4,0,-5) \not< 18$. Hence, $g(4,0,-5) = 18$.

6.3. $z = 4$

In this case we use

$$H = [\widehat{2,11}, \widehat{6,13}, 8, 10, 12, 14, 16, 17, 18, 19, 20, 21, 22, 26, 27, 28, 29, 30] \quad \text{and}$$

$$\mathcal{P} = [13, 13, 19, 19, 47, 83, 127, 179, 239, 17, 307, 43, 383, 53, 467, 659, 89, 59, 103, 883]$$

to construct the scheme

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18
883	59	659	103	467	383	307	239	179	127	83	47	19	53	13	43	13	17
17						89											

19	20	21	22	23	24	25	26	27	28	29	30	31	32	33	34	35
19	47	83	127	179	239	307	383	467	13	659	59	883	19	103	89	53
19						89										43.

We conclude that $g(4,0,-17) \leq 35$, but we are unable to verify that $g(4,0,-17) = 35$.

6.4. $z = 6$

In this case we use

$$H = [2, 3, 5, 6] \quad \text{and} \quad \mathcal{P} = [61, 7, 5, 29]$$

to construct the scheme

1	2	3	4	5	6	7	8
29	7	5	61	7	61	29	5.

Thus, $g(4, 0, -65) = 8$. □

7. The Case $\Delta = -q^k$

In this section we compute $g(a, b, c)$ when $\Delta = -q^k$, where q is an odd prime and $k \geq 1$ is an integer. We consider first the case when $q \geq 5$.

Theorem 7.1. *Let $q \geq 5$ be prime, and suppose that $\Delta = -q^k$ for some integer $k \geq 1$. Then $g(a, b, c) = 2$.*

Proof. First observe that $b \equiv 1 \pmod 2$ so that $b^2 \equiv 1 \pmod 8$. Next, note that if $k \equiv 0 \mod 2$ or $q \equiv 1 \pmod 8$, then

$$1 - 4ac \equiv \Delta = -q^k \equiv -1 \pmod 8,$$

which is impossible. Hence, $k \equiv 1 \pmod 2$ and $q \not\equiv 1 \pmod 8$.

Now, either $a \equiv 1 \pmod 2$ or $a \equiv 0 \pmod 2$. Assume first that $a \equiv 1 \pmod 2$. If $c \equiv 0 \pmod 2$, then $\Delta \equiv 1 \pmod 8$, and so $g(a, b, c) = 2$ by Lemma 4.5. Thus, assume that $c \equiv 1 \pmod 2$. Then $a \equiv b \equiv c \equiv 1 \pmod 2$, which implies that

$$-(q^k + a^2) = \Delta - a^2 \equiv -4 \pmod 8.$$

Hence,

$$q^k + a^2 = 4m, \tag{7.1}$$

for some $m \equiv 1 \pmod 2$, and so $q^k \equiv 3 \pmod 8$. Thus, $q \equiv 3 \pmod 8$ since $k \equiv 1 \pmod 2$. If $m = 1$, then $q = 3$, which we have excluded from consideration here. So, assume that $m \geq 3$. If there exists an odd prime p such that $m \equiv 0 \pmod p$ and $a \not\equiv 0 \pmod p$, then $g(a, b, c) = 2$ by Lemma 4.2. Thus, suppose for every odd prime p with

$$\Delta - a^2 = -(q^k + a^2) \equiv 0 \pmod p,$$

we have that $a \equiv 0 \pmod p$. It follows that $p = q$. Hence, since $q > 3$, and $q^k + a^2 \equiv 4 \pmod 8$, we can write

$$q^k + a^2 = 4 \cdot q^u, \tag{7.2}$$

for some integer $u \geq 1$.

If $u > k$, then

$$a^2 = q^k \left(4 \cdot q^{u-k} - 1\right),$$

which implies that q^k is a square since $\gcd(q^k, 4 \cdot q^{u-k} - 1) = 1$. But this is impossible since k is odd.

If $u \leq k$, then

$$a^2 = q^u \left(4 - q^{k-u}\right),$$

which implies that $u = k$ since $q > 3$. But then $a^2 = 3 \cdot q^k$, which is impossible since $q > 3$, and the proof is complete when a is odd.

Now assume that $a \equiv 0 \pmod 2$. Then $\Delta - a^2 \equiv 1 \pmod 2$ and if $\Delta - a^2 \equiv 0 \pmod p$, for some odd prime p with $a \not\equiv 0 \pmod p$, then $g(a, b, c) = 2$ by Lemma 4.2. If

$$a \equiv 0 \equiv \Delta - a^2 \pmod p,$$

for some odd prime p, then $p = q$ since

$$\Delta - a^2 = -(q^k + a^2).$$

Therefore, since $\Delta - a^2 \equiv 1 \pmod 2$, it follows that

$$q^k + a^2 = q^u, \tag{7.3}$$

for some integer $u \geq 1$. Note that $k < u$ in (7.3). Thus,

$$a^2 = q^k(q^{u-k} - 1),$$

which implies that q^k is a square since $\gcd(q^k, q^{u-k} - 1) = 1$. But q^k cannot be a square since $k \equiv 1 \pmod 2$, which completes the proof of the theorem. □

It turns out that the case of $q = 3$ not covered in Theorem 7.1 is the most interesting case, and we address this case in the next theorem.

Theorem 7.2. *If $\Delta = -3^k$, for some integer $k \geq 1$, then*

$$g(a, b, c) = \begin{cases} 6 & \text{if} \quad a = 3^{(k-1)/2} \\ 8 & \text{if} \quad a = 3^{(k+1)/2} \\ 2 & \text{otherwise.} \end{cases}$$

Proof. Note that if $a = 1$ and $\Delta = -3$, then this case is covered in Theorem 5.1. So we assume that $a > 1$. As in the proof of Theorem 7.1, we see that $b^2 \equiv 1 \pmod 8$ and $k \equiv 1 \pmod 2$.

Assume first that $a \equiv 1 \pmod 2$ so that $a \equiv b \equiv c \equiv 1 \pmod 2$. If there exists an odd prime p such that $a \not\equiv 0 \pmod p$ and $\Delta - a^2 \equiv 0 \pmod p$, then $g(a, b, c) = 2$ by Lemma 4.2. So, assume for every odd prime p with

$$\Delta - a^2 = -(3^k + a^2) \equiv 0 \pmod p,$$

we have that $a \equiv 0 \pmod{p}$. It follows that $p = 3$, and since $3^k + a^2 \equiv 4 \pmod{8}$, we can write

$$3^k + a^2 = 4 \cdot 3^u, \tag{7.4}$$

for some integer $u \geq 1$.

If $k < u$, then

$$a^2 = 3^k \left(4 \cdot 3^{u-k} - 1\right),$$

which implies that 3^k is a square since $\gcd(3^k, 4 \cdot 3^{u-k} - 1) = 1$. But this is impossible since k is odd.

If $k \geq u$, then

$$a^2 = 3^u \left(4 - 3^{k-u}\right),$$

which implies that $k - u \in \{0, 1\}$, and therefore

$$a = \begin{cases} 3^{(k-1)/2} & \text{if } u = k-1 \\ 3^{(k+1)/2} & \text{if } u = k. \end{cases} \tag{7.5}$$

Since $u \geq 1$, we have that

$$a \equiv 0 \equiv -(3^k + a^2) = b^2 - 4ac - a^2 \pmod{3},$$

and thus $b \equiv 0 \pmod{3}$. If $c \equiv 0 \pmod{3}$, then $\gcd(a, b, c) \equiv 0 \pmod{3}$ and $g(a, b, c) = 2$. So, assume that $c \not\equiv 0 \pmod{3}$.

Consider the first case in (7.5). Then

$$\left(\frac{-3^k}{p}\right) = \left(\frac{3^{k-1}}{p}\right)\left(\frac{-3}{p}\right) = \left(\frac{-3}{p}\right) \neq -1,$$

for each prime $p \in \{7, 19\}$. Thus, $z = 3^{(k-1)/2}\hat{z}$ is a square root of Δ, where $\hat{z}$ is a square root of -3 modulo p. This implies that any scheme we develop for $\Delta = -3$ can be applied to the general case $\Delta = -3^k$. When $p = 7$, we choose $\hat{z} \equiv 2 \pmod{7}$, and when $p = 19$, we choose $\hat{z} \equiv 4 \pmod{19}$. Since $a^{-1}z \equiv \hat{z} \pmod{p}$ in each of these cases, we have $r = 2, 4 \in H$ by (3) of Lemma 4.1. By (2) of Lemma 4.1, we also have that $r = 3 \in H$ corresponding to $p = 3$. Thus, $H = [2, 3, 4]$ and $\mathcal{P} = [7, 3, 19]$, and we get the scheme

1	2	3	4	5	6
19	7	3	7	19	3.

Hence, $g(a, b, c) \leq 6$. To see that $g(a, b, c) = 6$, we first note that the factorization of $t_r = \Delta - a^2r^2$ for $r \in \{1, 2, 3, 4\}$ is

r	Factorization of t_r
1	$-2^2 \cdot 3^{k-1}$
2	$-3^{k-1} \cdot 7$
3	$-2^2 \cdot 3^k$
4	$-3^{k-1} \cdot 19.$

Hence, we deduce from (3) of Lemma 4.8 that $g(a, b, c) = 6$.

Now consider the case $a = 3^{(k+1)/2}$ from (7.5). Suppose first that $u = k = 1$, so that $a = 3$. Consider the scheme

$$\begin{array}{cccccccc} 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 \\ \hline 109 & 7 & 5 & 13 & 7 & 13 & 109 & 5 \end{array} \tag{7.6}$$

with $H = [2, 3, 5, 6]$ and $\mathcal{P} = [13, 7, 19, 109]$. Note that $\left(\frac{-3}{p}\right) = 1$ for each prime $p \in \mathcal{P}$, and choose the square root $\widehat{z}_p$ of -3 modulo p as follows:

p	13	7	19	109
$\hat{z}$	6	2	15	18.

Then let $\widehat{r}_p$ be the corresponding value of r using (3) in Lemma 4.1. The scheme (7.6) can be applied to the general case, $a = 3^{(k+1)/2}$ with $k \geq 1$, since, as before,

$$\left(\frac{-3^k}{p}\right) = \left(\frac{-3}{p}\right) \neq -1.$$

Let z_p be a square root of -3^k modulo p, and let r_p be the corresponding value of r. Then, in the general case, we have

$$r_p \equiv a^{-1} z_p \equiv 3^{-(k+1)/2} z_p \equiv 3^{-(k+1)/2} 3^{(k-1)/2} \widehat{z}_p \equiv 3^{-1} \widehat{z}_p \equiv \widehat{r}_p \pmod{p}.$$

Thus, we have shown that $g(a, b, c) \leq 8$. To show that $g(a, b, c) = 8$, we fist note that the factorization of $t_r = \Delta - a^2 r^2$ for $r \in \{1, 2, 3, 4, 5, 6\}$ is

r	Factorization of t_r
1	$-2^2 \cdot 3^k$
2	$-3^k \cdot 13$
3	$-2^2 \cdot 3^k \cdot 7$
4	$-3^k \cdot 7^2$
5	$-2^2 \cdot 3^k \cdot 19$
6	$-3^k \cdot 109.$

Then an argument similar to the one used in the proof of (3) of Lemma 4.8 can be used to complete the proof. We omit the details.

In the case of $a \equiv 0 \pmod{2}$, the same argument used in the proof of Theorem 7.1 when $a \equiv 0 \pmod{2}$ applies here as well. Thus, $g(a, b, c) = 2$ in this case, which completes the proof of the theorem. □

8. Comments, Conclusions, and Conjectures

One question that we did not address in this article up to this point is whether or not $g(a, b, c)$ always exists. The answer to this question in general depends on the availability of "enough" odd prime divisors of the terms of the quadratic sequence $\{t_r\}$ defined in (4.3). Since we can only use the same prime more than once in very special situations, we are prompted to define the concept of a primitive divisor. A *primitive divisor* of t_r is an odd prime p such that $t_r \equiv 0 \pmod p$ and $t_i \not\equiv 0 \pmod p$ for all $i < r$. This idea is not new, and in fact, primitive divisors have been studied extensively for various sequences by many authors. For a good history of these studies and a comprehensive bibliography, see [9]. The monumental paper of Bilu, Hanrot and Voutier [2] settled this question for all Lucas and Lehmer sequences by showing that all terms beyond $n = 30$ of all such sequences have a primitive divisor. However, for quadratic sequences this subject, for the most part, remains a mystery. Everest and Harman [8] have investigated the existence of primitive divisors for the sequence $Q := \{n^2 + b\}$. Unfortunately, unlike the situation for Lucas and Lehmer sequences, they showed, using a result of Schinzel [24], that there are infinitely many terms of Q that do not have primitive divisors. Everest and Harman also showed that if $-b$ is not a square, then

$$.5324 < \frac{\rho_b(x)}{x} < 0.905,$$

for all sufficiently large x, where

$$\rho_b(x) = \left| \left\{ n \leq x \;\middle|\; n^2 + b \quad \text{has a primitive divisor} \right\} \right|.$$

While these results are certainly interesting, they do not seem strong enough alone to guarantee the existence of $g(a, b, c)$ in every case. Nevertheless, based on computer evidence, we conjecture that $g(a, b, c)$ always exists, and moreover that

$$g(a, b, c) \leq g(4, 0, -17) \leq 35.$$

Additional evidence to support the existence of $g(a, b, c)$ is that, for fixed a, b and c with $\Delta \neq 0$, the Diophantine equations $t_r = \pm 2^u$ in the variables r and u have only finitely many solutions [24]. Furthermore, in the case $t_r = -2^u$ with Δ odd, all the solutions are known. This fact follows from the combined efforts of Beukers and Le [1, 13, 14].

References

[1] F. Beukers, *On the generalized Ramanujan-Nagell equation I*, Acta Arith. **38** (1980/1981), 389-410.

[2] Y. Bilu, G. Hanrot, and P.M. Voutier, *Existence of primitive divisors of Lucas and Lehmer numbers, with an appendix by M. Mignotte*, J. Reine Angew. Math. **539** (2001), 75–122.

[3] A. T. Brauer, *On a property of k consecutive integers*, Bull. Amer. Math. Soc., **47** (1941), 328–331.

[4] Y. Caro, *On a division property of consecutive integers*, Israel J. Math., **33** (1979), No. 1, 32–36.

[5] P. Erdős, *On the difference of Consecutive primes*, Quarterly Journal of Mathematics, **6** (1935), 124–128.

[6] R. J. Evans, *On blocks of N consecutive integers*, Amer. Math. Monthly, **76** (1969), No. 1, 48–49.

[7] R. Evans, *On N consecutive integers in an arithmetic progression*, Acta Sci. Math. (Szeged), **33** (1972), 295–296.

[8] G. Everest and G. Harman, *On primitive divisors of n^2+b*, Number theory and polynomials, 142-154, London Math. Soc. Lecture Note Ser., **352**, Cambridge Univ. Press, Cambridge, 2008.

[9] G. Everest, A. van der Poorten, I. Shparlinski and T. Ward, *Recurrence Sequences*, **104**, American Mathematical Society, (2003).

[10] I. Gassko, *Stapled sequences and stapling coverings of natural numbers*, Electron. J. Combin., **3** (1996), No.1, #R 33, 20 pp.

[11] L. Hajdu and N. Saradha, *On a problem of Pillai and its generalizations*, Acta Arith. **144** (2010), no. 4, 323-347.

[12] L. Hajdu and M. Szikszai, *On the GCD-s of k consecutive terms of Lucas sequences*, J. Number Theory **132** (2012), no. 12, 3056-3069.

[13] M. Le, *On the number of solutions of the generalized Ramanujan-Nagell equation $x^2 - D = 2^{n+2}$*, Acta Arith. **60** (1991), 149-167.

[14] M. Le, *On the generalized Ramanujan-Nagell equation $x^2 - D = 2^{n+2}$*, Trans. Amer. Math. Soc.**334** (1992), 809-825.

[15] P. Mihăilescu, *Primary cyclotomic units and a proof of Catalan's conjecture*, J. Reine Angew. Math. 572 (2004), 167-195.

[16] M. Ohtomo and F. Tamari, *On relative prime number in a sequence of positive integers*, Experimental design and related combinatorics. J. Statist. Plann. Inference **106** (2002), no. 1–2, 509-515.

[17] S. S. Pillai, *On M consecutive integers - I*, Proc. Indian Acad. Sci., Sect. A, **11** (1940), 6–12.

[18] S. S. Pillai, *On M consecutive integers - II*, Proc. Indian Acad. Sci., Sect. A, **11** (1940), 73–80.

[19] S. S. Pillai, *On M consecutive integers - III*, Proc. Indian Acad. Sci., Sect. A, **13** (1941), 530–533.

[20] S. S. Pillai, *On M consecutive integers - IV*, Bull. Calcutta Math. Soc., **36** (1944), 99–101.

[21] J. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math., **6** (1962), 64–94.

[22] N. Saradha and R. Thangadurai, *Pillai's problem on consecutive integers*, Number theory and applications, 175-188, Hindustan Book Agency, New Delhi, 2009.

[23] A. Schinzel, *On two theorems of Gelfond and some of their applications*, Acta Arith. **13** (1978), 177-236.

[24] C. L. Siegel, *Approximation algebraischer Zahlen*, Math. Zeit. **10** (1921), 173–213.