

BOUNDS ON THE NUMBER OF SQUARES IN RECURRENCE SEQUENCES

PAUL M VOUTIER

ABSTRACT. We investigate the number of squares in a very broad family of binary recurrence sequences with $u_0 = 1$. We show that there are at most two distinct squares in such sequences (the best possible result), except under very special conditions where we prove there are at most three such squares.

1. INTRODUCTION

1.1. Background. The study of the arithmetic properties of recurrence sequences has a long history. Important problems include the open question of whether there are infinitely many primes in such sequences, lower bounds for the largest prime divisor of the n -th element [14], the zero-multiplicity of such sequences (how often zero occurs as an element) [11] and also the occurrence of powers in them [5].

While some progress on arithmetic questions has been achieved for sequences of Lucas numbers (numbers of the form $u_n = (\alpha^n - \beta^n) / (\alpha - \beta)$, where α and β are algebraic numbers such that $\alpha + \beta$ and $\alpha\beta$ are non-zero coprime rational numbers and α/β is not a root of unity) and their associated sequences ($v_n = \alpha^n + \beta^n$), much less is known for other binary recurrence sequences.

As with sequences of Lucas numbers, other binary recurrence sequences are connected with the solutions of Diophantine equations such as $aX^2 - bY^4 = c$. Such equations are important in their own right, and also as quartic models of elliptic curves.

This paper is concerned with such problems, in particular how many distinct squares can occur in non-degenerate binary recurrence sequences.

1.2. Notation. To define the sequences we are interested in and to express our results, we start with some notation.

Let a , b and d be positive integers such that d is not a square. Suppose $\alpha = a + b^2\sqrt{d}$ has $N_\alpha = N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha) = a^2 - b^4d$ and let $\varepsilon = (t + u\sqrt{d})/2$ be a unit in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ with t and u positive integers.

We define the two sequences $(x_k)_{k=-\infty}^\infty$ and $(y_k)_{k=-\infty}^\infty$ by

$$(1.1) \quad x_k + y_k\sqrt{d} = \alpha\varepsilon^{2k}.$$

Observe that $x_0 = a$, $y_0 = b^2$,

$$(1.2) \quad y_1 = \frac{b^2(t^2 + du^2) + 2atu}{4}, \quad y_{-1} = \frac{b^2(t^2 + du^2) - 2atu}{4}$$

Key words and phrases. binary recurrence sequences; Diophantine approximations.

and that both sequences satisfy the recurrence relation

$$(1.3) \quad u_{k+1} = \frac{t^2 + du^2}{2} u_k - u_{k-1},$$

for all $k \in \mathbb{Z}$. Note that $(t^2 + du^2)/2 = \text{Tr}_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\varepsilon^2)$.

To relate such sequences back to the quartic equations mentioned in the previous section, observe that from (1.1),

$$x_k^2 - dy_k^2 = N_\alpha.$$

We restrict to the coefficient of \sqrt{d} in α being a square since here we are interested in squares in the sequence of y_k 's. For such problems, we will choose α such that b^2 is the smallest square among the y_k 's.

For any non-zero integer, n , let $\text{sf}(n)$ be the unique squarefree integer such that $n/\text{sf}(n)$ is a square. We will put $\text{sf}(1) = 1$.

1.3. Conjectures. We start with some conjectures regarding squares in the sequence of y_k 's. The dependence on the arithmetic of N_α is noteworthy.

Conjecture 1.1. *There are at most four distinct integer squares among the y_k 's.*

If $\text{sf}(|N_\alpha|) = 2^\ell p^m$ where $\ell, m \in \{0, 1\}$ with $\ell + m \geq 1$ and p is an odd prime, then there are at most three distinct integer squares among the y_k 's.

Furthermore, if $|N_\alpha|$ is a perfect square, then there are at most two distinct integer squares among the y_k 's.

When $N_\alpha < 0$ and $b = 1$, a stronger result appears to hold.

Conjecture 1.2. *Suppose that $b = 1$ and $N_\alpha < 0$. There are at most three distinct integer squares among the y_k 's.*

If $-N_\alpha$ is a perfect square, then there are at most two distinct integer squares among the y_k 's.

In fact, a more general result than Conjecture 1.1 also appears to be true.

Conjecture 1.3. *Let $(y_k)_{k=-\infty}^\infty$ be the sequence formed by replacing ε^{2k} in (1.1) with ε^k .*

There are at most four distinct integer squares among the y_k 's.

If $|N_\alpha|$ is a prime power or a perfect square, then there are at most three distinct integer squares among the y_k 's.

Examples showing that if these conjectures are true, then they are best possible are provided in Subsections 6.1, 6.2 and 6.3.

We used PARI/GP [10] to search for squares among y_{-80}, \dots, y_{80} from Conjecture 1.3, where $\varepsilon = (t + u\sqrt{d})/2 > 1$ is the fundamental unit in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ with $t, u \in \mathbb{Z}$ and $u \leq 10^{30}$. Note that this also includes searching among y_{-40}, \dots, y_{40} from Conjectures 1.1 and 1.2. The range of b and d in this search was $1 \leq b \leq 2000$ and $1 \leq d \leq 1000$ with d squarefree. For a , we searched over two ranges: (1) $\max(1, \lfloor \sqrt{db^4} \rfloor - 1000) \leq a \leq \lceil \sqrt{db^4} \rceil + 1000$ (so $|N_\alpha|$ is small) and (2) $1 \leq a \leq 2000$. For both ranges of a , we considered only $\gcd(a, b^2)$ squarefree. The search across these ranges took just under 319 hours on a Windows 11 laptop with an Intel i7-13700H 2.40 GHz processor and 32 GB of RAM. No counterexamples to any of these conjectures were found in this search.

Remark. The distinctness condition in these conjectures, and in our results below, is important, as such sequences can have repeated elements. E.g., $(a, b, d, t, u) = (42, 4, 7, 16, 6)$ where $y_{-k} = y_{k-1}$ for all $k \geq 1$. But this can only happen when α divided by its algebraic conjugate is a unit in the ring of integers.

1.4. Results. In this paper, we prove Conjecture 1.2 when $-N_\alpha$ is a square, except for a very limited set of sequences, where we prove a slightly weaker result.

Theorem 1.4. *Let $b = 1$, a and d be positive integers, where d is not a square, $N_\alpha < 0$ and $-N_\alpha$ is a square.*

- (a) *If $u = 1$, $t^2 - du^2 = -4$, $N_\alpha \equiv 12 \pmod{16}$, $\gcd(a^2, d) = 1, 4$ and one of $y_{\pm 1}$ is a perfect square, then there are at most three distinct squares among the y_k 's.*
- (b) *If $u = 2$, $t^2 - du^2 = -4$, N_α is odd, $\gcd(a^2, d) = 1$ and one of $y_{\pm 1}$ is a perfect square, then there are at most three distinct squares among the y_k 's.*
- (c) *Otherwise, there are at most two distinct squares among the y_k 's.*

In Subsection 6.4, we present an infinite family of examples of sequences satisfying the conditions in part (a) with y_1 roughly one-tenth the size of the bounds in Proposition 4.1. The same is possible for y_{-1} in part (a) and $y_{\pm 1}$ in part (b).

1.5. Our method of proof. Our proof has its basis in the work of Siegel [13] (also see [7]). Foremost with our use of hypergeometric functions. But also with how we use them here. The definition and use of our quantity r_0 in Section 4 has similarities to the definition and use of ℓ_1 and ℓ_2 from Lemma 7 onwards in [7]. The idea is to treat ranges of hypothetical squares beyond those that can be treated by our gap principle alone.

We state and prove our results in Section 3 more generally than required here. This is because they will be useful in further work on binary recurrence sequences. An example is [18] where we prove Conjecture 1.2 when N_α is a prime power.

1.6. Structure of this article. Section 2 contains results on diophantine approximation, with a focus on the use of hypergeometric functions to do so. In Section 3, we collect various facts that we will require about elements of the sequence $(y_k)_{k=-\infty}^\infty$ defined by (1.1). These two sections are independent of each other. Their results are brought together in Section 4, where we state and prove Proposition 4.1. Our theorem follows from this proposition. Its proof is given in Section 5. Finally, in Section 6, we give examples showing that our results and conjectures are best possible.

1.7. Acknowledgements. The author deeply appreciates all the time and effort spent by Mihai Cipu, very carefully reading an earlier version of this work. His extensive comments, questions and our follow-up discussions led to significant improvements in the presentation of this work, as well as numerous corrections. The author is also grateful to the referee for their notes and suggestions, which improved this paper too.

2. DIOPHANTINE APPROXIMATION VIA HYPERGEOMETRIC FUNCTIONS

Recall that by an *effective irrational measure* for an irrational number, α , we mean an inequality of the form

$$\left| \alpha - \frac{p}{q} \right| > \frac{c}{|q|^\mu},$$

for all $p/q \in \mathbb{Q}$ with $\gcd(p, q) = 1$ and $|q| > Q$, where c , Q and μ are all effectively computable.

By Liouville's famous result [8], where he constructed the first examples of numbers proven to be transcendental, we have such effective irrational measures for algebraic numbers of degree n , with $\mu = n$. But for practically all applications we require $\mu < n$.

We can sometimes use the hypergeometric method to obtain effective irrationality measures that improve on Liouville's result for the algebraic numbers that arise here. This was first done by Baker [2, 3] building on earlier applications of hypergeometric functions to diophantine approximation such as those of Siegel [12]. However, that does not suffice for us to prove our results here. The problem here arises not because of the exponent, μ , in the effective irrationality measure, but because the constant, c , is too small. Upon investigating this further, we found that we can complete the proof of our results if we use not the effective irrationality measures from the hypergeometric method, but rather consider more carefully the actual results that we obtain from the use of hypergeometric functions.

The means of doing so is the following lemma.

Lemma 2.1. *Let $\theta \in \mathbb{C}$ and let \mathbb{K} be an imaginary quadratic field. Suppose that there exist $k_0, \ell_0 > 0$ and $E, Q > 1$ such that for all non-negative integers r , there are algebraic integers p_r and q_r in \mathbb{K} with $|q_r| < k_0 Q^r$ and $|q_r \theta - p_r| \leq \ell_0 E^{-r}$ satisfying $p_r q_{r+1} \neq p_{r+1} q_r$.*

For any algebraic integers p and q in \mathbb{K} , let r_0 be the smallest positive integer such that $(Q - 1/E) \ell_0 |q| / (Q - 1) < c E^{r_0}$, where $0 < c < 1$.

(a) *We have*

$$|q\theta - p| > \frac{1 - c/E}{k_0 Q^{r_0+1}}.$$

(b) *When $p/q \neq p_{r_0}/q_{r_0}$, we have*

$$|q\theta - p| > \frac{1 - c}{k_0 Q^{r_0}}.$$

Remark. This is a modification of Lemma 6.1 of [15] (and other similar results).

First, we replace $1/(2k_0)$ in both parts and define r_0 somewhat differently too.

Second, the terms in the lower bounds in both parts are no longer converted into ones involving $|q|^{-(\kappa+1)}$. For our use here, where an effective irrationality measure is not required, this results in further improvements.

Proof. Let p, q be algebraic integers in \mathbb{K} . Let $R = q\theta - p$ and $R_r = q_r \theta - p_r$. We can write

$$q_r R = q_r q \theta - q_r p = q(q_r \theta - p_r) + p_r q - q_r p = q R_r + p_r q - q_r p.$$

We consider two cases according to whether $p_{r_0} q - q_{r_0} p = 0$ or not.

If $p_r q - q_r p \neq 0$, then $|p_r q - q_r p| \geq 1$, since it is an algebraic integer in an imaginary quadratic field. From our upper bounds for $|q_r|$ and $|q_r \theta - p_r|$ in the statement of the lemma, we have

$$k_0 Q^r |R| > 1 - \ell_0 E^{-r} |q|.$$

With $r = r_0$, from the definition of r_0 , we have

$$k_0 Q^{r_0} |R| > 1 - c \frac{Q - 1}{Q - 1/E} > 1 - c.$$

Part (b) now follows from the upper bound for $|q_{r_0}|$ in the statement of the lemma.

If $p_{r_0}q - q_{r_0}p = 0$, then we use $r = r_0 + 1$. From the definition of r_0 , we have

$$k_0 Q^{r_0+1} |R| > 1 - c \frac{Q-1}{E(Q-1/E)} = \frac{QE-1-cQ+c}{QE-1} > 1 - c/E.$$

Part (a) now follows. \square

2.1. Construction of Approximations. Let t' , u_1 and u_2 be rational integers with $t' < 0$ ¹ such that $u = (u_1 + u_2\sqrt{t'})/2$ be an algebraic integer in $\mathbb{K} = \mathbb{Q}(\sqrt{t'})$ with $\sigma(u) = (u_1 - u_2\sqrt{t'})/2$ as its algebraic (and complex) conjugate. Put $\omega = u/\sigma(u)$ and write $\omega = e^{i\varphi}$, where $-\pi < \varphi \leq \pi$. For any real number ν , we shall put $\omega^\nu = e^{i\nu\varphi}$ – unless otherwise stated, we will use this convention throughout this paper.

Suppose that α , β and γ are complex numbers and γ is not a non-positive integer. We denote by ${}_2F_1(\alpha, \beta, \gamma, z)$ the classical (or Gauss) hypergeometric function of the complex variable z .

For integers m and n with $0 < m < n$, $(m, n) = 1$ and r a non-negative integer, put $\nu = m/n$ and

$$X_{m,n,r}(z) = {}_2F_1(-r-\nu, -r, 1-\nu, z), \quad Y_{m,n,r}(z) = z^r X_{m,n,r}(z^{-1})$$

and

$$R_{m,n,r}(z) = (z-1)^{2r+1} \frac{\nu \cdots (r+\nu)}{(r+1) \cdots (2r+1)} {}_2F_1(r+1-\nu, r+1; 2r+2; 1-z).$$

We collect here some facts about these functions that we will require.

Lemma 2.2. (a) Suppose that $|\omega - 1| < 1$. We have

$$\omega^\nu Y_{m,n,r}(\omega) - X_{m,n,r}(\omega) = R_{m,n,r}(\omega).$$

(b) We have

$$X_{m,n,r}(\omega) Y_{m,n,r+1}(\omega) \neq X_{m,n,r+1}(\omega) Y_{m,n,r}(\omega).$$

(c) If $|\omega| = 1$ and $|\omega - 1| < 1$, then

$$|R_{m,n,r}(\omega)| \leq \frac{\Gamma(r+1+\nu)}{r!\Gamma(\nu)} |\varphi| |1 - \sqrt{\omega}|^{2r}.$$

(d) If $|\omega| = 1$ and $|\omega - 1| < 1$, then

$$|X_{m,n,r}(\omega)| = |Y_{m,n,r}(\omega)| < 1.072 \frac{r!\Gamma(1-\nu)}{\Gamma(r+1-\nu)} |1 + \sqrt{\omega}|^{2r}.$$

(e) For $|\omega| = 1$ and $\operatorname{Re}(\omega) \geq 0$, we have

$$|{}_2F_1(r+1-\nu, r+1; 2r+2; 1-\omega)| \geq 1,$$

with the minimum value occurring at $\omega = 1$.

Proof. Part (a) is established in the proof of Lemma 2.3 of [6].

Part (b) is Lemma 4 of [3].

Part (c) is Lemma 2.5 of [6].

Part (d) is Lemma 4 of [17].

Part (e) is Lemma 5 of [17]. \square

¹To avoid confusion with t in the expression for ε , we use t' here to denote what was t in our previous works like [16]. Similarly, we will use d' where d was used in previous works.

We let $D_{n,r}$ denote the smallest positive integer such that $D_{n,r}X_{m,n,r}(x) \in \mathbb{Z}[x]$ for all m as above. For $d' \in \mathbb{Z}$, we define $N_{d',n,r}$ to be the largest integer such that $(D_{n,r}/N_{d',n,r})X_{m,n,r}(1 - \sqrt{d'}x) \in \mathbb{Z}[\sqrt{d'}][x]$, again for all m as above. We will use $v_p(x)$ to denote the largest power of a prime p which divides the rational number x . We put

$$(2.1) \quad \mathcal{N}_{d',n} = \prod_{p|n} p^{\min(v_p(d')/2, v_p(n)+1/(p-1))}.$$

In what follows, we shall restrict our attention to $m = 1$ and $n = 4$, so $\nu = 1/4$.

Lemma 2.3. (a) *We have*

$$(2.2) \quad \frac{\Gamma(3/4)r!}{\Gamma(r+3/4)} \frac{D_{4,r}}{N_{d',4,r}} < \mathcal{C}_{4,1} \left(\frac{\mathcal{D}_4}{\mathcal{N}_{d',4}} \right)^r \quad \text{and} \quad \frac{\Gamma(r+5/4)}{\Gamma(1/4)r!} \frac{D_{4,r}}{N_{d',4,r}} < \mathcal{C}_{4,2} \left(\frac{\mathcal{D}_4}{\mathcal{N}_{d',4}} \right)^r$$

for all non-negative integers r , where $\mathcal{C}_{4,1} = 0.83$, $\mathcal{C}_{4,2} = 0.2$ and $\mathcal{D}_4 = e^{1.68}$.

(b) *For any positive integer, r , we have*

$$(2.3) \quad \frac{5}{24 \cdot 4^r r^{1/4}} \leq \frac{(1/4) \cdots (r+1/4)}{(r+1) \cdots (2r+1)} \quad \text{and} \quad \frac{r! \Gamma(3/4)}{\Gamma(r+3/4)} \leq 4r^{1/4}/3.$$

Proof. (a) From Lemma 7.4(c) of [15], we have

$$\max \left(1, \frac{\Gamma(3/4)r!}{\Gamma(r+3/4)}, 4 \frac{\Gamma(r+5/4)}{\Gamma(1/4)r!} \right) \frac{D_{4,r}}{N_{d',4,r}} < 100 \left(\frac{e^{1.64}}{\mathcal{N}_{d',4}} \right)^r$$

However, the value 100 in this inequality results in us requiring a lot of computation to complete the proof of our results here (in particular, Proposition 4.1). Therefore, we seek a smaller value at the expense of replacing 1.64 by a larger value, whose value has less of an impact on our proof. For $r \geq 156$, we have $100 \exp(1.64r) < 0.2 \exp(1.68r)$, so we compute directly the left-hand sides of (2.2) for $r \leq 155$. We find that the maximum values of the left-hand sides of (2.2) divided by $\exp(1.68r)$ both occur for $r = 3$. Part (a) follows.

(b) We prove both of these by induction. A quick calculation shows that we have equality in both cases for $r = 1$. Then we take the expression for $r+1$ and divide it by the expression for r . For the first inequality, this ratio is $(1/4)(r+5/4)/(r+3/2)$, so the inequality will hold if $(r+5/4)/(r+3/2) > (r/(r+1))^{1/4}$. We take the fourth-power of both sides and subtract them, this gives us

$$\frac{224r^3 + 944r^2 + 1329r + 625}{16(2r+3)^4(r+1)},$$

which is clearly positive for $r \geq 1$. Since both $(r+5/4)/(r+3/2)$ and $(r/(r+1))^{1/4}$ are positive real numbers for $r \geq 1$, the required inequality holds.

We proceed in the very same way to prove the second inequality. □

As in [16, Theorem 1], put

$$\begin{aligned}
(2.4) \quad & g_1 = \gcd(u_1, u_2), \\
& g_2 = \gcd(u_1/g_1, t'), \\
& g_3 = \begin{cases} 1 & \text{if } t' \equiv 1 \pmod{4} \text{ and } (u_1 - u_2)/g_1 \equiv 0 \pmod{2}, \\ 2 & \text{if } t' \equiv 3 \pmod{4} \text{ and } (u_1 - u_2)/g_1 \equiv 0 \pmod{2}, \\ 4 & \text{otherwise,} \end{cases} \\
& g = g_1 \sqrt{g_2/g_3}.
\end{aligned}$$

Then we can put

$$\begin{aligned}
(2.5) \quad & p_r = \frac{D_{4,r}}{N_{d',4,r}} \left(\frac{u_1 - u_2 \sqrt{t'}}{2g} \right)^r X_{1,4,r}(\omega), \\
& q_r = \frac{D_{4,r}}{N_{d',4,r}} \left(\frac{u_1 - u_2 \sqrt{t'}}{2g} \right)^r Y_{1,4,r}(\omega) \quad \text{and} \\
& R_r = \frac{D_{4,r}}{N_{d',4,r}} \left(\frac{u_1 - u_2 \sqrt{t'}}{2g} \right)^r R_{1,4,r}(\omega),
\end{aligned}$$

where

$$(2.6) \quad d' = (u - \sigma(u))^2 / g^2 = u_2^2 t' / g^2.$$

From Lemma 2.2(a), we have

$$q_r \omega^{1/4} - p_r = R_r.$$

By the definitions of $D_{4,r}$ and $N_{d',4,r}$, we see that $X_{1,4,r}(1-z)$ is a polynomial of degree r with coefficients in $\mathbb{Z}[\sqrt{d'}]$ and

$$\begin{aligned}
p_r &= \frac{D_{4,r}}{N_{d',4,r}} \left(\frac{u_1 - u_2 \sqrt{t'}}{2g} \right)^r X_{1,4,r}(\omega) \\
&= \frac{D_{4,r}}{N_{d',4,r}} \left(\frac{u_1 - u_2 \sqrt{t'}}{2g} \right)^r X_{1,4,r} \left(1 - u_2 \sqrt{t'} \frac{-2}{u_1 - u_2 \sqrt{t'}} \right).
\end{aligned}$$

Since $d' = u_2^2 t' / g^2$ and $(u_1 - u_2 \sqrt{t'}) / (2g)$ is an algebraic integer, it follows that p_r is an algebraic integer in $\mathbb{Q}(\sqrt{t'})$. The analogous expression for q_r shows that it is also an algebraic integer.

So by applying these quantities, with Lemma 2.2(d) and Lemma 2.3(a), in Lemma 2.1, we can take

$$(2.7) \quad Q = \frac{\mathcal{D}_4 \left| |u_1| + \sqrt{u_1^2 - t' u_2^2} \right|}{|g| \mathcal{N}_{d',4}}$$

and

$$(2.8) \quad k_0 < 1.072 \mathcal{C}_{4,1} < 0.89.$$

Using Lemma 2.2(c) instead of Lemma 2.2(d), we also have

$$(2.9) \quad E = \frac{|g|\mathcal{N}_{d',4} \left| |u_1| + \sqrt{u_1^2 - t'u_2^2} \right|}{\mathcal{D}_4 u_2^2 |t'|}$$

and

$$(2.10) \quad \ell_0 = \mathcal{C}_{4,2}|\varphi| = 0.2|\varphi|.$$

3. LEMMAS ABOUT $(x_k)_{k=-\infty}^{\infty}$ AND $(y_k)_{k=-\infty}^{\infty}$

3.1. Representation Proposition. The proposition in this section plays a crucial role in this work. It is the expression for $f^2(x + N_\varepsilon \sqrt{N_\alpha})$ in this proposition that permits us to use the hypergeometric method described in the previous section. For this reason, we call it our representation proposition.

It is also because we have ε^2 , rather than ε , in (3.1) that we use ε^{2k} in (1.1).

For any non-zero integer, n , we let $\text{rad}(n)$ be the product of all distinct prime divisors of n . We will put $\text{rad}(\pm 1) = 1$.

Proposition 3.1. *Let $a \neq 0$, $b > 0$ and d be rational integers such that d is not a square. Put $\alpha = a + b^2 \sqrt{d}$ and denote $N_{\mathbb{Q}(\sqrt{d})/\mathbb{Q}}(\alpha)$ by N_α . Suppose that N_α is not a square, $x \neq 0$ and $y > 0$ are rational integers with*

$$(3.1) \quad x + y^2 \sqrt{d} = \alpha \varepsilon^2,$$

where $\varepsilon = (t + u\sqrt{d})/2 \in \mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ with t and u non-zero rational integers, norm N_ε .

(a) We can write

$$(3.2) \quad \begin{aligned} f^2(x + N_\varepsilon \sqrt{N_\alpha}) &= (a + \sqrt{N_\alpha}) (r + s \sqrt{\text{sf}(N_\alpha)})^4 \quad \text{and} \\ f y &= b(r^2 - \text{sf}(N_\alpha) s^2), \end{aligned}$$

for some integers f , r and s satisfying $f \neq 0$,

$$f \mid (4b^2 \text{rad}(f' \gcd(uN_\alpha / \text{sf}(N_\alpha), N_\varepsilon))),$$

where $f' \mid \text{sf}(N_\alpha)$ and $0 < f' < \max(2, \sqrt{|\text{sf}(N_\alpha)|})$.

(b) If $-N_\alpha$ is a square, then $f \mid (b^2 \text{rad}(\gcd(uN_\alpha, N_\varepsilon)))$, where the first relationship in part (a) is replaced by

$$\pm f^2(x + N_\varepsilon \sqrt{N_\alpha}) = (a + \sqrt{N_\alpha}) (r + s \sqrt{\text{sf}(N_\alpha)})^4.$$

(c) If $\text{sf}(|N_\alpha|) = 2^\ell p^m$ where $\ell, m \in \{0, 1\}$ with $\ell + m \geq 1$ and p is an odd prime, then we have $f \mid (4b^2 \text{rad}(\gcd(uN_\alpha / \text{sf}(N_\alpha), N_\varepsilon)))$ when $N_\alpha \equiv 1 \pmod{4}$ and $4 \nmid d$, and $f \mid (2b^2 \text{rad}(\gcd(uN_\alpha / \text{sf}(N_\alpha), N_\varepsilon)))$ otherwise.

Remark. For work with binary recurrence sequences, ε will be a power of an algebraic integer ε' . So $\text{rad}(N_\varepsilon) = \text{rad}(N_{\varepsilon'})$. This makes our representation proposition useful for more general sequences than those considered in this paper.

To prove this proposition, we will use the following three lemmas.

Lemma 3.2. Suppose that $a, b, d, t, u, x, y, \alpha$ and ε are as in Proposition 3.1. Put $r_1 = tb^2 + au \pm 2by$ and $s'_1 = -u\sqrt{N_\alpha/\text{sf}(N_\alpha)}$.

Then $\gcd(4b^2r_1/\text{sf}(r_1), r_1^2)$ is a divisor of $s_1'^2$.

Proof. Put $v_p(b) = k_1$ and $v_p(r_1) = k_2$ with $k_1, k_2 \geq 0$.

Suppose first that p is an odd prime.

With $g_1^2 = \gcd(4b^2r_1/\text{sf}(r_1), r_1^2)$, we have

$$(3.3) \quad v_p(g_1^2) = \begin{cases} 2k_1 + k_2, & \text{if } k_2 \text{ is even and } 2k_1 \leq k_2, \\ 2k_2, & \text{if } k_2 \text{ is even and } 2k_1 \geq k_2, \\ 2k_1 + k_2 - 1, & \text{if } k_2 \text{ is odd and } 2k_1 - 1 \leq k_2, \\ 2k_2, & \text{if } k_2 \text{ is odd and } 2k_1 + 1 \geq k_2. \end{cases}$$

From the definitions of r_1 and k_2 , it follows that $v_p(au) \geq \min(k_2, v_p(tb^2 \pm 2by))$.

Expanding the expression for y^2 in (3.1), we obtain

$$(3.4) \quad 4y^2 = 2atu + b^2t^2 + b^2du^2 = 2atu + 4b^2N_\varepsilon + 2b^2du^2.$$

Applying this equation, for odd primes, p , we have

$$\begin{aligned} 2v_p(y) &\geq \min(v_p(atu), v_p(b^2t^2), v_p(b^2du^2)) \\ &\geq \min(v_p(t^2b^2 \pm 2bty), k_2 + v_p(t), v_p(b^2t^2), v_p(b^2du^2)) \\ &\geq \min(v_p(bty), k_2 + v_p(t), v_p(b^2t^2), v_p(b^2du^2)) \\ &\geq \min(k_1 + v_p(t) + v_p(y), k_2 + v_p(t), 2k_1 + 2v_p(t), 2k_1 + v_p(d) + 2v_p(u)). \end{aligned}$$

This implies that $v_p(y) \geq \min(k_1, k_2/2)$.

We consider separately the two possibilities for the gcd defining g_1^2 for each odd prime, p .

(1) Suppose that $v_p(r_1^2) \leq v_p(4b^2r_1/\text{sf}(r_1)) = v_p(b^2r_1/\text{sf}(r_1))$.

If k_2 is even, then we have $v_p(r_1^2) \leq v_p(b^2r_1)$. I.e., $k_2 \leq 2k_1$. Similarly, if k_2 is odd, then we have $v_p(r_1^2) \leq v_p(b^2r_1) - 1$. So $k_2 \leq 2k_1 - 1$. In both cases, we have $k_1 \geq k_2/2$ and thus $v_p(y) \geq k_2/2$.

(1-a) If $v_p(a) < 2v_p(b) + v_p(d)/2$, then $v_p(N_\alpha) = v_p(N_\alpha/\text{sf}(N_\alpha)) = 2v_p(a)$. So $v_p(s_1'^2) = 2v_p(au)$.

From $v_p(y) \geq k_2/2$ and $k_1 \geq k_2/2$, it follows that $v_p(tb^2 \pm 2by) \geq k_2$. So from the definition of r_1 , we have $v_p(au) \geq k_2$. Hence $v_p(s_1'^2) \geq 2k_2$. From (3.3), we have $v_p(g_1^2) = 2k_2 \leq v_p(s_1'^2)$, as desired.

(1-b) If $v_p(a) \geq 2v_p(b) + v_p(d)/2$, then $v_p(N_\alpha) \geq v_p(N_\alpha/\text{sf}(N_\alpha)) \geq 4v_p(b)$. So $v_p(s_1'^2) \geq 4v_p(b) + 2v_p(u)$.

From (3.3), we have $v_p(g_1^2) = 2k_2$. Also $v_p(s_1'^2) \geq 4v_p(b) + 2v_p(u) \geq 2k_2 + 2v_p(u)$. So $v_p(g_1^2) \leq v_p(s_1'^2)$.

(2) Now suppose that $v_p(4b^2r_1/\text{sf}(r_1)) < v_p(r_1^2)$.

Put $r'_1 = tb^2 + au + 2by$ and $r''_1 = tb^2 + au - 2by$. We shall prove the lemma in this case (i.e., when $v_p(4b^2r_1/\text{sf}(r_1)) < v_p(r_1^2)$) for $r_1 = r'_1$. The proof is identical for $r_1 = r''_1$.

If k_2 is even, then we have $2k_1 < k_2$. If k_2 is odd, then we have $2k_1 - 1 < k_2$. So in both cases, $2k_1 \leq k_2$ (i.e., $v_p(4b^2) \leq v_p(r'_1)$) and $v_p(y) \geq k_1$.

We now show that in this case we have $v_p(4b^2) < v_p(r''_1)$.

Since $v_p(y) \geq v_p(b)$, from the definition of r'_1 and $v_p(r'_1) > v_p(4b^2)$, we also have $v_p(au) > v_p(b^2)$. So the p -adic valuation of each term in the definition of r'_1 is greater than $v_p(b^2)$. Thus $v_p(r''_1) > v_p(b^2)$ too.

Combining this with $r'_1 r''_1 = u^2 N_\alpha$, we have $v_p(b^2 r'_1) < v_p(r'_1 r''_1) = v_p(u^2 N_\alpha)$, as desired.

The proof when $p = 2$ is similar. But we will use the following information later in the proof of Proposition 3.1. We have

$$(3.5) \quad v_2(g_1^2) = \begin{cases} 2k_1 + k_2 + 2, & \text{if } k_2 \text{ is even and } 2k_1 + 2 \leq k_2, \\ 2k_2, & \text{if } k_2 \text{ is even and } 2k_1 + 2 \geq k_2, \\ 2k_1 + k_2 + 1, & \text{if } k_2 \text{ is odd and } 2k_1 + 1 \leq k_2, \\ 2k_2, & \text{if } k_2 \text{ is odd and } 2k_1 + 1 \geq k_2. \end{cases}$$

As above, we have $v_2(au) \geq \min(k_2, v_2(tb^2 \pm 2by))$.

Applying this and the right-hand expression in (3.4) for $4y^2$, we obtain

$$\begin{aligned} 2v_2(y) + 2 &\geq \min(v_2(2atu), v_2(b^2(4N_\varepsilon + 2du^2))) \\ &\geq \min(v_2(2t^2b^2 \pm 4bty), k_2 + v_p(t) + 1, v_2(2b^2)) \\ &\geq \min(v_2(4bty), k_2 + v_2(t) + 1, 2k_1 + 1) \\ &\geq \min(k_1 + v_2(t) + v_2(y) + 2, k_2 + v_2(t) + 1, 2k_1 + 1). \end{aligned}$$

Since $v_2(y)$ is an integer, this implies that

$$(3.6) \quad v_2(y) \geq \min(k_1, (k_2 - 1)/2)$$

and $v_2(y) \geq \min(k_1, k_2/2)$, if k_2 is even. □

Lemma 3.3. *In the notation of Proposition 3.1, put $r'_1 = tb^2 + au + 2by$, $g_1'^2 = \gcd(4b^2 r'_1 / \text{sf}(r'_1), r_1'^2)$, $r''_1 = tb^2 + au - 2by$ and $g_1''^2 = \gcd(4b^2 r''_1 / \text{sf}(r''_1), r_1''^2)$.*

(a) *For all primes, p ,*

$$\max(v_p(r'_1/g_1'^2), v_p(r''_1/g_1''^2)) \leq v_p(\text{rad}(\gcd(uN_\alpha, N_\varepsilon \text{sf}(N_\alpha)))).$$

(b) *For all primes, p , if $v_p(\text{sf}(N_\alpha)) > 0$, then*

$$(3.7) \quad \min(v_p(r'_1/g_1'^2), v_p(r''_1/g_1''^2)) \leq 0.$$

(c) *If r'_1 is even, then $v_2(r'_1/g_1'^2) < 0$. The same result holds for r''_1 .*

Proof. (a) We will prove that for all primes, p , we have $v_p(r'_1/g_1'^2) \leq v_p(\text{rad}(\gcd(uN_\alpha, N_\varepsilon \text{sf}(N_\alpha))))$. The proof is the same for $r''_1/g_1''^2$.

From (3.11), we can write

$$(3.8) \quad \frac{r'_1}{g_1'^2} = \frac{\text{sf}(r'_1)}{\gcd(4b^2, r'_1 \text{sf}(r'_1))}.$$

Since $v_p(\text{sf}(r'_1)) \leq 1$, for all primes, p , it follows from this expression that $v_p(r'_1/g_1'^2) \leq 1$, for all primes, p . So it remains to show that if $v_p(r'_1/g_1'^2) = 1$, then we also have $v_p(\text{rad}(\gcd(uN_\alpha, N_\varepsilon \text{sf}(N_\alpha)))) = 1$.

From the expression above for $r'_1/g_1'^2$, we see that we are considering primes, p , such that $p | \text{sf}(r'_1)$ and $p \nmid (4b^2)$ (i.e., $p \nmid (2b)$).

From the observation that $r'_1 r''_1 = N_\alpha u^2$, we have $r'_1 | (N_\alpha u^2)$.

We start by showing that if $v_p(r'_1/g_1'^2) = 1$, then $p | (N_\varepsilon \text{sf}(N_\alpha))$.

If $p | \text{sf}(r'_1)$, but $p \nmid \gcd(r'_1, r''_1)$, then $v_p(u^2 N_\alpha)$ must be odd. Hence $p | \text{sf}(N_\alpha)$.

So we need only consider what happens when $p \mid \text{sf}(r'_1)$, $p \nmid (2b)$ and $p \mid \gcd(r'_1, r''_1)$.

Suppose that $v_p(r'_1) = k_1$ and $v_p(r''_1) = k_2$ for positive integers k_1 and k_2 . Then $v_p(u^2 N_\alpha) = k_1 + k_2$. If $k_1 + k_2$ is odd, then $p \nmid \text{sf}(N_\alpha)$.

We also know that k_1 is odd (otherwise, $p \nmid \text{sf}(r'_1)$). So we need only consider when k_2 is also odd.

Since $p \mid (r'_1 - r''_1)$, $(r'_1 - r''_1) = 4by$ and $p \nmid (2b)$, it follows that $p \mid y$. We also have p is a divisor of $r'_1 + r''_1 = 2au + 2b^2t$.

We can write $4y^2 = 2atu + (t^2 + du^2)b^2$ and find that p is a divisor of $t(r'_1 + r''_1) - 4y^2 = b^2(t^2 - du^2)$. Since $p \nmid b$, we have $p \mid N_\varepsilon$, completing the proof that $p \mid (N_\varepsilon \text{sf}(N_\alpha))$.

Now we show that $p \mid (uN_\alpha)$ holds if $v_p(r'_1/g_1^2) = 1$. But this is immediate from $r'_1 r''_1 = u^2 N_\alpha$.

This completes the proof of part (a).

(b) Suppose $v_p(\text{sf}(N_\alpha)) > 0$. That is, $v_p(\text{sf}(N_\alpha)) = 1$. We will show that at least one of $v_p(r'_1/g_1^2)$ or $v_p(r''_1/g_1'^2)$ must be non-positive. Otherwise, by (3.8), $v_p(\text{sf}(r'_1)) = v_p(\text{sf}(r''_1)) = 1$. So $v_p(r'_1 r''_1)$ is even. But from $r'_1 r''_1 = u^2 N_\alpha$ and $v_p(\text{sf}(N_\alpha)) = 1$, we see that $v_p(r'_1 r''_1)$ is odd. Hence at least one of $v_p(r'_1/g_1^2)$ or $v_p(r''_1/g_1'^2)$ is non-positive, as required.

(c) This follows from (3.8). We have $v_2(\text{sf}(r'_1)) = 0$ or 1 . In both cases, since r'_1 is even, we find that v_2 of the denominator of the right-hand side of (3.8) is strictly greater than v_2 of its numerator. \square

We shall need the following lemma for the proofs of parts (b) and (c) of Proposition 3.1.

Lemma 3.4. *With the same notation as in Lemma 3.3, $\gcd(r'_1, r''_1)$ is even, unless $N_\alpha \equiv 1 \pmod{4}$ and $4 \nmid d$.*

Proof. From the expressions for r'_1 and r''_1 , we need only show that $tb^2 + au$ is even unless $N_\alpha \equiv 1 \pmod{4}$ and $4 \nmid d$. We do so by showing that if either (i) tb^2 even and au odd or (ii) tb^2 odd and au even, then $N_\alpha \equiv 1 \pmod{4}$ and $4 \mid d$.

(i) We first suppose that t is even in case (i). Since u is odd and $(t^2 - du^2)/4 \in \mathbb{Z}$, we have $4 \mid d$. But then $N_\alpha = a^2 - db^4 \equiv 1 \pmod{4}$, since a must be odd.

Now suppose that t is odd. Since $(t^2 - du^2)/4 \in \mathbb{Z}$ and u is odd, it follows that $d \equiv 1 \pmod{4}$. Here b must be even, since tb^2 is even. Again $N_\alpha = a^2 - db^4 \equiv 1 \pmod{4}$, since a must be odd. Applying these to the middle expression in (3.4), we find that $4y^2 \equiv 2 \pmod{4}$, so this case is not possible.

(ii) If u is even, then since t is odd, N_ε cannot be an integer. So we must have a even and b, t and u all odd. Since t and u are both odd, $d \equiv 1 \pmod{4}$. So we have $N_\alpha \equiv 3 \pmod{4}$. Hence $(b^2t + au)^2 - N_\alpha u^2 \equiv 2 \pmod{4}$. But this quantity is b^2 times the middle expression in (3.4), so it is $4b^2y^2$. Thus (ii) is not possible. \square

Proof of Proposition 3.1. (a) We start by writing $(x + N_\varepsilon \sqrt{N_\alpha}) / (a + \sqrt{N_\alpha})$ as a square.

By rationalising the denominator of $(x + N_\varepsilon \sqrt{N_\alpha}) / (a + \sqrt{N_\alpha})$ and then applying the expressions for N_ε and N_α , we find that

$$\frac{x + N_\varepsilon \sqrt{N_\alpha}}{a + \sqrt{N_\alpha}} = \frac{4ax - a^2t^2 + b^4dt^2 + a^2du^2 - b^4d^2u^2 + (at^2 - adu^2 - 4x)\sqrt{N_\alpha}}{4b^4d}.$$

Substituting

$$(3.9) \quad 4x = a(t^2 + du^2) + 2b^2dtu,$$

from the expression for $x + y^2\sqrt{d}$ in (3.1), we obtain

$$\frac{x + N_\varepsilon\sqrt{N_\alpha}}{a + \sqrt{N_\alpha}} = \frac{2a^2u^2 + 2ab^2tu + b^4t^2 - db^4u^2 - 2u(au + b^2t)\sqrt{N_\alpha}}{4b^4}.$$

We can write $2a^2u^2 + 2ab^2tu + b^4t^2 - db^4u^2 = (au + b^2t)^2 + u^2N_\alpha$, so

$$\frac{x + N_\varepsilon\sqrt{N_\alpha}}{a + \sqrt{N_\alpha}} = \left(\frac{(au + b^2t) - u\sqrt{N_\alpha}}{2b^2} \right)^2.$$

With $r_1 = tb^2 + au \pm 2by$ and $s_1 = -u$, a routine calculation, along with (3.4), shows that

$$\left(r_1 + s_1\sqrt{N_\alpha} \right)^2 = 2r_1 \left((au + b^2t) - u\sqrt{N_\alpha} \right).$$

Hence

$$\begin{aligned} (4b^2r_1)^2 \left(x + N_\varepsilon\sqrt{N_\alpha} \right) &= \left(a + \sqrt{N_\alpha} \right) \left(r_1 + s_1\sqrt{N_\alpha} \right)^4 \\ (3.10) \qquad \qquad \qquad &= \left(a + \sqrt{N_\alpha} \right) \left(r_1 + s'_1\sqrt{\text{sf}(N_\alpha)} \right)^4, \end{aligned}$$

where $s'_1 = s_1\sqrt{N_\alpha/\text{sf}(N_\alpha)}$.

From this relationship, we now show that we can find such a relationship for $x + N_\varepsilon\sqrt{N_\alpha}$ with the conditions on f in part (a) satisfied.

We want to take the largest common factor, g_1 , of r_1 and s'_1 such that $4b^2r_1/g_1^2$ is also an integer. That is,

$$g_1^2 = \gcd \left(\gcd \left(4b^2r_1/\text{sf}(r_1), r_1^2 \right), s_1'^2 \right).$$

First, note that we can write

$$(3.11) \qquad \gcd \left(4b^2r_1/\text{sf}(r_1), r_1^2 \right) = r_1 \gcd \left(4b^2, r_1 \text{sf}(r_1) \right) / \text{sf}(r_1).$$

From Lemma 3.2, we see that

$$g_1^2 = \gcd \left(4b^2r_1/\text{sf}(r_1), r_1^2 \right).$$

From Lemma 3.3(a), $4b^2r_1/g_1^2$ is a divisor of

$$4b^2 \text{rad} \left(\gcd(uN_\alpha, N_\varepsilon \text{sf}(N_\alpha)) \right) = 4b^2 \text{rad} \left(\text{sf}(N_\alpha) \gcd(uN_\alpha/\text{sf}(N_\alpha), N_\varepsilon) \right).$$

We put $r = r_1/g_1$, for either choice of r_1 , $s = s'_1/g_1$ and $f = 4b^2r_1/g_1^2$. By the definition of g_1^2 , we see that $f, r, s \in \mathbb{Z}$.

Lastly, we choose which of the two possible values of r_1 to use. As in the statement of Lemma 3.3, we let $r'_1 = tb^2 + au + 2by$ and $r''_1 = tb^2 + au - 2by$ be the two possibilities. We let g'_1 and g''_1 be the associated values of g_1 . We will use Lemma 3.3(b). We divide the prime divisors of $\text{sf}(N_\alpha)$ into three disjoint sets:

$$\begin{aligned} I' &= \{p : p \text{ prime, with } p|\text{sf}(N_\alpha) \text{ and } v_p(r'_1/g_1'^2) < v_p(r''_1/g_1''^2)\}, \\ I'' &= \{p : p \text{ prime, with } p|\text{sf}(N_\alpha) \text{ and } v_p(r''_1/g_1''^2) < v_p(r'_1/g_1'^2)\}, \\ I''' &= \{p : p \text{ prime, with } p|\text{sf}(N_\alpha) \text{ and } v_p(r'_1/g_1'^2) = v_p(r''_1/g_1''^2)\}. \end{aligned}$$

With $d' = \prod_{p \in I'} p$, $d'' = \prod_{p \in I''} p$ and $d''' = \prod_{p \in I'''} p$, we have $d'd''d''' = \text{sf}(N_\alpha)$.

We put $r_1 = r'_1$ if $d' > d''$ and $r_1 = r''_1$ otherwise. By Lemma 3.3(b),

$$\begin{aligned} v_p(r_1/g_1^2) &\leq 0 \leq v_p(\text{sf}(N_\alpha)/p) \\ &\leq v_p(\text{rad}((\text{sf}(N_\alpha)/p) \gcd(uN_\alpha/\text{sf}(N_\alpha), N_\varepsilon))), \end{aligned}$$

for all $p \in I' \cup I'''$ in the first case and for all $p \in I'' \cup I'''$ in the second case. Hence with $f' = \text{sf}(N_\alpha)/\max(d'd''', d''d''')$, we see that $f' < \sqrt{\text{sf}(N_\alpha)}$ and that $4b^2r_1/g_1^2$ is a divisor of

$$4b^2 \text{rad}(f' \gcd(uN_\alpha/\text{sf}(N_\alpha), N_\varepsilon)).$$

(b) If $4b^2r_1/g_1^2$ is odd, then there is nothing to prove, as $4b^2r_1/g_1^2$ dividing $b^2 \text{rad}(\gcd(uN_\alpha, N_\varepsilon))$ follows from $4b^2r_1/g_1^2$ being a divisor of $4b^2 \text{rad}(\gcd(uN_\alpha, N_\varepsilon))$. So we put $f = 4b^2r_1/g_1^2$ and need only consider when $4b^2r_1/g_1^2$ is even.

We consider the four cases for the parity of r and s .

(b-i) Suppose that r and s are both odd.

Here we will replace r and s .

We can write $(r + si)/(1 + i) = (r + s)/2 + (s - r)i/2$. Since r and s are both odd and $(1 + i)^4 = -4$, we find that $(s \pm r)/2$ are both integers and

$$-\left(\frac{2b^2r}{g_1^2}\right)^2 \left(x + N_\varepsilon \sqrt{N_\alpha}\right) = \left(a + \sqrt{N_\alpha}\right) ((r + s)/2 + (s - r)i/2)^4.$$

Since $4b^2r/g_1^2$ is even, we know that $2b^2r/g_1^2 \in \mathbb{Z}$.

Since $-N_\alpha$ is a square, we have $N_\alpha \not\equiv 1 \pmod{4}$, so by Lemmas 3.4 and 3.3(c), we see that $(4b^2r/g_1^2) \mid (2b^2 \text{rad}(\gcd(uN_\alpha, N_\varepsilon)))$. Hence $2b^2r/g_1^2$ is a divisor of $b^2 \text{rad}(\gcd(uN_\alpha, N_\varepsilon))$ and so we take $f = 2b^2r/g_1^2$ in this case.

(b-ii) Suppose that $r = r_1/g_1$ is odd and $s = s'_1/g_1$ is even.

In this case, as well as cases (b-iii) and (b-iv), we will assume that $r_1 = r'_1$. The proof is identical using $r_1 = r''_1$ instead.

Since r is odd, we have $v_2(g_1) = v_2(r_1)$. So from the definition of g_1^2 in the proof of part (a), it follows that $v_2(4b^2/\text{sf}(r_1)) \geq v_2(r_1)$.

For this case and case (b-iii), if $v_2(r'_1) \neq v_2(r''_1)$, then we must have $v_2(au + b^2t) = v_2(2by)$, since $r''_1 = r'_1 + 4by$.

(b-ii-1) Suppose first that $v_2(r_1)$ is even.

In this case, $v_2(4b^2) \geq v_2(r_1) = v_2(g_1)$. If we have equality, then $f = 4b^2r_1/g_1^2$ is odd and so $f \mid (b^2 \text{rad}(\gcd(uN_\alpha, N_\varepsilon)))$, as required. So we consider $v_2(4b^2) > v_2(r_1)$. Since both of these quantities are even, we must have $v_2(4b^2) \geq v_2(r_1) + 2$. That is, $v_2(b^2) \geq v_2(r_1)$.

Since s is even, we have

$$v_2(s_1'^2) = v_2(u^2 N_\alpha) = v_2(r'_1) + v_2(r''_1) > 2v_2(g_1).$$

Since r is odd, we also have $2v_2(g_1) = 2v_2(r'_1)$. Hence $v_2(r''_1) > v_2(r'_1)$. As we stated near the start of this case (case (b-ii)), since $v_2(r'_1) \neq v_2(r''_1)$, we have $v_2(au + b^2t) = v_2(2by)$.

We saw in the proof of Lemma 3.2 that $v_2(y) \geq \min(v_2(b), v_2(r'_1)/2)$. Since $v_2(b^2) \geq v_2(r_1)$, it follows that $v_2(y) \geq v_2(r'_1)/2$. Hence

$$v_2(2by) \geq 1 + v_2(r_1)/2 + v_2(r_1)/2 = v_2(r_1) + 1.$$

Thus $v_2(au + b^2t) = v_2(2by) \geq v_2(r_1) + 1$, which implies that $v_2(r_1) > v_2(r_1)$. Therefore, the case when $v_2(r_1)$ is even and $v_2(b^2) \geq v_2(r_1)$ never occurs and we find that in case (b-ii-1), $f \mid (b^2 \text{ rad}(\gcd(uN_\alpha, N_\varepsilon)))$, as required.

(b-ii-2) Now suppose that $v_2(r_1)$ is odd.

Here $v_2(2b^2) \geq v_2(r_1) = v_2(g_1)$.

As in case (b-ii-1), since s is even, we have $v_2(r'_1) \neq v_2(r''_1)$. Hence $v_2(au + b^2t) = v_2(2by)$.

Recall from (3.6) that $v_2(y) \geq \min(v_2(b), (v_2(r_1) - 1)/2)$. Hence, $v_2(au + b^2t) = v_2(2by) \geq v_2(r_1)$. Since $v_2(au + b^2t) = v_2(2by)$, we have $v_2(r_1) \geq v_2(2by) + 1 > v_2(r_1)$, which is not possible.

This completes the proof for case (b-ii).

(b-iii) Suppose that $r = r_1/g_1$ is even and $s = s'_1/g_1$ is odd.

Since r is even, we must have $v_2(g_1^2) = v_2(4b^2r_1/\text{sf}(r_1)) < v_2(r_1^2)$.

Since $v_2(s_1'^2) = v_2(u^2N_\alpha) = v_2(r'_1) + v_2(r''_1)$, by the assumption that s'_1/g_1 is odd, we have $v_2(r'_1) + v_2(r''_1) = v_2(g_1^2)$. Since r is even, we also have $v_2(g_1^2) < 2v_2(r_1)$, it follows that $v_2(r''_1) \neq v_2(r_1)$. Hence, by the comment at the start of case (b-ii), we have $v_2(au + b^2t) = v_2(2by)$.

(b-iii-1) If $v_2(r_1)$ is even, then $v_2(g_1^2) = v_2(4b^2r_1)$. Hence $f = 4b^2r_1/g_1^2$ is odd and $f \mid (b^2 \text{ rad}(\gcd(uN_\alpha, N_\varepsilon)))$ as required.

(b-iii-2) If $v_2(r_1)$ is odd, then $v_2(2b^2r_1) < v_2(r_1^2)$. So $v_2(b) < (v_2(r_1) - 1)/2$. Recall from (3.6) that $v_2(y) \geq \min(v_2(b), (v_2(r_1) - 1)/2)$. So $v_2(y) \geq v_2(b)$.

Hence, $v_2(au + b^2t) = v_2(2by) \geq 2v_2(b) + 1$. Since $v_2(au + b^2t) = v_2(2by)$, we have $v_2(r_1) \geq v_2(2by) + 1 \geq 2v_2(b) + 2$. Using the same argument, we have $v_2(r''_1) \geq 2v_2(b) + 2$ too.

But $v_2(2b^2r_1) = v_2(g_1^2) = v_2(s_1'^2) = v_2(r'_1) + v_2(r''_1)$. Hence $v_2(r''_1) = v_2(2b^2)$. But this contradicts $v_2(r''_1) \geq 2v_2(b) + 2$. Hence $v_2(r_1)$ cannot be odd.

(b-iv) Suppose that r and s are both even.

Since r is even, we know that $v_2(g_1^2) = v_2(4b^2r_1/\text{sf}(r_1)) < v_2(r_1^2)$. So $v_2(f) = 0$ or 1, depending on whether $v_2(r_1)$ is even or odd. So, as stated at the start of the proof of part (b), we need only consider the latter case.

Since s is even, we have

$$2 \leq v_2(s^2) = v_2(u^2N_\alpha) - v_2(2b^2r'_1) = v_2(r''_1) - v_2(2b^2).$$

So $v_2(r''_1) \geq 2v_2(b) + 3$.

Similarly, $2 \leq v_2(r_1'^2) - v_2(2b^2r'_1) = v_2(r'_1) - v_2(2b^2)$, so $v_2(r'_1) \geq 2v_2(b) + 3$.

A consequence of these two inequalities is that $64 \mid (u^2N_\alpha)$.

From (3.4), we have $4y^2 = 2atu + 2b^2du^2 + 4b^2N_\varepsilon$. So $atu + b^2du^2$ must be even. I.e., atu and b^2du^2 have the same parity.

(b-iv-1) If b^2du^2 is odd, then a and t are also odd. Since $4N_\varepsilon = t^2 - du^2$ is divisible by 4 and t and u are both odd, it must be the case that $d \equiv 1 \pmod{4}$.

If $d \equiv 1 \pmod{8}$, then $4N_\varepsilon = t^2 - du^2 \equiv 0 \pmod{8}$ and so N_ε is even. Furthermore, since abd is odd, we have N_α is even, so $b^2 \text{ rad}(\gcd(uN_\alpha, N_\varepsilon))$ is also even and the desired conclusion holds.

If $d \equiv 5 \pmod{8}$, then $N_\alpha = a^2 - db^4 \equiv 4 \pmod{8}$. Since u is odd, we get a contradiction with $64 \mid (u^2N_\alpha)$.

(b-iv-2) We now consider $b^2 du^2$ even. If b is even, then

$$v_2(b^2 \operatorname{rad}(\gcd(uN_\alpha, N_\varepsilon))) \geq 2 > v_2(f) = 1.$$

So the desired conclusion holds. Therefore, we may assume that b is odd and du^2 is even in what follows. We showed above that uN_α is even. We will show here that N_ε is also even. These facts will suffice to show that $v_2(b^2 \operatorname{rad}(\gcd(uN_\alpha, N_\varepsilon))) \geq 1 = v_2(f)$ and hence to prove part (b) in this case.

To prove that N_ε is even, we will assume that it is odd and obtain a contradiction.

Since $4N_\varepsilon = t^2 - du^2 \in \mathbb{Z}$ and du^2 is even, we have t is even and hence $4 \mid (du^2)$.

If u is odd, then $4 \mid d$. Also N_α is even, so a is even. As a result, we find that $v_2(2atu), v_2(2b^2 du^2) \geq$

3. So under our assumption that N_ε is odd, from (3.4) we have $v_2(4y^2) = 2$. I.e., y is odd.

The same reasoning shows that y is odd if u is even under the assumption that N_ε is odd.

Suppose that $v_2(r'_1) = v_2(r''_1)$. Then $v_2(4by) = v_2(\pm(r'_1 - r''_1)) > v_2(r'_1)$. So $v_2(y) > v_2(r'_1) - v_2(b) - 2 > v_2(b) + 1$.

Suppose that $v_2(r'_1) < v_2(r''_1)$. Then $v_2(4by) = v_2(r'_1)$. So $v_2(y) \geq v_2(b) + 1$.

In both cases, we find that y is even. This contradicts what we obtained (y is odd) under the assumption that N_ε is odd. Hence we know that in the case when $b^2 du^2$ is even, N_ε is even and the assertion in part (b) of the lemma holds.

(c) We consider two cases.

(c-i) Suppose that $|\operatorname{sf}(N_\alpha)| = p$, for a prime, p . Then we have $f' = 1$ in part (a) and so $f \mid (4b^2 \operatorname{rad}(\gcd(uN_\alpha / \operatorname{sf}(N_\alpha), N_\varepsilon)))$. Hence the result holds if $N_\alpha \equiv 1 \pmod{4}$ and $4 \mid d$.

From Lemma 3.4, r is even unless $N_\alpha \equiv 1 \pmod{4}$ and $4 \mid d$. So, from Lemma 3.3(c), we have $v_2(r/g_1^2) \leq -1$. With $f = 4b^2 r/g_1^2$, we have $f \mid (2b^2 \operatorname{rad}(\gcd(uN_\alpha / \operatorname{sf}(N_\alpha), N_\varepsilon)))$.

(c-ii) Suppose that $|\operatorname{sf}(N_\alpha)| = 2p$, where p is an odd prime. From Lemma 3.4, we see that r'_1 and r''_1 are both even. Hence, from Lemma 3.3(c), we have

$$\max(v_2(r'_1/g_1'^2), v_2(r''_1/g_1''^2)) < 0 \leq v_2(\operatorname{rad}(\gcd(uN_\alpha / \operatorname{sf}(N_\alpha), N_\varepsilon))).$$

Similar to the end of the proof of part (a), we let $r_1 = r'_1$ if $v_p(r'_1/g_1'^2) \leq v_p(r''_1/g_1''^2)$ and $r_1 = r''_1$ otherwise. From Lemma 3.3(b), we find that

$$v_p(r_1/g_1^2) \leq 0 \leq v_p(\operatorname{rad}(\gcd(uN_\alpha / \operatorname{sf}(N_\alpha), N_\varepsilon))).$$

So with $f = 4b^2 r_1/g_1^2$, we have $f \mid (2b^2 \operatorname{rad}(\gcd(uN_\alpha / \operatorname{sf}(N_\alpha), N_\varepsilon)))$. □

3.2. Lower bounds for y_k 's. Next we bound the y_k 's from below.

Lemma 3.5. *Let the y_k 's be defined by (1.1) with the notation and assumptions there. Suppose that $N_\alpha < 0$. Let K be the largest negative integer such that $y_K > b^2$.*

(a) *Put $\bar{\alpha} = a - b^2\sqrt{d}$. We have*

$$(3.12) \quad y_k > \begin{cases} \frac{\alpha \varepsilon^{2k}}{2\sqrt{d}} & \text{for } k \geq 0, \\ \frac{-\bar{\alpha} \varepsilon^{2|k|}}{2\sqrt{d}} & \text{for } k < 0. \end{cases}$$

(b) *For all k , $2y_k$ is a positive integer. The sequences $(y_k)_{k \geq 0}$ and $(y_{K+1}, y_K, y_{K-1}, y_{K-2}, \dots)$ are increasing sequences of positive numbers.*

(c) We have

$$(3.13) \quad y_k \geq \begin{cases} (|N_\alpha| u^2 / (4b^2)) (2du^2/5)^{k-1} & \text{for } k > 0, \\ (|N_\alpha| u^2 / (4b^2)) (2du^2/5)^{\max(0, K-k)} & \text{for } k < 0. \end{cases}$$

In fact, if $(d, t, u) \neq (5, 1, 1)$, then we can replace $2du^2/5$ by $5du^2/8$ and if $N_\varepsilon = 1$, then we can replace $2du^2/5$ by du^2 .

Remark. The condition $N_\alpha < 0$ is needed, since if $N_\alpha > 0$, then $y_k < 0$ can occur for $k < 0$.

Also, since $du^2 \geq 5$ holds under the conditions here, the lower bounds in (3.13) are increasing as $|k|$ increases.

Proof. (a) From (1.1), we can write

$$y_k = \frac{\alpha \varepsilon^{2k} - \bar{\alpha} \bar{\varepsilon}^{2k}}{2\sqrt{d}},$$

where $\bar{\varepsilon} = (t - u\sqrt{d})/2$. Since $N_\alpha = \alpha\bar{\alpha} < 0$ and $\alpha > 0$, we have $\bar{\alpha} < 0$. So the inequality (3.12) follows.

(b) From part (a), it follows that all the y_k 's are positive. Since $\alpha \varepsilon^{2k}$ is an algebraic integer, we have $2y_k \in \mathbb{Z}$.

Since d, t^2 and u^2 are all positive integers, a quick search over small values of d, t and u with $t^2 - du^2 = \pm 4$ shows that $t^2 + du^2 \geq 6$ (the minimum occurs for $(d, t, u) = (5, \pm 1, \pm 1)$). From this, (1.3) and $y_k > 0$, we have $y_{k+1} \geq 3y_k - y_{k-1}$ for $k \geq 1$.

From the expression for y_1 after (1.1) and $t^2 + du^2 \geq 6$, we have $y_1 > (3/2)b^2 > b^2 = y_0$. So using induction and $y_{k+1} \geq 3y_k - y_{k-1}$, we find that $y_{k+1} > y_k$ for all $k \geq 0$.

By the definition of K , $y_K > y_{K+1}$. Also $y_K > b^2 > 0$, so we can proceed as in the case of $k \geq 0$, using $y_{k-1} \geq 3y_k - y_{k+1}$ and induction.

(c) From (1.2), we find that

$$(3.14) \quad 4b^2 y_1 = b^4 (t^2 + du^2) + 2ab^2 tu = (b^2 t + au)^2 - N_\alpha u^2.$$

From the second equality in (3.14) and $N_\alpha < 0$, equation (3.13) follows for $k = 1$.

Writing $\varepsilon^\ell = t_\ell + u_\ell \sqrt{d}$ for $\ell \geq 1$ (note that $u_1 = u/2$ in the notation of this lemma), we can show by an easy induction that $(u_\ell)_{\ell \geq 1}$ is an increasing sequence. Hence, for $k < 0$,

$$\begin{aligned} 4b^2 y_k &= b^4 (t_{|2k|}^2 + du_{|2k|}^2) - 2ab^2 t_{|2k|} u_{|2k|} = (b^2 t_{|2k|} - au_{|2k|})^2 - N_\alpha u_{|2k|}^2 \\ &\geq |N_\alpha| u^2. \end{aligned}$$

So equation (3.13) holds for k satisfying $K \leq k < 0$.

Recalling the recurrence in (1.3) for $k \geq 0$ and using the monotonicity established in part (b), we obtain

$$y_{k+1} = (du^2 + 2N_\varepsilon) y_k - y_{k-1} \geq (du^2 + 2N_\varepsilon - 1) y_k.$$

If $N_\varepsilon = 1$, then the stronger form of the desired inequality stated after equation (3.13) in the lemma holds, so we need only consider $N_\varepsilon = -1$. We always have $du^2 \geq 5$ (with equality only if $(d, t, u) = (5, 1, 1)$). Otherwise, $du^2 \geq 8$, which we use to establish the other inequality after equation (3.13) in the lemma). Hence the desired inequality holds.

Using the recurrence $y_{k-1} = (du^2 + 2N_\varepsilon)y_k - y_{k+1}$, we obtain equation (3.13) for $k \leq K$ in the same way. \square

We will also need to know when K in Lemma 3.5 is not equal to -1 for $b = 1$.

Lemma 3.6. *Let the y_k 's be defined by (1.1) with the notation and assumptions there. Suppose that $b = 1$ and $N_\alpha < 0$.*

We have $y_{-1} > 1$, except for

- (i) $a \geq 1$, $d = a^2 + 4$, $t = a$ and $u = 1$, where $\alpha = 2\varepsilon$ and $N_\alpha = -4$,
- (ii) $a \geq 1$, $d = a^2 + 1$, $t = 2a$ and $u = 2$, where $\alpha = \varepsilon$ and $N_\alpha = -1$.

In these cases, we have $y_{-2} = a^2 + 1$ and $y_{-2} = 4a^2 + 1$, respectively. So in each of these cases, $K = -2$.

Proof. From (3.13), we have $y_1 \geq |N_\alpha|u^2/4$. So if $y_{-1} = 1$, we must have either (1) $N_\alpha = -4$ and $u = 1$, or (2) $N_\alpha = -1$ and $u = 2$.

In case (1), we have $d = t^2 \pm 4$ and $a^2 - d = -4$. Substituting the expression for d into the second equation, we get $a^2 - t^2 = -4 \pm 4 = 0, -8$.

$a^2 - t^2 = -8$ can only occur for $a = 1$ and $t = 3$ (since we are assuming that a and t are positive integers). But in this case, $b^2t - au = 2$, so $4y_{-1} = (b^2t - au)^2 - N_\alpha u^2 = 8$.

Otherwise, we have $t = a$. So $d = a^2 + 4$, $\alpha = 2\varepsilon$ and $N_\varepsilon = -1$. Here $b^2t - au = 0$, so $y_{-1} = 1$.

In case (2), we have $d = (t^2 \pm 4)/4$ and $a^2 - d = -1$. We proceed similarly, obtaining $4a^2 - t^2 = -8$ (which is never possible) when $N_\varepsilon = 1$ and $4a^2 - t^2 = 0$ when $N_\varepsilon = -1$. Here we have $t = 2a$ and $d = a^2 + 1$, so $\alpha = \varepsilon$. Once again, $b^2t - au = 0$, so $y_{-1} = 1$.

A direct calculation, done using Maple, provides the values of y_{-2} . \square

3.3. Gap Principle. In Lemma 3.8 below, we establish a gap principle separating distinct squares in the sequence (1.1). We first need the following technical lemma to help us prove our gap principle.

Lemma 3.7. *Let $\omega = e^{i\theta}$ with $-\pi < \theta \leq \pi$.*

- (a) *Put $\omega^{1/4} = e^{i\theta/4}$. If*

$$0 < |\omega^{1/4} - z| < c_1,$$

for some $z \in \mathbb{C}$ with $|z| = 1$ and $0 < c_1 < \sqrt{2}$, then

$$|\omega - z^4| > c_2 |\omega^{1/4} - z|,$$

where $c_2 = (2 - c_1^2) \sqrt{4 - c_1^2}$.

- (b) *If*

$$0 < |\omega - z^4| < c_0,$$

for some $z \in \mathbb{C}$ with $|z| = 1$ and $0 < c_0 \leq 2$, then

$$0 < |\omega^{1/4} - z| < c_3,$$

for some choice of $\omega^{1/4}$, where c_3 is the smallest positive real root of $x^8 - 8x^6 + 20x^4 - 16x^2 + c_0^2$.

Proof. (a) We can write

$$|\omega - z^4| = |\omega^{1/4} - z| \times \prod_{k=1}^3 |\omega^{1/4} - e^{2\pi i k/4} z|.$$

Multiplying by $\omega^{-3/4}$ and expanding the resulting expression, the product above equals

$$\prod_{k=1}^3 |e^{2\pi i k/4 - i\theta/4} z - 1| = |e^{3i\varphi} + e^{2i\varphi} + e^{i\varphi} + 1|,$$

for $-\pi < \varphi \leq \pi$ such that $e^{i\varphi} = e^{-i\theta/4} z$. Squaring this quantity and simplifying, we obtain

$$(3.15) \quad 8 \cos^2(\varphi) (\cos(\varphi) + 1).$$

If $|\omega^{1/4} - z| = |1 - \omega^{-1/4} z| = c_1$, we have $2 - 2 \cos(\varphi) = c_1^2$ and, substituting this expression for $\cos(\varphi)$ into (3.15), we find that $|\omega - z^4| = c_2 |\omega^{1/4} - z|$. Since c_2 is a decreasing function of c_1 , part (a) of the lemma holds (i.e., if $|\omega^{1/4} - z| < c_1$).

(b) Using the same argument as in part (a), but supposing that $|\omega - z^4| = |1 - \omega^{-1} z^4| = c_0$, then we have $2 - 2 \cos(4\varphi) = c_0^2$. Thus

$$\begin{aligned} |\omega^{1/4} - z|^2 &= \left(\frac{|\omega - z^4|}{|e^{3i\varphi} + e^{2i\varphi} + e^{i\varphi} + 1|} \right)^2 = \frac{c_0^2}{8 \cos^2(\varphi) (\cos(\varphi) + 1)} \\ &= \frac{2 - 2 \cos(4\varphi)}{8 \cos^2(\varphi) (\cos(\varphi) + 1)}. \end{aligned}$$

Since $\cos(4\varphi) = 8 \cos^4(\varphi) - 8 \cos^2(\varphi) + 1$, we have $16 \cos^4(\varphi) - 16 \cos^2(\varphi) + c_0^2 = 0$ and using this relation, we find that $c_0^2 / (8 \cos^2(\varphi) (\cos(\varphi) + 1))$ is a root of the polynomial $x^4 - 8x^3 + 20x^2 - 16x + c_0^2$. Part (b) now follows and follows with inequalities too, since the smallest positive real root of $x^4 - 8x^3 + 20x^2 - 16x + c_0^2$ grows with c_0 . \square

Lemma 3.8. *Let the y_k 's be defined as in (1.1) with $N_\alpha < 0$.*

(a) *Suppose that $-N_\alpha$ is a square. If y_i and y_j are distinct squares with $i, j \neq 0$ and $y_j > y_i \geq \max(4\sqrt{|N_\alpha|/d}, b^2 |N_\alpha|/d)$, then*

$$y_j > 57.32 \left(\frac{d}{b^2 |N_\alpha|} \right)^2 y_i^3.$$

(b) *Suppose $-N_\alpha$ is not a square. If y_{k_1}, y_{k_2} and y_{k_3} are three distinct squares with $k_1, k_2, k_3 \neq 0$ and $y_{k_3} > y_{k_2} > y_{k_1} \geq 4\sqrt{|N_\alpha|/d}$, then there exist distinct $i, j \in \{k_1, k_2, k_3\}$ such that*

$$y_j > 15.36 \left(\frac{b^2 d}{f_i f_j |N_\alpha|} \right)^2 y_i^3,$$

where f_i and f_j are the values of f in Proposition 3.1 associated with y_i and y_j , respectively.

If $y_j > y_i \geq \max(4\sqrt{|N_\alpha|/d}, 4.27b^2 |N_\alpha|^2/d)$, then we can replace 15.36 with 182.

Proof. We start by considering the two parts together and what is common to their proofs.

Since we have assumed that $i \neq 0$ and $j \neq 0$, we can apply Proposition 3.1 to show that there are integers f_j, r_j and s_j , and choices of signs such that

$$(3.16) \quad \begin{aligned} \pm f_j^2 (x_j + N_{\varepsilon^j} \sqrt{N_\alpha}) &= (a + \sqrt{N_\alpha}) (r_j + s_j \sqrt{\text{sf}(N_\alpha)})^4 \quad \text{and} \\ f_j \sqrt{y_j} &= b (r_j^2 - \text{sf}(N_\alpha) s_j^2), \end{aligned}$$

where f_j satisfies $f_j | (4b^2 \text{sf}(|N_\alpha|))$ and $f_j^2 < 16b^4 \text{sf}(|N_\alpha|)$. Recall that the other terms in the relationships for f_j in Proposition 3.1 are not present here since $N_{\varepsilon^j} = \pm 1$.

For any two distinct squares among the y_k 's, say y_i and y_j with $i \neq 0$ and $j \neq 0$, we will assume that the \pm on the left-hand side of (3.16) is always $+$. That is,

$$(3.17) \quad \begin{aligned} f_i^2 \left(x_i + N_{\varepsilon^i} \sqrt{N_\alpha} \right) &= \left(a + \sqrt{N_\alpha} \right) \left(r_i + s_i \sqrt{\text{sf}(N_\alpha)} \right)^4 \text{ and} \\ f_j^2 \left(x_j + N_{\varepsilon^j} \sqrt{N_\alpha} \right) &= \left(a + \sqrt{N_\alpha} \right) \left(r_j + s_j \sqrt{\text{sf}(N_\alpha)} \right)^4, \end{aligned}$$

as the argument for the other cases is exactly the same. Subtracting the complex conjugate of one of these equations from the equation itself, we obtain

$$(3.18) \quad \begin{aligned} &\left(a + \sqrt{N_\alpha} \right) \left(r_j + s_j \sqrt{\text{sf}(N_\alpha)} \right)^4 - \left(a - \sqrt{N_\alpha} \right) \left(r_j - s_j \sqrt{\text{sf}(N_\alpha)} \right)^4 \\ &= 2i \operatorname{Im} \left(f_j^2 \left(x_j + N_{\varepsilon^j} \sqrt{N_\alpha} \right) \right) = \pm 2f_j^2 \sqrt{|N_\alpha|}, \end{aligned}$$

and the analogous equation with the index j replaced by i also holds.

Putting $\omega = (a - \sqrt{N_\alpha}) / (a + \sqrt{N_\alpha})$, by (3.18) and the relationship for $f_j \sqrt{y_j}$ in Proposition 3.1(a), we have

$$(3.19) \quad \begin{aligned} \left| \omega - \left(\frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right)^4 \right| &= \left| \frac{\pm 2f_j^2 \sqrt{|N_\alpha|}}{\left(a + \sqrt{N_\alpha} \right) \left(r_j - s_j \sqrt{\text{sf}(N_\alpha)} \right)^4} \right| \\ &= \frac{2b^2 \sqrt{|N_\alpha|}}{\sqrt{a^2 + |N_\alpha|} y_j} \leq \frac{1}{2}, \end{aligned}$$

the last inequality holds because $a^2 + |N_\alpha| = db^4$ and $y_j \geq 4\sqrt{|N_\alpha|/d}$.

Let $\zeta_4^{(j)}$ be the 4-th root of unity such that

$$(3.20) \quad \left| \omega^{1/4} - \zeta_4^{(j)} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right| = \min_{0 \leq k \leq 3} \left| \omega^{1/4} - e^{2k\pi i/4} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right|.$$

From (3.19), we can apply Lemma 3.7(b) with $c_0 = 1/2 + 0.0001$ to obtain

$$\left| \omega^{1/4} - \zeta_4^{(j)} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right| < 0.1263.$$

Applying Lemma 3.7(a) with $c_1 = 0.1263$, we obtain

$$\left| \omega - \left(\frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right)^4 \right| > 3.96 \left| \omega^{1/4} - \zeta_4^{(j)} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right|$$

and combining this with the equalities in (3.19) yields

$$(3.21) \quad \left| \omega^{1/4} - \zeta_4^{(j)} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right| < 0.5051 \frac{b^2 \sqrt{|N_\alpha|}}{\sqrt{a^2 + |N_\alpha|}} \frac{1}{y_j}.$$

In the same way, we define $\zeta_4^{(i)}$ for any square y_i with $i \neq 0$ in our sequence and (3.21) also holds with j replaced by i . Hence, for any two distinct squares, $y_i, y_j \geq 4\sqrt{|N_\alpha|/d}$, among

the y_k 's, we have

$$\begin{aligned}
(3.22) \quad & \left| \zeta_4^{(i)} \frac{r_i + s_i \sqrt{\text{sf}(N_\alpha)}}{r_i - s_i \sqrt{\text{sf}(N_\alpha)}} - \zeta_4^{(j)} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right| \\
& \leq \left| \omega^{1/4} - \zeta_4^{(i)} \frac{r_i + s_i \sqrt{\text{sf}(N_\alpha)}}{r_i - s_i \sqrt{\text{sf}(N_\alpha)}} \right| + \left| \omega^{1/4} - \zeta_4^{(j)} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right| \\
& < 0.5051b^2 \sqrt{\frac{|N_\alpha|}{a^2 + |N_\alpha|}} \left(\frac{1}{y_i} + \frac{1}{y_j} \right).
\end{aligned}$$

Next we obtain a lower bound for this same quantity. We first show that it cannot be zero.

If

$$\zeta_4^{(i)} \frac{r_i + s_i \sqrt{\text{sf}(N_\alpha)}}{r_i - s_i \sqrt{\text{sf}(N_\alpha)}} = \zeta_4^{(j)} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}},$$

then from our expressions for $f_i \sqrt{y_i}$ and $f_j \sqrt{y_j}$ from Proposition 3.1 we have

$$\frac{\left(r_i + s_i \sqrt{\text{sf}(N_\alpha)} \right)^4}{f_i^2 y_i} = \pm \frac{\left(r_j + s_j \sqrt{\text{sf}(N_\alpha)} \right)^4}{f_j^2 y_j}.$$

From (3.17), it follows that

$$\left(x_i + N_{\varepsilon^i} \sqrt{N_\alpha} \right) y_j = \pm \left(x_j + N_{\varepsilon^j} \sqrt{N_\alpha} \right) y_i.$$

Comparing the imaginary parts of both sides of this equation, we find that $y_i = y_j$, but this contradicts our assumption that $y_j > y_i$. Hence the left-hand side of (3.22) cannot be 0.

Let $x + y \sqrt{\text{sf}(N_\alpha)} = \left(r_i - s_i \sqrt{\text{sf}(N_\alpha)} \right) \left(r_j + s_j \sqrt{\text{sf}(N_\alpha)} \right)$. We can write

$$\begin{aligned}
(3.23) \quad & \zeta_4^{(i)} \frac{r_i + s_i \sqrt{\text{sf}(N_\alpha)}}{r_i - s_i \sqrt{\text{sf}(N_\alpha)}} - \zeta_4^{(j)} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \\
& = \frac{2\zeta_4^{(i)} x - \left(\zeta_4^{(i)} + \zeta_4^{(j)} \right) \left(x + y \sqrt{\text{sf}(N_\alpha)} \right)}{\left(r_i - s_i \sqrt{\text{sf}(N_\alpha)} \right) \left(r_j - s_j \sqrt{\text{sf}(N_\alpha)} \right)}.
\end{aligned}$$

The numerator on the right-hand side is

$$\begin{aligned}
(3.24) \quad & \begin{aligned} & -2\zeta_4^{(i)} y \sqrt{\text{sf}(N_\alpha)} & \text{if } \zeta_4^{(j)} = \zeta_4^{(i)}, \\ & 2\zeta_4^{(i)} x & \text{if } \zeta_4^{(j)} = -\zeta_4^{(i)}, \\ & \zeta_4^{(i)} (1 - \sqrt{-1}) \left(x - y \sqrt{-\text{sf}(N_\alpha)} \right) & \text{if } \zeta_4^{(j)} = \sqrt{-1} \zeta_4^{(i)} \text{ and} \\ & \zeta_4^{(i)} (1 + \sqrt{-1}) \left(x + y \sqrt{-\text{sf}(N_\alpha)} \right) & \text{if } \zeta_4^{(j)} = -\sqrt{-1} \zeta_4^{(i)}. \end{aligned}
\end{aligned}$$

Here we use $\sqrt{-1}$ to denote $\exp(2\pi i/4)$.

Using (3.2), we find that

$$(3.25) \quad \left| r_i - s_i \sqrt{\text{sf}(N_\alpha)} \right| \left| r_j - s_j \sqrt{\text{sf}(N_\alpha)} \right| = \frac{\sqrt{f_i f_j} (y_i y_j)^{1/4}}{b}.$$

At this point, our proofs of the two parts of the lemma separate.

(a) Suppose that $-N_\alpha$ is a square. From (3.24), we see that at least one of $1 \pm \sqrt{-1}$ always divides the numerator of the right-hand side of (3.23) and so

$$\begin{aligned} & \left| \zeta_4^{(i)} \frac{r_i + s_i \sqrt{\text{sf}(N_\alpha)}}{r_i - s_i \sqrt{\text{sf}(N_\alpha)}} - \zeta_4^{(j)} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right| \\ & \geq \frac{|1 + \sqrt{-1}|}{\left| \left(r_i - s_i \sqrt{\text{sf}(N_\alpha)} \right) \left(r_j - s_j \sqrt{\text{sf}(N_\alpha)} \right) \right|} = \frac{\sqrt{2} b}{\sqrt{f_i f_j} (y_i y_j)^{1/4}}, \end{aligned}$$

using (3.25) above.

Furthermore, from Proposition 3.1(b), we know that $f_i, f_j | b^2$, since $-N_\alpha$ is a square. So

$$\left| \zeta_4^{(i)} \frac{r_i + s_i \sqrt{\text{sf}(N_\alpha)}}{r_i - s_i \sqrt{\text{sf}(N_\alpha)}} - \zeta_4^{(j)} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right| \geq \frac{\sqrt{2}}{b (y_i y_j)^{1/4}}.$$

Combining this with (3.22), we have

$$(3.26) \quad \frac{\sqrt{2}}{b (y_i y_j)^{1/4}} < 0.5051 b^2 \sqrt{\frac{|N_\alpha|}{a^2 + |N_\alpha|}} \left(\frac{1}{y_i} + \frac{1}{y_j} \right).$$

From $y_j > y_i$, it follows that $1/y_i + 1/y_j < 2/y_i$ and so

$$y_j > \frac{4}{1.01024 b^{12}} \left(\frac{a^2 + |N_\alpha|}{|N_\alpha|} \right)^2 y_i^3.$$

Since $N_\alpha = a^2 - b^4 d < 0$, we have

$$(3.27) \quad y_j > \frac{3.84 d^2}{b^4 |N_\alpha|^2} y_i^3.$$

We can use this gap principle to improve its constant term. Combining (3.27) with $y_i \geq b^2 |N_\alpha| / d$, we obtain

$$y_j > \frac{3.84 d^2}{b^4 |N_\alpha|^2} \left(\frac{b^2 |N_\alpha|}{d} \right)^2 y_i = 3.84 y_i.$$

Applying this to (3.26) yields

$$\frac{\sqrt{2}}{b (y_i y_j)^{1/4}} < 0.5051 b^2 \sqrt{\frac{|N_\alpha|}{a^2 + |N_\alpha|}} \frac{1 + 1/3.84}{y_i}.$$

This implies that

$$y_j > \frac{24.34}{b^{12}} \left(\frac{a^2 + |N_\alpha|}{|N_\alpha|} \right)^2 y_i^3 = \frac{24.34 d^2}{b^4 |N_\alpha|^2} y_i^3.$$

Repeating the process from (3.27) onwards with 3.84 replaced by 24.34, we obtain

$$y_j > \frac{52.31 d^2}{b^4 |N_\alpha|^2} y_i^3.$$

Repeating it again with 52.31 instead of 3.84, we improve the constant to 56.97. Repeating it one final time with 56.97, we obtain the inequality in part (a).

(b) We again use (3.23) and (3.24). Notice that $x + y\sqrt{-\text{sf}(N_\alpha)}$ on the left-hand side of (3.24) for $\zeta_4^{(j)} = \pm\sqrt{-1}\zeta_4^{(i)}$ can be as small as $1/\left(2\sqrt{-\text{sf}(N_\alpha)}y\right)$ when $-N_\alpha$ is not a square, so the proof of part (a) breaks down here.

Among the three values $\zeta_4^{(k_1)}$, $\zeta_4^{(k_2)}$ and $\zeta_4^{(k_3)}$, there must be at least one pair such that one member of the pair is ± 1 times the other. Choose any such pair and let i and j be the associated indices, ordered so that $y_i < y_j$.

Thus,

$$\left| \zeta_4^{(i)} \frac{r_i + s_i \sqrt{\text{sf}(N_\alpha)}}{r_i - s_i \sqrt{\text{sf}(N_\alpha)}} - \zeta_4^{(j)} \frac{r_j + s_j \sqrt{\text{sf}(N_\alpha)}}{r_j - s_j \sqrt{\text{sf}(N_\alpha)}} \right| \geq \frac{2b}{\sqrt{f_i f_j} (y_i y_j)^{1/4}}.$$

The argument is the same as in the proof of part (a) except we have an extra factor of $\sqrt{2}$ on the right-hand side of this inequality. Thus

$$(3.28) \quad \frac{2b}{\sqrt{f_i f_j} (y_i y_j)^{1/4}} < 0.5051b^2 \sqrt{\frac{|N_\alpha|}{a^2 + |N_\alpha|}} \left(\frac{1}{y_i} + \frac{1}{y_j} \right).$$

As in the proof of part (a), this gives

$$y_j > 15.36 \left(\frac{b^2 d}{f_i f_j |N_\alpha|} \right)^2 y_i^3,$$

which establishes the first lower bound for y_j in part (b).

If $y_i > f_i f_j |N_\alpha| \sqrt{1.09/15.36}/(b^2 d)$, then this lower bound for y_j yields $y_j > 1.09y_i$. Applying this to (3.28), we obtain

$$y_j > 18.25 \left(\frac{b^2 d}{f_i f_j |N_\alpha|} \right)^2 y_i^3.$$

Repeating this process eight more times yields

$$y_j > 182 \left(\frac{b^2 d}{f_i f_j |N_\alpha|} \right)^2 y_i^3.$$

Since $f_i f_j \leq (4b^2)^2 |N_\alpha|$, if $y_i \geq 4.27b^2 |N_\alpha|^2 / d$, then $y_i > f_i f_j |N_\alpha| \sqrt{1.09/15.36}/(b^2 d)$, as required. \square

3.4. Miscellaneous Lemmas. Here we collect some results that we will need for bounding quantities that arise in the proof of the main result in the following section (Section 4).

Lemma 3.9. *Let the y_k 's be defined as in (1.1) with the notation and assumptions there. Suppose that $N_\alpha < 0$.*

(a) *Let $y_k \geq 4\sqrt{|N_\alpha|}/d$ be a square and put*

$$\omega_k = \left(x_k + N_{\varepsilon^k} \sqrt{N_\alpha} \right) / \left(x_k - N_{\varepsilon^k} \sqrt{N_\alpha} \right) = e^{i\varphi_k}$$

with $-\pi < \varphi_k \leq \pi$. Then

$$|\varphi_k| < \frac{2.29\sqrt{|N_\alpha|}}{|x_k|} < 0.6.$$

(b) Let y_k and y_ℓ be two squares with $k, \ell \neq 0$, $y_\ell > y_k \geq 4\sqrt{|N_\alpha|/d}$, ω_k be as in part (a) and put

$$x + y\sqrt{\text{sf}(N_\alpha)} = \left(r_k - s_k\sqrt{\text{sf}(N_\alpha)}\right) \left(r_\ell + s_\ell\sqrt{\text{sf}(N_\alpha)}\right)$$

with r_k, r_ℓ, s_k and s_ℓ as in Proposition 3.1. Furthermore, suppose that the quantities $\zeta_4^{(k)}$ and $\zeta_4^{(\ell)}$ defined in (3.20) in the proof of Lemma 3.8 satisfy $\zeta_4^{(k)} = \pm\zeta_4^{(\ell)}$. Then

$$\min_{0 \leq j \leq 3} \left| \omega_k^{1/4} - \zeta_4^j \frac{x + y\sqrt{\text{sf}(N_\alpha)}}{x - y\sqrt{\text{sf}(N_\alpha)}} \right|$$

occurs for either $j = 0$ or $j = 2$, where ζ_4 is a primitive 4-th root of unity.

Proof. (a) We can write $\omega_k = (|x_k| \pm \sqrt{N_\alpha})^2 / (x_k^2 + |N_\alpha|)$, so with $\omega_k = e^{i\varphi_k}$, we have $|\tan(\varphi_k)| = \left| 2x_k\sqrt{|N_\alpha|} / (x_k^2 + N_\alpha) \right|$. From (1.1) and $N_\alpha > -b^4d$, we have

$$x_k^2 + N_\alpha = dy_k^2 + 2N_\alpha = dy_k^2 \left(1 + \frac{2N_\alpha}{dy_k^2} \right) \geq 0.875dy_k^2 > 0.875x_k^2,$$

since $y_k \geq 4\sqrt{|N_\alpha|/d}$ and $x_k^2 - dy_k^2 = N_\alpha < 0$.

From $|\varphi_k| \leq |\tan(\varphi_k)|$, we have

$$|\varphi_k| \leq \left| \frac{2\sqrt{|N_\alpha|}x_k}{x_k^2 + N_\alpha} \right| < \left| \frac{2\sqrt{|N_\alpha|}x_k}{0.875x_k^2} \right| < \frac{2.29\sqrt{|N_\alpha|}}{|x_k|}.$$

Since $y_k \geq 4\sqrt{|N_\alpha|/d}$, we have $dy_k^2 \geq 16|N_\alpha|$ and so

$$x_k^2 = dy_k^2 + N_\alpha \geq 15|N_\alpha|.$$

Combining this with the inequality above it yields $|\varphi_k| < 2.29\sqrt{|N_\alpha|}/|x_k| < 2.29/\sqrt{15} < 0.6$.

(b) Recall that from (3.18) in the proof of Lemma 3.8, we can write

$$\begin{aligned} & \left(a + \sqrt{N_\alpha} \right) \left(r_i + s_i\sqrt{\text{sf}(N_\alpha)} \right)^4 - \left(a - \sqrt{N_\alpha} \right) \left(r_i - s_i\sqrt{\text{sf}(N_\alpha)} \right)^4 \\ &= \pm 2f_i^2\sqrt{N_\alpha} \end{aligned}$$

for $i = k, \ell$. There are other cases according to the signs in the result in Proposition 3.1, but the argument for them is identical to the argument that follows below.

Using this relationship for $i = \ell$ and using our expressions in Proposition 3.1 for $x_k + N_{\varepsilon^k} \sqrt{N_\alpha}$ and $f_k \sqrt{y_k}$, we have

$$\begin{aligned}
& \left(x_k + N_{\varepsilon^k} \sqrt{N_\alpha} \right) \left(r_k - s_k \sqrt{\text{sf}(N_\alpha)} \right)^4 \left(r_\ell + s_\ell \sqrt{\text{sf}(N_\alpha)} \right)^4 \\
& - \left(x_k - N_{\varepsilon^k} \sqrt{N_\alpha} \right) \left(r_k + s_k \sqrt{\text{sf}(N_\alpha)} \right)^4 \left(r_\ell - s_\ell \sqrt{\text{sf}(N_\alpha)} \right)^4 \\
& = \frac{(r_k^2 - \text{sf}(N_\alpha) s_k^2)^4}{f_k^2} \left[\left(a + \sqrt{N_\alpha} \right) \left(r_\ell + s_\ell \sqrt{\text{sf}(N_\alpha)} \right)^4 \right. \\
& \quad \left. - \left(a - \sqrt{N_\alpha} \right) \left(r_\ell - s_\ell \sqrt{\text{sf}(N_\alpha)} \right)^4 \right] \\
& = \frac{f_k^2 y_k^2}{b^4} \left[\left(a + \sqrt{N_\alpha} \right) \left(r_\ell + s_\ell \sqrt{\text{sf}(N_\alpha)} \right)^4 \right. \\
& \quad \left. - \left(a - \sqrt{N_\alpha} \right) \left(r_\ell - s_\ell \sqrt{\text{sf}(N_\alpha)} \right)^4 \right].
\end{aligned}$$

Applying equation (3.18) with $j = \ell$ to the last expression and with $x + y \sqrt{\text{sf}(N_\alpha)}$ as defined in the statement of this lemma, we have

$$\begin{aligned}
(3.29) \quad |f(x, y)| &= \left| \left(x_k + N_{\varepsilon^k} \sqrt{N_\alpha} \right) \left(x + y \sqrt{\text{sf}(N_\alpha)} \right)^4 \right. \\
&\quad \left. - \left(x_k - N_{\varepsilon^k} \sqrt{N_\alpha} \right) \left(x - y \sqrt{\text{sf}(N_\alpha)} \right)^4 \right| \\
&= \frac{2 f_k^2 f_\ell^2 y_k^2}{b^4} \sqrt{|N_\alpha|}.
\end{aligned}$$

Let ζ_4 be the 4-th root of unity satisfying

$$\left| \omega_k^{1/4} - \zeta_4 \frac{x - y \sqrt{\text{sf}(N_\alpha)}}{x + y \sqrt{\text{sf}(N_\alpha)}} \right| = \min_{0 \leq j \leq 3} \left| \omega_k^{1/4} - e^{2j\pi i/4} \frac{x - y \sqrt{\text{sf}(N_\alpha)}}{x + y \sqrt{\text{sf}(N_\alpha)}} \right|.$$

From (3.29), our expression in the statement of this lemma for $x + y \sqrt{\text{sf}(N_\alpha)}$, the expressions for y_k and y_ℓ in Proposition 3.1, and (1.1) (which implies that $|x_k - N_{\varepsilon^k} \sqrt{N_\alpha}|^2 = x_k^2 - N_\alpha = d y_k^2$), we have

$$\begin{aligned}
(3.30) \quad & \left| \omega_k - \left(\frac{x - y \sqrt{\text{sf}(N_\alpha)}}{x + y \sqrt{\text{sf}(N_\alpha)}} \right)^4 \right| \\
&= \frac{2 \sqrt{|N_\alpha|} f_k^2 f_\ell^2 y_k^2}{b^4 |x_k - N_{\varepsilon^k} \sqrt{N_\alpha}| \left| r_k \mp s_k \sqrt{\text{sf}(N_\alpha)} \right|^4 \left| r_\ell \mp s_\ell \sqrt{\text{sf}(N_\alpha)} \right|^4} \\
&= \frac{2 \sqrt{|N_\alpha|}}{\sqrt{d} y_\ell} \leq \frac{1}{2}.
\end{aligned}$$

since $y_\ell \geq 4 \sqrt{|N_\alpha|/d}$.

By Lemma 3.7(b) with $c_0 = 1/2 + 0.0001$,

$$(3.31) \quad \left| \omega_k^{1/4} - \zeta_4 \frac{x - y\sqrt{\text{sf}(N_\alpha)}}{x + y\sqrt{\text{sf}(N_\alpha)}} \right| < 0.1263.$$

From (3.22), along with $y_k, y_\ell \geq 4\sqrt{|N_\alpha|/d}$, we have

$$\begin{aligned} \left| \frac{\zeta_4^{(k)} x - y\sqrt{\text{sf}(N_\alpha)}}{\zeta_4^{(\ell)} x + y\sqrt{\text{sf}(N_\alpha)}} - 1 \right| &= \left| \zeta_4^{(k)} \frac{r_k + s_k\sqrt{\text{sf}(N_\alpha)}}{r_k - s_k\sqrt{\text{sf}(N_\alpha)}} - \zeta_4^{(\ell)} \frac{r_\ell + s_\ell\sqrt{\text{sf}(N_\alpha)}}{r_\ell - s_\ell\sqrt{\text{sf}(N_\alpha)}} \right| \\ &< 0.5051b^2 \frac{\sqrt{|N_\alpha|}}{\sqrt{a^2 + |N_\alpha|}} \left(\frac{1}{y_k} + \frac{1}{y_\ell} \right) < 0.253. \end{aligned}$$

From part (a), we have $|\varphi_k| < 0.6$, so $|\omega_k^{1/4} - 1| < 0.15$ and

$$\left| \omega_k^{1/4} - \frac{\zeta_4^{(k)} x - y\sqrt{\text{sf}(N_\alpha)}}{\zeta_4^{(\ell)} x + y\sqrt{\text{sf}(N_\alpha)}} \right| \leq \left| \omega_k^{1/4} - 1 \right| + \left| \frac{\zeta_4^{(k)} x - y\sqrt{\text{sf}(N_\alpha)}}{\zeta_4^{(\ell)} x + y\sqrt{\text{sf}(N_\alpha)}} - 1 \right| < 0.403.$$

Recalling (3.31), it follows that

$$\begin{aligned} &\left| \omega_k^{1/4} - \zeta'_4 \frac{(x - y\sqrt{\text{sf}(N_\alpha)})}{(x + y\sqrt{\text{sf}(N_\alpha)})} \right| \\ &= \left| \omega_k^{1/4} - \zeta_4 \frac{x - y\sqrt{\text{sf}(N_\alpha)}}{x + y\sqrt{\text{sf}(N_\alpha)}} + (\zeta_4 - \zeta'_4) \frac{x - y\sqrt{\text{sf}(N_\alpha)}}{x + y\sqrt{\text{sf}(N_\alpha)}} \right| \\ &\geq |\zeta_4 - \zeta'_4| - \left| \omega_k^{1/4} - \zeta_4 \frac{x - y\sqrt{\text{sf}(N_\alpha)}}{x + y\sqrt{\text{sf}(N_\alpha)}} \right| > \sqrt{2} - 0.127, \end{aligned}$$

for any 4-th root of unity, ζ'_4 , with $\zeta'_4 \neq \zeta_4$. Since this exceeds 0.403, it follows that $\zeta_4 = \zeta_4^{(k)}/\zeta_4^{(\ell)} = \pm 1$, the last equality holding by our assumption in the statement of this lemma. \square

In Lemma 3.10, we establish a gcd result for elements of a generalisation of our sequences. This will help us prove Lemmas 3.11 and 3.12. Lemma 3.12 is used in the proof of Proposition 4.1, as well as in the proof of Theorem 1.4. Lemma 3.12 will be particularly important for showing that the possible exceptions to Conjecture 1.2 in the statement of Theorem 1.4 can only possibly occur for $u = 1$ or $u = 2$.

Lemma 3.10. *Let $(x_k)_{k=0}^\infty$ and $(y_k)_{k=0}^\infty$ be sequences defined by $x_k + y_k\sqrt{d} = (a + b\sqrt{d})\varepsilon^k$, where a, b, d are positive integers, d is not a square and $\varepsilon = (t + u\sqrt{d})/2 \neq \pm 1$, with t and u integers, is a unit in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$.*

If x_k and y_k are both integers and $\gcd(a, b)$ is odd, then $\gcd(x_k, y_k) / \gcd(a, b) = 1$ or 2 .

The additional hypothesis that $\gcd(a, b)$ is odd was omitted from the published version of this lemma. If $\gcd(a, b)$ is even, then $\gcd(x_k, y_k) / \gcd(a, b) = 1/2$ also occurs.

Proof. We may assume without loss of generality that $\gcd(a, b) = 1$. Otherwise, consider below the sequences $(x_k / \gcd(a, b))_{k=0}^{k=\infty}$ and $(y_k / \gcd(a, b))_{k=0}^{k=\infty}$ instead of $(x_k)_{k=0}^{k=\infty}$ and $(y_k)_{k=0}^{k=\infty}$. Since $x_0 = a$, $x_1 = (at + bdu)/2$, $x_{-1} = \pm(at - dbu)/2$, $y_0 = b$, $y_1 = (au + bt)/2$, $y_{-1} = \pm(au - bt)/2$, the recurrence relation satisfied by both sequences has integer coefficients and $\gcd(a, b)$ is odd, we see that $x_k / \gcd(a, b)$ and $y_k / \gcd(a, b)$ are integers if and only if x_k and y_k are integers.

We start with some relationships that we will require for the proof itself.

Throughout the proof, we will use the fact that both the x_k 's and y_k 's satisfy the recurrence relation

$$(3.32) \quad u_k = \text{Tr}(\varepsilon) u_{k-1} - N_\varepsilon u_{k-2} = tu_{k-1} \pm u_{k-2}.$$

Next, we show that

$$(3.33) \quad ux_k - ty_k = -2N_\varepsilon y_{k-1} \quad \text{and} \quad tx_k - duy_k = 2N_\varepsilon x_{k-1}$$

for $k \geq 1$.

For $k = 1$, we have $x_1 = (at + bdu)/2$ and $y_1 = (au + bt)/2$, so we find $ux_1 - ty_1 = -2bN_\varepsilon = -2y_0N_\varepsilon$. Similarly, $tx_1 - duy_1 = 2N_\varepsilon x_0$ holds.

Similarly, we can prove the relationship holds for $k = 2$.

For $k \geq 3$, we use induction and the recurrence relations in (3.32):

$$\begin{aligned} ux_k - ty_k &= u \text{Tr}(\varepsilon) x_{k-1} - uN_\varepsilon x_{k-2} - t \text{Tr}(\varepsilon) y_{k-1} + tN_\varepsilon y_{k-2} \\ &= \text{Tr}(\varepsilon) (-2)N_\varepsilon y_{k-2} - N_\varepsilon (-2)N_\varepsilon y_{k-3} \\ &= (-2)N_\varepsilon y_{k-1}. \end{aligned}$$

The proof of $tx_k - duy_k = 2N_\varepsilon x_{k-1}$ is identical, so we omit it here.

We will also need

$$(3.34) \quad \begin{aligned} \frac{tu}{N_\varepsilon} x_k - \frac{t^2 + du^2}{2N_\varepsilon} y_k &= -2N_\varepsilon y_{k-2} \quad \text{and} \\ \frac{t^2 + du^2}{2N_\varepsilon} x_k - \frac{dtu}{N_\varepsilon} y_k &= 2N_\varepsilon x_{k-2}, \end{aligned}$$

for $k \geq 2$ and

$$(3.35) \quad \begin{aligned} \left(\frac{u(3t^2 + du^2)}{4N_\varepsilon^2} \right) x_k - \left(\frac{t(t^2 + 3du^2)}{4N_\varepsilon^2} \right) y_k &= -2N_\varepsilon y_{k-3} \quad \text{and} \\ \left(\frac{t(t^2 + 3du^2)}{4N_\varepsilon^2} \right) x_k - \left(\frac{du(3t^2 + du^2)}{4N_\varepsilon^2} \right) y_k &= 2N_\varepsilon x_{k-3}, \end{aligned}$$

for $k \geq 3$, which both follow from (3.33).

Writing $3t^2 + du^2 = -4N_\varepsilon + 4t^2$ and $t^2 + 3du^2 = 4N_\varepsilon + 4du^2$, we see that the coefficients of x_k and y_k in the relationships in (3.35) are integers.

We divide the remainder of the proof into cases according to the parity of t and u .

(i) Suppose that t and u are both even. Then x_k and y_k are both integers. Furthermore in this case, the coefficients of x_k and y_k in (3.33) can all be divided by 2 to eliminate the factors of 2 on the right-hand sides. So in this case, we find that

$$\gcd(x_k, y_k) \mid \gcd(x_{k-1}, y_{k-1}) \mid \cdots \mid \gcd(x_0, y_0) = 1.$$

(ii) Next suppose that t and u are both odd. In this case, we must have $d \equiv 5 \pmod{8}$, since ε is a unit and hence $t^2 - du^2 \equiv 4 \pmod{8}$.

(ii-a) Suppose that a and b have opposite parities. In this case, $y_1 = (au + bt)/2$ cannot be an integer. Similarly, $2x_1$ is odd.

Since $\left(\frac{t + u\sqrt{d}}{2}\right)^2 = (t^2 + u^2d)/4 + (tu/2)\sqrt{d} = (t_2 + u_2\sqrt{d})/2$, where $t^2 + u^2d = \pm 4 + 2du^2 \equiv 2 \pmod{4}$, it follows that t_2 and u_2 are both odd. Hence x_2 and y_2 are not integers. However,

$$\left(\frac{t + u\sqrt{d}}{2}\right)^3 = \frac{t^3 + 3tu^2d}{8} + \frac{3t^2u + u^3d}{8}\sqrt{d} = \frac{t_3 + u_3\sqrt{d}}{2},$$

where $t^3 + 3tu^2d = t(t^2 + 3u^2d) = t(\pm 4 + 4u^2d) \equiv 0 \pmod{8}$ and $3t^2u + u^3d = -u(-4t^2 \pm 4) \equiv 0 \pmod{8}$. So both t_3 and u_3 are even. Hence x_3 and y_3 are both integers.

By an inductive argument using the recurrence relations for the x_k 's and y_k 's in (3.32), one finds that x_k and y_k are both integers if and only if $3|k$, when t and u are both odd and a and b have opposite parities. So we consider only $\gcd(x_{3k}, y_{3k})$.

Since t and du are both odd in this case, we have $3t^2 + du^2 = -4N_\varepsilon + 4t^2 \equiv 0 \pmod{8}$ and $t^2 + 3du^2 = 4N_\varepsilon + 4du^2 \equiv 0 \pmod{8}$, so the coefficients of x_k and y_k in (3.35) can all be divided by 2 to eliminate the factors of 2 on the right-hand sides there. Thus, $\gcd(x_k, y_k) \mid \gcd(x_{k-3}, y_{k-3}) \mid \cdots \mid \gcd(x_0, y_0) = 1$.

(ii-b) If a and b have the same parity, then $y_1 = (au + bt)/2 \in \mathbb{Z}$. Similarly, $x_1 \in \mathbb{Z}$. Using the recurrence relations in (3.32), the x_k 's and y_k 's are integers.

As in case (ii-a), we can remove the factor of 2 on the right-hand side of (3.35). So we find that if $k \equiv k_1 \pmod{3}$ with $0 \leq k_1 \leq 2$, then $\gcd(x_k, y_k) \mid \gcd(x_{k_1}, y_{k_1})$.

So if $3|k$, then $\gcd(x_k, y_k) \mid \gcd(x_0, y_0)$.

If $k \equiv 1 \pmod{3}$, then $\gcd(x_k, y_k) \mid \gcd(x_1, y_1)$. From (3.33),

$$\gcd(x_1, y_1) \mid 2 \gcd(x_0, y_0).$$

If $k \equiv 2 \pmod{3}$, then $\gcd(x_k, y_k) \mid \gcd(x_2, y_2)$. From (3.33),

$$\gcd(x_2, y_2) \mid (2 \gcd(x_1, y_1)) \mid (4 \gcd(x_0, y_0)).$$

We now consider the parity of x_k and y_k . Since $\gcd(a, b) = 1$, at least one of x_0 or y_0 is odd.

Suppose first that y_0 is odd. Since t is odd, we find that $y_2 = ty_1 \pm y_0$ is even if y_1 is odd and y_2 is odd otherwise.

In the first case (when y_1 is odd), we have $\gcd(x_1, y_1) \mid \gcd(x_0, y_0)$ and hence

$$\gcd(x_2, y_2) \mid (2 \gcd(x_1, y_1)) \mid (2 \gcd(x_0, y_0)).$$

In the second case (when y_1 is even), we have $\gcd(x_2, y_2) \mid \gcd(x_1, y_1)$ and hence

$$\gcd(x_2, y_2) \mid \gcd(x_1, y_1) \mid (2 \gcd(x_0, y_0)).$$

Now we suppose that x_0 is odd. Since t is odd, we find that $x_2 = tx_1 + x_0$ is even if x_1 is odd and x_2 is odd otherwise. As above, we find that

$$\gcd(x_2, y_2) \mid (2 \gcd(x_0, y_0)).$$

(iii) Now suppose that t is even and u is odd. In this case, $4|d$.

Since $y_1 = (au + bt)/2$, we see that $y_1 \in \mathbb{Z}$ if and only if a is even. Hence all the y_k 's are integers if a is even. Since t is even, using the recurrence relation for the y_k 's in (3.32), we see that for a odd, $y_k \in \mathbb{Z}$ when k is even and $y_k \notin \mathbb{Z}$ otherwise.

Since $x_1 = (at + bdu)/2$ and t and d are both even, we see that $x_1 \in \mathbb{Z}$. Hence, by the recurrence relation for the x_k 's in (3.32), $x_k \in \mathbb{Z}$ always holds.

Here we use (3.34), observing that the coefficients of x_k and y_k on the left-hand sides are all even. So we have relationships with integer coefficients and without the factor of 2 on the right-hand sides. Hence

$$\gcd(x_k, y_k) \text{ divides } \begin{cases} \gcd(x_0, y_0) = 1 & \text{if } k \text{ is even,} \\ \gcd(x_1, y_1) \mid (2 \gcd(x_0, y_0)) = 2 & \text{if } k \text{ is odd.} \end{cases}$$

(iv) We cannot have t odd and u even because $t^2 - du^2 \equiv 0 \pmod{4}$. \square

We will use Lemma 3.11 in the proof of Lemma 3.12.

Lemma 3.11. *Let the sequences $(x_k)_{k=-\infty}^{\infty}$ and $(y_k)_{k=-\infty}^{\infty}$ be as defined in (1.1), with the notation and assumptions there. Suppose that $k \neq 0$, $\gcd(a, b) = 1$, $N_\alpha < 0$ and that x_k and y_k are both integers. Using the notation of Subsection 2.1 with $t' = \text{sf}(N_\alpha)$, $u_1 = 2x_k$ and $u_2 = \pm 2\sqrt{N_\alpha/\text{sf}(N_\alpha)}$, then*

$$g^2/\gcd(a^2, db^4) = 2^m, \text{ where } m \geq 0.$$

Remark. With more work, one can show that $m = 0, 1, 2, 4$.

Proof. We break the proof into several cases.

(1) Suppose that $p > 2$ is prime.

Put $v_p(g^2) = v_p(g_1^2 g_2/g_3) = \ell$. Since g_3 is a power of 2, it follows that $v_p(g_3) = 0$ and hence $\ell \geq 0$. We will prove that $v_p(\gcd(a^2, d)) = \ell$. We also put $v_p(g_1^2) = \ell_1$ and $v_p(g_2) = \ell_2$. Note that $\ell_2 = 0$ or 1, since $g_2 \mid \text{sf}(N_\alpha)$ (from the definition of g_2 , we have $g_2 \mid t'$ and here $t' = \text{sf}(N_\alpha)$). Since $v_p(g_3) = 0$, we have $\ell = \ell_1 + \ell_2$.

Since $g_1 \mid u_2$, by the definition of g_1 , and from the expression for u_2 here, we have $p^{\ell_1} \mid (N_\alpha/\text{sf}(N_\alpha))$. Similarly, from $g_2 \mid \text{sf}(N_\alpha)$, it follows that $p^{\ell_2} \mid \text{sf}(N_\alpha)$. So $p^\ell \mid N_\alpha$.

In the same way, we find that $p^{\ell_1+2\ell_2} \mid x_k^2$. So $p^\ell \mid x_k^2$ too.

By Lemma 3.10 and $\gcd(a, b) = 1$, since p is odd, $p \nmid \gcd(x_k, y_k)$. Hence, from $x_k^2 - dy_k^2 = N_\alpha$, we have $p^\ell \mid d$. Combining this with $p^\ell \mid N_\alpha$ and $N_\alpha = a^2 - db^4$, we find that $p^\ell \mid a^2$. So $p^\ell \mid \gcd(a^2, d)$.

We now show that $p^{\ell+1} \nmid \gcd(a^2, d)$, so that the denominator of $g^2/\gcd(a^2, d)$ has no odd prime factors.

Suppose that $p^{\ell+1} \mid \gcd(a^2, d)$. Then $p^{\ell+1} \mid N_\alpha$. Also $p^{\ell+1} \mid x_k^2$ follows from $x_k^2 - dy_k^2 = N_\alpha$. By the definition of ℓ_1 and g_1 , this means that $p^{\ell_1} \parallel N_\alpha/\text{sf}(N_\alpha)$.

If $p \nmid \text{sf}(N_\alpha)$, then $p^{\ell_1} \parallel N_\alpha$, but $\ell_1 < \ell + 1 = \ell_1 + \ell_2 + 1$, contradicting $p^{\ell+1} \mid N_\alpha$.

If $p \mid \text{sf}(N_\alpha)$, then $p^{\ell_1+1} \parallel N_\alpha$. We must have $\ell_2 = 0$, since otherwise $\ell_1 + 1 < \ell_1$ and we get a contradiction to $p^{\ell+1} \mid N_\alpha$. In this case, $p \nmid (x_k^2/g_1^2)$. So $p^{\ell_1} \parallel x_k^2$. But this contradicts $p^{\ell+1} \mid x_k^2$. Hence $p^{\ell+1} \nmid \gcd(a^2, d)$. Therefore, for all primes $p > 2$, $v_p(g^2/\gcd(a^2, d)) = 0$.

(2) We now consider $p = 2$.

Put $v_2(\gcd(a^2, db^4)) = \ell$. Since $\gcd(a, b) = 1$, we also have $v_2(\gcd(a^2, d)) = \ell$. So $2^\ell | N_\alpha$ too. From $x_k^2 - dy_k^2 = N_\alpha$, we find that $2^\ell | x_k^2$. Hence $2^\ell | \gcd(x_k^2, N_\alpha)$.

Furthermore, if $v_2(a^2) = v_2(db^4) = \ell$, then $2^{\ell+1} | N_\alpha$.

(2.1) Suppose that $2 \nmid \text{sf}(N_\alpha)$.

We have $v_2(g_1^2) = v_2(4 \gcd(x_k^2, N_\alpha)) \geq \ell + 2$. Also $v_2(g_2) = 1$. Hence $v_2(g^2) = v_2(g_1^2/g_3) \geq \ell$, recalling that $g_3 = 1, 2$ or 4 .

(2.2) Suppose that $2 | \text{sf}(N_\alpha)$.

Here $v_2(g_1^2) = v_2(\gcd(4x_k^2, 4N_\alpha/\text{sf}(N_\alpha))) = v_2(4 \gcd(x_k^2, N_\alpha/2)) \geq \ell + 1$. We break this case into subcases.

(2.2.1) If $v_2(a^2) = v_2(db^4) = \ell$, then $v_2(N_\alpha) \geq \ell + 1$. So $v_2(g_1^2) = v_2(4 \gcd(x_k^2, N_\alpha/2)) \geq \ell + 2$. Here $v_2(g_2) \geq 1$, so as in case (2.1), we have $v_2(g^2) \geq \ell$, as required.

(2.2.2) If $v_2(a^2) \neq v_2(db^4)$, then $v_2(N_\alpha) = \ell$. So $v_2(g_1^2) = v_2(4N_\alpha/\text{sf}(N_\alpha)) = \ell + 1$, since $2 | \text{sf}(N_\alpha)$. From $v_2(g_1^2) = \ell + 1$, it also follows that ℓ must be odd.

From $x_k^2 - dy_k^2 = N_\alpha$ and $v_2(N_\alpha) = \ell$, we have either $v_2(x_k^2) = \ell$ and $v_2(dy_k^2) \geq \ell + 1$; or else $v_2(x_k^2) \geq \ell + 1$ and $v_2(dy_k^2) = \ell$. The first case is not possible because ℓ is odd. In the latter case, we must have $v_2(d) = \ell$ and $2 \nmid y_k$. Also,

$$v_2(u_1/g_1) = (1/2)v_2(4x_k^2/g_1^2) \geq (1/2)(\ell + 3 - (\ell + 1)) = 1,$$

so $v_2(g_2) = 1$. Hence $v_2(g^2) = v_2(g_1^2 g_2/g_3) = v_2(g_1^2 g_2/4) = \ell$. \square

Lemma 3.12. Suppose that $a, b, d, g, t', u_1, u_2, x_k$ and y_k are as in Lemma 3.11, $d' = u_2^2 t'/g^2$, as defined in (2.6), $\mathcal{N}_{d',4}$ is as defined in (2.1) and put $b' = N_\alpha/\gcd(a^2, db^4)$. Then

$$(3.36) \quad |g| \mathcal{N}_{d',4} = \sqrt{\gcd(a^2, db^4)} 2^{1+\min(2, v_2(b')/2)} \geq 2^{1+\min(2, v_2(N_\alpha)/2)}.$$

Proof. Since $\gcd(a^2, db^4) \geq 2^{v_2(\gcd(a^2, db^4))}$, the inequality in equation (3.36) holds.

To establish the equality in equation (3.36), we use Lemma 3.11. From that lemma, we can write $g^2 = 2^m \gcd(a^2, db^4)$, where $m \geq 0$. From (2.1) with $n = 4$, we find that $\mathcal{N}_{d',4}^2 = 2^{\min(v_2(d'), 6)}$. So, squaring both sides of the equality in (3.36), it is equivalent to

$$2^{\min(6+m, v_2(d')+m)} = 2^{\min(6, v_2(4b'))}.$$

From the definition of d' and Lemma 3.11, we have $d' = 4N_\alpha/g^2 = 4N_\alpha/(2^m \gcd(a^2, db^4))$. Applying this, along with the definition of b' , it follows that the equality in (3.36) is equivalent to

$$\min(6 + m, v_2(4N_\alpha/\gcd(a^2, db^4))) = \min(6, v_2(4N_\alpha/\gcd(a^2, db^4))).$$

To show that this equality holds, we prove that if $v_2(4N_\alpha/\gcd(a^2, db^4)) > 6$, then $m = 0$ (i.e., $g^2 = \gcd(a^2, db^4)$). Putting $\ell = v_2(\gcd(a^2, db^4))$, we must have $v_2(a^2) = v_2(db^4) = v_2(d) = \ell$. The second-last equality holds because $\gcd(a, b) = 1$. From Lemma 3.10, we have $\gcd(x_k, y_k) = 1, 2$. We will show that y_k is odd and hence $\gcd(x_k, y_k) = 2$ is not possible here.

We assume that y_k is even and derive a contradiction. From $x_k^2 - dy_k^2 = N_\alpha$, we have $(x_k/2^{\ell/2+1})^2 - (d/2^\ell)(y_k/2)^2 = N_\alpha/2^{\ell+2}$. Since $v_2(4N_\alpha/\gcd(a^2, db^4)) > 6$, we have $v_2(N_\alpha) \geq \ell + 5$. It follows that $x_k/2^{\ell/2+1}$ and $y_k/2$ are both odd. Arguing mod 8, we find that $d \equiv 1 \pmod{8}$ and that t and u must both be even.

From (1.2), we can write $4y_k = (b^2(2du^2 \pm 4) \pm 2atu)$ for some positive integers t and u with $t^2 - du^2 = \pm 4$. Since t and u are both even, it follows that $v_2(4y_k) = v_2(2du^2 \pm 4) = 2$. This contradicts the assumption that y_k is even.

From y_k is odd and $(x_k/2^{\ell/2})^2 - (d/2^\ell)y_k^2 = N_\alpha/2^\ell$, we have

$$v_2(g_1^2) = \min(v_2(4x_k^2), v_2(4N_\alpha/\text{sf}(N_\alpha))) = v_2(4x_k^2) = \ell + 2.$$

This also implies that $v_2(4x_k^2/g_1^2) = 0$, so $v_2(g_2) = 0$.

Furthermore, since $v_2(4x_k^2) < v_2(4N_\alpha/\text{sf}(N_\alpha))$, we also have $g_3 = 4$. Hence $g^2 = \gcd(a^2, db^4)$, as desired and the lemma follows. \square

The quantities in Lemma 3.13 are related to the quantities E and Q that we will use in the proof of Proposition 4.1.

Lemma 3.13. *Suppose that $b = 1$, x_k and y_k are both integers with $y_k > 1$ and that g and $\mathcal{N}_{d',4}$ are as above.*

If $d \geq 105$, then

$$(3.37) \quad \frac{0.1832|g|\mathcal{N}_{d',4}\sqrt{d}y_k}{|N_\alpha|} > 1.13$$

and

$$(3.38) \quad \frac{21.12\sqrt{d}y_k}{|g|\mathcal{N}_{d',4}} > 217.$$

Remark. Our choice of the lower bound for d comes from an example of $E < 1$ for $d = 104$: $a = 9$, $d = 104$, $N_\alpha = -23$, $k = -1$, $x_k = -61$ and $y_k = 11$ where $E = 0.973\dots$

Proof. We first obtain an analytic lower bound for d such that (3.37) and (3.38) hold for larger d .

We have $|g|\mathcal{N}_{d',4} \geq 2^{1+\min(v_2(N_\alpha)/2,2)} \geq 2$ from (3.36). Since $b = 1$, from Lemma 3.5(c), we find that $y_k \geq |N_\alpha|/4$ holds, so

$$\frac{0.1832|g|\mathcal{N}_{d',4}\sqrt{d}y_k}{|N_\alpha|} > 0.091\sqrt{d}.$$

For $d \geq 155$, we find that $0.091\sqrt{d} > 1.13$ holds.

Similarly,

$$\frac{21.12\sqrt{d}y_k}{|g|\mathcal{N}_{d',4}} \geq \frac{21.12\sqrt{d}(|N_\alpha|/4)}{8\sqrt{|N_\alpha|}} \geq 0.66\sqrt{d},$$

where we use $|g|\mathcal{N}_{d',4} \leq 8\sqrt{|N_\alpha|}$ from (3.36) and Lemma 3.5(c) with $u \geq 1$ to establish the first inequality. For $d \geq 109,000$, we find that $0.66\sqrt{d} > 217$ holds.

We complete the proof computationally, checking all the remaining pairs, (a, d) . Since d is bounded and $N_\alpha < 0$ (so $a^2 < d$), there are only finitely many such pairs.

For each pair, we check (3.37) and (3.38) by computing their left-hand sides for all $k \neq 0$ such that $0.1832 \cdot 2^{1+\min(v_2(b)/2,2)}\sqrt{d}y_k/b < 2$ and $21.12y_k/2^{1+\min(v_2(b)/2,2)} < 300$. No counterexamples to (3.37) and (3.38) were found. A PARI/GP program took 112 seconds to run on a Windows 10 laptop with an Intel i7-9750H processor and 16 GB of RAM.

The smallest value of the left-hand side of (3.37) found for $d \geq 105$ was $1.139\dots$, for $a = 11$, $d = 140$, $N_\alpha = -19$, $k = -1$, $x_k = -59$ and $y_k = 5$. The smallest value of the

left-hand side of (3.38) found for $d \geq 105$ was $217.3\dots$, for $a = 10$, $d = 140$, $N_\alpha = -40$, $k = -1$, $x_k = -130$ and $y_k = 11$. □

4. PROPOSITION 4.1 AND ITS PROOF

Our results in Subsection 1.4 follow from the next proposition.

Proposition 4.1. *Let $(y_k)_{k=-\infty}^\infty$ be defined by (1.1).*

If $b = 1$ and $-N_\alpha$ is a square, then there is at most one integer square among all distinct elements of $(y_k)_{k=-\infty}^\infty$ which satisfies

$$y_k > \max \left(1, \frac{76 |N_\alpha|^{3/2}}{\sqrt{d} (|g| \mathcal{N}_{d',4})^2} \right).$$

Conjecture 1.2 would immediately follow when $-N_\alpha$ is a square, if we could replace the lower bound for y_k in Proposition 4.1 with $\max(1, |N_\alpha|/4)$. This is due to Lemma 3.5.

4.1. Prerequisites. In this subsection, we collect some inequalities what will be required in the subsections that follow.

We will suppose that there are two distinct squares, y_k and y_ℓ , in the sequence with $y_\ell > y_k > 1$. So $y_\ell > y_k \geq 4 \geq \max \left(4\sqrt{|N_\alpha|/d}, |N_\alpha|/d \right)$ (since $b = 1$ and $N_\alpha = a^2 - bd^4 < 0$, so $|N_\alpha| < d$), as required in our lemmas above.

We shall initially assume that

$$(4.1) \quad d \geq 105.$$

This is the condition in Lemma 3.13, which will allow us to bound E and Q from below. This assumption shall be removed at the end of the proof in Subsection 4.6.

As in Lemma 3.9, we put $\omega_k = (x_k + N_{\varepsilon^k} \sqrt{N_\alpha}) / (x_k - N_{\varepsilon^k} \sqrt{N_\alpha})$ and let ζ_4 be the 4-th root of unity such that

$$\left| \omega_k^{1/4} - \zeta_4 \frac{x - y \sqrt{\text{sf}(N_\alpha)}}{x + y \sqrt{\text{sf}(N_\alpha)}} \right| = \min_{0 \leq j \leq 3} \left| \omega_k^{1/4} - e^{2j\pi i/4} \frac{x - y \sqrt{\text{sf}(N_\alpha)}}{x + y \sqrt{\text{sf}(N_\alpha)}} \right|,$$

where $x + y \sqrt{\text{sf}(N_\alpha)} = (r_k - s_k \sqrt{\text{sf}(N_\alpha)}) (r_\ell + s_\ell \sqrt{\text{sf}(N_\alpha)})$ with (r_k, s_k) and (r_ℓ, s_ℓ) as in Proposition 3.1, which are associated with (x_k, y_k) and (x_ℓ, y_ℓ) , respectively. From (3.31) in the proof of Lemma 3.9(b), we have

$$\left| \omega_k^{1/4} - \zeta_4 \frac{x - y \sqrt{\text{sf}(N_\alpha)}}{x + y \sqrt{\text{sf}(N_\alpha)}} \right| < 0.127.$$

Thus we can apply Lemma 3.7(a) with $c_1 = 0.127$ to find that

$$(4.2) \quad \frac{2\sqrt{|N_\alpha|}}{\sqrt{d} y_\ell} = \left| \omega_k - \left(\frac{x - y \sqrt{\text{sf}(N_\alpha)}}{x + y \sqrt{\text{sf}(N_\alpha)}} \right)^4 \right| > 3.959 \left| \omega_k^{1/4} - \zeta_4 \frac{x - y \sqrt{\text{sf}(N_\alpha)}}{x + y \sqrt{\text{sf}(N_\alpha)}} \right|.$$

The equality on the left-hand side is from the equalities in (3.30).

By our choice of k and ℓ , and by Lemma 3.9(b) when $-N_\alpha$ is not a square, $\zeta_4 = \pm 1 \in \mathbb{Q}(\sqrt{\text{sf}(N_\alpha)})$. This is important for us here as $\zeta_4 \left(x - y\sqrt{\text{sf}(N_\alpha)} \right) / \left(x + y\sqrt{\text{sf}(N_\alpha)} \right)$ must be in an imaginary quadratic field in order to apply Lemma 2.1 to obtain a lower bound for the rightmost quantity in (4.2).

We need to derive a lower bound for the far-right quantity in (4.2). To do so, we shall use the lower bounds in Lemma 2.1 with a sequence of good approximations p_r/q_r obtained from the hypergeometric functions. So we collect here the required quantities.

Since $y_k \geq 4$ and $N_\alpha > -db^4 = -d$ with $b = 1$ here, we obtain

$$(4.3) \quad x_k^2 = dy_k^2 + N_\alpha > d(y_k^2 - 1) \geq 0.9375dy_k^2.$$

So

$$(4.4) \quad \sqrt{x_k^2 - N_\alpha} = \sqrt{dy_k^2} < 1.04|x_k|.$$

Using the notation of Subsection 2.1, let $t' = \text{sf}(N_\alpha)$, $u_1 = 2x_k$, $u_2 = 2\sqrt{N_\alpha/\text{sf}(N_\alpha)}$ and d' is as defined in (2.6).

Substituting these quantities along with $\mathcal{D}_4 = e^{1.68}$ from Lemma 2.3(a) into the definition of E in (2.9) and applying (4.3), we have

$$(4.5) \quad \begin{aligned} E &= \frac{|g|\mathcal{N}_{d',4}||u_1| + \sqrt{u_1^2 - t'u_2^2}|}{\mathcal{D}_4 u_2^2 |t'|} = \frac{|g|\mathcal{N}_{d',4}||2x_k| + 2\sqrt{x_k^2 - N_\alpha}|}{4e^{1.68}|N_\alpha|} \\ &> \frac{|g|\mathcal{N}_{d',4}||x_k| + \sqrt{x_k^2 - N_\alpha}|}{10.74|N_\alpha|} > \frac{|g|\mathcal{N}_{d',4}(1 + \sqrt{0.9375})\sqrt{d}y_k}{10.74|N_\alpha|} \\ &> \frac{0.1832|g|\mathcal{N}_{d',4}\sqrt{d}y_k}{|N_\alpha|}. \end{aligned}$$

From (3.38) in Lemma 3.13, we have $E > 1.13 > 1$, as required for its use with Lemma 2.1.

Similarly, using (4.3) and (3.38) in Lemma 3.13, we have

$$(4.6) \quad Q > \frac{2e^{1.68}(1 + \sqrt{0.9375})\sqrt{d}y_k}{|g|\mathcal{N}_{d',4}} > 217,$$

so the condition $Q > 1$ in Lemma 2.1 is satisfied.

From $N_\alpha < 0$ and the equality in (4.4), we have $x_k < \sqrt{x_k^2 - N_\alpha} = \sqrt{d}y_k$, so from Lemma 2.3(a) we have

$$(4.7) \quad Q = \frac{e^{1.68}||2x_k| + 2\sqrt{x_k^2 - N_\alpha}||}{|g|\mathcal{N}_{d',4}} < 4\frac{e^{1.68}\sqrt{d}y_k}{|g|\mathcal{N}_{d',4}} < \frac{21.47\sqrt{d}y_k}{|g|\mathcal{N}_{d',4}}.$$

Recall from (2.8) that we take $k_0 = 0.89$.

Writing $\omega_k = e^{i\varphi_k}$, with $-\pi < \varphi_k \leq \pi$, from Lemmas 2.3(a) and 3.9(a), we can take

$$(4.8) \quad \ell_0 = \mathcal{C}_{4,2}|\varphi_k| < 0.458\sqrt{|N_\alpha|}/|x_k|.$$

Also from Lemma 3.9(a), we have $|\varphi_k| < 0.6$, so the condition $|\omega_k - 1| < 1$ in Lemma 2.2 is satisfied.

Let $q = x + y\sqrt{\text{sf}(N_\alpha)} = \left(r_k - s_k\sqrt{\text{sf}(N_\alpha)}\right)\left(r_\ell + s_\ell\sqrt{\text{sf}(N_\alpha)}\right)$ and $p = x - y\sqrt{\text{sf}(N_\alpha)}$. Recall from (3.25) with $b = 1$ that

$$(4.9) \quad |q| = \sqrt{f_k f_\ell} (y_k y_\ell)^{1/4}.$$

We are now ready to deduce the required contradiction from the assumption that there are two sufficiently large squares when $-N_\alpha$ is a square. We will break the proof into five parts.

With r_0 as in Lemma 2.1, we separate the case of $\zeta_4 p/q \neq p_{r_0}/q_{r_0}$ for all 4-th roots of unity, ζ_4 , from the case of $\zeta_4 p/q = p_{r_0}/q_{r_0}$ for some 4-th root of unity, ζ_4 . In the first case, Lemma 2.1 provides a suitable lower bound for the approximation. But in the second case, Lemma 2.1 is not strong enough, so we work directly with the approximations themselves.

4.2. $r_0 = 1$ and $\zeta_4 p/q \neq p_1/q_1$ for all 4-th roots of unity, ζ_4 . We start by determining an upper bound for y_ℓ for all $r_0 \geq 1$ when $\zeta_4 p/q \neq p_{r_0}/q_{r_0}$, since we will also need such a result in Subsection 4.4.

From (4.2), along with Lemma 2.1(b) and (4.9), we have

$$(4.10) \quad \frac{2\sqrt{|N_\alpha|}}{\sqrt{d}y_\ell} > 3.959 \left| \omega_k^{1/4} - \zeta_4 \frac{x - y\sqrt{\text{sf}(N_\alpha)}}{x + y\sqrt{\text{sf}(N_\alpha)}} \right| > \frac{3.959(1-c)}{k_0 Q^{r_0} \sqrt{f_k f_\ell} (y_k y_\ell)^{1/4}}.$$

Applying (2.8) and (4.7) to (4.10), we obtain

$$\frac{2\sqrt{|N_\alpha|}}{\sqrt{d}y_\ell} > \frac{3.959(1-c)}{0.89 \left(21.47\sqrt{d}y_k / (|g|\mathcal{N}_{d',4}) \right)^{r_0} \sqrt{f_k f_\ell} (y_k y_\ell)^{1/4}}.$$

After taking the fourth power of both sides and rearranging, we find that

$$(4.11) \quad (|N_\alpha| f_k f_\ell)^2 \left(\frac{0.45}{1-c} \right)^4 \left(\frac{21.47}{|g|\mathcal{N}_{d',4}} \right)^{4r_0} d^{2r_0-2} y_k^{4r_0+1} > y_\ell^3.$$

Specialising to the case when $r_0 = 1$ and using $|g|\mathcal{N}_{d',4} \geq 2$ from (3.36), we have

$$(4.12) \quad y_\ell^3 < 545(1-c)^{-4} (|N_\alpha| f_k f_\ell)^2 y_k^5.$$

We will now combine (4.12) with the gap principle in Lemma 3.8(a) to show that this case cannot occur.

Since $-N_\alpha$ is a square, we have $f_k = f_\ell = 1$ from Proposition 3.1(b), so combining the upper bound for y_ℓ^3 in (4.12) with Lemma 3.8(a) and cancelling the common factor of y_k^5 on both sides, we find that

$$57.32^3 \left(\frac{d}{|N_\alpha|} \right)^6 y_k^4 < 545(1-c)^{-4} N_\alpha^2,$$

which we can rewrite as

$$y_k < \frac{0.24}{1-c} \frac{|N_\alpha|^2}{d^{3/2}} < \frac{|0.24N_\alpha|}{(1-c)d^{1/2}}.$$

The last inequality holds because $|N_\alpha| = d - a^2 < d$.

By (4.1), we have $0.24/((1-c)d^{1/2}) < 0.25$ if $c < 0.9$. We will see in Subsection 4.4 that $c = 0.75$ is a good choice. So $y_k < |N_\alpha|/4$, which contradicts parts (b) and (c) of Lemma 3.5. Hence this case cannot hold.

4.3. $r_0 = 1$ **and** $\zeta_4 p/q = p_1/q_1$ **for some 4-th root of unity**, ζ_4 . As in Subsection 4.2, we start by proving an upper bound for y_ℓ that holds for all $r_0 \geq 1$ with $\zeta_4 p/q = p_{r_0}/q_{r_0}$ for some 4-th root of unity, ζ_4 .

From the definitions of p_{r_0} , q_{r_0} and R_{r_0} in (2.5), along with parts (a) and (e) of Lemma 2.2, we have

$$\begin{aligned}
& \left| \omega_k^{1/4} - \zeta_4 \frac{p}{q} \right| = \frac{1}{q_{r_0}} \left| q_{r_0} \omega_k^{1/4} - p_{r_0} \right| \\
&= \left| \frac{N_{d',4,r_0}}{D_{4,r_0} Y_{1,4,r_0}(\omega_k) \left(\frac{u_1 - u_2 \sqrt{t'}}{2g} \right)^{r_0}} \right| \left| \frac{D_{4,r_0}}{N_{d',4,r_0}} R_{1,4,r_0}(\omega_k) \left(\frac{u_1 - u_2 \sqrt{t'}}{2g} \right)^{r_0} \right| \\
&= \left| \frac{(\omega_k - 1)^{2r_0+1}}{Y_{1,4,r_0}(\omega_k)} \frac{(1/4) \cdots (r_0 + 1/4)}{(r_0 + 1) \cdots (2r_0 + 1)} {}_2F_1(r_0 + 3/4, r_0 + 1; 2r_0 + 2; 1 - \omega_k) \right| \\
(4.13) \quad & \geq \left| \frac{(\omega_k - 1)^{2r_0+1}}{Y_{1,4,r_0}(\omega_k)} \frac{(1/4) \cdots (r_0 + 1/4)}{(r_0 + 1) \cdots (2r_0 + 1)} \right|.
\end{aligned}$$

From Lemma 2.2(d), we have

$$(4.14) \quad |Y_{1,4,r_0}(\omega_k)| < 1.072 \frac{r_0! \Gamma(3/4)}{\Gamma(r_0 + 3/4)} |1 + \sqrt{\omega_k}|^{2r_0}.$$

We can write $\omega_k - 1$ as $(2N_\alpha + 2x_k N_{\varepsilon^k} \sqrt{N_\alpha}) / (x_k^2 - N_\alpha)$, so

$$|\omega_k - 1| = \sqrt{\frac{4|N_\alpha|}{x_k^2 - N_\alpha}} = 2\sqrt{\frac{|N_\alpha|}{d}} \frac{1}{y_k}.$$

Since $|\sqrt{\omega_k} + 1| < 2$, it follows that

$$|\sqrt{\omega_k} - 1| = \frac{|\omega_k - 1|}{|\sqrt{\omega_k} + 1|} > \sqrt{\frac{|N_\alpha|}{d}} \frac{1}{y_k}.$$

From these two inequalities, we also obtain

$$\left| \frac{(\omega_k - 1)^{2r_0+1}}{(1 + \sqrt{\omega_k})^{2r_0}} \right| = |(\omega_k - 1)(\sqrt{\omega_k} - 1)^{2r_0}| > 2 \left(\frac{|N_\alpha|}{d} \right)^{r_0+1/2} \left(\frac{1}{y_k} \right)^{2r_0+1}.$$

Applying this inequality together with the upper bound for $|Y_{1,4,r_0}(\omega_k)|$ in (4.14) and the inequalities (2.3) in Lemma 2.3(b) to (4.13), it follows that

$$\left| \omega_k^{1/4} - \zeta_4 \frac{p}{q} \right| > \frac{0.2915}{4^{r_0} \cdot r_0^{1/2}} \left(\frac{|N_\alpha|}{d} \right)^{r_0+1/2} \left(\frac{1}{y_k} \right)^{2r_0+1}.$$

Applying (4.2) with this inequality, we obtain

$$\frac{2\sqrt{|N_\alpha|}}{\sqrt{d} y_\ell} > \frac{1.154}{4^{r_0} \cdot r_0^{1/2}} \left(\frac{|N_\alpha|}{d} \right)^{r_0+1/2} \left(\frac{1}{y_k} \right)^{2r_0+1},$$

so

$$(4.15) \quad 1.734 r_0^{1/2} \left(4 \frac{d}{|N_\alpha|} \right)^{r_0} y_k^{2r_0+1} > y_\ell.$$

We now specialise to the case of $r_0 = 1$ and apply the gap principle in Lemma 3.8. Our gap principle in Lemma 3.8(a) with $b = 1$, along with (4.15), implies that

$$6.96 \frac{d}{|N_\alpha|} y_k^3 > y_\ell > 57.32 \frac{d^2}{|N_\alpha|^2} y_k^3 > 57.32 \frac{d}{|N_\alpha|} y_k^3,$$

since $-N_\alpha$ is a square and $d < |N_\alpha|$. But this inequality is impossible. Hence this case cannot hold.

4.4. $r_0 > 1$, $\zeta_4 p/q \neq p_{r_0}/q_{r_0}$ **for all 4-th roots of unity**, ζ_4 . Here we establish a stronger gap principle for y_k and y_ℓ than the one in Lemma 3.8. We then use this with the upper bound for y_ℓ in (4.11) to obtain a contradiction.

We start by deriving a lower bound for y_ℓ that holds in both this step and in the next step.

From the definition of r_0 in Lemma 2.1, along with (4.6) and $E > 1$, we have

$$(4.16) \quad |q| \geq \frac{c(Q-1)}{\ell_0(Q-1/E)} E^{r_0-1} > 0.995cE^{r_0-1}/\ell_0.$$

Recall that $|q| = \sqrt{f_k f_\ell} (y_k y_\ell)^{1/4}$ by (4.9). Thus

$$(y_k y_\ell)^{1/4} > \frac{0.995cE^{r_0-1}}{\ell_0 \sqrt{f_k f_\ell}}.$$

Applying (4.5) and (4.8), and then (4.3), to this inequality, we obtain

$$\begin{aligned} (y_k y_\ell)^{1/4} &> \frac{0.995c|x_k|}{0.458\sqrt{|N_\alpha|} f_k f_\ell} \left(\frac{0.1832|g|\mathcal{N}_{d',4}\sqrt{d}y_k}{|N_\alpha|} \right)^{r_0-1} \\ &> \frac{2.103c\sqrt{d}y_k}{\sqrt{|N_\alpha|} f_k f_\ell} \left(\frac{0.1832|g|\mathcal{N}_{d',4}\sqrt{d}y_k}{|N_\alpha|} \right)^{r_0-1}. \end{aligned}$$

Taking the fourth power of both sides and rearranging, we find that this inequality implies

$$(4.17) \quad y_\ell > \left(\frac{11.47}{|g|\mathcal{N}_{d',4}} \sqrt{\frac{|N_\alpha|}{f_k f_\ell}} \right)^4 c^4 \left(\frac{0.1832|g|\mathcal{N}_{d',4}}{|N_\alpha|} \right)^{4r_0} d^{2r_0} y_k^{4r_0-1}.$$

With this lower bound for y_ℓ , we now focus for the rest of this subsection on when $\zeta_4 p/q \neq p_{r_0}/q_{r_0}$ for all 4-th roots of unity, ζ_4 .

We now take the third power of both sides of this inequality and combine it with the upper bound for y_ℓ^3 in (4.11), obtaining

$$\begin{aligned} (4.18) \quad &(|N_\alpha| f_k f_\ell)^2 \left(\frac{0.45}{1-c} \right)^4 \left(\frac{21.47}{|g|\mathcal{N}_{d',4}} \right)^{4r_0} d^{2r_0-2} y_k^{4r_0+1} \\ &> \left(\frac{11.47}{|g|\mathcal{N}_{d',4}} \sqrt{\frac{|N_\alpha|}{f_k f_\ell}} \right)^{12} c^{12} \left(\frac{0.1832|g|\mathcal{N}_{d',4}}{|N_\alpha|} \right)^{12r_0} d^{6r_0} y_k^{12r_0-3}. \end{aligned}$$

Using elementary calculus, $c^{12}(1-c)^4$ is monotonically increasing for $0 < c \leq 0.75$. So we put $c = 0.75$ and find that for such c , $c^{12}(1-c)^4 > 0.000124$. Applying this to (4.18) and

simplifying, we have

$$(4.19) \quad (f_k f_\ell)^8 \frac{0.00078 |N_\alpha|^2 (|g| \mathcal{N}_{d',4})^4}{d^4} \left(\frac{1.22 \cdot 10^7}{(|g| \mathcal{N}_{d',4})^8} \right)^{2r_0-1} > \left(\frac{y_k^4 d^2}{|N_\alpha|^6} \right)^{2r_0-1}.$$

Since $-N_\alpha$ is a square, we have $f_k = f_\ell = 1$ from Proposition 3.1(b), so

$$\frac{0.00078 |N_\alpha|^2 (|g| \mathcal{N}_{d',4})^4}{d^4} (1.22 \cdot 10^7)^{2r_0-1} > \left(\frac{y_k^4 d^2 (|g| \mathcal{N}_{d',4})^8}{|N_\alpha|^6} \right)^{2r_0-1}$$

and then

$$\frac{0.00078 |N_\alpha|^2 (|g| \mathcal{N}_{d',4})^4}{d^4} > \left(\frac{y_k^4 d^2 (|g| \mathcal{N}_{d',4})^8}{59.2^4 |N_\alpha|^6} \right)^{2r_0-1}.$$

Using the equality in (3.36) of Lemma 3.12, we can compute that $|N_\alpha|^2 (|g| \mathcal{N}_{d',4})^4 / d^4 \leq 2^{20} / 17^4$ (the max value occurs when $d = 17a^2$ so that $|N_\alpha| = 16a^2$) to obtain

$$(4.20) \quad 0.01 > \left(\frac{y_k^4 d^2 (|g| \mathcal{N}_{d',4})^8}{59.2^4 |N_\alpha|^6} \right)^{2r_0-1}.$$

But if

$$(4.21) \quad y_k > 59.2 |N_\alpha|^{3/2} / \left(\sqrt{d} (|g| \mathcal{N}_{d',4})^2 \right),$$

then the right-hand side is greater than 1, so this is not possible.

4.5. $r_0 > 1$ **and** $\zeta_4 p/q = p_{r_0}/q_{r_0}$ **for some 4-th root of unity**, ζ_4 . We now combine our upper bound for y_ℓ in (4.15) with our lower bound for y_ℓ in (4.17). Thus

$$1.734 r_0^{1/2} \left(4 \frac{d}{|N_\alpha|} \right)^{r_0} y_k^{2r_0+1} > \left(\frac{11.47}{|g| \mathcal{N}_{d',4}} \sqrt{\frac{|N_\alpha|}{f_k f_\ell}} \right)^4 c^4 \left(\frac{0.1832 |g| \mathcal{N}_{d',4}}{|N_\alpha|} \right)^{4r_0} d^{2r_0} y_k^{4r_0-1}$$

and so

$$1.734 r_0^{1/2} > \left(\frac{11.47}{|g| \mathcal{N}_{d',4}} \sqrt{\frac{|N_\alpha|}{f_k f_\ell}} \right)^4 c^4 \left(\frac{0.1832^4 |g|^4 \mathcal{N}_{d',4}^4}{4 |N_\alpha|^3} \right)^{r_0} d^{r_0} y_k^{2r_0-2}.$$

We can show that $0.1832^{4r_0} / r_0^{1/2} > 0.175^{4r_0}$, with the minimum being attained at $r_0 = 3$. Applying this, along with $c = 0.75$ and collecting the terms taken to the power $r_0 - 1$, yields

$$1 > \frac{0.7405 d}{f_k^2 f_\ell^2 |N_\alpha|} \left(\frac{0.0002344 |g|^4 \mathcal{N}_{d',4}^4}{|N_\alpha|^3} d y_k^2 \right)^{r_0-1}.$$

Combined with $d > N_\alpha$, this implies that

$$(4.22) \quad 1 > \frac{0.7405}{f_k^2 f_\ell^2} \left(\frac{0.0002344 |g|^4 \mathcal{N}_{d',4}^4}{|N_\alpha|^3} d y_k^2 \right)^{r_0-1}.$$

We now proceed similarly to the way we did in Subsection 4.4.

Since $-N_\alpha$ is a square, we have $f_k = f_\ell = 1$ from Proposition 3.1(b). Also, as $r_0 - 1 \geq 1$, it follows that $0.7405 \cdot 0.0002344^{r_0-1} > 0.0001735^{r_0-1}$. So the above inequality implies

$$1 > \left(\frac{0.0001735 |g|^4 \mathcal{N}_{d',4}^4}{|N_\alpha|^3} dy_k^2 \right)^{r_0-1} > \left(y_k^2 \frac{d(|g| \mathcal{N}_{d',4})^4}{5764 |N_\alpha|^3} \right)^{r_0-1}.$$

But if

$$(4.23) \quad y_k \geq \frac{76 |N_\alpha|^{3/2}}{\sqrt{d} (|g| \mathcal{N}_{d',4})^2},$$

then the right-hand side is greater than 1, so this is not possible.

4.6. Small d . To complete the proof of Proposition 4.1, we need to remove the assumption on d in (4.1).

We check directly all pairs (a, d) of positive integers with $2 \leq d \leq 104$ not a square and $-N_\alpha = d - a^2$ a square. Note that there are only finitely many such pairs, since $N_\alpha = a^2 - d < 0$.

If $y_k = y^2$ is a square, then from (1.1), we know that $x_k^2 - dy^4 = N_\alpha$. By Theorem 1.1 of [1], our theorem holds for $N_\alpha = -1$, so we may also assume that $N_\alpha \leq -4$. There are 59 such pairs (a, d) .

For each such pair, we solved $x^2 - dy^4 = N_\alpha$ using Magma (version V2.28-2) [4] and its `IntegralQuarticPoints()` function. For the 59 equations, this calculation took 17.66 seconds using MAGMA's online calculator. 21 of the equations had at least two solutions in positive integers. Only two of these had three solutions in positive integers:

$x^2 - 17y^4 = -16$ has the solutions $(x, y) = (1, 1), (16, 2), (103, 5)$,

$x^2 - 68y^4 = -64$ has the solutions $(x, y) = (2, 1), (32, 2), (206, 5)$.

None of the equations had more solutions.

For $x^2 - 17y^4 = -16$, since $(103 + 5^2\sqrt{17}) / (1 + \sqrt{17}) = (161 + 39\sqrt{17}) / 8$, the solutions $(103, 5)$ and $(1, 1)$ arise from different sequences. Hence Proposition 4.1 holds for $(a, d) = (1, 17)$. Similarly, Proposition 4.1 holds for $(a, d) = (2, 68)$ too. This completes the proof of Proposition 4.1.

5. PROOF OF THEOREM 1.4

If N_α is even, then $|g| \mathcal{N}_{d',4} \geq 4$ by Lemma 3.12. So the right-hand side of the inequality in Proposition 4.1 is $\max \left(1, 4.75 |N_\alpha|^{3/2} / \sqrt{d} \right)$. But for $u \geq 5$ and $k \neq 0$, we have $y_k \geq 25 |N_\alpha| / 4$ by Lemma 3.5(c). So Theorem 1.4 holds for $u \geq 5$ and we need only consider $1 \leq u \leq 4$.

Similarly, if N_α is odd and $u \geq 9$, then we have $y_k \geq 81 |N_\alpha| / 4 > \max \left(1, 19 |N_\alpha|^{3/2} / \sqrt{d} \right)$ for $k \neq 0$ and we need only consider $1 \leq u \leq 8$.

Next we treat the case when $K < -1$, where, as in Lemma 3.5, K is the largest negative integer such that $y_K > 1$.

Lemma 5.1. *If $K < -1$, then there are at most two distinct integer squares among the y_k 's.*

Proof. From Lemma 3.6, we know that $K < -1$ can only happen in the following two cases:

- (i) $a \geq 1$, $d = a^2 + 4$, $t = a$ and $u = 1$, where $\alpha = 2\varepsilon$ and $N_\alpha = -4$,
- (ii) $a \geq 1$, $d = a^2 + 1$, $t = 2a$ and $u = 2$, where $\alpha = \varepsilon$ and $N_\alpha = -1$.

In case (i), we have $x_k^2 - dy_k^2 = -4$.

If $d = a^2 + 4$ is even, then it is divisible by 4 and x_k is also even. So the equation becomes $(x_k/2)^2 - (d/4)y_k^2 = -1$. From Theorem 1.1 of [1], there are at most two distinct squares among the y_k 's here, so the lemma holds in this case.

If d is odd, the conditions in Theorem 1 of [9] hold with $A = d = a^2 + 4$, $B = 1$ both odd and the minimal solution of equation (1) there in odd positive integers being $(1, a)$. Hence there are at most two distinct squares among the y_k 's in this case too.

In case (ii), we can also apply Theorem 1.1 of [1]. \square

For the remainder of this section, we may assume that $K = -1$.

Lemma 5.2. *If $y_\ell > y_k > 1$ are two squares, then $k = \pm 1$.*

Proof. From Theorem 1.1 of [1], we cannot have three distinct squares among the y_k 's for $N_\alpha = -1$, so we may assume $|N_\alpha| \geq 4$ for N_α even and $|N_\alpha| \geq 9$ for N_α odd.

We will suppose that y_k is a square with $|k| > 1$, but show that this is not possible.

From Lemma 3.5(c) and $|N_\alpha| = d - a^2 < d$, we obtain $y_k \geq |N_\alpha|^2 u^4 / 10$. So, for $u \geq 2$ and $|N_\alpha| \geq 4$, we have $y_k \geq (8/5) |N_\alpha|^2 \geq (32/5) |N_\alpha| > (32/5) |N_\alpha|^{3/2} / \sqrt{d}$.

However, we saw at the start of this section that for N_α even, there can be no squares y_k and y_ℓ satisfying $y_\ell > y_k > \max(1, 4.75 |N_\alpha|^{3/2} / \sqrt{d})$. So we need only consider $u = 1$ when N_α is even.

Similarly, if $-N_\alpha$ is an odd square with $N_\alpha \leq -9$ and $u \geq 3$, then we have $y_k > (81/10) |N_\alpha|^2 \geq (729/10) |N_\alpha| > (729/10) |N_\alpha|^{3/2} / \sqrt{d}$. But, we saw at the start of this section that for N_α odd, there can be no squares y_k and y_ℓ satisfying $y_\ell > y_k > \max(1, 19 |N_\alpha|^{3/2} / \sqrt{d})$. So we need only consider $u \leq 2$ when N_α is odd.

For $u = 2$, we have $y_k > (8/5) |N_\alpha|^2$ for $|k| \geq 2$. So if $|N_\alpha| \geq 25$ is odd, then we have $y_k \geq (200/5) |N_\alpha| > 40 |N_\alpha|^{3/2} / \sqrt{d}$. So, for odd N_α , we need only consider $N_\alpha = -9$. In this case, $N_\varepsilon = (t^2 - 4d)/4 = \pm 1$, so $t^2 - 4a^2 = -4N_\alpha \pm 4 = 32, 40$. This means that $(t, a, d) = (6, 1, 10)$ (recall from Subsection 1.2 that we only consider positive values of t and u). Here we have $y_{\pm 2} \geq y_{-2} = 493 > 19.75 |N_\alpha|^{3/2} / \sqrt{d}$.

For $u = 1$, we proceed similarly. Here we have $y_k > |N_\alpha|^2 / 10$ for $|k| \geq 2$, so we need to consider $4 \leq |N_\alpha| \leq 36$ when $-N_\alpha$ is an even square and $9 \leq |N_\alpha| \leq 169$ when $-N_\alpha$ is an odd square.

For each value of N_α , the norm of ε leads us to an equation of the form $t^2 - a^2 = -N_\alpha \pm 4$. We solve each of these equations over the integers using PARI/GP and calculate y_k and y_{-k} for $k \geq 2$ until the lower bound from Proposition 4.1 is exceeded (we never had to go beyond $|k| = 5$). No squares were found. \square

Lemma 5.3. *If both $y_{\pm 1}$ are squares, then y_k is not a square for any $|k| > 1$.*

Proof. From Lemmas 3.8(a) and 3.5(c), we have

$$y_1 > \frac{57.32d^2}{|N_\alpha|^2} y_{-1}^3 \geq \frac{57.32d^2}{|N_\alpha|^2} \left(\frac{|N_\alpha| u^2}{4} \right)^3 = \frac{57.32d^2 |N_\alpha| u^6}{64}.$$

By Proposition 4.1 and Lemma 3.12, if the quantity on the right-hand side exceeds $\max(1, 19 |N_\alpha|^{3/2} / \sqrt{d})$, then the lemma follows. Since $d > |N_\alpha|$, this holds if $d^2 u^6 >$

$19 \cdot 64/57.32$, which holds unless $d^2 < 21.3$ and $u = 1$. This leaves $d = 2$ or 3 , but for neither of these does $u = 1$ yield a unit. \square

Lemma 5.4. *Suppose that $-N_\alpha$ is an odd square and $y_{\pm 1}$ is a square integer.*

- (a) *If $t^2 - du^2 = 4$, then $t \equiv 2 \pmod{4}$ and $u \equiv 0 \pmod{4}$.*
- (b) *If $t^2 - du^2 = -4$, then $u \equiv 2 \pmod{4}$.*

Proof. For $t^2 - du^2 = \pm 4$, if t is odd, then $d \equiv u^2 \equiv 1 \pmod{4}$. Since N_α is odd, it follows that a is even. Therefore $4y_{\pm 1} = 2du^2 \pm 2atu \pm 4 \equiv 2 \pmod{4}$, which is not possible since $y_{\pm 1} \in \mathbb{Z}$. Therefore, if N_α is odd, t must be even.

(a) Next we show that if $t^2 - du^2 = 4$, then $4 \nmid t$. If $4 \mid t$, then $du^2 \equiv 12 \pmod{16}$. Since $-N_\alpha$ is an odd square, we have $-N_\alpha \equiv 1, 9 \pmod{16}$. If a is odd, then $a^2 \equiv 1 \pmod{8}$. So $d \equiv 2 \pmod{8}$ and hence $u^2 \equiv 6 \pmod{8}$, which is not possible. If a is even, then $a^2 \equiv 0, 4 \pmod{16}$. Since $-N_\alpha = d - a^2 \equiv 1, 9 \pmod{16}$, it follows that $d \equiv 1 \pmod{8}$. So $u^2 \equiv 12 \pmod{16}$, which is also impossible. So $4 \nmid t$.

Therefore, we must have $t \equiv 2 \pmod{4}$, if $t^2 - du^2 = 4$ and N_α is an odd square.

From $t \equiv 2 \pmod{4}$ and $t^2 - du^2 = 4$, we have $du^2 \equiv 0 \pmod{16}$.

Since N_α is odd, we have $-N_\alpha \equiv 1, 9 \pmod{16}$. Also $a^2 \equiv 0, 1, 4, 9 \pmod{16}$. Hence $d \equiv 1, 2, 5, 9, 10, 13 \pmod{16}$ and so $8 \mid u^2$. Thus $4 \mid u$.

(b) We proceed similarly. Suppose that $4 \mid t$, then $du^2 \equiv 4 \pmod{16}$. As in the proof of part (a), if a is odd, then $d \equiv 2 \pmod{8}$. Hence $u^2 \equiv 2 \pmod{8}$, which is not possible.

If a is even, as in the proof of part (a), then $d \equiv 1 \pmod{8}$. So $u^2 \equiv 4 \pmod{16}$. I.e., $u \equiv 2 \pmod{4}$.

If $t \equiv 2 \pmod{4}$, then $du^2 \equiv 8 \pmod{16}$. Again, if a is odd, then $d \equiv 2 \pmod{8}$ and so $u^2 \equiv 4 \pmod{8}$.

If a is even, then $d \equiv 1 \pmod{8}$ and $u \equiv 8 \pmod{16}$, which is not possible. \square

Lemma 5.5. *If $-N_\alpha$ is an odd square, $1 \leq u \leq 8$ and $y_{\pm 1} \in \mathbb{Z}$ a square with $y_{\pm 1} < \max\left(1, \frac{76|N_\alpha|^{3/2}}{\sqrt{d}(|g|\mathcal{N}_{d',4})^2}\right)$, then we must have $u = 2$, $t^2 - du^2 = -4$ and $\gcd(a^2, d) = 1$.*

Proof. We proceed in steps.

(1) We start by showing that $t^2 - du^2 = 4$ is not possible.

From Lemma 5.4(a), if $t^2 - du^2 = 4$ and $-N_\alpha$ is an odd square, then $4 \mid u$, so we are left with $u = 4$ or 8 here.

(1-i) First, we eliminate $u = 4$.

We can write $N_\alpha = -(2n+1)^2$, so $t^2 - (a^2 + (2n+1)^2)u^2 = 4$ becomes $t^2 - 64n^2 - 64n = 16a^2 + 20$. But $t^2 \equiv 20 \pmod{64}$, has no solution, so a must be odd. Hence $t^2 - 64n^2 - 64n = 16a^2 + 20$ implies $t^2 \equiv 36 \pmod{64}$. So $t \equiv \pm 6 \pmod{16}$.

Expanding the expressions for $4y_{\pm 1}$, with $a = 2a_1 + 1$, $N_\alpha = -(2n+1)^2$ and $t = 16t_1 \pm 6$, we find that $4y_{\pm 1} \equiv 20 \pmod{32}$. But this congruence has no solution with $y_{\pm 1}$ a square. Hence $u = 4$ is not possible.

(1-ii) Now we eliminate $u = 8$.

Arguing modulo 9, from $t^2 - 64d = 4$, we see that $d \equiv 0, 3, 5, 6 \pmod{9}$. From this, $-N_\alpha = d - a^2$ being a square and the squares modulo 9 being $0, 1, 4, 7$, we must have $(a^2 \pmod{9}, d \pmod{9}) = (0, 0), (1, 5), (4, 5)$ or $(7, 5)$.

We will show that $d \equiv 5 \pmod{9}$ is not possible. In this case, from $t^2 - 64d = 4$, we find that $t^2 \equiv 0 \pmod{9}$. So $t \equiv 0 \pmod{3}$. Since $d \equiv 5 \pmod{9}$, we have $y_{\pm 1} =$

$1 + 32d \pm 4at \equiv 2 \pm 4at \pmod{3}$. Since $3|t$, it follows that $y_{\pm 1} \equiv 2 \pmod{3}$, which can never be square. Hence $9|\gcd(a^2, d)$.

(Since we will use this same argument in several places in the proof of this lemma and the next, we wrote programs (in both Maple and PARI/GP) to automate these steps and prove that $\gcd(a^2, d)$ has certain factors (typically, powers of 2 and 3). In fact, using this same code, we could have eliminated case (1-i) above too.)

Therefore by Lemma 3.12, we have $(|g|\mathcal{N}_{d',4})^2 \geq 36$. Hence $\frac{76|N_\alpha|^{3/2}}{\sqrt{d}(|g|\mathcal{N}_{d',4})^2} < (76/36)|N_\alpha|$.

But by Lemma 3.5(c), we know that $y_{\pm 1} \geq 16|N_\alpha|$ here. So the case where $u = 8$, $-N_\alpha$ is an odd square and $t^2 - du^2 = 4$ is excluded.

Thus for N_α odd, we do not need to consider $t^2 - du^2 = 4$.

(2) Now we consider $t^2 - du^2 = -4$.

(2-i) From Lemma 5.4(b), we have $u \equiv 2 \pmod{4}$. For $u = 6$, $t^2 - du^2 = -4$ is not possible modulo 9. So we must have $u = 2$ if $t^2 - du^2 = -4$.

(2-ii) We show that $\gcd(a^2, d) = 1$ when $u = 2$.

We suppose otherwise. Since N_α is odd, $\gcd(a^2, d)$ must be odd and since $d = (t^2 + 4)/4$, any odd prime factor, p , of the gcd must also be a factor of $t^2 + 4$. This means that $t^2 \equiv -4 \pmod{p}$. Hence $p \equiv 1 \pmod{4}$. Since $p^2|a^2$ and $-N_\alpha = d - a^2$ is a perfect square, this also implies that $p^2|d$. Therefore by Lemma 3.12, we have $(|g|\mathcal{N}_{d',4})^2 \geq 100$. Hence the theorem holds if $y_{\pm 1} > (76/100)|N_\alpha|$, by Proposition 4.1. But by Lemma 3.5(c), we know that $y_{\pm 1} \geq |N_\alpha|$ here. So the theorem holds if $u = 2$, $-N_\alpha$ is an odd square and $\gcd(a^2, d) > 1$. \square

We now prove an analogous lemma for N_α even.

Lemma 5.6. *If $-N_\alpha$ is an even square, $1 \leq u \leq 4$ and $y_{\pm 1} < \max\left(1, \frac{76|N_\alpha|^{3/2}}{\sqrt{d}(|g|\mathcal{N}_{d',4})^2}\right)$, then we must have $u = 1$, $t^2 - du^2 = -4$, $N_\alpha \equiv 12 \pmod{16}$ and $\gcd(a^2, d) = 1, 4$.*

Proof. As in the proof of Lemma 5.5, we proceed in steps.

(1) We start by showing that $t^2 - du^2 = 4$ is not possible.

(1-i) We show that $u = 4$, $-N_\alpha$ an even square and $t^2 - du^2 = 4$ is not possible.

Here we can argue as for $u = 8$ in the proof of Lemma 5.5 and use the Maple program mentioned there modulo 9 to show that $9|\gcd(a^2, d)$. Therefore by Lemma 3.12, we have $(|g|\mathcal{N}_{d',4})^2 \geq 144$. Hence $\frac{76|N_\alpha|^{3/2}}{\sqrt{d}(|g|\mathcal{N}_{d',4})^2} \leq (76/144)|N_\alpha|$. But by Lemma 3.5(c), we know that $y_{\pm 1} \geq 4|N_\alpha|$ here. So we can exclude $u = 4$ and $t^2 - du^2 = 4$ from consideration.

(1-ii) We show that $u = 3$, $-N_\alpha$ an even square and $t^2 - du^2 = 4$ is not possible.

We will again argue as for $u = 8$ in the proof of Lemma 5.5 and use the Maple program mentioned there modulo 32 to show that $64|\gcd(a^2, d)$.

Therefore by Lemma 3.12, we have $(|g|\mathcal{N}_{d',4})^2 \geq 256$. Hence the theorem holds if $y_{\pm 1} > (76/256)|N_\alpha|$, by Proposition 4.1. But by Lemma 3.5(c), we know that $y_{\pm 1} \geq (9/4)|N_\alpha|$ here.

(1-iii) We show that $u = 2$, $-N_\alpha$ an even square and $t^2 - du^2 = 4$ is not possible.

Using the argument for $u = 8$ in the proof of Lemma 5.5 and the Maple program mentioned there modulo 16, we obtain $16|\gcd(a^2, d)$.

Doing the same modulo 9, we obtain $9 \mid \gcd(a^2, d)$. Combining this with $16 \mid \gcd(a^2, d)$ and applying Lemma 3.12, we have $|g|\mathcal{N}_{d',4} \geq 24$. Hence $\frac{76|N_\alpha|^{3/2}}{\sqrt{d}(|g|\mathcal{N}_{d',4})^2} \leq (76/24^2)|N_\alpha|$. But by Lemma 3.5(c), we know that $y_{\pm 1} \geq |N_\alpha|u^2/4 = |N_\alpha|$ here. So we can exclude $u = 2$ and $t^2 - du^2 = 4$ from consideration.

(1-iv) We show that $u = 1$, $-N_\alpha$ an even square and $t^2 - du^2 = 4$ is not possible.

Here too we use the argument and Maple program from the proof of Lemma 5.5, first modulo 9 and then modulo 16. From the latter, we obtain $64 \mid \gcd(a^2, d)$. So by Lemma 3.12, $|g|\mathcal{N}_{d',4} \geq 48$. Hence $\frac{76|N_\alpha|^{3/2}}{\sqrt{d}(|g|\mathcal{N}_{d',4})^2} \leq (76/48^2)|N_\alpha|$. But by Lemma 3.5(c), we know that $y_{\pm 1} \geq |N_\alpha|/4$ here. So we can exclude $u = 1$ and $t^2 - du^2 = 4$ from consideration.

(2) We now consider $t^2 - du^2 = -4$.

Independent of the parity of N_α , for $u = 3$ and 4 , $t^2 - du^2 = -4$ is not possible modulo 9 and 16, respectively. So we can only have $u = 1, 2$ with $t^2 - du^2 = -4$.

(2-i) We show that if $u = 1$, $-N_\alpha$ is an even square and $t^2 - du^2 = -4$, then $N_\alpha \equiv 12 \pmod{16}$.

We find that $y_{\pm 1} \equiv 0, 1, 4, 9 \pmod{16}$ is not possible if $-N_\alpha = b_1^2$ where $b_1 \equiv 4 \pmod{8}$.

If $8 \mid b_1$, then $a \equiv 2 \pmod{4}$ and $|g|\mathcal{N}_{d',4} \geq 16$. So $\frac{76|N_\alpha|^{3/2}}{(\sqrt{d}(|g|\mathcal{N}_{d',4})^2)} \leq (76/16^2)|N_\alpha|^{3/2}/\sqrt{d}$.

However $76/16^2$ is bigger than $1/4$, so we must work a bit harder to eliminate $8 \mid b_1$.

If $a^2 \geq 0.292d$, then

$$\frac{76|N_\alpha|^{3/2}}{(\sqrt{d}(|g|\mathcal{N}_{d',4})^2)} < (76\sqrt{1-0.292}/16^2)|N_\alpha| < 0.2498|N_\alpha|.$$

By Lemma 3.5(c), we know that $y_{\pm 1} \geq |N_\alpha|/4$. So $a^2 \geq 0.292d$ is excluded.

Suppose that $d \geq 80$. Then $t^2 = d - 4$, so $t^2 \geq (76/80)d$. If $a^2 < 0.292d$, then $t - a > \sqrt{76d/80} - \sqrt{0.292d}$ and so $(t - a)^2/4 > 0.047d > 0.047|N_\alpha|$. We can write $4y_{\pm 1} = (t \pm au)^2 - N_\alpha u^2$. So here with $u = 1$, we have $y_{\pm 1} \geq (t - a)^2/4 + |N_\alpha|/4 > 0.297|N_\alpha|$. But $76|N_\alpha|/16^2 = 0.296875|N_\alpha|$. So we can exclude $8 \mid b_1$, provided $d \geq 80$.

For $d < 80$ with $u = 1$ and $-N_\alpha$ an even square divisible by 64, there is just one possibility: $d = 68$, $t = 8$, $u = 1$, $a = 2$, so $N_\alpha = -64$ and $y_{-1} = 25$. But here, $\frac{76|N_\alpha|^{3/2}}{(\sqrt{d}(|g|\mathcal{N}_{d',4})^2)} < (76/16^2)|N_\alpha|^{3/2}/\sqrt{d} < 19$, so this case is excluded too and hence we can exclude $8 \mid b_1$ altogether.

Hence $b_1 \equiv 2 \pmod{4}$ and so $-N_\alpha \equiv 4 \pmod{16}$.

(2-ii) We show that if $u = 1$, $-N_\alpha$ is an even square, $t^2 - du^2 = -4$, and $N_\alpha \equiv 12 \pmod{16}$, then $\gcd(a^2, d) = 1$ or 4 .

We have $v_2(\gcd(a^2, d)) = 0$ or 2 . Since $-N_\alpha \equiv 4 \pmod{16}$, we have $v_2(b') = 2$ in the first case and 0 in the second case.

We consider first $\gcd(a^2, d) > 4$ odd. So by Lemma 3.12 and the argument in the previous paragraph, $|g|\mathcal{N}_{d',4} = 4\sqrt{\gcd(a^2, d)}$. Hence $\frac{76|N_\alpha|^{3/2}}{\sqrt{d}(|g|\mathcal{N}_{d',4})^2} = \frac{76|N_\alpha|^{3/2}}{16\sqrt{d}\gcd(a^2, d)}$. If $\gcd(a^2, d) \geq 25$, then the right-hand side is less than $0.19|N_\alpha| < |N_\alpha|/4$, the right-hand side being the lower bound for $y_{\pm 1}$ from Lemma 3.5(c).

Since $d = t^2 + 4$, arguing modulo 3, we see that $3 \nmid d$ and hence $\gcd(a^2, d) = 9$ is not possible.

Now consider $\gcd(a^2, d) > 4$ even. Then $v_2(\gcd(a^2, d)) = 2$ (so $\gcd(a^2, d) \equiv 4 \pmod{16}$). So by Lemma 3.12 and the argument above, $|g|\mathcal{N}_{d',4} = 2\sqrt{\gcd(a^2, d)}$. Hence $\frac{76|N_\alpha|^{3/2}}{\sqrt{d}(|g|\mathcal{N}_{d',4})^2} =$

$$\frac{76|N_\alpha|^{3/2}}{4\sqrt{d}\gcd(a^2, d)}.$$

We saw above that $3 \nmid d$, so we can ignore $\gcd(a^2, d) = 6^2$. If $\gcd(a^2, d) \geq 100$, then $\frac{76|N_\alpha|^{3/2}}{4\sqrt{d}\gcd(a^2, d)} \leq 0.19|N_\alpha| < |N_\alpha|/4$, the lower bound for $y_{\pm 1}$ from Lemma 3.5(c).

(2-iii) We show that $u = 2$, $-N_\alpha$ an even square and $t^2 - du^2 = -4$ is not possible.

Arguing modulo 64, we have $d \equiv a^2 \equiv 1 \pmod{16}$ and $8|t$. So $16|N_\alpha$ and, in the notation of Lemma 3.12, $16|b'$. Thus $|g|\mathcal{N}_{d',4} = 8\sqrt{\gcd(a^2, d)}$, where $\gcd(a^2, d)$ is odd.

It follows that $\frac{76|N_\alpha|^{3/2}}{(\sqrt{d}(|g|\mathcal{N}_{d',4})^2)} \leq \frac{76|N_\alpha|^{3/2}}{64(\sqrt{d}\gcd(a^2, d))}$. However $76/64$ is bigger than 1, so we proceed as in case (2-i) above.

If $a^2 \geq 0.292d$, then

$$\frac{76|N_\alpha|^{3/2}}{(64\sqrt{d}\gcd(a^2, d))} < \frac{76\sqrt{1-0.292}}{64}|N_\alpha| < 0.9992|N_\alpha|.$$

By Lemma 3.5(c), we know that $y_{\pm 1} \geq |N_\alpha|$. So $a^2 \geq 0.292d$ is excluded.

Suppose that $d \geq 2$. Then $t^2 = 4d - 4$, so $t^2 \geq 2d$. If $a^2 < 0.292d$, then $t - a > \sqrt{2d} - \sqrt{0.292d}$ and so $(t - a)^2/4 > 0.19d > 0.19|N_\alpha|$. We can write $4y_{\pm 1} = (t \pm au)^2 - N_\alpha u^2$. So here with $u = 2$, we have $y_{\pm 1} \geq (t - a)^2/4 + |N_\alpha| > 1.19|N_\alpha|$. But $76|N_\alpha|/64 = 1.1875|N_\alpha|$. So we can exclude the case where $u = 2$, $-N_\alpha$ an even square and $t^2 - du^2 = -4$. \square

Theorem 1.4(c) now follows from the bounds on u that we obtained from Proposition 4.1 at the start of Section 5, along with Lemmas 5.1, 5.2, 5.5 and 5.6. Furthermore, from Lemma 5.3, if y_{-1} and y_1 are both squares, then there are no further squares. So we may assume that precisely one of $y_{\pm 1}$ is a square. From Lemma 3.5(c), we obtain $y_k > 19|N_\alpha|^{3/2}/\sqrt{d}$ for $|k| \geq 2$, provided that $d > 190$ when $u = 1$ and that $d > 11$ when $u = 2$. This leaves 26 values of d . For each of these, we compute y_{-2} directly for each possibility of N_α and compare the value to the bound in Proposition 4.1. Where the bound was exceeded, Proposition 4.1 tells us that there are no further squares, completing the proof for them. There were only four cases where y_{-2} did not exceed that bound: $(a, b, d, t, u) = (1, 1, 2, 2, 2)$, $(1, 1, 5, 1, 1)$, $(2, 1, 8, 2, 1)$, $(3, 1, 13, 3, 1)$. These were treated in Subsection 4.6.

6. EXAMPLES

In this section, we give examples showing that our conjectures and results are best possible.

6.1. Examples for Conjecture 1.1.

In addition to the examples for $d = 2$ in Table 1, we also found examples with four squares for $(d, t, u, a, b) = (3, 4, 2, 672, 91)$, $(6, 10, 4, 78, 7)$, $(6, 10, 4, 34986, 149)$, $(6, 10, 4, 3663828, 2257)$, $(30, 22, 4, 826320, 1111)$ and $(37, 12, 2, 138, 5)$.

At least for $d = 2$ and $d = 6$, it appears there may be infinitely many such examples.

a	b	indices, k	$\sqrt{y_k}$
1	3	[0, -1, 3, -5]	[3, 5, 31, 167]
1019	27	[0, 1, -3, -7]	[27, 65, 29, 983]
167	13	[0, 1, -3, 4]	[13, 29, 71, 407]
157	29	[0, -1, 3, -4]	[29, 47, 307, 649]
1	41	[0, -1, -9, 11]	[41, 71, 80753, 470861]
1633	65	[0, -1, -4, 7]	[65, 97, 1331, 24791]
48479	211	[0, -3, 4, -7]	[211, 1007, 6743, 34205]
45649	677	[0, -1, -4, 4]	[677, 1133, 15679, 16825]
1940147	1217	[0, -3, 4, -11]	[1217, 3289, 40573, 3794239]
600589	2213	[0, -1, -4, 4]	[2213, 3673, 50801, 55415]
20509501	8689	[0, -1, 3, -4]	[8689, 13619, 94393, 187603]
255488029	13457	[0, -1, 3, -4]	[13457, 5683, 189241, 15821]
409660129	17023	[0, -1, -4, -8]	[17023, 7073, 7949, 269495]
3032771269	46313	[0, -1, -4, -8]	[46313, 19213, 15269, 516625]

TABLE 1. Examples for $d = 2$ with $t = u = 2$

6.2. Examples for Conjecture 1.2. Let $n \geq 5$ be an odd integer. Put $a = (n^2 - 9)/4$ and $d = (n^4 - 2n^2 + 17)/16$, so that $N_\alpha = 4 - n^2$. With $t = (n^2 - 1)/2$ and $u = 2$, $\varepsilon = (t + u\sqrt{d})/2$ is a unit in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$. We have $y_1 = (n^2 - 3)^2/4$ and $y_{-1} = n^2$. This example shows that Conjecture 1.2 is best possible, if true.

Let $n > 5$ satisfy $n \equiv 1 \pmod{4}$ and not divisible by 5. Put $a = (n - 5)/4$, $d = (n^2 + 6n + 25)/16$. Here $N_\alpha = -n$. With $t = 2a + 4$ and $u = 2$, $\varepsilon = (t + u\sqrt{d})/2$ is a unit in $\mathcal{O}_{\mathbb{Q}(\sqrt{d})}$ and we have $y_1 = (n + 1)^2/4$. If n is a square, then this example shows that Conjecture 1.2 is best possible when $|N_\alpha|$ is a perfect square.

6.3. Examples for Conjecture 1.3. The examples in Subsection 6.1 also apply in this more general case to show there can be at least four distinct squares.

Here are two examples showing that there are at least three distinct squares when $|N_\alpha|$ is a square:

$$(d, t, u, a, b) = (5, 1, 1, 43, 3): N_\alpha = 38^2, y_{-3} = 5^2, y_0 = 3^2, y_{11} = 53^2;$$

$$(d, t, u, a, b) = (10, 6, 2, 1, 1): N_\alpha = -3^2, y_0 = 1^2, y_1 = 2^2, y_2 = 5^2.$$

Here are two examples showing that the same is true when $|N_\alpha|$ is a prime power:

$$(d, t, u, a, b) = (5, 1, 1, 153, 4): N_\alpha = 22129, y_{-3} = 11^2, y_0 = 4^2, y_{30} = 8862^2;$$

$$(d, t, u, a, b) = (51, 100, 14, 2, 1): N_\alpha = -47, y_{-1} = 6^2, y_0 = 1^2, y_1 = 8^2.$$

Here is an example showing that if $|N_\alpha|$ is not a prime power, but $\text{sf}(|N_\alpha|)$ is a prime, then there can be distinct four squares (unlike in Conjecture 1.1):

$$(d, t, u, a, b) = (5, 1, 1, 7, 1): N_\alpha = 2^2 \cdot 11, y_{-9} = 9^2, y_0 = 1, y_1 = 2^2, y_3 = 3^2.$$

And finally, an example showing that if $\text{sf}(|N_\alpha|)$ is twice an odd prime, then there can be distinct four squares (again unlike in Conjecture 1.1):

$$(d, t, u, a, b) = (6, 10, 4, 2, 3): N_\alpha = -2 \cdot 241, y_{-3} = 63^2, y_0 = 3^2, y_1 = 7^2, y_3 = 69^2.$$

6.4. Examples for Theorem 1.4(a). From (3.14) with $b = u = 1$, we find that $(2t + a)^2 - 8y_1 = a^2 - 8$. Since $-N_\alpha = d - a^2 = t^2 + 4 - a^2$ is a square, we put $a = 2$, so if y_1 is a square,

then $2t+2$ is an element of the sequence $(t_n)_{n \geq 0}$ with $t_0 = 6$, $t_1 = 238$ and $t_{n+1} = 34u_n - u_{n-1}$. The corresponding values of $\sqrt{y_1}$ are the elements of the sequence $(u_n)_{n \geq 0}$ with $u_0 = 5$, $u_1 = 169$ and $u_{n+1} = 34u_n - u_{n-1}$. Then y_1 is approximately $t^2/2 \approx |N_\alpha|/2 \approx |N_\alpha|^{3/2}/(2\sqrt{d})$.

In fact, such y_1 's are the ones that are squares satisfying the conditions in Theorem 1.4(a) with the smallest ratio compared to $|N_\alpha|^{3/2}/\sqrt{d}$, the quantity in Proposition 4.1.

6.5. Examples for Lemma 3.5. We can show that the lower bound in Lemma 3.5(c) is actually best possible. Let n be a positive integer such that $a = 2n^2 - 3$ is not divisible by 5 and put $d = 4n^4 - 8n^2 + 8$. We have $N_\alpha = 1 - 4n^2$. Then $(t, u) = (a + 1, 1)$, $y_{-1} = n^2$ and so $y_{-1}/|N_\alpha| \rightarrow 1/4$ from above as $n \rightarrow +\infty$. There exist families with the same limit for $y_{-1}/|N_\alpha|$ when $-N_\alpha$ is a square too.

The sequences given in Lemma 3.6 show that for $k = -1$, the lower bound in Lemma 3.5(c) can be attained too. At least, when the lower bound is 1.

REFERENCES

- [1] S. Akhtari, *The Diophantine equation $aX^4 - bY^2 = 1$* , Journal für die reine und angewandte Mathematik **630** (2009), 33–57.
- [2] A. Baker, *Rational approximations to certain algebraic numbers*, Proc. London. Math. Soc. (3) **14** (1964), 385–398.
- [3] A. Baker, *Rational approximations to $\sqrt[3]{2}$ and other algebraic numbers*, Quart. J. Math. Oxford **15** (1964), 375–383.
- [4] W. Bosma, J. Cannon, C. Playoust, *The Magma algebra system. I. The user language*, J. Symbolic Comput. **24** (1997), 235–265.
- [5] Y. Bugeaud, M. Mignotte, S. Siksek, *Classical and modular approaches to exponential Diophantine equations I. Fibonacci and Lucas perfect powers*, Ann. Math. **163** (2006), 969–1018.
- [6] Chen Jian Hua, P. Voutier, *Complete solution of the diophantine equation $X^2 + 1 = dY^4$ and a related family of quartic Thue equations*, J. Number Theory **62** (1997), 71–99.
- [7] J.-H. Evertse, *On the Representation of Integers by Binary Cubic Forms of Positive Discriminant*, Invent. Math. **73** (1983), 117–138.
- [8] J. Liouville, *Sur des classes très-étendues de quantités dont la valeur n'est ni algébrique, ni même réductible à des irrationnelles algébriques*, C. R. Acad. Sci. Paris, Sér. **A 18** (1844) 883–885.
- [9] W. Ljunggren, *On the Diophantine equation $Ax^4 - By^2 = C$ ($C = 1, 4$)*, Math. Scand. **21** (1967) 149–158.
- [10] The PARI Group, PARI/GP version 2.12.0, Univ. Bordeaux, 2019, <http://pari.math.u-bordeaux.fr/>.
- [11] W. M. Schmidt, *The zero multiplicity of linear recurrence sequences*, Acta Math. **182** (1999), 243–282.
- [12] C. L. Siegel, *Über einige Anwendungen diophantischer Approximationen*, Abh. Preuss. Akad. Wiss. **1** (1929), 41–69.
- [13] C. L. Siegel, *Die Gleichung $ax^n - by^n = c$* , Math. Ann. **114** (1937), 57–68.
- [14] C. L. Stewart, *On divisors of Lucas and Lehmer numbers*, Acta Math. **211** (2013), 291–314.
- [15] P. M. Voutier, *Thue's Fundamentaltheorem, I: The General Case*, Acta Arith. **143** (2010), 101–144.
- [16] P. M. Voutier, *Thue's Fundamentaltheorem, II: Further Refinements and Examples*, J. Number Theory **160** (2016), 215–236.
- [17] P. M. Voutier, *Improved constants for effective irrationality measures from hypergeometric functions*, Combinatorics and Number Theory **11** (2022), 161–180 <https://doi.org/10.2140/moscow.2022.11.161>.
- [18] P. M. Voutier, *Sharp bounds on the number of squares in recurrence sequences and solutions of $X^2 - (a^2 + b)Y^4 = -b$* , Research Number Theory (accepted) <https://arxiv.org/abs/1807.04116>.

7. CORRECTIONS FROM PUBLISHED VERSION

The most significant one is the change from 20 August 2025 for Lemma 3.10.

2 Aug 2024:

removed the PV footnote that should not be present.

25 Aug 2024:

in Lemma 3.9, added comment at the end that ζ_4 is any primitive 4-th root of unity.

1 Oct 2024:

in the statement of Lemma 3.9(b) added the condition that $k, \ell \neq 0$.

This is needed for use of Prop 3.1.

8 Dec 2024:

used 0.1263 and 3.96 consistently throughout paper

had some 0.127 and 3.959 and some 0.1263 and 3.96 before

(see 3 May 2025 change below too).

20 Jan 2025:

towards bottom of page 299 of published file, had $d' = u_2^2 t'$, but should be $d' = u_2^2 t' / g^2$.

arxiv location: page 7, line -8.

3 Feb 2025:

displayed formula on line 2 of the proof of Lemma 5.3:

y_{-1} on the right-hand side of first inequality should be y_{-1}^3 . (but y_{-1}^3 correctly used afterwards)

27 Feb 2025:

Near beginning of Subsection, “Construction of Approximations”

change “We let $u = \dots$ ” to “such that $u = \dots$ ”.

23 Apr 2025:

added $N_\alpha < 0$ to proof of Lemma 3.5(c) when $k = 1$.

23 Apr 2025:

–a few lines after that, $u_1 = u$ should be $u_1 = u/2$

–also removed redundant ()’s in expressions for $y_{\pm 1}$ in equation (1.2)

–journal name for reference [17] corrected.

3 May 2025:

third line of Section 4.2:

“From the equality in (4.2)...” should read “From (4.2)...”

Also reverted the numerical changes from 8 Dec 2024 and only changed 0.127 to 0.1263 in equation (3.31) so that the argument there to use (3.22) (where we need 0.1263) would be correct. No other changes are needed.

5 May 2025:

where appropriate (i.e., where they arise from the Representation Proposition), all ω ’s, ε ’s and φ ’s changed to ω_k ’s, ε^k ’s and φ_k ’s, respectively.

22 May 2025:

page 297, line 3:

in the definition of $Y_{m,n,r}$ in Section 2, I added the argument, z , that was missing.

I.e., changed “ $Y_{m,n,r}$ ” to “ $Y_{m,n,r}(z)$ ”.

arxiv location: page 5, line 14.

22 June 2025:

page 306, after line 4. State what $g_1'^2$ and $g_1''^2$ are.

I did not previously state this explicitly before.

arxiv location: page 12, line -6.

3 July 2025:

for max, use $()$ rather than $\{\}$

E.g., in gap principle (Lemma 3.8)

referee suggestion for the $-N_\alpha$ square for any b paper (the “ $\dots y_0 = b^2$ (I)” paper).

31 July 2025:

page 330, line -7: remove period before “to show that”.

arxiv location: page 33, sentence after equation (4.12).

10 Aug 2025: page 300, last line in Section 2: give this an equation number (2.10).

arxiv location: page 8, last line in Section 2.

20 Aug 2025:

Lemma 3.10 requires the condition that $\gcd(a, b)$ is odd.

The existing proof is fine with that condition added.

LONDON, UK

Email address: Paul.Voutier@gmail.com