PRIMITIVE DIVISORS OF SOME LEHMER-PIERCE SEQUENCES

ANTHONY FLATTERS

ABSTRACT. We study the primitive divisors of the terms of $(\Delta_n)_{n\geqslant 1}$, where $\Delta_n = N_{K/\mathbb{Q}}(u^n - 1)$ for K a real quadratic field, and $u > 1$ a unit element of its ring of integers. The methods used allow us to find the terms of the sequence that do not have a primitive prime divisor.

1. Introduction

Let $A = (a_n)_{n\geqslant 1}$ be an integer sequence. A prime p dividing a term a_n is called a *primitive prime divisor* (PPD for short) of a_n if p does not divide a_m for any $m < n$ with $a_m \neq 0$. Sequences whose terms all have primitive divisors beyond some point are of great interest in number theory.

Definition 1.1. Let $A = (a_n)_{n\geqslant 1}$ be an integer sequence. Define

$$Z(A) = \max\{n : a_n \text{ does not have a primitive prime divisor}\}$$

if this set is finite, otherwise set $Z(A) = \infty$. The number $Z(A)$ is called the *Zsigmondy Bound* for the sequence A.

In [1], Bang considered the sequence $(a^n - 1)_{n\geqslant 1}$, where $1 < a \in \mathbb{Z}$ and showed that $Z((a^n - 1)_{n\geqslant 1}) \leqslant 6$. Zsigmondy in [16] proved the more general result that given any positive coprime integers a, b with $a > b$, the sequence $(a^n - b^n)_{n\geqslant 1}$ has a primitive prime divisor for all terms beyond the sixth. The sequence studied by Zsigmondy satisfies a binary linear recurrence relation, and much of the work in this area has concentrated on these types of sequences. In [3], Carmichael showed that for any real Lucas or Lehmer sequence L, $Z(L) \leqslant 12$. Carmichael's result was later completed by Bilu, Hanrot and Voutier, and in [2] they showed, using powerful methods from transcendence theory and computational number theory, that for any Lucas or Lehmer sequence L', $Z(L') \leqslant 30$. Moreover, they were able to explicitly describe all Lucas and Lehmer numbers without a primitive divisor and hence show that this bound is sharp.

Many arithmetic properties of linear recurrence sequences have analogues for elliptic recurrence sequences. In [14], it is shown that if E is an elliptic curve in Weierstrass form defined over $\mathbb{Q}$, and $P \in E(\mathbb{Q})$ is a non-torsion point, then the associated elliptic divisibility sequence (the denominators of the x-coordinates of nP) has a finite Zsigmondy bound. For elliptic curves in global minimal form, it seems likely that this bound is uniform, and the papers [6], [8] exhibit infinite families of elliptic curves with a uniform Zsigmondy bound.

The result of Zsigmondy can be generalised to a number field setting, where a, b are now algebraic integers of a number field K, so $a^n - b^n$ lies in the ring of integers R, of K. The principal ideal $(a^n - b^n)$ has a factorisation into a product of prime ideals of R, which is unique. Therefore, we can ask which terms of a sequence S of algebraic integers have a primitive prime ideal divisor (or PPID for short), i.e. for which n is there a prime ideal $\mathfrak{p}$ which divides the nth term, but not any preceding term. We therefore define the Zsigmondy bound $Z_I(S)$, to be the maximal value of n for which the nth term of the sequence does not have a PPID.

In Schinzel's paper [13], he proved the following theorem;

Theorem 1.2 (Schinzel)**.** Let A, B be coprime integers of an algebraic number field such that $\frac{A}{B}$ is not a root of unity. Then the expression $A^n - B^n$ has a PPID for all $n > n_0(d)$, where d is the degree of the extension $\mathbb{Q}\left(\frac{A}{B}\right)/\mathbb{Q}$.

So, for these sequences the Zsigmondy bound Z_I is finite and an easy corollary of Schinzel's theorem is the following.

Corollary 1.3. Let K be a real quadratic field, R its ring of integers, and let $\alpha \in R \setminus \{\pm 1\}$ be a unit. Let f denote the minimum polynomial of α over $\mathbb{Q}$ and define the integer sequence, $\Delta = (\Delta_n(f))_{n\geqslant 1}$, by setting

$$\Delta_n(f) = N_{K/\mathbb{Q}}(\alpha^n - 1).$$

Then there exists a positive integer C_1, so that for all units α of norm 1, $Z(\Delta) \leqslant C_1$. There exists a positive integer C_2 such that for all units α of norm -1, $\Delta_n(f)$ has a primitive prime divisor for any $n > C_2$ with $n \not\equiv 2 \pmod 4$.

The sequence Δ, for a general algebraic integer α, was examined by Pierce in his paper [12], where he looked at what form the factors of $\Delta_n(f)$ take and what conditions are necessary for the congruence $f(x) \equiv 0 \pmod p$, where p is a prime, to have a solution $x \in \mathbb{F}_p$. In [10], Lehmer developed a deeper insight into the factors of the terms $\Delta_n(f)$, and applied this information to show that certain $\Delta_n(f)$ were prime. Lehmer was interested in the growth rate of the sequence Δ, and he remarked that if none of the roots of f had absolute value 1, then $\frac{\Delta_n(f)}{\Delta_{n-1}(f)}$ converges, and $M(f)$ was written for the limit. For his purposes, polynomials with small values of $M(f)$ were desirable; in [4] a heuristic argument is put forward that suggests the density of primes in Δ is proportional to $\frac{1}{M(f)}$. We therefore say that for α an algebraic integer, the sequence Δ, defined in Corollary 1.3, is called the *Lehmer-Pierce sequence* associated to α. The sequence Δ is also of interest in algebraic dynamics, since to f there is an associated matrix called the companion matrix and multiplication by this matrix induces an endomorphism $E : \mathbb{T}^N \longrightarrow \mathbb{T}^N$. When none of the roots of f have absolute value 1, E is an *ergodic* transformation with respect to Lebesgue measure, $|\Delta_n(f)|$ counts the number of points of period n under E, and the topological entropy of E is equal to $\log M(f)$. A much more detailed account of the connection between $M(f)$ and dynamical systems can be found in [5].

The sequence Δ also has some combinatorial applications. For example, when $u = 1 + \sqrt{2}$, $|\Delta_n|$ counts the number of 2×2 tiles in all tilings of a $3 \times (n + 1)$ rectangle with 1×1 and 2×2 square tiles; more details about this sequence are provided on Sloane's website [11, A095977]. Similarly, when $u = \frac{3+\sqrt{5}}{2}$, Δ_n appears in combinatorics - see [11, A004146]. In addition, certain quadratic Lehmer-Pierce sequences count the sizes of groups: the groups being $E(\mathbb{F}_{p^n})$, where E is a given elliptic curve and p is a fixed prime.

In this article our aim is to find the numbers C_1, C_2 from Corollary 1.3 associated to the sequence $\Delta = (\Delta_n)_{n\geqslant 1} = (N_{K/\mathbb{Q}}(u^n - 1))_{n\geqslant 1}$, where K is a real quadratic field and u is a fixed unit in its ring of integers.

Theorem 1.4. Let K be a quadratic field, $\alpha \neq \pm 1$ a positive quadratic unit, and let Δ be the Lehmer-Pierce sequence associated to α. Then for each α of norm 1, Δ has a primitive prime divisor for all terms beyond the twelfth. For each α of norm -1, then for $n > 24$, Δ_n fails to have a primitive prime divisor if and only if $n \equiv 2 \pmod 4$.

It is easy to see that when u has norm 1, Δ satisfies a ternary linear recurrence relation, and when u has norm -1, a quaternary linear recurrence - see [7]. In addition, it is remarked that it seems likely that when $u = 2 + \sqrt{3}$, $Z(\Delta) = 6$, and in our later discussion we verify that this is indeed the case. To date, not much is known about primitive prime divisors of the terms Δ_n for arbitrary algebraic integers α, and it would be interesting to know which other Lehmer-Pierce sequences have the property that $Z(\Delta)$ is finite.

2. A Criterion for Primitive Divisor Failure

We begin with a proof of Corollary 1.3 as it will be instrumental in obtaining a condition that will need to be satisfied if Δ_n fails to have a PPD.

Proof of Corollary 1.3. Define $A_n = \alpha^n - 1$ and $B_n = \beta^n - 1$, where β is the algebraic conjugate of α. There are only two ways in which Δ_n could fail to have a primitive prime divisor, and they are the following:

(1) Both A_n and B_n fail to have PPIDs;
(2) Every PPID of A_n has already appeared before as a divisor of B_m for some $m < n$.

Suppose then that $\mathfrak{p}$ is a PPID of A_n but that $\mathfrak{p}|B_m$ for some $m < n$. Then

$$(\beta^m - 1) = \mathfrak{p}\mathfrak{q}$$

for some integral ideal $\mathfrak{q}$. Hence, multiplying through by (α^m),

$$(\alpha^m)(\beta^m - 1) = \mathfrak{p}\mathfrak{q}.$$

If α has norm 1, this therefore implies that $\mathfrak{p}$ divides A_m, which cannot be the case as $\mathfrak{p}$ is a PPID of A_n. If α has norm -1 and m is even, then by the same method as above we can deduce that possibility 2 will not occur. If α has norm -1 and m is odd, a slightly different argument is needed. If possibility 2 occurs in this case, we have that $\mathfrak{p}|(\alpha^m + 1)$. Therefore, $\alpha^m \equiv -1 \pmod{\mathfrak{p}}$ and so $\alpha^{2m} \equiv 1 \pmod{\mathfrak{p}}$. Now as $\mathfrak{p}$ is a primitive divisor of A_n, α has order n in the group $(R/\mathfrak{p})^*$. Therefore $n|2m$. Since $m < n$, this is enough to secure that $n = 2m$, and we conclude that possibility 2 can only hold in the case when n is twice an odd integer. If $n \equiv 2 \pmod 4$, then $n = 2k$ for some odd integer k and in this case $\Delta_n = -\Delta_k^2$, so Δ_n can never have any primitive prime divisors. We have deduced that if Δ_n fails to have a PPD, then both A_n and B_n fail to have PPIDs except in the case where α has norm -1 and then all terms which satisfy property 2, are those with $n \equiv 2 \pmod 4$. The fact that Δ_n fails to have a primitive divisor beyond some point if $n \equiv 2 \pmod 4$ was first pointed out by Győry.

Hence for units of norm 1, Δ_n will only fail to have a PPD, when condition 1 holds. So by Theorem 1.2, this tells us that $Z_I((A_n)_{n\geqslant 1}) < c_1$, and $Z_I((B_n)_{n\geqslant 1}) < c_2$, where c_1, c_2 are uniform constants, and so for all units α of norm 1, $Z(\Delta)$ is uniformly bounded. If α has norm -1, then Δ_n will fail to have a PPD when $n \equiv 2 \pmod 4$ and when condition 1 holds. Applying Theorem 1.2 again gives the required result. □

From now on, K denotes a real quadratic field we will write N for the field norm $N_{K/\mathbb{Q}}$.

Lemma 2.1. Let $u \in R \setminus \{\pm 1\}$ be a quadratic unit of norm 1. Then for any $n > 6$, if Δ_n fails to have a primitive prime divisor we have

$$N(\phi_n(u)) \Big| n^2, \tag{1}$$

where $\phi_n(x) \in \mathbb{Z}[x]$ denotes the nth cyclotomic polynomial. Moreover, if u has norm -1 then for any $n > 6$ with $n \not\equiv 2 \pmod 4$, if Δ_n fails to have a PPD then (1) holds.

Proof. Apply Lemma 4 of [13] to deduce that if $\mathfrak{p}$ is not a PPID of A_n or B_n, then for $n > 6$,

$$\operatorname{ord}_{\mathfrak{p}}(\phi_n(u)) \leqslant \operatorname{ord}_{\mathfrak{p}}(n)$$

and

$$\operatorname{ord}_{\mathfrak{p}}(\phi_n(v)) \leqslant \operatorname{ord}_{\mathfrak{p}}(n).$$

Adding these two inequalities together tells us that

$$\operatorname{ord}_{\mathfrak{p}}(N(\phi_n(u))) \leqslant \operatorname{ord}_{\mathfrak{p}}(n^2),$$

and so we have proved the statement of the Lemma. □

Using (1), we can express this result in a way that will allow us to obtain an upper bound on n such that Δ_n has no PPD.

Theorem 2.2. Let $1 < u \in R$ be a unit, and $6 < n \in \mathbb{N}$. If u has norm 1 and Δ_n has no primitive prime divisor, then

$$\log n - 2\log\log n - \frac{4}{\log n} < 2.02819 - \log\log u. \tag{2}$$

If u has norm -1, $n \not\equiv 2 \pmod 4$, and Δ_n has no primitive prime divisor, then

$$\log n - 2\log\log n - \frac{4}{\log n} < 2.71072 - \log\log u. \tag{3}$$

Proof. Recall the factorisation of $x^n - 1$ into a product of cyclotomic polynomials as follows

$$x^n - 1 = \prod_{d|n} \phi_d(x).$$

Hence we have the following factorisation of Δ_n

$$|\Delta_n| = \prod_{d|n} |N(\phi_d(u))|.$$

Taking logarithms now gives

$$\log(|N(u^n - 1)|) = \sum_{d|n} \log(|N(\phi_d(u))|).$$

Applying the Möbius Inversion Formula for arithmetical functions now yields

$$\log(|N(\phi_n(u))|) = \sum_{d|n} \log(|N(u^d - 1)|)\mu\left(\frac{n}{d}\right). \tag{4}$$

Now using (4), we are going to estimate the size of $|N(\phi_n(u))|$. If u is a unit of norm 1, then

$$\begin{aligned} \log|N(u^d - 1)| &= \log|u^d - 1| + \log|v^d - 1| \\ &= \log|u^d - 1| + \log\left|\frac{1}{u^d} - 1\right| \\ &= \log|u^d| + 2\log\left|1 - \frac{1}{u^d}\right|. \end{aligned}$$

Therefore, by (4) we have

$$\begin{aligned} \log(|N(\phi_n(u))|) &= \sum_{d|n} \log|u^d|\mu\left(\frac{n}{d}\right) + 2\sum_{d|n} \log\left|1 - \frac{1}{u^d}\right| \mu\left(\frac{n}{d}\right) \\ &= \phi(n)\log u + 2\sum_{d|n} \log\left|1 - \frac{1}{u^d}\right| \mu\left(\frac{n}{d}\right). \end{aligned}$$

Define $S := 2\sum_{d|n} \log\left|1 - \frac{1}{u^d}\right| \mu\left(\frac{n}{d}\right)$. Using the Taylor expansion for $\log(1-x)$, we obtain that

$$|S| = 2\left|\sum_{m=1}^{\infty} \frac{1}{m} \sum_{d|n} \frac{1}{u^{md}}\mu\left(\frac{n}{d}\right)\right|.$$

Hence,

$$\begin{aligned} |S| &< 2\sum_{m=1}^{\infty} \frac{1}{m} \sum_{d=1}^{\infty} \frac{1}{u^{md}} \\ &= 2\sum_{m=1}^{\infty} \frac{1}{m}\left(\frac{u^{-m}}{1 - u^{-m}}\right). \end{aligned}$$

Since u has norm 1, $u \geqslant \frac{3+\sqrt{5}}{2}$. In addition, $m \geqslant 1$ so

$$|S| < 3.23607 \sum_{m=1}^{\infty} \frac{1}{m\left(\frac{3+\sqrt{5}}{2}\right)^m}. \tag{5}$$

The sum in (5) is equal to $-\log\left(1 - \frac{2}{3+\sqrt{5}}\right)$, and so

$$|S| < 1.55724,$$

which therefore yields that

$$\log(|N(\phi_n(u))|) > \phi(n)\log u - 1.55724.$$

Now we use the fact that if Δ_n has no PPDs, then $|N(\phi_n(u))| \leqslant n^2$. Therefore, we have the following relation

$$u^{\phi(n)} < e^{1.55724} n^2. \tag{6}$$

Taking logarithms twice of both sides we obtain

$$\log(\phi(n)) + \log\log u < \log(1.55724 + 2\log n).$$

Since $n > 6$, $\log n > 1$, hence we have that

$$\log n + \sum_{p|n} \log\left(1 - \frac{1}{p}\right) < \log(3.55724) - \log\log u + \log\log n,$$

and therefore

$$\log n < 1.26899 - \log\log u + \log\log n - \sum_{p|n} \log\left(1 - \frac{1}{p}\right).$$

Noting now that for all primes p, $-\log\left(1 - \frac{1}{p}\right) \leqslant \frac{1}{p} + \frac{1}{p^2}$ yields that

$$\log n < 1.26899 - \log\log u + \log\log n + \sum_{p|n} \frac{1}{p} + \sum_{p|n} \frac{1}{p^2}.$$

By Proposition 2.3.3, page 72 in [9], the last term in our previous inequality is at most $\log(\zeta(2))$, where $\zeta(s)$ denotes the Riemann-Zeta function. Therefore,

$$\log n < 1.76669 - \log\log u + \log\log n + \sum_{p \leqslant n} \frac{1}{p}.$$

In [15], the following estimate is derived

$$\sum_{p \leqslant n} \frac{1}{p} < \log\log n + B + \frac{4}{\log n},$$

where B is a numerical constant whose value is approximately equal to 0.2614972128. Inserting all this information into our inequality yields

$$\log n - 2\log\log n - \frac{4}{\log n} < 2.02819 - \log\log u.$$

If u is a unit of norm -1, then

$$\log|N(u^d - 1)| = \log|u^d| + \log\left|1 - \frac{1}{u^d}\right| + \log\left|1 - \frac{(-1)^d}{u^d}\right|.$$

Plugging this in to equation (4), we have

$$\begin{aligned}
\log(|N(\phi_n(u))|) &= \sum_{d|n} \log|u^d| \mu\left(\frac{n}{d}\right) + \sum_{d|n} \log\left|1 - \frac{1}{u^d}\right| \mu\left(\frac{n}{d}\right) + \sum_{d|n} \log\left|1 - \frac{(-1)^d}{u^d}\right| \mu\left(\frac{n}{d}\right) \\
&= \phi(n)\log u + \sum_{d|n} \log\left|1 - \frac{1}{u^d}\right| \mu\left(\frac{n}{d}\right) + \sum_{d|n} \log\left|1 - \frac{(-1)^d}{u^d}\right| \mu\left(\frac{n}{d}\right).
\end{aligned}$$

Define $S_1 = \sum_{d|n} \log\left|1 - \frac{1}{u^d}\right| \mu\left(\frac{n}{d}\right)$ and $S_2 = \sum_{d|n} \log\left|1 - \frac{(-1)^d}{u^d}\right| \mu\left(\frac{n}{d}\right)$. Again, using the Taylor expansion for $\log(1-x)$, and estimating these sums in the same way we did for S, we get

$$\begin{aligned}
|S_i| &\leqslant \sum_{m=1}^{\infty} \frac{1}{m} \sum_{d|n} \frac{1}{u^{md}} \\
&< \sum_{m=1}^{\infty} \frac{1}{m} \left(\frac{u^{-m}}{1 - u^{-m}}\right).
\end{aligned}$$

Noting that since u is a unit of norm -1, $u \geqslant \frac{1+\sqrt{5}}{2}$, we see that

$$|S_i| < 2.61804 \sum_{m=1}^{\infty} \frac{1}{m\left(\frac{1+\sqrt{5}}{2}\right)^m}.$$

Once again, this sum is equal to $-\log\left(1 - \frac{2}{1+\sqrt{5}}\right)$, thus

$$|S_i| < 2.51966,$$

and so

$$\log(|N(\phi_n(u))|) > \phi(n)\log u - 5.03933.$$

Exponentiating this relation, we arrive at

$$|N(\phi_n(u))| > \frac{u^{\phi(n)}}{e^{5.03933}}. \tag{7}$$

Running through the same calculation as before gives us the desired inequality. □

3. Main Results

3.1. **Units of Norm 1.** If $u > 1$ is a unit of norm 1, then $u \geqslant (\frac{1+\sqrt{5}}{2})^2$. Inserting this into (2), we have that if Δ_n has no PPD, then

$$\log n - 2\log\log n - \frac{4}{\log n} < 2.06650$$

It is now clear that n is bounded, since $g(x) := \log x - 2\log\log x - \frac{4}{\log x}$ is an increasing function on (e, ∞). Then, since $g(n)$ is bounded above, n is also and so using Maple 9.5 to solve $g(x) = 2.06650$ we conclude that

$$n \leqslant 604.$$

We can now improve this further because we know that inequality (6) must be satisfied in order that Δ_n has no PPD. We also know that $u \geqslant \left(\frac{1+\sqrt{5}}{2}\right)^2$. So we do a case by case check of the values of n between 7 and 604 for which

$$\left(\frac{1+\sqrt{5}}{2}\right)^{2\phi(n)} - e^{1.55724}n^2 < 0. \tag{8}$$

Instructing Maple 9.5 to compute the left hand side of the above inequality for each n in our range and observing when the quantity is negative yields that

$$n \leqslant 30.$$

More precisely, inequality (8) only holds when $n = 8, 9, 10, 12, 14, 18, 24$ or 30. Now a bare hands approach is required to see if we can lower the bound.

If we choose u so that $u \geqslant C > \left(\frac{1+\sqrt{5}}{2}\right)^2$, the nature of the inequality in (6) will allow us to reduce the bound for n. Some experimenting shows that if we choose $C = 6$, we can deduce that $n \leqslant 6$ using the same case checking procedure as before.

Therefore, our strategy will be to find all the units of norm 1 which are between 1 and 6 (of which there are finitely many) and using (1) to look at the terms of the sequence up to the 30th and deduce the Zsigmondy bound. For $u > 6$, we know from our above comments that the Zsigmondy bound is at most 6, and there is little more we can say on this point.

To find norm 1 units $1 < u \leqslant 6$, we note that when $d \not\equiv 1 \pmod 4$, u is of the shape $u = a + b\sqrt{d}$, where a, b are integers. Hence, the following inequality holds

$$2.618 < a + b\sqrt{d} \leqslant 6.$$

Taking reciprocals we have

$$0.166 < a - b\sqrt{d} < 0.382,$$

and it is clear that

$$2 \leqslant a \leqslant 3.$$

If $a = 2$ and $N(u) = 1$ then we have $b^2 d = 3$. The only solutions of this are when $b^2 = 1$ and $d = 3$ thus giving us $u = 2 \pm \sqrt{3}$. Hence, $u = 2 + \sqrt{3}$ is the only valid solution. Similarly if $a = 3$ the only valid unit is $u = 3 + 2\sqrt{2}$.

We now come to the case where $d \equiv 1 \pmod 4$. A similar analysis for $u = \frac{a+b\sqrt{d}}{2}$ yields

$$3 \leqslant a \leqslant 6.$$

The only solutions to $N(u) = 1$ with a in this range are $u = \frac{3\pm\sqrt{5}}{2}$ and $u = \frac{5\pm\sqrt{21}}{2}$, but again since $u > 2.618$, we take the positive sign. Hence there are four units of norm 1 which are greater than 1 but less than 6, namely $2 + \sqrt{3}, 3 + 2\sqrt{2}, \frac{3+\sqrt{5}}{2}, \frac{5+\sqrt{21}}{2}$.

We start with the case when $u = 2 + \sqrt{3}$, and we observe that for $7 \leqslant n \leqslant 30$ inequality (6) holds when $n = 8, 10, 12$. We also note that condition (1) fails when $n = 8, 10, 12$ so Δ_8, Δ_{10} and Δ_{12} all have PPDs, so we can restrict our attention to when $n \leqslant 6$. Here is a table illustrating the prime factors of Δ_n for n from 1 to 6.

n	Δ_n	Prime factors of Δ_n
1	-2	2
2	-12	$2, 3$
3	-50	$2, 5$
4	-192	$2, 3$
5	-722	$2, 19$
6	-2700	$2, 3, 5$

Therefore, the 4th and 6th terms of this sequence are the only ones which do not have a PPD.

We now turn our attention to $u = 3 + 2\sqrt{2}$, where inequality (6) does not hold for any $n \geqslant 7$. So we can say immediately that $Z(\Delta) \leqslant 6$. We illustrate the prime factors of Δ_n in a table as previously.

n	Δ_n	Prime factors of Δ_n
1	-4	2
2	-32	2
3	-196	$2, 7$
4	-1152	$2, 3$
5	-6724	$2, 41$
6	-39200	$2, 5, 7$

It is therefore clear that when $u = 3 + 2\sqrt{2}$ that all terms beyond the second have a PPD, so $Z(\Delta) = 2$.

When $u = \frac{5+\sqrt{21}}{2}$, we have that the inequality (6) holds when $n = 12$ and that (1) is false when $n = 12$. So we only need check terms from the sixth downwards to see which ones, if any, have no PPDs. We again list these terms and their prime factors in the table below.

n	Δ_n	Prime factors of Δ_n
1	-3	3
2	-21	$3, 7$
3	-108	$2, 3$
4	-525	$3, 5, 7$
5	-2523	$3, 29$
6	-12096	$2, 3, 7$

Hence, we deduce again that Δ_n has a PPD for all terms beyond the sixth, and Δ_6 is the only term which fails to have a PPD.

Finally, when $u = \frac{3+\sqrt{5}}{2}$ we find inequality (6) holds when $n = 8, 9, 10, 12, 14, 18, 24, 30$. Our condition (1) does not hold when n is equal to 14, 18, 24, or 30. So we now need to check cases $n \leqslant 12$, to see which terms of Δ_n have primitive prime factors. These have all been listed in the table below.

n	Δ_n	Prime factors of Δ_n
1	-1	None
2	-5	5
3	-16	2
4	-45	$3, 5$
5	-121	11
6	-320	$2, 5$
7	-841	29
8	-2205	$3, 5, 7$
9	-5776	$2, 19$
10	-15125	$5, 11$
11	-39601	199
12	-103680	$2, 3, 5$

It is immediately clear that Δ_n has no PPDs precisely when $n = 6, 10, 12$.

We have therefore proven the following theorem

Theorem 3.1. Let R be the ring of integers of the field $\mathbb{Q}(\sqrt{d})$, where d is a squarefree positive integer. Let $0 < u \in R$ be a unit of norm 1. If $u < \frac{1}{6}$ or $u > 6$, then $Z(\Delta) \leqslant 6$. For all other such units u, one of the following holds:

- $u = 3 + 2\sqrt{2}, 3 - 2\sqrt{2}$, where $Z(\Delta) = 2$.
- $u = 2 + \sqrt{3}, 2 - \sqrt{3}$, where $Z(\Delta) = 6$ and the only terms without a primitive prime divisor are Δ_4 and Δ_6.
- $u = \frac{3+\sqrt{5}}{2}, \frac{3-\sqrt{5}}{2}$, where $Z(\Delta) = 12$ and the only terms without a primitive prime divisor are Δ_6, Δ_{10} and Δ_{12}.
- $u = \frac{5+\sqrt{21}}{2}, \frac{5-\sqrt{21}}{2}$, where $Z(\Delta) = 6$ and the only term without a primitive prime divisor is Δ_6.

3.2. **Units of Norm** -1**.** We now wish to establish a similar result when u is a unit of norm -1. If u has norm -1 and $n = 2k$ where k is an odd integer, then (1) will not hold, but when n is of this form Δ_n does not have a PPD, so we just ignore these values of n. Define Δ' to be the sequence obtained by removing from Δ, the terms Δ_n for which $n \equiv 2 \pmod 4$.

If u is a quadratic unit of norm -1, then $u > \frac{1+\sqrt{5}}{2}$ and so by substituting into (3) we obtain that

$$g(n) < 3.44217,$$

where $g(x)$ is as before. Solving this inequality again using Maple 9.5 yields that

$$n \leqslant 3375.$$

Observing that if u is norm -1, inequality (7) holds, so by Theorem 2.1 we have

$$u^{\phi(n)} < e^{5.03933} n^2. \tag{9}$$

Since $u \geqslant \frac{1+\sqrt{5}}{2}$, we are led to solve the following inequality

$$\left(\frac{1+\sqrt{5}}{2}\right)^{\phi(n)} < e^{5.03933} n^2,$$

checking cases on Maple 9.5 for n between 7 and 3375 finds that this inequality is only true when

$$n \leqslant 90.$$

Using the same trick as for norm 1, we observe that for $u > 13$, inequality (9) implies that $n \leqslant 6$. We will therefore look at the cases $u > 13$ and $u \leqslant 13$ separately. Finding the positive units of norm -1 that are between 1 and 13 is a finite problem and using the method from earlier we find that they are $1+\sqrt{2}, \frac{1+\sqrt{5}}{2}, 2+\sqrt{5}, \frac{11+5\sqrt{5}}{2}, 3+\sqrt{10}, \frac{3+\sqrt{13}}{2}, 4+\sqrt{17}, 5+\sqrt{26}, \frac{5+\sqrt{29}}{2}, 6+\sqrt{37}, \frac{7+\sqrt{53}}{2}, \frac{9+\sqrt{85}}{2}$.

Now we need to look at the terms of the sequence for $1 \leqslant n \leqslant 90$ where $n \not\equiv 2 \pmod 4$ to see which have no PPDs. Doing the individual case checks as in the norm 1 case we find that when

$u = 1 + \sqrt{2}$, inequality (9) holds when $n = 7, 8, 9, 10, 11, 12, 14, 15, 16, 18, 20, 21, 22, 24, 26, 28, 30, 36, 42$. We are however ignoring the terms Δ_n for which $n \equiv 2 \pmod 4$, so this leaves us to check the cases $n = 7, 8, 9, 11, 12, 15, 16, 20, 21, 24, 28, 36$. However (1) is violated, for all these values of n, therefore we conclude that $Z(\Delta') \leqslant 4$. Once again we check to see if Δ_n has a primitive divisor for the relevant values of n between 1 and 5. Again we illustrate the factors of Δ_n in tabular form

n	Δ_n	Prime factors of Δ_n
1	-2	2
3	-14	2, 7
4	-32	2
5	-82	2, 41

It is at once clear that $\Delta_4 = \Delta'_3$ is the only term of Δ' without a PPD.

For $u = \frac{1+\sqrt{5}}{2}$, relations (1) and (9) are enough to ensure that for $n > 6$, Δ_n has a PPD unless $n = 12, 20, 24$. So we now need to check all the terms up to the 24th to see which ones have primitive prime divisors, and then we are done. Here is the table

n	Δ_n	Prime factors of Δ_n
1	-1	None
3	-4	2
4	-5	5
5	-11	11
7	-29	29
8	-45	3, 5
9	-76	2, 19
11	-199	199
12	-320	2, 5
13	-521	521
15	-1364	2, 11, 31
16	-2205	3, 5, 7
17	-3571	3571
19	-9349	9349
20	-15125	5, 11
21	-24476	2, 19, 211
23	-64079	139, 461
24	-103680	2, 3, 5

We see that $\Delta_{12} = \Delta'_9, \Delta_{20} = \Delta'_{15}$ and $\Delta_{24} = \Delta'_{18}$ are the only terms of Δ' that fail to have a PPD.

For all of the other units $u \leqslant 13$, conditions (9) and (1) are enough to secure that $n < 6$, and hence that $Z(\Delta') \leqslant 4$. Checking for primitive divisors of the remaining terms in exactly the same way as above, yields that all terms have a primitive prime divisor and so $Z(\Delta') = 1$.

Our case checking is now complete and we have derived the following result.

Theorem 3.2. Let R be as in Theorem 3.1 and $1 < u \in R$ be a unit of norm -1. Then for all $u > 13$, $Z(\Delta') \leqslant 4$. If $u \leqslant 13$, then one of the following is true:

- $u = 1 + \sqrt{2}$, where $Z(\Delta') = 3$ and the only term without a primitive prime divisor is Δ'_3;
- $u = \frac{1+\sqrt{5}}{2}$, where $Z(\Delta') = 18$ and the only terms without a primitive prime divisor are Δ'_9, Δ'_{15} and Δ'_{18};
- $Z(\Delta') = 1$.

Combining the results of Theorems 3.1 and 3.2, gives us the statement of Theorem 1.4.

References

[1] A.S. Bang *Taltheoretiske Undersølgelser* Tidskrifft Math., **5** 1886, 70–80 and 130–137.

[2] Y. Bilu, G. Hanrot and P. Voutier *Existence of Primitive Divisors of Lucas and Lehmer Numbers* J. Reine Angew. Math., **539** 2001, 75–122, (with an appendix by M. Mignotte).
[3] R.D. Carmichael *On the Numerical Factors of the Arithmetic Forms* $\alpha^n \pm \beta^n$ Ann. Math., **15** 1913/14, 30–48 and 49–70.
[4] M. Einsiedler, G.R. Everest and T. Ward *Primes in Sequences Associated to Polynomials (After Lehmer)* LMS J. Comput. Math., **3** 2000, 125–139.
[5] G.R. Everest and T. Ward *Heights of Polynomials and Entropy in Algebraic Dynamics* Springer-Verlag, London, 1999.
[6] G.R. Everest, G. Mclaren and T. Ward *Primitive Divisors of Elliptic Divisibility Sequences* J. Number Theory, **118** 2006, 71–89.
[7] G.R. Everest, S.A.R. Stevens, D. Tamsett and T. Ward *Primes Generated by Recurrence Sequences* Amer. Math. Monthly, **114** 2007, 417–431.
[8] P. Ingram *Elliptic Divisibility Sequences over Certain Curves* J. Number Theory, **123** 2007, 473–486.
[9] G.J.O. Jameson *The Prime Number Theorem* LMS Student Texts, vol 53, Cambridge University Press, Cambridge, 2003.
[10] D.H. Lehmer *Factorization of Certain Cyclotomic Functions* Ann. Math., **34** 1933, 461–479.
[11] N.J.A. Sloane *Online Encyclopedia of Integer Sequences* `www.research.att.com/~njas/sequences`
[12] T.A. Pierce *The Numerical Factors of the Arithmetic Forms* $\prod_{i=1}^{n}(1-\alpha_i^m)$ Ann. Math., **18** 1916, 53–64.
[13] A. Schinzel, *Primitive Divisors of the Expression* $A^n - B^n$ *in Algebraic Number Fields* J. Reine Angew., **268/9** 1974, 27–33.
[14] J.H. Silverman *Wieferich's Criterion and the abc-conjecture* J. Number Theory, **30** 1988, 226–237.
[15] M.B. Villarino *Mertens' Proof of Mertens' Theorem* `ArXiv:math.HO/0504289v3`, 2005.
[16] K. Zsigmondy *Zur Theorie der Potenzreste* Monatsh. Math., **3** 1892, 265–284.

School of Mathematics, University of East Anglia, Norwich NR4 7TJ, UK
E-mail address: `Anthony.Flatters@uea.ac.uk`