On the Furstenberg closure of a class of binary recurrences

KEVIN A. BROUGHAN
Department of Mathematics
University of Waikato
Private Bag 3105, Hamilton, New Zealand
kab@waikato.ac.nz

FLORIAN LUCA
Instituto de Matemáticas
Universidad Nacional Autonoma de México
C.P. 58089, Morelia, Michoacán, México
fluca@matmor.unam.mx

23rd January 2009

Abstract
In this paper, we determine the closure in the full topology over $\mathbb{Z}$ of the set $\{u_n : n \geq 0\}$, where $(u_n)_{n \geq 0}$ is a nondegenerate binary recurrent sequence with integer coefficients whose characteristic roots are quadratic units. This generalizes the result for the case when $u_n = F_n$ was the $n$th Fibonacci number.

Keywords: Full topology, Binary recurrence sequences, Primitive divisors

AMS Subject Classification: 1B39, 11B50
1 Introduction

Let $\mathbb{Z}$ be the ring of integers equipped with the topology $\tau$ in which the base of neighborhoods for a point $a \in \mathbb{Z}$ is given by the sets

$$N_{a,b} = \{ a + nb : n \in \mathbb{Z} \} \quad \text{for } b \in \mathbb{Z}, \ b \geq 1.$$  \hfill (1)

This topology was proposed by H. Fürstenberg in [7]. It can be used to give a very elegant proof of the fact that the set of prime numbers is infinite (see [1]). It is called the full topology. This topology was studied in detail in the recent paper [3], where the following conjecture was proposed.

Let $F = \{ F_n \}_{n \geq 0}$ denote the Fibonacci sequence given by $F_0 = 0$, $F_1 = 1$ and

$$F_{n+2} = F_{n+1} + F_n \quad \text{for all } n \geq 0.$$  \hfill (2)

Let $F^{-}$ denote the set $\{(-1)^{n+1}F_n : n \in \mathbb{N}\}$. Then the closure of $F \subset \mathbb{Z}$ in the topology $\tau$ is $F \cup F^{-}$. Some numerical evidence supporting the above conjecture was given in the last section of [3]. The above conjecture was confirmed in [8].

In this paper, we revisit the arguments from [8] and prove a more general version of the above result. Namely, let $(u_n)_{n \geq 0}$ be any sequence of integers satisfying the recurrence

$$u_{n+2} = ru_{n+1} + su_n \quad \text{for all } n \geq 0.$$  \hfill (3)

Here, $r$ and $s$ are some fixed integers. We assume that $rs(r^2 + 4s) \neq 0$. It is then well-known that if one writes $\alpha$ and $\beta$ for the two roots of the characteristic equation $x^2 - rx - s = 0$, then there exist constants $\gamma$ and $\delta$ in $\mathbb{K} = \mathbb{Q}(\alpha)$ such that

$$u_n = \gamma \alpha^n + \delta \beta^n \quad \text{for all } n \geq 0.$$  \hfill (4)

We assume further that $\gamma \delta \neq 0$ and that $\alpha/\beta$ is not a root of unity. Under these conditions, it is said that the sequence $(u_n)_{n \geq 0}$ is nondegenerate.

Here, we only consider the case when $s = \pm 1$. In this case, one checks easily that $\mathbb{K}$ is a real quadratic field in which $\alpha$ and $\beta$ are units. We may also define $u_n$ for $n < 0$, either recursively via formula (3), or simply by allowing $n$ to be negative in formula (4). We have the following result.
Theorem 1. The closure of the set \( \{u_n : n \geq 0\} \) in the full topology is the set \( \{u_n : n \in \mathbb{Z}\} \).

The above result applies to the Fibonacci sequence \((F_n)_{n \geq 0}\) which satisfies the recurrence relation (3) with \( s = 1 \). Since \((-1)^{n+1}F_n = F_{-n}\), the main result of [8] is an immediate consequence of our Theorem 1.

2 Some Conventions

We first make some reductions. Put

\[ v_n = u_{2n} = \gamma \alpha^{2n} + \delta \beta^{2n} \quad \text{and} \quad w_n = u_{2n+1} = (\gamma \alpha)\alpha^{2n} + (\delta \beta)\beta^{2n} \]

for all \( n = 0, 1, \ldots \). Both \((v_n)_{n \geq 0}\) and \((w_n)_{n \geq 0}\) are binary recurrent sequences, with the same characteristic equation having roots \( \alpha^2 \) and \( \beta^2 \), and the closure \( U \) of \( \{u_n : n \geq 0\} \) is the union of the closures of \( V = \{v_n : n \geq 0\} \) and \( W = \{w_n : n \geq 0\} \).

This argument shows that it suffices to prove Theorem 1 for the two sequences \((v_n)_{n \geq 0}\) and \((w_n)_{n \geq 0}\). In particular, it suffices to prove Theorem 1 when \( \alpha \) and \( \beta \) are both positive. Thus, \( r > 0 \) and \( s = -1 \). Furthermore, we use \( \alpha \) for the root which is \( > 1 \). We put \( \Delta = r^2 + 4s = r^2 - 4 = dt^2 \), where \( d \) is squarefree. Then

\[ \alpha = \frac{r + \sqrt{\Delta}}{2} \quad \text{and} \quad \beta = \frac{r - \sqrt{\Delta}}{2}. \]

Since the multiplication by any nonzero integer is a continuous map, we may assume that \( \gamma > 0 \) for if not, we may then replace the sequence \((u_n)_{n \geq 0}\) by the sequence \((-u_n)_{n \geq 0}\), which has as effect replacing the pair \((\gamma, \delta)\) by \((-\gamma, -\delta)\). Observe that with these conditions we have \( u_n > 0 \) for all \( n \) sufficiently large, say \( n > n_0 \).

We write \( K = \mathbb{Q}(\sqrt{d}) \) for the real quadratic field containing \( \alpha \) and \( \beta \). We also put \( \alpha_1 \) for the fundamental unit in \( K \) and \( \beta_1 \) for its conjugate. Since \( \alpha > 1 \), it follows that there exists a positive integer \( k \) such that \( \alpha = \alpha_1^k \). Clearly, \( \beta = \beta_1^k \). Observe that \( k \) is even if the norm of \( \alpha_1 \); i.e., the number
$\alpha_1\beta_1$, equals $-1$. We write $N_{K/Q}$ for the norm of an element, or norm of an integer or fractional ideal, of $K$ relative to $Q$.

Throughout, for three algebraic integers $\mu_1$, $\mu_2$ and $\nu \neq 0$ we say that $\mu_1 \equiv \mu_2 \pmod{\nu}$ if $(\mu_1 - \mu_2)/\nu$ is an algebraic integer.

We use the Landau symbol $O$ and the Vinogradov symbols $\gg$ and $\ll$ with their usual meanings. We shall also use $c_1, c_2, \ldots$ for positive computable constants depending on the sequence $(u_n)_{n \geq 0}$.

### 3 The Proof of Theorem 1

We first prove that $\{u_n : n \in \mathbb{Z}\} \subseteq \overline{U}$. Indeed, since $s = \pm 1$, it is known that for every positive integer $m$ the sequence $(u_n)_{n \geq 0}$ is periodic modulo $m$ with some period $T(m)$. In fact, since $\alpha$ and $\beta$ are units, it follows that they remain units in the finite ring $\mathbb{Z}[\alpha]/(\Delta m \mathbb{Z}[\alpha])$. Thus, there exists a positive integer $T(m)$ such that both relations $\alpha^{T(m)} \equiv 1 \pmod{\Delta m}$ and $\beta^{T(m)} \equiv 1 \pmod{\Delta m}$ hold. Observe now that since

\[ u_0 = \gamma + \delta \quad \text{and} \quad u_1 = \gamma\alpha + \delta\beta, \]

it follows that

\[ \gamma = \frac{u_1 - \beta u_0}{\alpha - \beta} \quad \text{and} \quad \delta = \frac{\alpha u_0 - u_1}{\alpha - \beta}. \]

In particular, both numbers $(\alpha - \beta)\gamma$ and $(\alpha - \beta)\delta$ are algebraic integers. Now note that

\[
(\alpha - \beta)u_{n+T(m)} = ((\alpha - \beta)\gamma)\alpha^{n+T(m)} + ((\alpha - \beta)\delta)\beta^{n+T(m)}
\equiv ((\alpha - \beta)\gamma)\alpha^n + ((\alpha - \beta)\delta)\beta^n \pmod{\Delta m}
\equiv (\alpha - \beta)u_n \pmod{\Delta m},
\]

therefore $(\alpha - \beta)(u_{n+T(m)} - u_n) \equiv 0 \pmod{\Delta m}$. Since $\Delta = (\alpha - \beta)^2$, it follows that $(u_{n+T(m)} - u_n)/m$ is an algebraic integer. Since it is also a rational number, it follows that it is an integer. The above argument was valid for all integers $n$. Thus, given any integer $n$ and any modulus $m$, we
may let $T$ be a sufficiently large positive integer such that $n + T(m)T$ is positive. Then $u_n \equiv u_{n+T(m)T} \pmod{m}$. Since $m$ was arbitrary, we conclude that \{\{u_n : n \in \mathbb{Z}\} \subseteq \overline{U}\}, which is what we wanted to prove.

We next demonstrate the reverse containment.

We let $U = \{u_n : n \geq 0\}$ and let $a \in \overline{U}$. We want to show that $a = u_n$ for some $n \in \mathbb{Z}$. We start with the case $a = 0$.

**The case $a = 0$.**

In this case, since $0 \in \overline{U}$, it follows that the equation $u_n \equiv 0 \pmod{p}$ has a solution $n$ for each large prime $p$. Writing

$$u_n = \gamma \beta^n \left(\alpha^{2n} + \frac{\delta}{\gamma}\right),$$

it follows that if $p$ is sufficiently large, say if $p$ is large enough so that it is coprime with the prime ideals of $K$ appearing in the factorization of either $\gamma$ or $\delta$, then the congruence

$$-\frac{\delta}{\gamma} \equiv \alpha^{2n} \pmod{p}$$

has an integer solution $n$. It follows from the lemma [9, Page 108], that $\delta/\gamma$ is a unit in $K$. In particular, $\delta/\gamma = \pm \alpha_s^i$ for some integer $s$. Thus,

$$u_n = \gamma \alpha_i^{-kn+s} \left(\alpha_i^{2kn-s} \pm 1\right). \tag{5}$$

We next show that $s$ is a multiple of $k$ and that the sign is $-1$. Consider the sequence with the general term

$$V_n = \alpha_1^n - 1 \in \mathcal{O}_K \quad \text{for } n = 1, 2, \ldots$$

We say a prime ideal $\mathcal{P}$ of $\mathcal{O}_K$ is primitive for $V_n$ if it has the property that $\mathcal{P} \mid V_n$ but $\mathcal{P}$ does not divide $V_m$ for any $1 \leq m < n$. It follows from results of Schinzel [10] and Stewart [11, Theorem 1] that $V_n$ always has primitive divisor $\mathcal{P}$ if $n$ exceeds some absolute constant.

If $\mathcal{P}$ is such a primitive divisor and $p$ is the prime number such that $\mathcal{P} \mid p$, then $p \gg n^{1/2}$: to see this since $K$ is quadratic, $N(\mathcal{P}) = p$ or $N(\mathcal{P}) = p^2$.
where $p$ is the unique rational prime with $\mathcal{P} \mid p$. Therefore the order of the multiplicative group of $\mathcal{O}_K / \mathcal{P}$ is $p - 1$ or $p^2 - 1$ and $\alpha_i^{N(P)-1} \equiv 1 \mod \mathcal{P}$ shows that $n \mid p$ or $n \mid p^2 - 1$, from which the inequality follows [10].

Armed with these facts, let us go back to relation (5). Assume that $s$ is not a multiple of $k$. Let $m$ be large, let $\mathcal{P}$ be a primitive prime for $V_{2km}$, and let $p$ be the prime number such that $\mathcal{P} \mid p$. For large enough $m$, $p$ is coprime with the prime ideals appearing in the factorization of either or in $K$. There exists $n$ such that $u_n \equiv 0 \mod p$. We may assume that $n > s = (2k) = s_1 = 2$. Since $p$ is large, it follows that $s / (2k)$ is a proper divisor of $2km$, which contradicts the choice of $\mathcal{P}$ as a primitive prime ideal divisor of $\alpha_i^{2km} - 1$. Thus, $s = ks_1$.

We next show that the sign is $-1$. Assume that it were $+1$. Then

$$u_n = \gamma \alpha_1^{-(n+1)} \left( \alpha_1^{(2n-s_1)k} + 1 \right).$$

We now take a large prime $q$, put $m = kq$, and consider a primitive prime ideal $\mathcal{P}$ of $V_{kq}$. Let $p$ be the prime such that $\mathcal{P} \mid p$, and let $n$ be such that $u_n \equiv 0 \mod p$. Again, we assume that $n > s / (2k) = s_1 / 2$. Since $p$ is large, it follows that $\alpha_1^{(2n-s_1)k} \equiv -1 \mod \mathcal{P}$. But we also have that $\alpha_1^{kq} \equiv 1 \mod \mathcal{P}$. If $2n - s_1$ is a multiple of $q$, we then get that $-1 \equiv \alpha_1^{(2n-s_1)k} \mod \mathcal{P}$, so $\mathcal{P} \mid 2$, giving $p = 2$, which is false since we have assumed that $p$ is large. So assuming $q$ does not divide $(2n - s_1)$, we then have $\mathcal{P} \mid \alpha_1^{(2n-s_1)k} + 1 \mid V_{(2n-s_1)k}$ and $\mathcal{P} \mid V_{kq}$, therefore $\mathcal{P} \mid V_{\gcd((2n-s_1)k,kq)} \mid V_k$, where we used the fact that $q > 2$ and $q$ does not divide $2n - s_1$. This
contradicts the definition of $\mathcal{P}$ as a primitive divisor of $V_{ik}$. Hence, the sign is $-1$.

We have arrived at the conclusion that

$$u_n = \gamma \beta^n \alpha_1^s \left( \alpha_1^{(2n-s_1)k} - 1 \right).$$

Finally, we show that $s_1$ is odd. We use a similar method to that used above.

If $s_1$ were odd, let $m$ be a large even number and choose a primitive prime factor $\mathcal{P}$ of $V_{km}$. With $p$ the prime such that $\mathcal{P} \mid p$ and $n$ such that $p \mid u_n$ and large, we get that $\mathcal{P} \mid V_{[2n-s_1]k}$. Hence, $\mathcal{P} \mid V_{\gcd((2n-s_1)k, km)} \mid V_{mk/2}$, where we used the fact that $2n - s_1$ and odd and $m$ is even. This contradicts the choice of $\mathcal{P}$ as a primitive prime factor of $V_{km}$.

Thus, $s_1$ is even and we can write it as $s_1 = 2s_0$ for some integer $s_0$.

Thus,

$$u_n = \gamma \beta^n \alpha_1^s \left( \alpha_1^{2(n-s_0)k} - 1 \right),$$

and taking $n = s_0 \in \mathbb{Z}$, we get that $a = 0 \in \{u_n : n \in \mathbb{Z}\}$, which is what we wanted.

The case $a \neq 0$.

This case is much more interesting and harder. Here, we put $U_n = (\alpha^n - \beta^n)/(\alpha - \beta)$ for all $n \geq 0$. The sequence $(U_n)_{n \geq 0}$ satisfies the same recurrence relation (3) as $(u_n)_{n \geq 0}$ does and its initial values are $U_0 = 0$ and $U_1 = 1$.

We proceed in ten steps.

1. First we show that the sequence $(u_n : n \geq 0)$, when taken modulo $U_m$, has a well determined period.

Lemma 2. Let $m \geq 1$. The sequence $(u_n)_{n \geq 0}$ is periodic modulo $U_m$ with period $4m$.

Proof. Note that

$$\alpha^{4m} - 1 = \alpha^{4m} - (\alpha \beta)^{2m} = \alpha^{2m}(\alpha^{2m} - \beta^{2m}) \equiv 0 \pmod{\alpha^m - \beta^m}.$$ 

Thus, $\alpha^{4m} \equiv 1 \pmod{\alpha^m - \beta^m}$. Similarly, $\beta^{4m} \equiv 1 \pmod{\alpha^m - \beta^m}$. Hence,

$$(\alpha - \beta)u_{n+4m} = ((\alpha - \beta)\gamma)\alpha^n \alpha^{4m} + ((\alpha - \beta)\delta)\beta^n \beta^{4m} \equiv ((\alpha - \beta)\gamma)\alpha^n + ((\alpha - \beta)\delta)\beta^n \pmod{\alpha^m - \beta^m}$$

$$\equiv (\alpha - \beta)u_n \pmod{\alpha^m - \beta^m}.$$ 

7
Canceling the factor of \((\alpha - \beta)\), we get that \(u_{n+4m} \equiv u_n \pmod{U_m}\), which is what we wanted. \(\square\)

2. We next take a close look at the number \(u_n - a\). Observe that

\[
\begin{align*}
  u_n - a &= \gamma \alpha^n + \delta \beta^n - a = \gamma \beta^n \left(\frac{\alpha^{2n} - a}{\gamma} \alpha^n + \delta \right) \\
  &= \gamma \beta^n (\alpha^n - z_1)(\alpha^n - z_2),
\end{align*}
\]

where

\[
  z_{1,2} = \frac{a \pm \sqrt{\Delta_1}}{2\gamma} \quad \text{and} \quad \Delta_1 = a^2 - 4\gamma \delta.
\]

Recall that a primitive prime factor of \(U_m\) is a rational prime dividing \(U_m\) which does not divide \(U_{\ell}\) for any \(1 \leq \ell < m\) and which does not divide \(\Delta\) either. It is known that if \(m > 12\), then \(U_m\) has primitive divisors [11, Theorem 1]. In fact, putting

\[
  W_m = \prod_{\substack{p \nmid \gcd(n, 3) \text{ primitive}}} p^{e_p},
\]

then we have the following lemma due to Stewart [12, Page 603], but see also [2, Eqn. 17]. In the next statement we use \(P(n)\) for the largest prime factor of \(n\) and \(\Phi_n(X, Y)\) for the homogeneous cyclotomic polynomial of order \(n\).

**Lemma 3.** For all \(n > 12\), \(P(\frac{n}{\gcd(n, 3)}) W_n \geq \Phi_n(\alpha, \beta)\).

**Proof.** Any primitive prime divisor of \(U_n\) divides \(\Phi_n := \Phi_n(\alpha, \beta)\). If \(p\) is a prime divisor of \(\Phi_n\) and \(p \nmid n\) then \(p\) is a primitive divisor of \(\Phi_n\). The only possible prime dividing both \(n\) and \(\Phi_n\) is \(P(n/\gcd(n, 3))\) and it divides \(\Phi_n\) to the first power, so the lemma follows from the prime factorization of \(\Phi_n\). \(\square\)

Therefore

\[
  W_m \geq \frac{1}{m} \prod_{1 \leq \ell \leq m \atop \gcd(\ell, m) = 1} (\alpha - e^{2\pi i \ell / m} \beta) > \frac{(\alpha - \beta)^{\phi(m)}}{m} \exp((\log(\alpha - \beta)) \phi(m) - \log m),
\]

8
where \( \phi(m) \) is the Euler function. Using the fact that \( \phi(m) \gg m/\log \log m \), it follows that for all large \( m \) we have

\[
W_m \geq \exp(c_1 \phi(m)),
\]

where we can take \( c_1 = (\log(\alpha - \beta))/2 = (\log \Delta)/4 \).

3. Next we take a large positive integer \( m \) which is a multiple of \( 8k \) and we shall look at the simultaneous solutions \( n \) of the congruences

\[
u_n - a \equiv 0 \pmod{M},
\]

with

\[
M \in \{W_m, W_m/2W_m/4, W_mW_m/2W_m/4\}
\]

for reasons which will become clear later. Since \( M \mid U_m \), it follows, by Lemma 2, that we can take \( n \in [4m, 8m) \). We have

\[
e^{c_1 \phi(m)} \leq M \ll N_{L/Q} \left( \gcd(M, (\alpha^n - z_1)(\alpha^n - z_2)) \right) \\
\ll N_{L/Q} \left( \gcd(M, \alpha^n - z_1) N_{L/Q} (\gcd(M, \alpha^n - z_2)) \right).
\]

In the above, the greatest common divisors are to be thought of as fractional ideals of \( O_L \), where \( L = \mathbb{K}(z_1) \). It now follows that there exists a constant \( c_2 \), which can be taken to be \( c_1/3 \), such that if \( m \) is large, then for some \( i \in \{1, 2\} \) we have

\[
N_{L/Q} (\gcd(M, \alpha^n - z_i)) > \exp(c_2 \phi(m)).
\] (6)

4. The following argument has appeared in the proof of the main result in [8]. We supply the proof of it for convenience.

**Lemma 4.** With the previous notations, if \( z_i \) and \( \alpha \) are multiplicatively independent, and \( n \in [4m, 8m) \), then

\[
N_{L/Q} (\gcd(M, \alpha^n - z_i)) = \exp(O(\sqrt{m})).
\] (7)

**Proof.** Let

\[
S = \{\lambda n + 2\mu m : \lambda, \mu \in \{1, \ldots, \lfloor m^{1/2} \rfloor\}\}.
\]
If $s = \lambda n + 2\mu m$, then $1 \leq s \leq (n + 2m)m^{1/2} < 10m^{3/2}$. Since there are $(\lfloor m^{1/2} \rfloor)^2$ pairs of positive integers $(\lambda, \mu)$ with $\lambda, \mu \in \{1, \ldots, \lfloor m^{1/2} \rfloor\}$, it follows, by the Pigeon-Hole Principle, that there exist two distinct pairs $(\lambda_1, \mu_1) \neq (\lambda_2, \mu_2)$ such that

$$|(\lambda_1 - \lambda_2)n + 2(\mu_1 - \mu_2)m| < \frac{10m^{3/2}}{\lfloor m^{1/2} \rfloor^2 - 1} < 11m^{1/2}$$

for $m$ large enough.

Writing $x = \lambda_1 - \lambda_2$ and $y = \mu_1 - \mu_2$, we get that $(x, y) \neq (0, 0)$, that $x, y \in [-m^{1/2}, m^{1/2}]$, and that if we write $s = nx + 2my$, then $|s| < 11m^{1/2}$. Note now that if we define the fractional ideals

$$\mathcal{I}_i = \gcd([M], [\alpha^n - z_i]),$$

where $[\theta]$ represents the principal ideal generated by $\theta$ in $\mathbb{L} \ast$, then since $M | (\alpha^n - \beta^n)$, we have

$$\alpha^{2n} \equiv -1 \pmod{\mathcal{I}_i} \quad \text{and} \quad \alpha^n \equiv z_i \pmod{\mathcal{I}_i}.$$

Here, $z_i$ is invertible modulo $\mathcal{I}_i$ for large $m$ although $z_i$ might not be an algebraic integer. The reason here is that $M$ consists only of primitive prime factors of $U_m$, or of $U_{m/2}$, or of $U_{m/4}$, and all of them are congruent to $\pm 1$ modulo $m/4$. In particular, if $m$ is sufficiently large, then $z_i$ is invertible modulo $\mathcal{I}_i$.

Raising the first congruence to the power $y$ and the second to the power $x$ (notice that such operations are justified even if $x$ and $y$ are negative since $\alpha$ is a unit in $\mathbb{K}$, therefore also in $\mathbb{L}$), and multiplying the resulting congruences we get

$$\alpha^x \equiv (-1)^y z_i^x \pmod{\mathcal{I}_i}.$$

Thus, $\mathcal{I}_i$ divides $(\alpha^x - (-1)^y z_i^x)$. Note that this last ideal is not zero. Indeed, for if not, then we would get that $\alpha^{2x} = z_i^{2x}$. Since we are assuming that $\alpha$ and $z_i$ are multiplicatively independent, we get $x = s = 0$, and since $s = nx + 2my$, we get that $y = 0$ as well, which contradicts the fact that $(x, y) \neq (0, 0)$. Hence, $\mathcal{I}_i$ divides the nonzero ideal $(\alpha^x - (-1)^y z_i^x)$. Taking norms in $\mathbb{L}$ and observing that the degree of $\mathbb{L}$ over $\mathbb{Q}$ is at most 4, we get that

$$N_{\mathbb{L}/\mathbb{Q}}(\mathcal{I}_i) \leq (Z^{1/4} \alpha^{1/4} + \max\{|Z_{ij}^{(j)}| : i, j\}^{1/4})^4 = \exp(O(\sqrt{m})).$$
where we put \( z_i = Z_i/Z \) with some integer \( Z \) and algebraic integer \( Z_i \) and let \( Z_i^{(j)} \) stand for all the conjugates of \( Z_i \) in \( L \) for \( i = 1, 2 \). This is what we wanted to prove.

5. From Lemma 4, we conclude that if both \( z_1 \) and \( z_2 \) are both multiplicatively independent with respect to \( \alpha \), then both

\[
N_{L/Q}(M, \alpha^n - z_i) = \exp(O(\sqrt{m})) \quad \text{hold for } i = 1, 2.
\]

Since \( \phi(m) \gg m/\log \log m \), we get a contradiction with estimate (6) for large \( m \). Thus, there exists \( i \in \{1, 2\} \) such that \( z_i \) and \( \alpha \) are multiplicatively dependent. Let it be \( z_1 \).

6. We next show that \( z_1 \in \mathbb{K} \). If \( \Delta_1 = 0 \), there is nothing to prove. If not, write \( \Delta_1 = d_1 t_1^2 \), where \( d_1 \) is a squarefree integer and \( t_1 \) is a nonzero rational. Then, since \( z_1 \) and \( x \) are multiplicatively dependent, there exist integers \( x \) and \( y \) not both zero and \( \varepsilon \in \{\pm 1\} \) such that \( z_1^x = \alpha^y \) i.e.

\[
\left( \frac{a + \varepsilon t_1 \sqrt{d_1}}{2} \right)^x = \gamma^x \alpha^y. \tag{8}
\]

By replacing \( x \) with \( -x \) if needed, we may assume that \( x \geq 0 \). By replacing the pair \((x, y)\) by the pair \((2x, 2y)\), we may assume that both \( x \) and \( y \) are even. The left hand side is in \( \mathbb{Q}(\sqrt{d_1}) \), while the right hand side is in \( \mathbb{Q}(\sqrt{d}) \).

If \( d_1 = 1 \) or \( d \), then \( z_1 \in \mathbb{K} \), which is what we wanted. Assume that \( d_1 \neq 1, d \).

Then the two numbers in both sides of (8) are in \( \mathbb{Q}(\sqrt{d}) \cap \mathbb{Q}(\sqrt{d_1}) = \mathbb{Q} \). Since the right hand side is real and positive (since \( \gamma \) and \( \alpha_1 \) are real and \( x \) and \( y \) are even), it follows that there exists a positive rational number \( q \) such that \( \gamma^x \alpha_1^{ky} = q \). Thus, \( \gamma^x = q \alpha_1^{-ky} \). Conjugating we get \( \delta^x = q \beta_1^{-ky} \). Multiplying the above relations and using the fact that \( (\alpha_1 \beta_1)^{-ky} = 1 \) (because \( y \) is even), we get \( (\gamma \delta)^x = q^2 \). Now \( \gamma \delta = q_1 \) is a rational number. Thus, \( q_1^x = q^2 \), and since \( q \) is positive, we get that \( q = |q_1|^{x/2} \). Hence,

\[
\left( \frac{a + \varepsilon t_1 \sqrt{d_1}}{2} \right)^x = q = |q_1|^{x/2},
\]

leading to

\[
\left( \frac{a + \varepsilon t_1 \sqrt{d_1}}{2} \right)^2 = \pm q_1.
\]
We are thus lead to
\[(a^2 + d_1 t_1^2) + 2\varepsilon a t_1 \sqrt{d_1} = \pm 4q_1,\]
which is false for \(a t_1 \neq 0 \) and \(d_1 \neq 1 \) and squarefree. Thus, indeed \(z_1 \in \mathbb{K}\). Since \(z_1 \in \mathbb{K}\) and is multiplicatively dependent with respect to \(\alpha\), it follows that it is an algebraic integer since from what we have seen above it is a solution \(X = z_1\) of an equation of the form \(X^x - \alpha^{ky}_1\) with some integers \(x > 0\) and even and \(y\), and \(\alpha^{ky}_1\) is an algebraic integer. Thus, \(z_1 \in \mathcal{O}_\mathbb{K}\) and some power of it is a unit, therefore itself is a unit. Thus, \(z_1 = \pm \alpha^{s}_1\) for some integer \(s\).

7. It remains to prove that \(s\) is a multiple of \(k\) and that the sign is +1. (Compare this with the case \(a = 0\) where the sign was \(-1\).) Indeed, to see that we have finished in this way, observe that if this is the case, then writing \(s = ks_1\) for some integer \(s_1\), the relation
\[\frac{a + \varepsilon t_1 \sqrt{d_1}}{2} = \gamma \alpha^{ks_1}_1 = \gamma \alpha^{s_1}_1\] (9)
holds. Conjugating this relation in \(\mathbb{K}\), we also get
\[\frac{a - \varepsilon t_1 \sqrt{d_1}}{2} = \delta \beta^{s_1},\] (10)
and summing up relations (9) and (10) we arrive at
\[a = \gamma \alpha^{s_1}_1 + \delta \beta^{s_1} = u_{s_1} \in \{u_n : n \in \mathbb{Z}\},\]
which is what we wanted.

8. So, let us assume first that \(z_1 = \pm \alpha^{s}_1\), where \(s\) is not a multiple of \(k\). Then
\[\alpha^n - z_1 = \alpha^s (\alpha^{kn-s}_1 \pm 1) (\alpha^{2kn-2k}_1 - 1).\]

We now take \(M = W_m\) and observe that \(W_m \mid (\alpha^m - \beta^m) \mid \alpha^{2km}_1 - 1\). Thus,
\[
\gcd(M, \alpha^n - z_1) = \gcd(\alpha^{2km}_1 - 1, \alpha^{2kn-2k}_1 - 1) = \gcd(V_{2km}, V_{2kn-2k}) = V_{\gcd(2km, 2kn-2k)}.
\]
Since \( k \) does not divide \( s \), it follows that \( \gcd(2km, 2kn-2s) \) is a proper divisor of \( 2km \). Thus, there exists a prime \( q \) dividing \( km \) such that \( \gcd(2km, 2kn-2s) \mid 2km/q \), and so
\[
\gcd(M, \alpha^n - z_1) \mid V_{2km/q} = \alpha_1^{2km/q} - 1 = \alpha_1^{km/q}(\alpha - \beta)U_{m/q}.
\]
Here, we used the fact that \( m \) is a multiple of 4 (so, \( km/q \) is even for all prime factors \( q \) of \( km \)), as well as the fact that \( m \) is divisible by \( k \). However, since \( M = W_m \) consists of the primitive prime factors of \( U_m \), it follows that \( M \) is coprime to \( U_{m/q} \). We thus get that
\[
\gcd(M, \alpha^n - z_1) = O(1),
\]
contradicting (6) with \( i = 1 \) for large \( m \). Thus, \( s = k s_1 \) holds with integer \( s_1 \).

9. Now assume that the sign is \(-1\), i.e. \( z_1 = -\alpha_1^{k s_1} = -\alpha^{s_1} \). Here we take \( M = W_mW_{m/2}W_{m/4} \) and we look at the solutions \( n \) of the congruence
\[
un - a \equiv 0 \pmod{M}.
\]
The left hand side is
\[
\gamma \beta^n(a^n - z_1)(a^n - z_2).
\]
We have
\[
\alpha^n - z_1 = \alpha_1^{kn} + \alpha_1^{k s_1} = \alpha_1^{k s_1}(\alpha^{n-s_1} + 1).
\]
Now \( M \) divides \( \alpha^n - \beta^n = \beta^n(\alpha^{2m} - 1) \). Writing \( v_2(u) \) for the exact power of 2 appearing in a positive integer \( u \) we have the following result which is implicit in [5, 6] for integers \( a \) and which is easily extended to algebraic integers:

**Lemma 5.** If \( u, v, a \geq 1 \) and \( v_2(v) \leq v_2(u) \) then \( \gcd(a^u + 1, a^v - 1) \mid 2 \), otherwise \( \gcd(a^u + 1, a^v - 1) = a^{v_2(u)+1} + 1 \).

**Proof.** If \( v_2(v) \leq v_2(u) \), set \( g = \gcd(a^u + 1, a^v - 1) \) and \( k = \gcd(2u, v) \). Then
\[
g \mid \gcd(a^{2u} - 1, a^v - 1) = a^{v_2(2u)} - 1 = a^k - 1,
\]
so \( g \mid a^k - 1 \). But if we write \( u = 2^{v_2(u)}u_1 \) and \( v = 2^{v_2(v)}v_1 \) then
\[
\frac{k}{2^{v_2(v)}} = \gcd(u_1 \cdot 2^{1+v_2(u)-v_2(v)}, v_1)
\]
13
which is an odd integer. Hence \( k \mid 2^{v_2(u_1)}u_1 \mid u \). Therefore \(-1 \equiv a^n \equiv a^{k^2} \equiv 1 \mod g\) so \( g \mid 2 \). If \( v_2(v) > v_2(u) \), first set \( b = a^{2^v(v)} \) so
\[
gcd(a^n + 1, a^n - 1) = \gcd(b^{u_1} + 1, b^{2^{v_2(u_1)-v_2(u)}} - 1)
\]
where \( r = u_1 \) is odd and \( s = 2^{v_2(v)-v_2(u)}v_1 \) is even. Then \( b^{\gcd(r, s)} + 1 \mid \gcd(b^{u_1} + 1, b^r - 1) \). There exist \( y, z \) with \( yr + zs = \gcd(r, s) \) and \( y \) must be odd. If \( x \mid \gcd(b^{u_1} + 1, b^r - 1) \) then \( b^r \equiv -1 \mod x \) and \( b^s \equiv 1 \mod x \) implies \( b^{\gcd(r, s)} \equiv b \equiv (-1)^y \equiv -1 \mod x \) so \( x \mid b^{\gcd(r, s)} + 1 \). Hence \( \gcd(b^{u_1} + 1, b^r - 1) = b^{\gcd(r, s)} + 1 \) and the lemma is proved.

It follows that
\[
gcd(a^{n-1} + 1, a^{2m} - 1) = a^{\gcd(n-s, 2m)} + 1
\]
provided that \( 2^u \) divides \( m \). Otherwise, the greatest common divisor appearing on the left hand side above is \( O(1) \). By estimate (6), it follows that we may assume that \( 2^u \) divides \( m \). Now
\[
(a - \beta)U_m = \beta^m(\alpha^{2m} - 1) = \beta^m(\alpha^m + 1)(\alpha^m - 1),
\]
and \( \gcd(\alpha^n - z_1, \alpha^{2m} - 1) \) divides one of the two factors \( \alpha^m + 1 \) or \( \alpha^m - 1 \), and has a bounded greatest common divisor with the other factor. In particular, \( \alpha^n - z_1 \) is coprime to either \( W_m \), which divides \( \alpha^m + 1 = \beta^{m^2}U_m/U_m^{m/2} \), or to \( W_m/W_m^{m/4} \), which divides \( \alpha^m - 1 = \beta^{m/2}U_m^{m/2} \). Since at any rate we have that \( u_n \equiv 0 \pmod{M} \), we must deduce that with either \( N = W_m \), or \( N = W_m/W_m^{m/4} \), the estimate
\[
N \ll N^{1/3} (\gcd(N, \alpha^n - z_2))
\]
holds. Since also \( N \geq \exp(c_1\phi(m/2)) \), Lemma 4 shows that \( z_2 \) and \( \alpha \) must also be multiplicatively dependent. In particular, \( z_2 = \pm \alpha^{s'} \) for some integer \( s' \).

Thus,
\[
\alpha^n - z_2 = \alpha_1^{s'}(\alpha_{1}^{k^n-s'} + 1) \mid (\alpha_1^{2kn}-s' - 1).
\]
Again we show that \( s' \) is a multiple of \( k \). Assume that it is not. Then \( N \mid \alpha_1^{2kn} - 1 \). Thus,
\[
\gcd(N, \alpha^n - z_2) \mid \gcd(V_{2kn}, V_{2kn-s'}) \mid V_{\gcd(2kn, 2kn-s')} \mid V_{kn/8}.
\]
14
Indeed, the last relation above follows from the fact that $2k$ cannot divide the greatest common divisor of $2km$ and $2kn - 2s'$, together with the fact that $m$ is a multiple of $8$. However, since $N \mid W_m W_{m/2} W_{m/4}$, we get that $N$ is coprime to $V_{km/n}$, so $N_{L/Q} (\gcd(N, \alpha^n - z_2)) = O(1)$, which is false. Thus, $s' = ks'$.  

10. If the sign is $+1$ we are through. So, assume again that the sign is $-1$, i.e. $z_2 = -\alpha^{s'}$. Then

$$u_n - a = \gamma \beta^n \alpha_1^{s' + s'} (\alpha^{n-s} + 1)(\alpha^{n-s} + 1).$$

Putting now $u_1$ for the exact power of 2 in the factorization of $n - s_1'$; i.e., such that $2^{u_1} \mid n - s_1'$, we see that the only situation in which the gcd($\alpha^{n-s} + 1, \alpha^{2n} - 1$) is not $O(1)$ is when $2^{u_1} \mid m$. In this case, the given greatest common divisor is $\alpha^{\gcd(n-s_1', 2m)} + 1$ and, as in a previous argument, this number can be divisible by only one of $W_m, W_{m/2}$ or $W_{m/4}$ and must be coprime to the other two. To summarize, in this last case,

$$\gcd(u_n - a, W_m W_{m/2} W_{m/4}) \ll W_m W_{m/2}.$$

Since the number on the left should in fact be $\gg W_m W_{m/2} W_{m/4}$, we get a contradiction for large $m$. The theorem is therefore proved.

**Acknowledgements**

Research of F. L. was supported in part by Grant SEP-CONACyT 79685 and PAPIIT 100508.

**References**


