Intervals without primes near elements
of linear recurrence sequences

Artūras Dubickas
Department of Mathematics and Informatics
Vilnius University, Naugarduko 24
Vilnius LT-03225, Lithuania
arturas.dubickas@mif.vu.lt

Received 9 January 2017
Accepted 18 May 2017
Published 25 August 2017

Let \((f_n)_{n=1}^\infty\) be an unbounded sequence of integers satisfying a linear recurrence relation with integer coefficients. We show that for any \(k \in \mathbb{N}\) there exist infinitely many \(n \in \mathbb{N}\) for which 2\(^k + 1\) consecutive integers \(f_n - k, \ldots, f_n, \ldots, f_n + k\) are all divisible by certain primes. Moreover, if the sequence of integers \((f_n)_{n=1}^\infty\) satisfying a linear recurrence relation is unbounded and non-degenerate then for some constant \(c > 0\) the intervals \((|f_n| - c \log n, |f_n| + c \log n)\) do not contain prime numbers for infinitely many \(n \in \mathbb{N}\).

Applying this argument to sequences of integer parts of powers of Pisot and Salem numbers \(\alpha\) we derive a similar result for those sequences as well which implies, for instance, that the shifted integer parts \(\lfloor \alpha^n \rfloor + \ell\), where \(\ell = -k, \ldots, k\) and \(n\) runs through some infinite arithmetic progression of positive integers, are all composite.

**Keywords**: Linear recurrence sequence; composite integer; integer part; Pisot and Salem numbers.

**Mathematics Subject Classification 2010**: 11B37, 11B50, 11B83, 11R06

1. Introduction

A classical problem in number theory is to determine whether a given sequence of positive integers contains infinitely many prime numbers or not. This question is wide open for sequences like \(n^2 + 1, n \in \mathbb{N}\), and \(2^n + 1, n \in \mathbb{N} \cup \{0\}\). For the latter sequence (called the sequence of Fermat numbers) it is not even known whether it contains infinitely many composite numbers or not. In 1947, Mills [21] proved that there exists a constant \(\zeta > 1\) such that all the integer parts \(\lfloor \zeta^{3^n} \rfloor\), where \(n \in \mathbb{N}\), are prime numbers. Mills’ result was then generalized in [1, 20]. The results of the latter paper imply that there exist continuum numbers \(\zeta > 2\) for which the integer parts \(\lfloor \zeta^{2^n} \rfloor, n \in \mathbb{N}\), are all prime.
In [15] (see the problem E19 on p. 220), the problem on whether the sequence \([\alpha^n], n \in \mathbb{N}\), where \(\alpha > 1\) is a real number which is not in \(\mathbb{N}\), contains infinitely prime numbers (or infinitely many composite numbers) is raised. More generally, one may ask the same questions for the sequence \([\xi \alpha^n], n \in \mathbb{N}\), where \(\xi > 0\) and \(\alpha > 1\). We remark that, with \(\xi\) introduced, already for \(\alpha \in \mathbb{N}\) these questions become very difficult.

The part of the question concerning prime numbers is completely out of reach. It may seem a bit surprising, but almost nothing is known about the part of the question concerning infinitely many composite numbers in a sequence as well. For instance, one version of the questions considered by van der Poorten [24] (see also [2]) is whether there is an infinite chain of prime numbers when one starts with a prime number written in base \(b\) and then adds infinitely many digits to the right. The question is whether each of the obtained numbers can be a prime number. This is equivalent to the existence of \(\xi > 0\) for which the integer parts \(\lfloor \xi b^n \rfloor\) are prime for all \(n \in \mathbb{N}\). This question is still open. The results established by Forman, Shapiro and Sparer in [13, 23] and subsequently by the author and Novikas in [9] deal with some special rational numbers \(\alpha\). In [9], it was proved, for instance, that the sequence \(\lfloor \xi \alpha^n \rfloor, n \in \mathbb{N}\), contains infinitely many composite numbers for any \(\xi > 0\) when \(\alpha \in \{2, 3, 4, 5, 6, 7, 3/2, 4/3, 5/4\}\). Note that this implies that in the above mentioned problem of van der Poorten the base \(b\) of a potential infinite chain of primes should be at least 8.

For \(\xi = 1\) some algebraic irrational values (for instance, all Pisot and Salem numbers \(\alpha\)) can be added to this list; see the papers of Cass [4], the author [5, 7, 8] and Zaimi [26]; see also [18] for some other arithmetical problems concerning the sequence \([\alpha^n], n \in \mathbb{N}\), with algebraic \(\alpha > 1\). Recall that an algebraic integer \(\alpha > 1\) is a Pisot (respectively, Salem) number if its conjugates over \(\mathbb{Q}\) (if any) all lie in the open unit disc \(|z| < 1\) (respectively, in the closed unit disc \(|z| \leq 1\) with at least two conjugates lying on the circle \(|z| = 1\)).

In this paper, let \((f_n)_{n=1}^{\infty}\) be a sequence of integers satisfying the linear recurrence relation

\[
    f_n = a_d f_{n-1} \cdots + a_0 f_{n-d} \tag{1.1}
\]

for each \(n = d+1, d+2, d+3, \ldots\), where \(d \in \mathbb{N}, a_i \in \mathbb{Z}\) for \(i = 0, \ldots, d-1, a_0 \neq 0\). To avoid bounded sequences we assume that

\[
    \limsup_{n \to \infty} |f_n| = \infty. \tag{1.2}
\]

Recall that the sequence \((f_n)_{n=1}^{\infty}\) defined in (1.1) is called non-degenerate if no quotient of two distinct roots of its characteristic polynomial

\[
    P_f(x) := x^d - a_d - 1 x^{d-1} - \cdots - a_0 \in \mathbb{Z}[x] \tag{1.3}
\]

(which may have multiple roots) is a root of unity.
We first prove the following general theorem.

**Theorem 1.1.** Let \((f_n)_{n=1}^\infty\) be a sequence satisfying (1.1) and (1.2).

(i) Then, given a positive integer \(k\) there exist a collection of (not necessarily distinct) prime numbers \(p_\ell\), where \(\ell = -k, \ldots, k\), and two positive integers \(m, q\) such that for each \(\ell \in \{-k, \ldots, k\}\) and each integer \(r \geq 0\), the number \(f_{m+q} + \ell\) is divisible by \(p_\ell\).

(ii) If, in addition, \((f_n)_{n=1}^\infty\) is non-degenerate then there is a constant \(c > 0\) depending on \(d, a_{d-1}, \ldots, a_0\) only such that the intervals

\[
(|f_n| - c \log n, |f_n| + c \log n)
\]

do not contain prime numbers for infinitely many \(n \in \mathbb{N}\).

In particular, when \((f_n)_{n=1}^\infty\) is an increasing sequence of positive integers satisfying (1.1), Theorem 1.1 implies that the \(2k + 1\) consecutive numbers \(f_n - k, \ldots, f_n, \ldots, f_n + k\) are all composite for infinitely many \(n \in \mathbb{N}\). Therefore,

\[
\limsup_{n \to \infty} \min_{p \in P} |f_n - p| = \infty,
\]

where \(P := \{2, 3, 5, \ldots\}\) is the set of all prime numbers. Moreover, by part (ii) of Theorem 1.1 if the sequence of positive integers \((f_n)_{n=1}^\infty\) satisfies (1.1), (1.2) and is non-degenerate then the inequality

\[
\min_{p \in P} |f_n - p| \geq c \log n
\]

holds for infinitely many \(n \in \mathbb{N}\).

It would be of interest to show that

\[
\liminf_{n \to \infty} \min_{p \in P} |f_n - p| < \infty,
\]

but already for the sequence of powers of 2 the corresponding inequality

\[
\liminf_{n \to \infty} \min_{p \in P} |2^n - p| < \infty
\]

seems to be out of reach. Note that the latter inequality is equivalent to the existence of \(k \in \mathbb{N}\) such that the interval \([2^n - k, 2^n + k]\) contains a prime number for infinitely many \(n \in \mathbb{N}\). Of course, this statement would follow from the infinitude of Mersenne primes or Fermat primes.

It seems likely that the length \(2c \log n\) of the interval \((|f_n| - c \log n, |f_n| + c \log n)\) that appears in Theorem 1.1(ii) cannot be increased by a lot. For instance, for the sequence of \(d\)th powers \(f_n = n^d\), where \(d \in \mathbb{N}\), satisfying the linear recurrence with characteristic polynomial \((x - 1)^{d+1}\) the best known function in
Theorem 1.1(ii) is
\[ c \log n (\log \log n)(\log \log \log \log n) \]
\[ (\log \log \log n)^2 \]
This was recently proved in [19]; see also [12].

From Theorem 1.1 we will derive the following.

**Theorem 1.2.** Let \( \alpha \neq 0 \) be an algebraic integer of degree \( d \) with conjugates \( \alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d \) over \( \mathbb{Q} \) which is not a root of unity. Set
\[ S_n := \alpha^n_1 + \cdots + \alpha^n_d \]
for \( n \in \mathbb{N} \). Then, for any \( k \in \mathbb{N} \) the \( 2k + 1 \) consecutive integers
\[ S_n - k, \ldots, S_n, \ldots, S_n + k \]
are all positive and composite for infinitely many \( n \in \mathbb{N} \).

An important ingredient in the proof of Theorem 1.2 is Lemma 2.6 below, where we show that \( S_n \) can be chosen to be positive when \( n \) runs over some subsequence of an arithmetic progression.

Sometimes, e.g., when \( P_f(x) \) is irreducible and has a unique dominating root, i.e. either \( \rho > 1 \) or \( -\rho \) is the root of \( P_f \) and its other roots are all in the open disc \( |z| < \rho \), the conditions of positivity and non-degeneracy of the sequence \( (S_n)_{n=1}^\infty \) hold automatically. In particular, one has the following corollaries.

**Corollary 1.3.** Let \( \alpha \) be a Salem number. Then, for any \( k \in \mathbb{N} \) there exist \( m, q \in \mathbb{N} \) such that for each \( r \in \mathbb{N} \) the \( 2k + 1 \) consecutive integers
\[ [\alpha^m + qr] - k, \ldots, [\alpha^m + qr], \ldots, [\alpha^m + qr] + k \]
are all composite. Furthermore, there is a constant \( c = c(\alpha) > 0 \) such that the intervals
\[ (\alpha^n - c \log n, \alpha^n + c \log n) \]
do not contain prime numbers for infinitely many \( n \in \mathbb{N} \).

For Pisot numbers this result can be given in a stronger form.

**Corollary 1.4.** Let \( \alpha \) be a Pisot number, and let \( G \in \mathbb{Q}[z] \) be a polynomial with positive leading coefficient satisfying \( G(n) \in \mathbb{Z} \) for each \( n \in \mathbb{N} \). Then, for any \( k \in \mathbb{N} \) there exist \( m, q \in \mathbb{N} \) such that for each \( r \in \mathbb{N} \) the \( 2k + 1 \) consecutive integers
\[ [G(m + qr)\alpha^m + qr] - k, \ldots, [G(m + qr)\alpha^m + qr], \ldots, [G(m + qr)\alpha^m + qr] + k \]
are all composite. Furthermore, there is a constant \( c = c(G, \alpha) > 0 \) such that the intervals
\[ (G(n)\alpha^n - c \log n, G(n)\alpha^n + c \log n) \]
do not contain prime numbers for infinitely many \( n \in \mathbb{N} \).
For a quadratic Pisot number $\alpha$ Cass showed that the integer parts $[\alpha^n]$, $n \in \mathbb{N}$, can only rarely be prime; see [4]. The results in [5, 23] are also weaker than the ones given in the above corollaries (and, moreover, they have been proved for $k = 0$ only). Corollary [4] strengthens the corresponding result of [9] asserting that $|G(n)\alpha^n|$ are composite for infinitely many $n \in \mathbb{N}$.

With arbitrary $\xi > 0$ the results are not so strong as those in Theorem [22] and Corollary [4]. The next theorem implies that for $\alpha = 2$ two consecutive numbers are both composite for infinitely many $n \in \mathbb{N}$.

**Theorem 1.5.** For any $\xi > 0$ there are infinitely many $n \in \mathbb{N}$ for which the numbers $[\xi 2^n]$ and $[\xi 2^n] + 1$ are both composite.

In the next section, we shall give some auxiliary statements. Then, in Sec. 3, we will prove all the results stated above.

## 2. Auxiliary Lemmas

The following lemma is standard.

**Lemma 2.1.** Let $(f_n)_{n=1}^{\infty}$ be a sequence of integers satisfying the linear recurrence relation (1.1) for each $n = d + 1, d + 2, d + 3, \ldots$, where $d \in \mathbb{N}$, $a_i \in \mathbb{Z}$ for $i = 0, \ldots, d - 1$, $a_0 \neq 0$, and let $p$ be a prime number. Then, for each $n_0 \geq |a_0|^d$ the sequence $(f_n)_{n=n_0}^{\infty}$ is purely periodic modulo $p$ with period at most $p^d$.

**Proof.** Consider the vectors $v_n := (f_n, f_{n+1}, \ldots, f_{n+d-1}) \in \mathbb{Z}^d$, where $n \in \mathbb{N}$. Such vectors can take at most $p^d$ distinct values modulo $p$. So, there exist $m, T \in \mathbb{N}$ satisfying $m + T \leq p^d + 1$ and $v_m = v_{m+T}$ modulo $p$. Hence, $f_{m+j} = f_{m+j+T}$ modulo $p$ for $j = 0, 1, \ldots, d - 1$. The relation (1.1) implies that $f_{m+d} = f_{m+d+T}$ modulo $p$, and hence $v_{m+1} = v_{m+1+T}$ modulo $p$. On applying this argument step by step, we deduce that $f_{m+j} = f_{m+j+T}$ modulo $p$ for each integer $j \geq 0$. Hence, the sequence $(f_n)_{n=n_0}^{\infty}$ is purely periodic modulo $p$ with (not necessarily smallest) period $T \leq p^d$.

If $p$ does not divide $a_0$ then, by the same argument as above, one can easily see that $(f_n)_{n=1}^{\infty}$ is purely periodic modulo $p$ (and so is $(f_n)_{n=n_0}^{\infty}$ for any $n_0 \in \mathbb{N}$). In the alternative case, $p|a_0$, in view of

$$n_0 \geq |a_0|^d \geq p^d \geq p^d + 1 - T \geq m$$

the assertion of the lemma also follows.

The next theorem is due to Kronecker (see [15] for the original source or, e.g., [22, Theorem 2.5]).

**Theorem 2.2.** Let $\alpha \neq 0$ be an algebraic integer which is not a root of unity. Then, the maximal modulus of its conjugates over $\mathbb{Q}$ is strictly greater than 1.
Let \( \|x\| \) be the distance from a real number \( x \) to the nearest integer. The statement below is a version of Kronecker’s approximation theorem. See [17] for the original paper and also a recent survey of Gonek and Montgomery [14] which contains a long list of references on this problem.

**Theorem 2.3.** Let \( 1, \omega_1, \ldots, \omega_s \in \mathbb{R} \) be linearly independent over \( \mathbb{Q} \), and let \( b_1, \ldots, b_s \in \mathbb{R} \). Then, for any \( \varepsilon > 0 \) there are infinitely many \( n \in \mathbb{N} \) for which \( \|n\omega_j + b_j\| < \varepsilon \) for each \( j = 1, \ldots, s \).

We will also need the following theorem.

**Theorem 2.4.** If \( F \in \mathbb{Z}[z] \) is an irreducible polynomial which has \( m \geq 2 \) roots on a circle \( |z| = R > 0 \), at least one of which is real, then one has \( F(z) = G(z^m) \), where the polynomial \( G \in \mathbb{Z}[z] \) has at most one real root on any circle in the plane.

Theorem 2.4 was proved by Ferguson in [11], although its partial case (which we actually use below) was earlier obtained by Boyd in [3].

Next, applying Theorem 2.4 we will derive the following.

**Lemma 2.5.** Let \( \alpha \neq 0 \) be an algebraic number of degree \( d \geq 1 \). Then, there are a positive integer \( t \) and a positive integer \( k \leq d \), which is either 1 or even, i.e. \( k = 2l \), \( l \in \mathbb{N} \), such that for each \( v \in \mathbb{N} \) the algebraic number \( \alpha^{tv} \) has exactly 1 conjugate with largest modulus which is positive (when \( k = 1 \)) or exactly \( l \) pairs of complex conjugate numbers conjugate to \( \alpha^{tv} \) over \( \mathbb{Q} \) with largest moduli (when \( k = 2l \)).

**Proof.** Let \( \alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d \) be the conjugates of \( \alpha \) over \( \mathbb{Q} \). Put

\[
\rho := \max_{1 \leq j \leq d} |\alpha_j|. \tag{2.1}
\]

Without restriction of generality we may assume that \( \rho = |\alpha| \). Take the smallest \( t \in \mathbb{N} \) for which \( \alpha^t \) is non-degenerate, i.e. no quotient of two distinct conjugates of \( \alpha^t \) over \( \mathbb{Q} \) is a root of unity. Suppose exactly \( k \) conjugates of \( \alpha^t \) have moduli \( \rho^l \).

Assume first that \( \alpha^t \) is real. Then, \( \alpha^t = \pm \rho^l \). Furthermore, by Theorem 2.4 \( \alpha^t \) must be the only conjugate on the circle \( |z| = \rho^l \), since, by the choice of \( t \), all other conjugates of \( \alpha^t \) (if any) must have moduli strictly smaller than \( \rho^l \). In case \( \alpha^t < 0 \), we can replace \( t \) by \( 2t \), so that one can assume that \( \alpha^t = \rho^l > 0 \) is the only conjugate of \( \alpha^t \) on the circle \( |z| = \rho^l \). However, then for any \( v \in \mathbb{N} \) the only conjugate of \( \alpha^{tv} \) with the largest modulus \( \rho^{vl} \) will be \( \alpha^{tv} = \rho^{vl} \) itself, and hence \( k = 1 \).

Alternatively, suppose that \( \alpha^t \) is nonreal. Then, by Theorem 2.4 again, \( \alpha^t \) has no real conjugates on the circle \( |z| = \rho^l \). Hence, \( \alpha^t \) must have \( k = 2l \), where \( l \in \mathbb{N} \), conjugates on \( |z| = \rho^l \). By the choice of \( t \), for any \( v \in \mathbb{N} \) the number \( \alpha^{tv} \) also has \( 2l \) conjugates on the circle \( |z| = \rho^{vl} \) which are all nonreal. (Otherwise, for some conjugate \( \beta \) of \( \alpha^t \) on \( |z| = \rho^l \) we would obtain \( \beta^v = \beta \), which is impossible, since the quotient \( \beta/\beta \) is not a root of unity.) This completes the proof of the lemma. \( \square \)
Now, we can state the main result of this section.

**Lemma 2.6.** Let \( \alpha \neq 0 \) be an algebraic integer which is not a root of unity with conjugates \( \alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d \) over \( \mathbb{Q} \), and let \( c > 0 \). Then, there exists a positive integer \( m \) such that \( S_m > c \). (Here, \( S_n = \sum_{j=1}^{d} \alpha_j^n \) for \( n \in \mathbb{N} \).) Moreover, for any \( q \in \mathbb{N} \) there are some integers \( r_0 = 0 < r_1 < r_2 < r_3 < \cdots \) such that the sequence \( (S_{m+mr})_{n=0}^{\infty} \) consists of positive integers and is increasing.

Below, in the proof of Lemma 2.6 for a given \( \alpha \) first one chooses the integers \( m \) (which depends only on \( \alpha \) and \( u \neq 1 \) only if \( k \) described in Lemma 2.5 is greater than 1) and a large integer \( d \) (divisible by \( tu \)), then the integer \( q \) which depends on \( m \) and, finally, the sequence of integers \( r_0 = 0 < r_1 < r_2 < r_3 < \cdots \).

**Proof.** Let \( t, k \) be positive integers as described in Lemma 2.5 and let \( \rho = |\alpha| \) be as defined in (2.1). Put \( d_1 \) for the degree of \( \alpha^t \) over \( \mathbb{Q} \) and \( d_2 := d/d_1 \in \mathbb{N} \).

Suppose first that \( k = 1 \). Then, by Lemma 2.5 for any \( v \in \mathbb{N} \) the number \( \alpha^v = \rho^v \) is positive. All its other conjugates (if any, i.e. if \( d_1 > 1 \)) lie in a disc \( |z| \leq \rho_1^v \), where \( 0 < \rho_1 < \rho \) and \( \rho_1 \) depends only on \( \alpha \) by Theorem 2.4. \( \rho > 1 \).

Observe that \( S_v \) equals \( d_2 \) times the sum of \( d_1 \) conjugates of \( \alpha^v \) over \( \mathbb{Q} \) and bounding the moduli of other \( d_1 - 1 \) conjugates of \( \alpha^v \) by \( \rho_1^v \), we get

\[
|S_v - d_2 \rho^v| \leq d_2(d_1 - 1)\rho_1^v. \tag{2.2}
\]

Now, selecting \( v = rN \) with \( N \in \mathbb{N} \) (which is a sufficiently large integer), \( r \in \mathbb{N} \) and \( m = tN \) from (2.2) we derive that \( S_m > c \) and in view of \( d_2(d_1 - 1) \leq d \)

\[
|S_m - d_2 \rho^m| \leq d\rho_1^m. \tag{2.3}
\]

In particular, the inequality (2.3) implies that the sequence \( (S_m)_{n=1}^{\infty} \) is increasing provided that

\[
d_2 \rho^{m} + d\rho_1^m < d_2 \rho^{m(r+1)} - d\rho_1^{m(r+1)}.
\]

Dividing both sides by \( \rho^m \) we obtain

\[
d_2 + d(\rho_1/\rho)^m + d\rho_1^m(\rho_1/\rho)^m < d_2 \rho^m. \tag{2.4}
\]

This is clearly true if \( N \) (and so \( m \)) is large enough, because \( \rho > 1 \) and \( 0 < \rho_1 < \rho \), and so the left-hand side of (2.4) does not exceed \( d_2 + d + d\rho_1^m < 3d\max(1, \rho_1)^m \).

Selecting \( r_j = j \) for \( j \in \mathbb{N} \) we conclude the proof of the lemma in case \( k = 1 \).

From now on we suppose that \( k = 2l \) with \( l \in \mathbb{N} \). Set \( m = tN \), where \( N \in \mathbb{N} \) is a large multiple of \( u \) which will be chosen later (\( u \) will depend of \( \alpha \) only). This time, by Lemma 2.5 with \( v = 1 \), \( \alpha^t \) has \( 2l \) conjugates of the form \( \rho e^{\pm t\gamma_i} \), \( i = 1, \ldots, l \), where \( 0 < \gamma_i < \pi \). Therefore, as above for each \( w \in \mathbb{N} \) we find that

\[
|S_{mw} - d_2 \rho^{mw} (\cos(Nw\gamma_1) + \cdots + \cos(Nw\gamma_l))| \leq d_2(d_1 - 2l)\rho_1^{mw}. \tag{2.5}
\]

Our aim is to choose \( w_j = 1 + qr_j \) with certain \( r_j \in \mathbb{N} \) (and \( r_0 = 0 \)) such that \( \cos(Nw_j\gamma_i) \geq 1/2 \) for \( j \geq 0 \) and \( i = 1, \ldots, l \). Assuming that this inequality holds,
namely, $1/2 \leq \cos(Nw_j \gamma_i) \leq 1$, one can bound the term on the left-hand side of (2.5) as follows:

$$d_2 \rho^m \geq 2d_2 \rho^m \geq d_2 \rho^m (\cos(Nw_j \gamma_1) + \cdots + \cos(Nw_j \gamma_l)) \geq d_2 \rho^m (l/2) \geq \rho^m.$$  

Clearly, $d_2 (d_1 - 2l) \rho^m \leq d_1 \rho^m$. Hence, by (2.5), selecting $u_0 = 1$ we deduce that $S_n \geq \rho^m - d_1 \rho^m > e$. Furthermore, this yields

$$S_n < S_{n+m qr_1} < S_{n+m qr_2} < S_{n+m qr_3} < \cdots$$  

provided that

$$d_1 \rho^m + d_1 \rho^m < \rho^m + m qr_{j1} - d_1 \rho^m.$$  

As above, dividing both sides by $\rho^m$ we find that this is true for each sufficiently large $m$. This proves (2.6) if such integers $r_0 = 0 < r_1 < r_2 < r_3 < \cdots$ exist.

It remains to choose $u$ and to establish the inequality

$$\cos(N(1 + qr_j) \gamma_i) \geq 1/2$$  

for $i = 1, \ldots, l$ and some integers $r_0 = 0 < r_1 < r_2 < \cdots$.

For this, we consider the set $X := \{x_1, \ldots, x_l\}$, where $x_i := \gamma_i/(2\pi)$ for $i = 1, \ldots, l$. All the numbers in this set are irrational, since otherwise some powers of $\alpha_i^r = e^{i \gamma_i}$ and $\alpha_i^s$ are equal, and so their quotient is a root of unity, contrary to the definition of $t$. Take the largest integer $s$ for which the numbers $1$ and some $s$ numbers from the set $X$, say $y_1, \ldots, y_s \in X$, are linearly independent over $\mathbb{Q}$. Then, there exists an integer $u \in \mathbb{N}$ (depending on $\alpha$ only) such that each $ux_i$ ($i = 1, \ldots, \ell$) can be uniquely expressed as $a_i,0 + a_i,1 y_1 + \cdots + a_i,s y_s$ with $a_i,s \in \mathbb{Z}$, where $u \in \mathbb{N}$ and all $a_i,s \in \mathbb{Z}$ depend on $\alpha$ only. (In case $x_i \in Y$ we have $a_i,s = u$ and other $a_i,j = 0$, since $ux_i = u x_i$.) Fix this $u$, and let $A$ be the maximum among the moduli of all integers $a_i,j$.

We first prove (2.7) for $r = r_0 = 0$. Fix a small positive number $\varepsilon$ and take a large $M \in \mathbb{N}$ for which $\|My_i\| < \varepsilon$ for every $i = 1, \ldots, s$. (Such $M$ exists, by Dirichlet’s approximation theorem, and, moreover, by Theorem 2.3.) Then, $\|Mux_i\| < \varepsilon$ for each $x_i \in Y$. For $x_i \in X \setminus Y$, we can write $ux_i = a_i,0 + a_i,1 y_1 + \cdots + a_i,s y_s$, and so

$$\|Mux_i\| \leq \sum_{j=1}^s \|Ma_{i,j} y_j\| \leq \sum_{j=1}^s |a_{i,j}| \varepsilon \leq s A \varepsilon.$$  

Hence, $\|Mux_i - 2\pi \ell_i\| \leq s A \varepsilon$ for $\ell_i \in \mathbb{Z}$, which implies $\cos(Mux_i) \geq 1/2$ for $i = 1, \ldots, l$ and $\varepsilon$ small enough. Therefore, with the choice $N = Mu$, the inequality (2.7) holds for $r_0 = 0$ and $i = 1, \ldots, l$.

Next, with this choice of $N$, namely, $N = Mu$, we will establish (2.7) for some positive integers $r_1 < r_2 < r_3 < \cdots$. As the numbers $1, y_1, \ldots, y_s$ are linearly independent, there exist $a_{i,j} \in \mathbb{Z}$ such that

$$a_{i,0} + a_{i,1} y_1 + \cdots + a_{i,s} y_s = 0.$$  

Then, for $u \geq 1$,

$$\|Mux_i - 2\pi \ell_i\| \leq u \varepsilon \leq 2 \pi \varepsilon,$$  

where $\ell_i \in \mathbb{Z}$.

Using (2.7), we conclude that

$$\cos(Nu x_i) \geq 1/2$$  

for $i = 1, \ldots, l$, $u \in \mathbb{N}$, and $\varepsilon > 0$ small enough.
3. Proofs of the Main Results

independent over \( \mathbb{Q} \), by Theorem 2.3 applied to \( \omega_i := MQy_i \) and \( b_i := M_y_i \), we find that for each \( \varepsilon > 0 \)

\[
\|MQr_jy_i + M_y_i\| < \varepsilon
\tag{2.8}
\]

for \( i = 1, \ldots, s \) and some \( r_1 < r_2 < r_3 < \cdots \in \mathbb{N} \). In particular, when \( x_i = \gamma_i/(2\pi) \in Y \) selecting \( \varepsilon < 1/(6\alpha) \) from (2.8) we find that

\[
|N(1 + qr_j)\gamma_i - 2\pi\ell| = |M\alpha qr_j\gamma_i + M\alpha y_i - 2\pi\ell| < 2\pi\varepsilon < \pi/3
\]

for each \( \ell \in \mathbb{Z} \). This implies (3.1) for every \( i \) satisfying \( x_i \in Y \).

Otherwise, when \( x_i \in X \setminus Y \) using the expression \( u_i = a_i,0 + a_1y_i + \cdots + a_i,sy_i \) and \( N = Mu \) we obtain

\[
N(1 + qr_j)x_i = M\alpha_i,0(qr_j + 1) + M(a_i,1y_jqr_j + a_i,1y_i) + \cdots + (a_i,sy_jqr_j + a_i,sy_i).
\]

Since \( M\alpha_i,0(qr_j + 1) \in \mathbb{Z} \) and, by (2.8), \( \|a_1,1M_y qr_j + a_i,1M_y_i\| \leq |a_i,1|\varepsilon \), etc., this yields

\[
\|N(1 + qr_j)x_i\| \leq (|a,1| + \cdots + |a_i,s|)\varepsilon \leq s\varepsilon.
\]

So, selecting \( \varepsilon < 1/(6s\alpha) \), we derive that \( |N(1 + qr_j)\gamma_i - 2\pi\ell| \leq 2\pi s\varepsilon < \pi/3 \) for any \( \ell \in \mathbb{Z} \). Hence, the inequality (2.7) holds for \( i = 1, \ldots, l \) such that \( x_i \notin Y \) as well. Therefore, (2.7) is true for each \( i = 1, \ldots, l \) and infinitely many integers \( r_0 = 0 < r_1 < r_2 < r_3 < \cdots \).

3. Proofs of the Main Results

Proof of Theorem 1.1

Fix \( k \in \mathbb{N} \) and take \( m \) so large that \( m \geq |a,0|^d \) and \( |f_m| \geq k + 2 \). Then, \( |f_m + \ell| \geq 2 \) for each \( \ell \in \{-k, \ldots, 0, \ldots, k\} \). Let \( p_{\ell} \) be the smallest prime divisor of \( f_m + \ell \). By Lemma 2.4 and the choice of \( m \), the sequence \( (f_{n})_{n=m}^{\infty} \) is purely periodic modulo \( p_{\ell} \). Let \( t_\ell \) be the length of the smallest period of \( (f_{n})_{n=m}^{\infty} \) modulo \( p_{\ell} \).

Consider the arithmetic progression \( A := \{m + qr\}, r = 0, 1, 2, \ldots \), where

\[
q := \prod_{\ell} t_\ell
\tag{3.1}
\]

and the product in (3.1) is taken over \( \ell \in \{-k, \ldots, 0, \ldots, k\} \) with distinct \( p_{\ell} \). We claim that for each \( n \in A \) the number \( f_n + \ell \) modulo \( p_{\ell} \) is 0. Indeed, in view of \( t_\ell|(n - m) \) we find that \( f_n = f_m \) modulo \( p_{\ell} \). Also, \( p_{\ell}|(f_m + \ell) \), by the choice of \( p_{\ell} \). Hence, for each \( \ell \in \{-k, \ldots, 0, \ldots, k\} \) and each \( n \in A \) the number \( f_n + \ell \) is divisible by \( p_{\ell} \), as claimed. This completes the proof of part (i).

To prove part (ii) we will show that for each sufficiently large \( m \) there is a positive integer

\[
n \leq \varepsilon c_1 k,
\tag{3.2}
\]

where \( k := |f_m| - 2 \) and \( c_1 \) depends only on \( d \) and the characteristic polynomial \( [1,3] \), such that the numbers

\[
|f_n| - k, \ldots, |f_n|, \ldots, |f_n| + k
\tag{3.3}
\]
are all positive and composite. Then, the distance from \(|f_n|\) to the nearest prime is at least \(k + 1 > c \log n\), where \(c = 1/c_1\), which implies the assertion of the theorem. Throughout, the constants \(c_2, c_3, \ldots\) depend only on \(d\) and the polynomial (1.3).

Take \(m \geq |a_0|^d\). Then, by part (i) of Theorem 1.1 (see also its proof above, where \(p_\ell\) is defined to be the smallest prime divisor of \(f_m + \ell\) for each \(\ell = -k, \ldots, 0, \ldots, k\)) the number \(f_n + \ell\) is divisible by \(p_\ell\) for \(n = m + qr\), where \(q\) is given in (3.1) and \(r\) is an arbitrary positive integer.

By Lemma 2.1, each \(t_\ell\) is bounded above by \(p_\ell^d\). The largest prime among \(p_\ell\), \(\ell = -k, \ldots, k\), does not exceed \(2^k + 2\) (and hence \(2^k + 1\), since \(2^k + 2\) is not a prime).

Thus, by (3.1) and the prime number theorem, we derive that
\[
q \leq \prod_{p \leq 2^k + 1} p^d e^{\theta(2k + 1)} \leq e^{3kd},
\]
where \(\theta(x) := \sum_{p \leq x} \log p\). Selecting \(r = \lfloor e^{3kd}/q \rfloor \in \mathbb{N}\), we further find that
\[
e^{3kd}/2 < qr < e^{3kd}.
\] (3.4)

Now, let us take \(n = m + qr\). Then, each of the numbers
\[
f_n - k, \ldots, f_n, \ldots, f_n + k
\] (3.5) is divisible by one of the primes \(p_\ell\), where \(p_\ell \leq 2^k + 1\). Consequently, the numbers (3.3) are all composite provided that
\[
|f_n| > 3k + 1.
\] (3.6)
(Indeed, in case \(f_n < 0\) the list (3.3) is the same list of numbers (3.5) with opposite signs.)

Below, we shall use the fact that for any linear non-degenerate sequence \((f_n)_{n=1}^\infty\) and any \(\delta > 0\) there is a constant \(n_0\) such that
\[
|f_N| \geq \rho^{(1-\delta)N}
\] (3.7) for \(N > n_0\) (see [10, Theorem 2.3]). Here, \(\rho\) is the largest modulus of the roots of the characteristic polynomial \(P_f(x)\) defined in (1.3).

We now consider two cases: \(\rho > 1\) and \(\rho = 1\). In the first case, by (3.7), \(|f_N| \geq \rho^{N/2}\) for each sufficiently large \(N\). Hence, using the fact that \(\rho - 1\) is bounded below in terms of \(d\) only (see, e.g., [25]),
\[
N \leq \frac{2 \log |f_N|}{\log \rho} \leq c_2 \log |f_N|.
\] (3.8)

In the second case, when \(\rho = 1\), by Theorem 2.2 and by the conditions of part (ii) on the sequence \((f_n)_{n=1}^\infty\), the polynomial (1.3) must be of the form \((x + 1)^d\) or \((x - 1)^d\), where \(d \geq 2\). Thus, \(f_N\) must be equal to \(G(N)\), where \(G \in \mathbb{Q}[x]\) is a polynomial of degree at least \(\ell := d - 1 \geq 1\) satisfying \(G(N) \in \mathbb{Z}\) for each \(N \in \mathbb{N}\). If \(\ell \in \mathbb{N}\) is the degree of \(G\) and \(a \neq 0\) is its coefficient for \(x^\ell\) we clearly find that
\[
|f_N| = |G(N)| \geq \frac{|a|N^\ell}{2} \geq \frac{|a|N}{2}.
\]
and so

$$N \leq c_3 |f_N|.$$  \hfill (3.9)

Now, applying (3.8) and (3.9) to $N = m$, we find that $m \leq c_4 |f_m| = c_4 (k + 2)$. Combining this with the upper bound in (3.4) we deduce

$$n = m + qr \leq c_4 (k + 2) + e^{kd} < e^{kd}$$

for $k$ large enough. This proves the inequality (3.2).

Similarly, applying (3.8) and (3.9) to $N = n + m$, in view of the lower bound in (3.4) we deduce

$$|f_n| \geq c_5 n > c_5 q m > c_6 e^{kd}.$$  \hfill (3.6)

This clearly implies the bound (3.6) for $k$ large enough and so completes the proof of part (ii) of the corollary.

---

**Proof of Theorem 1.1.** By Lemma 2.6 (with $c = k + 2$), we can take $m$ such that $S_m > k + 2$. With this $m$, let us take $q$ as in Theorem 1.1(i). Then, by Theorem 1.1(i), for each $\ell \in \{−k, \ldots, 0, \ldots, k\}$ and each integer $r \geq 0$, the integer $S_{m+qr} + \ell$ is divisible by $p_\ell$. By Lemma 2.6 there are positive integers $r_1 < r_2 < r_3 < \cdots$ such that the sequence of $(S_{m+qr_i})_{i=0}^\infty$, where $r_0 = 0$, consists of positive integers and is increasing. Hence, starting with some $i \in \mathbb{N}$ such that $S_{m+qr_i} > k + \max_{-k \leq \ell \leq k} p_\ell$, the shifts of all its elements $S_{m+qr_i} + \ell$, where $\ell \in \{-k, \ldots, k\}$ and $j = i, i + 1, i + 2, \ldots$, are all positive composite integers.

---

**Proof of Corollary 1.3.** For a Salem number $\alpha$ we have $|S_n − |\alpha^n|| \leq d$. So, for a given $d = \deg \alpha$ applying the argument of the proof of Theorem 1.2 to the sequence $S_{m+qr}, r \in \mathbb{N}$, and $k + d$ (instead of $k$) we find that $|\alpha^{m+q} − k| \geq S_{m+qr} - k - d$ and $|\alpha^{m+q} + k| \leq S_{m+qr} + k + d$. This implies the first part of the corollary. The second part follows immediately from Theorem 1.2(ii).

---

**Proof of Corollary 1.4.** Let $\alpha$ be a Pisot number of degree $d \geq 1$ with conjugates $\alpha_1 = \alpha, \alpha_2, \ldots, \alpha_d$, and let $G$ be a polynomial of degree $g$. Then, the integer sequence $f_n := \sum_{j=1}^d G(n)\alpha_j^n$ satisfies the linear recurrence (1.1) with characteristic polynomial

$$(z - \alpha_1)^{g+1} \cdots (z - \alpha_d)^{g+1}.$$  \hfill (3.1)

Since $\alpha$ is a Pisot number, for a large enough we obtain $|\sum_{j=2}^d G(n)\alpha_j^n| < 1$. Hence, $f_n = [G(n)\alpha^n]$ for $f_n = [G(n)\alpha^n] + 1$ and also $f_n \rightarrow \infty$ as $n \rightarrow \infty$. Now, it is clear that for a large enough $f_n < f_{n+1} < f_{n+2} < \cdots$. So, selecting $m$ and $q$ as in part (i) of Theorem 1.1 we get the first assertion by taking a subsequence of $[G(n)\alpha^n], n \in \mathbb{N}$, with indices $n = m + qMr$, where $m$ is large enough, $r$ runs through all positive integers and $M \in \mathbb{N}$ is so large that $[G(m + qM)\alpha^{m+qM}] - [G(m)\alpha^m] > 3k$. The second assertion of the corollary follows from Theorem 1.1(ii).
Proof of Theorem 1.5. Set \( x_n := \lfloor 2^n \rfloor \). Then, \( x_{n+1} - 2x_n = 0 \) or 1. Among two consecutive integers \( x_{n+1} \) and \( x_{n+1} + 1 \) one is even and so composite if \( n \) is large enough. The other one is odd. In both cases, \( x_{n+1} = 2x_n \) and \( x_{n+1} + 1 = 2x_n + 1 \), the odd one is \( 2x_n + 1 \). So, it remains to show that \( u_n := 2x_n + 1 \) is composite for infinitely many \( n \in \mathbb{N} \).

Note that

\[
\begin{align*}
u_{n+1} &= 2x_{n+1} + 1 = 2(2x_n + 1) \pm 1 = 2u_n \pm 1.
\end{align*}
\]

Set \( \delta_n := u_{n+1} - 2u_n \in \{-1, 1\} \). Take \( n \) so large that \( u_n > 3 \) is odd and assume that \( u_n, u_{n+1}, \ldots \) are all prime. Then, \( u_n \) modulo 3 is either 1 or \(-1\).

Suppose \( u_n \) modulo 3 is 1. Then, \( \delta_n \) must be \(-1\), since otherwise \( 3 \mid u_{n+1} \). Hence, \( u_{n+1} = 2u_n + 1 \) modulo 3 is also 1. By the same argument applied to \( n + 1, n + 2, \ldots \), we find that \( \delta_n = \delta_{n+1} = \cdots = -1 \) and \( u_{n+k} = 2u_{n+k-1} - 1 \) for every \( k \in \mathbb{N} \).

By induction on \( k \), it follows that

\[
\begin{align*}
u_{n+k} &= 2^ku_n - 2^k + 1
\end{align*}
\]

for each \( k \in \mathbb{N} \). Since \( u_n \) is odd, there is a positive integer \( k \) for which \( u_n \mid (2^k - 1) \) (for instance, \( k = \varphi(u_n) \)). Thus, \( u_n \mid u_{n+k} \) and \( u_n < u_{n+k} \), so the number \( u_{n+k} \) is composite, contrary to our assumption.

Similarly, if \( u_n \) modulo 3 is 2, we find that \( \delta_n = \delta_{n+1} = \cdots = 1 \) and \( u_{n+k} = 2u_{n+k-1} + 1 \) for every \( k \in \mathbb{N} \). Clearly, this yields

\[
\begin{align*}
u_{n+k} &= 2^ku_n + 2^k - 1
\end{align*}
\]

for each \( k \in \mathbb{N} \). As above, using the fact that \( u_n > 3 \) is odd and taking \( k \in \mathbb{N} \) for which \( u_n \mid (2^k - 1) \) we conclude that \( u_n \mid u_{n+k} \), and hence \( u_{n+k} \) must be composite. This completes the proof of the theorem. \( \square \)

References