The almost PV behavior of some far from PV algebraic integers

A.S. Fraenkel, H. Porta, K.B. Stolarsky

Department of Mathematics, University of Illinois, Urbana IL 61801, USA

Received 12 December 1990

Abstract

This paper studies divisibility properties of sequences defined inductively by

\[ a_1 = 1, \]
\[ a_{n+1} = sa_n + t \lfloor \theta a_n \rfloor, \]

where \( s, t \) are integers, and \( \theta \) is a quadratic irrationality. Under appropriate hypotheses (especially that \( s + t \theta \) be a PV-number) it is proved that the highest power of \( A \) that divides \( a_n \), where \( A \) is the discriminant of \( \theta \), tends to infinity. This is noteworthy in that truncation would normally be expected to destroy any simple algebraic structure. Moreover, we establish related results that imply the \( a_n \) are not uniformly distributed modulo \( A \) in cases where the smaller conjugate of \( s + t \theta \) exceeds 1 in modulus (the non-PV case).

1. Introduction

If \( \alpha > 1 \) is an irrational algebraic integer, it is hard to say much about the distribution of the powers \( \alpha^n \) (e.g. modulo 1) unless all conjugates of \( \alpha \) lie strictly inside the unit circle (i.e. \( \alpha \) is a PV-number) or at least lie inside or on the unit circle (if at least one has modulus one then \( \alpha \) is a Salem number). Here we investigate certain divisibility properties of some integer sequences associated with the powers of \( \alpha \). We obtain a strong result when \( \alpha > 1 \) belongs to certain infinite classes of quadratic PV numbers. However, the property under consideration still persists, in a weaker form, for certain infinite classes of such \( \alpha > 1 \) whose smaller conjugate is considerably larger than 1.

Let \( \theta = 1.618... \) denote the golden mean and \( \lfloor x \rfloor \) the greatest integer in \( x \). In [1] we announced the following proposition.

* Corresponding author.

0012-365X/94/$07.00 © 1994—Elsevier Science B.V. All rights reserved
SSDI 0012-365X(93)E0097-N
Proposition. The highest power of 5 dividing $a_n$, where $a_1 = 1$ and $a_{n+1} = 7a_n + 11\lfloor \theta a_n \rfloor$, tends to infinity with $n$.

This seems a bit surprising, since unrestricted truncation is usually expected to destroy any reasonable algebraic structure, starting with the associative law itself. However, it was shown in [1] that the binary operation

$$m \ast n := mn + \lfloor \theta n \rfloor \lfloor \theta m \rfloor$$

is in fact associative, and that there is an infinite sequence of such associative operations connected to the Lucas sequence $1, 3, 4, 7, 11, \ldots$.

$$m \ast n := 2mn + m\lfloor \theta n \rfloor + n\lfloor \theta m \rfloor + 3\lfloor \theta m \rfloor \lfloor \theta n \rfloor,$$

$$m \ast n := 3mn + 4m\lfloor \theta n \rfloor + 4n\lfloor \theta m \rfloor + 7\lfloor \theta m \rfloor \lfloor \theta n \rfloor,$$

$$m \ast n := 7mn + 11m\lfloor \theta n \rfloor + 11n\lfloor \theta m \rfloor + 18\lfloor \theta m \rfloor \lfloor \theta n \rfloor,$$

etc. For a general study of the algebraic intricacies of such multiplications (see [1, 2, 4]). In the particular case of the above Lucas multiplications, the triple product can be shown to have the form

$$l \ast m \ast n = P_k lm + Q_k (lm \lfloor \theta n \rfloor + \cdots) + R_k (l\lfloor \theta n \rfloor + \cdots) + S_k (\lfloor \theta l \rfloor \lfloor \theta n \rfloor \lfloor \theta m \rfloor),$$

where $P_k \equiv Q_k \equiv R_k \equiv S_k \equiv 0 \mod 5$. This indeed is what suggested the proposition above. Observe also that $7 + 11\theta$ is a PV-number.

Now $\theta^2 - \theta - 1 = 0$ and the discriminant of $x^2 - x - 1$ is 5. This motivates the first theorem.

Theorem 1. Let $R \geq 1$ be an odd integer, and $\theta$ the largest root of $x^2 - Rx - 1 = 0$. Set $\Delta = R^2 + 4$. For every pair of integers $(s, t)$ define a sequence $a_n = a_n(s, t)$ inductively by

$$a_1 = 1,$$

$$a_{n+1} = sa_n + t\lfloor \theta a_n \rfloor.$$

Then there is an infinite sequence of integer pairs $(s_i, t_i)$ such that (i) the highest power of $\Delta$ that divides $a_n = a_n(s_i, t_i)$ tends to infinity with $n$ and (ii) the following technical conditions are satisfied. The $s_i$ are odd and pairwise relatively prime, the $t_i$ are distinct,

$$(s_i, \Delta) = (t_i, \Delta) = 1,$$

and

$$\frac{t_i}{s_i} \to \theta \quad \text{as} \quad i \to \infty.$$

Here the pairs $(s_i, t_i)$ are constructed so that $s_i + t_i\theta$ or its negative is a PV number, and the proof relies heavily on this fact. Theorem 1 is a special case of Theorem 2 that we state and prove below in Section 4.
Moreover, the technique used to prove Theorem 2 also enables us to obtain similar results for algebraic integers that are far from PV.

Let \( \theta > 1 \) be the larger root of an irreducible quadratic \( x^2 - Rx - S \) where \( R \) and \( S \) are integers. Denote by \( \bar{\theta} \) the conjugate of \( \theta \), and set \( \Delta = R^2 + 4S \).

**Theorem 3.** Let \( \varepsilon > 0 \). There are infinitely many
\[
s + t\theta > 1
\]
with \( s \) and \( t \) integers that have (i) a smaller conjugate
\[
s + t\bar{\theta} > 2 - \varepsilon
\]
and are such that (ii) the \( a_n \) defined inductively by
\[
a_1 = 1,
\]
\[
a_{n+1} = sa_n + t\lfloor \theta a_n \rfloor,
\]
lie in at most two congruence classes modulo \( \Delta \) for \( n \geq 3 \).

**Theorem 4.** Let \( \varepsilon > 0 \). There are infinitely many
\[
s + t\theta > 1
\]
with \( s \) and \( t \) integers that have (i) a smaller conjugate
\[
s + t\bar{\theta} > \Delta - \varepsilon
\]
and are such that (ii) none of the \( a_n \) (defined as in Theorem 2) belong to a certain equivalence class modulo \( \Delta \) for \( n \geq 3 \).

We feel that nothing so peculiar can be expected of quadratic irrationalities whose smaller conjugate has a modulus exceeding the discriminant.

Before establishing Theorems 2-4 in Section 4 we obtain some properties of the greatest integer function (especially the ‘KLM formula’ — see also [1]) in Section 2, and express them in terms of a certain ‘almost linear’ multiplication \( \alpha \otimes n \). In Section 3 we prove Lemma 3.1 about first order ‘almost linear’ recurrences that involve this multiplication, and also give some lemmas that follows easily from well-known facts about uniform distribution. (Lemma 3.1 shows that our recurrences are pseudo-linear in the sense of Shapiro [6, p. 613].)

2. The ‘KLM formula’

Let \( p \) and \( q \) be integers such that the roots of \( F(x) = x^2 - px - q \) are real. Let \( \theta \) be a root of \( F(x) \) and define \( \Theta(n) = \lfloor n\theta \rfloor \).
Lemma (the 'KLM formula', cf. [1]). For any integers $K, L,$ and $M$ we have
\[ \Theta(K\Theta(n)+L\nu+M) = (Kp+L)\Theta(n)+K\nu+(L+K\bar{\theta})\{n\theta\}, \]
where $\bar{\theta}$ is the conjugate of $\theta$ and $\{x\}$ denotes the fractional part of $x$.

Proof. Denote the right-hand side by $R$. Then
\[ R = (Kp+L)\Theta(n)+K\nu+(L+K\bar{\theta})(n\theta-\Theta(n)) \]
\[ = Kp\Theta(n)+M\theta+(L+K\bar{\theta})(n\theta-\Theta(n)) \]
\[ = \left[ (K\Theta(n)+L\nu+M)\theta \right] \]
and this proves the formula. \( \square \)

Next, for any integers $K$ and $L$, and $\alpha = K\theta + L$, we define
\[ \alpha \otimes n = Kn\theta+L. \]
Clearly $\alpha \otimes n$ is an integer if $n$ is, and
\[ \Theta(n) = \alpha \otimes n. \]
Also, since
\[ \alpha \otimes n = (Kp+L)\theta+K\nu, \]
we have
\[ (\alpha \otimes n) = (Kp+L)\Theta(n)+K\nu. \]
Now the KLM formula says that $\otimes$ is 'almost' left distributive, since it may be written in the form
\[ \theta \otimes (\alpha \otimes n+M) = (\theta\alpha) \otimes n+\theta \otimes M+\left\lfloor \{M\theta\} + \bar{\alpha}\{n\theta\} \right\rfloor. \]
Also
\[ (\alpha_1+\alpha_2) \otimes n = \alpha_1 \otimes n + \alpha_2 \otimes n \quad \text{and (for } k \text{ an integer)} \]
\[ (k\alpha) \otimes n = k(\alpha \otimes n). \]
Let $U$ and $V$ be integers, and $\beta = U\theta+V$. From the above rules we find that
\[ \beta \otimes (\alpha \otimes n+M) = (\beta\alpha) \otimes n+\beta \otimes M+U\left\lfloor \{M\theta\} + \bar{\alpha}\{n\theta\} \right\rfloor, \]
a somewhat more general statement of 'almost' left distributive. In particular, we find that
\[ \beta \otimes (\alpha \otimes n) = (\beta\alpha) \otimes n \]
is bounded as a function of $n$. Moreover, if $\alpha$ is a PV or Salem number, then
\[ \beta \otimes (\alpha \otimes n) = (\beta\alpha) \otimes n. \]
Finally we mention
\[ \alpha(\beta 
abla n) = (\alpha \beta) \nabla n + \frac{\alpha - \tilde{\alpha}}{\theta - \tilde{\theta}} \tilde{\beta} \{n\theta\}; \]
this reduces to a previous formula when \( \alpha \) is a rational integer, and also yields
\[ \alpha(\beta \nabla n) - \beta(\alpha \nabla n) = \frac{\alpha \tilde{\beta} - \beta \tilde{\alpha}}{\theta - \tilde{\theta}} \{n\theta\}. \]

3. First order 'almost linear' recurrences

We begin with some notation. For any quadratic irrationality \( \beta \), let \( F_\beta(x) \) denote its characteristic polynomial, i.e.
\[ F_\beta(x) = (x - \beta)(x - \tilde{\beta}). \]
As before, let \( \theta \) be a fixed real algebraic integer of degree 2, let \( s \) and \( t \) be rational integers, and set
\[ \alpha = \alpha(s, t) = s + t\theta. \]
Now introduce \( E \) to denote the forward shift (thus \( Eb_n = b_{n+1} \) for the elements of any sequence \( \{b_n\} \)).

Lemma 3.1. If the \( a_n \) are defined inductively by
\[ a_1 = 1, \]
\[ a_{n+1} = \alpha \nabla a_n, \quad n \geq 1, \]
then
\[ F_\alpha(E)a_n = t\{\tilde{\alpha} \{\theta a_n\}\}. \]

Remark. If the \( \nabla \) were replaced by ordinary multiplication, we would have
\[ F_\alpha(E)a_n = 0. \]

Proof. Say \( \theta^2 = p\theta + q \) with \( p, q \) integers. Define a sequence \( b_n \) by \( b_1 = a_1 = u_1, b_2 = a_2, \) and
\[ b_n - (\alpha + \tilde{\alpha})b_{n-1} + \alpha \tilde{\alpha} b_{n-2} = t\{\tilde{\alpha} \{\theta b_{n-2}\}\}, \quad n \geq 3. \]
We shall show by complete induction that \( a_n = b_n \) for all \( n \geq 1. \) Since \( \tilde{\alpha} = s + t\theta \) we have
\[ b_n = (2s + tp)b_{n-1} - (s^2 + tsp - t^2 q)b_{n-2} + t\{s + t\theta\}{\theta b_{n-2}}, \]
and
\[ a_n = \alpha \nabla a_{n-1} = sa_{n-1} + t\{\theta a_{n-1}\}. \]
Thus it suffices to show that
\[(s+tp)a_{n-1}+t\lfloor \tilde{a}\{\theta a_{n-2}\}\rfloor = t\lfloor \theta a_{n-1}\rfloor +(s^2+tsp-t^2q)a_{n-2}.
\]
By the KLM formula
\[\lfloor \theta a_n\rfloor = (tp+s)\lfloor \theta a_{n-1} \rfloor + tqa_{n-1} + \lfloor \tilde{a}\{a_{n-1} \theta \}\rfloor.
\]
By the definition of \(a_n\),
\[(s+pt)a_n = (s^2+stp-t^2q)a_{n-1} + t(s+pt)\lfloor \theta a_{n-1}\rfloor + qt^2a_{n-1}.
\]
From the previous formula,
\[t\lfloor \theta a_n\rfloor = t(s+pt)\lfloor \theta a_{n-1}\rfloor + qt^2a_{n-1} + t\lfloor \tilde{a}\{a_{n-1} \theta \}\rfloor.
\]
Thus
\[(s+pt)a_n + t\lfloor \tilde{a}\{a_{n-1} \theta \}\rfloor = (s^2+stp-t^2q)a_{n-1} + t\lfloor \theta a_n\rfloor
\]
is always true, and the result follows. \(\Box\)

Note that \(F_n(E)a_n\) has a bound independent of \(n\), and assumes only integer values. Hence the \(a_n\) satisfy a pseudo-linear difference equation in the sense of Shapiro [6, p. 613].

**Lemma 3.2.** If \(m_1\) and \(m_2\) are integers, \(m_1 \neq 0\), and \(\phi\) is irrational, then \((m_1n+m_2)\phi\), for \(n=1,2,3,\ldots\), is uniformly distributed mod 1.

**Lemma 3.3.** Given \(E \geq \varepsilon\) and \(\theta\) and \(\phi\) irrational, there are infinitely many integers \(s \geq 0\) such that
\[s\phi - E < k < s\phi - \varepsilon,
\]
where \(k\) is an integer. In fact, there are infinitely many such pairwise relatively prime \(s\), each of which is also relatively prime to a preassigned positive integer \(D\).

**Proof.** Lemma 3.2 is well known. Next, by uniform distribution we can have (with \(k\) an integer and \(0 < \eta < E - \varepsilon\))
\[-\eta < s\phi - E - k < 0.
\]
Hence
\[0 < E - \varepsilon - \eta < s\phi - \varepsilon - k
\]
and
\[s\phi - E < k < s\phi - \varepsilon.
\]
The first statement follows. We could also replace \(s\) by \(Dn + 1\) and vary \(n\) rather than \(s\) (e.g. by Lemma 3.2). By replacing \(D\) with \(D(Dn + 1)\) we can create an infinite sequence.
of such $Dn+1$'s, each relatively prime (pairwise) to the others, and even with distinct $k$'s. □

4. Proofs

We shall deduce Theorem 1 from a more general result that we label as Theorem 2. In the proof of Theorem 2 we shall introduce two positive parameters $K_1 < K_2$. The proofs of Theorems 3 and 4 will be almost the same as that of Theorem 2 — there will simply be a different choice of parameters.

**Theorem 2.** Let $R, S$ be integers such that $\Delta = R^2 + 4S$ is positive and $\sqrt{\Delta}$ is irrational. Assume further that $S > 1 + |R|$ if $R < 0$. Let $\theta$ be the largest root of $x^2 - Rx - S = 0$, and $g = (R, \Delta)$. Then there are integers $s$ and $t$ with

$$ (s, \Delta) = \frac{\Delta}{g}, \quad \left( t, \frac{\Delta}{g} \right) = 1 \text{ or } 2, \quad s \text{ odd,} $$

such that the sequence

$$ a_n \in \mathbb{Z} $$

$$ a_{n+1} = sa_n + t \lfloor \theta a_n \rfloor $$

has the following property. The highest power of $\Delta$ that divides $a_n$ tends to infinity as $n \to \infty$.

**Remarks.** (1) We could say more concisely that $a_n \to 0$ in the $\Delta$-adic sense.

(2) Always $\theta > 1$. To see this, note that

$$ \theta = \frac{R + \sqrt{R^2 + 4S}}{2}. $$

The statement is clear if $R$ is a positive integer. If $R = 0$ the constraints on $\Delta$ require $4S > 0$, hence $4S > 4$, hence $4S > 8$, so again $\theta > 1$. If $R < 0$, then

$$ R^2 + 4S > R^2 + 4|R| + 4 $$

so

$$ \theta > \frac{R + |R| + 2}{2} = 1. $$

In particular, both roots are real.

(3) It is easily seen from the proof that we can create an infinite set of such $(s, t)$ pairs such that the $s$'s are all pairwise relatively prime and the $t$'s are all distinct. Moreover an easy calculation shows that for the pairs of our construction

$$ \frac{t}{s} \to \frac{g\theta}{|S|} \quad \text{as } s \to \infty. $$
We now proceed with the proof. Since \((R, A) = g\), there is an integer \(R^*\) such that

\[
\frac{R}{g} R^* \equiv \text{sgn}(S) \mod \frac{\Delta}{g}.
\]

Set

\[
\phi = \frac{g \theta}{|S| \Delta} + \frac{2R^*}{\Delta}
\]

and \(D = 2\Delta\). Next, introduce positive parameters \(K_1 < K_2\) that shall be specialized later. By Lemma 3.3 there are infinitely many pairwise relatively prime integers \(s\), each relatively prime to \(D\), such that

\[
s \phi - \frac{K_2 \theta}{|S| \Delta} < k < s \phi - \frac{K_1 \theta}{|S| \Delta}
\]

with \(k \geq 0\) an integer. Hence

\[
(sg - K_2) \theta < t|S| < (sg - K_1) \theta,
\]

where

\[
t = -2sR^* + k\Delta.
\]

(Note that \(t \geq 0\) for large \(s\).)

Hence

\[
K_1 \theta < sg \theta - |S| t < K_2 \theta
\]

or

\[
K_1 < sg + \text{sgn}(S)t\theta < K_2
\]

since \(\theta \theta = -S\). Now let

\[
s^* = sg, \quad t^* = \text{sgn}(S)t.
\]

Observe that

\[
2s^* + Rt^* \equiv 2sg + \text{sgn}(S)(-2sR^*)R \equiv 2sg - 2sg \equiv 0 \mod \Delta
\]

and

\[
s^* t^* - t^* S = s^2 g^2 + sg R \text{sgn}(S)(-2sR^*) - S(4s^2 R^*^2) \mod \Delta
\]

\[
\equiv s^2 g^2 - 2s^2 g^2 - 4s^2 R^*^2 S \mod \Delta
\]

\[
\equiv s^2 (-R^2 R^*^2 - 4SR^*^2) \mod \Delta
\]

\[
\equiv 0 \mod \Delta.
\]

Also

\[(s^*, \Delta) = (sg, \Delta) = g \left( s, \frac{\Delta}{g} \right) = g\]
and
\[
\left( t^*, \frac{A}{g} \right) = \left( -2sR^*, \frac{A}{g} \right) = \left( 2, \frac{A}{g} \right) = 1 \text{ or } 2.
\]
By Lemma 3.1 the recurrence
\[
a_n = s^*a_{n-1} + t^*[\theta a_{n-1}]
\]
satisfies
\[
a_n = (2s^* + R^*)a_{n-1} - (s^*t^* + t^*s^*R - t^*s^*) a_{n-2}
+ t^*[s^* + t^*\bar{\theta}][\theta a_{n-2}],
\]
and by construction
\[
K_1 < s^* + t^*\bar{\theta} < K_2.
\]
Now take \( K_1 = 0 \) and \( K_2 = 1 \). Since \( 0 < \{ \theta a_{n-2} \} < 1 \), the \( t^*[\cdots] \) term in the second order recurrence for \( a_n \) is zero. By the above congruences, the coefficients of \( a_{n-1} \) and \( a_{n-2} \) are 0 mod \( \Delta \). The result follows.

We can now obtain the promised results (Theorems 3 and 4) for non-PV, non-Salem numbers. For Theorem 3 choose \( K_1 = 2 - \varepsilon \) and \( K_2 = 2 \). Then the \( [\ ] \) factor in the last term of the second order recurrence for \( a_n \) can have only the values 0 or 1. For Theorem 4 choose \( K_1 = A - \varepsilon \) and \( K_2 = A \).

5. Further remarks

For a guide to the literature on properties of sequences of the form \( \lfloor n\alpha \rfloor \), \( n = 1, 2, 3, \ldots \), see [3] and the references therein. An excellent reference for PV and Salem numbers is [5].

References