Periods of $\beta$-expansions and linear recurrent sequences

by

YAN-HUI QU, HUI RAO and YA-MIN YANG (Beijing)

1. Introduction

1.1. $\beta$-numeration system. Let $\beta > 1$ be a real number. The $\beta$-transformation is a piecewise linear transformation on $[0, 1)$ defined by

$$T_\beta : x \mapsto \beta x - \lfloor \beta x \rfloor,$$

where $\lfloor \alpha \rfloor$ is the largest integer not exceeding $\alpha$. By iterating this map and considering its trajectory

$$x \xmapsto{T_\beta} x_1 \xmapsto{T_\beta^2} x_2 \xmapsto{T_\beta^3} \cdots$$

with $x_i = \lfloor \beta T_{\beta}^{i-1}(x) \rfloor$, we obtain the $\beta$-expansion of $x$,

$$x = \frac{x_1}{\beta} + \frac{x_2}{\beta^2} + \frac{x_3}{\beta^3} + \cdots = 0.x_1x_2x_3\ldots.$$

An expansion is finite if $(x_i)_{i\geq1}$ is eventually 0. A $\beta$-expansion is periodic if there exists $p \geq 1$ and $M \geq 1$ such that $x_k = x_{k+p}$ for all $k \geq M$; if $x_k = x_{k+p}$ for all $k \geq 1$, then it is strictly periodic (or purely periodic). When the $\beta$-expansion of $x$ is periodic, we denote by $L_\beta(x)$ its minimal period.

When $\beta = b \geq 2$ is an integer, the $\beta$-expansion is the $b$-adic expansion. In this case, it is well known that:

(i) A number $x \in [0, 1)$ has periodic expansion if and only if $x$ is a rational number.

(ii) The expansion of $x = p/q$ is strictly periodic if and only if $\gcd\{q, b\} = 1$.

(iii) The minimum period of the $b$-adic expansion of $p/q$ coincides with the minimum period of the sequence $\{b^n \mod q\}_{n\geq0}$.
It is natural to ask the same questions for $\beta$-expansions when $\beta$ is not an integer.

(Q1) For which $x \in [0, 1)$, is the $\beta$-expansion periodic?
(Q2) For which $x \in [0, 1)$, is the $\beta$-expansion strictly periodic?
(Q3) If the $\beta$-expansion of $x$ is periodic, what is the minimum period?

1.2. Periodic $\beta$-expansions and Pisot numbers. Question (Q1) has been settled for all Pisot numbers (see Schmidt [Sch], 1980). An algebraic integer strictly greater than 1 is a Pisot number if all its algebraic conjugates have modulus strictly less than 1. A number is called a Pisot unit if it is a Pisot number and an algebraic unit. Let $\mathbb{Q}(\beta)$ be the smallest field containing the rational numbers and $\beta$. The following is well known:

**Theorem A** (Schmidt [Sch]). Let $\beta$ be a Pisot number and $x \in [0, 1)$. Then $x$ has periodic $\beta$-expansion if and only if $x \in \mathbb{Q}(\beta)$.

The $\beta$-expansion with a Pisot base has drawn attention of many mathematicians. For a Pisot unit $\beta$, Rauzy ([Rau], 1982) and Thurston ([Thu], 1989) constructed a self-similar tiling system. The tiles (usually with fractal boundaries) are called Rauzy fractals or atomic surfaces. Several interesting dynamical system are related to Rauzy fractals (cf. [AI, IR2]).

According to the behavior of the $\beta$-expansion, several algebraic properties of $\beta$ have been defined, for example, the (F)-property introduced by Frougny and Solomyak ([FS]) and the (W)-property introduced by Akiyama [Aki]. Further investigation of these properties can be found in [Hol] (for the (F)-property) and [ARS] (for the (W)-property).

Akiyama [Aki] showed that the algebraic properties of $\beta$ characterize the tiling and dynamical properties of the associated Rauzy fractals.

On the other hand, Ito and his coauthors ([HI, IS, IR1]) employed the Rauzy fractals to study the $\beta$-expansions. They answered Question (Q2) when $\beta$ is a Pisot unit (see Section 1.3). The goal of this paper is to answer Question (Q3) when $\beta$ is a quadratic Pisot unit.

1.3. Strictly periodic $\beta$-expansions with Pisot unit base. Let $\beta$ be a Pisot unit of degree $d$. By using Rauzy fractals, a region $K$ has been constructed to serve as a Markov partition of a group automorphism on $d$-dimensional torus ([Pra, IR2]). It has been proved that the region $K$ completely characterizes the strictly periodic $\beta$-expansions in base $\beta$. The result was first obtained for quadratic Pisot units in [HI], generalized to a family of Pisot units in [IS], and to all Pisot units in [IR2].

Here we state only the result for quadratic Pisot units, which is needed in the present paper. A number $\beta > 1$ is a quadratic Pisot unit if either $\beta^2 = n\beta + 1$ ($n \geq 1$) or $\beta^2 = n\beta - 1$ ($n \geq 3$). Since $1, \beta$ is a basis of the field $\mathbb{Q}(\beta)$, each $x \in \mathbb{Q}(\beta)$ can be uniquely expressed as $x = x_1 + x_2\beta$ with
$x_1, x_2 \in \mathbb{Q}$. The number $x' = x_1 + x_2 \beta'$ is the conjugate of $x$ in $\mathbb{Q}(\beta)$ by definition, where $\beta'$ is the algebraic conjugate of $\beta$.

**Theorem B ([HI, IS, IR1]).** (i) If $\beta > 1$ satisfies $\beta^2 = n\beta + 1$ and $x \in [0, 1]$ then $x$ has strictly periodic $\beta$-expansion if and only if $x \in \mathbb{Q}(\beta)$ and $(x, x')$ belongs to the closed set $K$ in Figure 1.a minus the lines $x = 1/\beta$ and $x = 1$.

(ii) If $\beta > 1$ satisfies $\beta^2 = n\beta - 1$ and $x \in [0, 1]$ then $x$ has strictly periodic $\beta$-expansion if and only if $x \in \mathbb{Q}(\beta)$ and $(x, x')$ belongs to the closed set $K$ in Figure 1.b.

If we use the concept of “weakly admissible”, then we have a uniform statement of Theorem B, which is discussed in full detail in Section 2.

As a consequence, if $\beta^2 = n\beta + 1$, then every rational number in $[0, 1)$ has strictly periodic $\beta$-expansion since the segment $oa$ in Figure 1.a is contained in $K$ (this result was first proved by Schmidt [Sch]); if $\beta^2 = n\beta - 1$, then none of the $\beta$-expansions of the rational numbers $\neq 0$ is strictly periodic.

**1.4. Periods of $\beta$-expansions with quadratic Pisot unit base.** The main purpose of this paper is to investigate the periods of $\beta$-expansions.

When $\beta^2 = n\beta + 1$, the length of the period of the $\beta$-expansion of $p/q$ has been studied by Schmidt [Sch]. He characterized the function $L_\beta(p/q)$ by a certain dynamical system.

Using the dynamical and tiling properties of the Rauzy fractal, we obtain a satisfactory answer to Question (Q3) when $\beta$ is a quadratic Pisot unit. Precisely, we show that $L_\beta(x)$ is determined by a linear recurrent sequence related to $\beta$ and $x$.

Let $\beta$ be a quadratic Pisot unit with minimal polynomial $P(x) = x^2 - a_1 x - a_0$ with $a_0 = \pm 1$. We set

$$\mathbb{Z}[\beta] := \{c_0 + c_1 \beta; c_0, c_1 \in \mathbb{Z}\}.$$
For \( x \in \mathbb{Q}(\beta) \), \( x \neq 0 \), let \( q \geq 1 \) be the smallest integer such that \( qx \in \mathbb{Z}[\beta] \). Notice that 1, \( a_0 \beta^{-1} \) is a basis of \( \mathbb{Z}[\beta] \), hence \( x \) can be uniquely written as

\[
x = \frac{u_0(a_0 \beta^{-1}) + u_1}{q}
\]

with \( u_0, u_1 \) integers and \( \gcd\{u_0, u_1, q\} = 1 \).

Let \( \{u_k\} \) be the sequence of integers defined by the initial set \( u_0, u_1 \) and the recurrence relation

\[
(1.1) \quad u_{k+1} = a_1 u_k + a_0 u_{k-1} \quad (k \geq 1).
\]

We denote this sequence by \( u_k = u_k(u_0, u_1) \). It is easy to show that \( \{u_k \text{ (mod } q)\}_{k \geq 0} \) is always strictly periodic ([Eng, W]). It is interesting that this sequence characterizes the periods of \( \beta \)-expansions.

**Theorem 1.1.** Let \( \beta \) be a quadratic Pisot unit. Suppose \( x \neq 0 \) and \( x = (u_0(a_0 \beta^{-1}) + u_1)/q \) with \( u_0, u_1, q \) integers and \( \gcd\{u_0, u_1, q\} = 1 \). If the \( \beta \)-expansion of \( x \) is strictly periodic, then its periods coincide with the periods of the sequence \( \{u_k(u_0, u_1) \text{ (mod } q)\}_{k \geq 0} \).

Theorem 1.1 is the main result of this paper. It is proved in Section 2. The fact that the region \( K \) translationally tiles \( \mathbb{R}^2 \) plays a crucial role in our proof (see Figure 2).

![Fig. 2. A tiling by K](image-url)

In the following, we give a second characterization of the function \( L_\beta(x) \). Denote by \( D = a_1^2 + 4a_0 \) the discriminant of the polynomial \( P(x) \). Let \( d_0 \) be the maximal square-free factor of \( D \); clearly \( \mathbb{Q}(\beta) = \mathbb{Q}(\sqrt{d_0}) \). Let \( D_0 \) be the discriminant of the field \( \mathbb{Q}(\beta) \); then \( D_0 = d_0 \) when \( d_0 \equiv 1 \pmod{4} \) and \( D_0 = 4d_0 \) otherwise. We note that \( I = \sqrt{D/D_0} \), the index of the polynomial \( P(x) \) in \( K \), is an integer. (See for example Hecke [Hec].)
Let $q \geq 1$ be an integer. Then the sequence $\beta^k$ modulo $q$ is strictly periodic since $\beta$ is an algebraic unit. We will prove in Section 3 that this sequence also characterizes the periods of $\beta$-expansions.

**Theorem 1.2.** Let $\beta$ be a quadratic Pisot unit. Suppose the $\beta$-expansion of $x$ is strictly periodic and $q$ is the smallest integer such that $qx \in \mathbb{Z}[\beta]$. If $q$ is prime to $D/D_0$, then the periods of the $\beta$-expansion of $x$ coincide with the periods of the sequence $\{qx^k \mod q\}_{k \geq 0}$.

Let $N(\beta) = \beta \beta' = -a_0$ denote the norm of $\beta$. When $N(\beta) = -1$, every rational number $p/q$ has strictly periodic $\beta$-expansion. If $q$ is prime to $D/D_0$, then the periods coincide with the periods of the sequence $\{qx^k \mod q\}$, which is an analogue of the result for $b$-adic expansions.

If $q$ is not prime to $D/D_0$, then $L_{\beta}(x)$ is usually a multiple of the minimum period of the sequence $\{qx^k \mod q\}_{k \geq 0}$.

**Example 1.3.** Let $\beta = (1 + \sqrt{5})/2$ (which satisfies $\beta^2 = \beta + 1$) be the golden number. Then every rational number $p/q$ in $[0, 1)$ has strictly periodic $\beta$-expansion by Theorem B. According to Theorem 1.1, the minimum period $L_{\beta}(p/q)$ coincides with the minimum period of the sequence $f_k$ modulo $q$, where $f_k$ is the famous Fibonacci sequence which is defined by

$$f_0 = 0, \quad f_1 = 1, \quad f_{k+1} = f_k + f_{k-1} \quad (k \geq 1).$$

The first few terms of the sequence are

$$0, 1, 1, 2, 3, 5, 8, 13, 21, 34, 55, 89, 144, 233, 377, 610, 987, \ldots .$$

For example, since the sequence $f_k$ modulo 7 is

$$0, 1, 1, 2, 3, 5, 1, 6, 0, 6, 6, 5, 4, 2, 6, 1, 0, 1, \ldots$$

and has minimum period 16, we conclude that $L_{\beta}(1/7) = 16$. Actually the $\beta$-expansion of $1/7$ is $1/7 = 0.\overline{000010101010000}$. It is easy to show that $L_{\beta}(p/7) = 16$ for all $1 \leq p \leq 6$.

**1.5. Linear recurrent sequences modulo $q$.** The periods of linear recurrent sequences modulo $q$ have been studied as early as 1920 by Carmichael [Car] and 1931 by Engstrom [Eng]. By using Dedekind’s theorem on decomposition of primes in a number field, Engstrom obtained very general results. Wall [W] (1960) studied the Fibonacci sequence modulo $q$. He obtained many precise and interesting results by a simple method. A complete investigation of linear recurrent sequences of degree 2 modulo $q$ is done in [WY].

**2. Proof of Theorem 1.1.** In this section, first we investigate the weakly admissible $\beta$-expansions, which is closely related to the boundary
of the region $K$. Then we show that $K$ can tile $\mathbb{R}^2$. Thanks to this tiling property, finally we prove Theorem 1.1.

2.1. Admissible and weakly admissible. Let

$$\Omega = \{x_1x_2 \ldots ; 0.x_1x_2 \ldots \text{ is a } \beta\text{-expansion}\}.$$ 

We may endow the space $\Omega$ with the discrete metric ([Wal]). The space $\Omega$ is not complete under this metric. Let $\overline{\Omega}$ be the completion of $\Omega$. We will see that $\overline{\Omega}$ consists of weakly admissible sequences.

Formally we may consider the trajectory of 1:

$$1 \xrightarrow{b_1} T_\beta(1) \xrightarrow{b_2} T_\beta^2(1) \xrightarrow{b_3} \ldots.$$ 

We call $b_1b_2b_3 \ldots$ the expansion of 1 and denote it by $d_\beta(1)$. Define

$$d^*_\beta(1) = \begin{cases} 
  d_\beta(1) & \text{if } d_\beta(1) \text{ is infinite}, \\
  (b_1 \ldots b_{d-1}(b_d - 1))^\infty & \text{if } d_\beta(1) = b_1 \ldots b_{d-1}b_d \text{ is finite with } b_d \neq 0.
\end{cases}$$

A sequence over the alphabet $\{0, 1, \ldots, \lfloor \beta \rfloor\}$ is admissible if starting from any place of the sequence, the right side truncation is lexicographically strictly less than $d^*_\beta(1)$. If the right side truncations are less than or equal to $d^*_\beta(1)$, then the sequence is called weakly admissible.

A sequence is a $\beta$-expansion of a certain number if and only if this sequence is admissible. If a $\beta$-expansion is infinite, then it is admissible and weakly admissible. If a $\beta$-expansion of $x$ is finite, then $x$ has another infinite expansion in base $\beta$ which is weakly admissible but not admissible. One can show that $\overline{\Omega}$ is the set of all weakly admissible sequences (cf. [P, Thu]).

Each weakly admissible sequence $(x_i)_{i \geq 1}$ determines a real number $x$, and we call $(x_i)$ the weakly admissible $\beta$-expansion of $x$. Let $\text{Pur}(\beta)$ be the set of numbers in $[0, 1)$ with strictly periodic $\beta$-expansions, and let $\text{Pur}'(\beta)$ be the set of numbers in $[0, 1]$ with strictly periodic, weakly admissible $\beta$-expansions. The difference between $\text{Pur}'(\beta)$ and $\text{Pur}(\beta)$ is very small.

**Theorem 2.1.** Let $\beta > 1$ be a real number. If $d_\beta(1)$ is infinite, then $\text{Pur}(\beta) = \text{Pur}'(\beta)$; if $d_\beta(1) = b_1b_2 \ldots b_d$ is finite, then $\text{Pur}'(\beta) = \text{Pur}(\beta) \cup \{r_1, \ldots, r_d\}$, where $r_i = 0.b_i \ldots b_d$.

**Proof.** Suppose $x \in \text{Pur}(\beta)$. Then the $\beta$-expansion of $x$ is infinite and thus it is also admissible. This proves that $\text{Pur}(\beta) \subset \text{Pur}'(\beta)$.

Suppose $\text{Pur}(\beta) \neq \text{Pur}'(\beta)$. Take any $x \in \text{Pur}'(\beta) \setminus \text{Pur}(\beta)$. Then the $\beta$-expansion of $x$ is finite, say $x = 0.x_1 \ldots x_k$. The weakly admissible $\beta$-expansion of $x$ is

$$x = 0.x_1x_2 \ldots (x_k - 1)x_{k+1}x_{k+2} \ldots.$$
where \(x_{k+1}x_{k+2} \ldots = d^*_\beta(1)\). Since the above expansion is strictly periodic, we see that \(d^*_\beta(1)\) is strictly periodic. It follows that \(d\beta(1)\) is finite, and \(x_1x_2 \ldots (x_{k-1})x_{k+1}x_{k+2} \ldots\) coincides with a right side truncation of \(d^*_\beta(1)\). These together imply that \(x = r_i\) for some \(i\). ■

The following theorem is a special case of a result of [IR1].

**Theorem B'.** Let \(\beta\) be a quadratic Pisot unit. Then \(x \in \text{Pur}'(\beta)\) if and only if \(x \in \mathbb{Q}(\beta) \cap [0, 1]\) and \((x, x') \in K\).

If \(\beta^2 = n\beta + 1\), then \(d\beta(1) = n1\); if \(\beta^2 = n\beta - 1\), then \(d\beta(1) = (n - 1)(n - 2)\infty\). We see that Theorem B in Section 1 follows directly from Theorem B' and Theorem 2.1.

**2.2. A tiling by \(K\).** Let \(\beta\) be a quadratic Pisot unit with minimal polynomial \(P(x) = x^2 - a_1x - a_0\) where \(a_0 = \pm 1\). Set
\[
\mathcal{J} = \{(x, x') ; x \in \mathbb{Z}[\beta]\}.
\]
Then \(\mathcal{J}\) is a lattice of \(\mathbb{R}^2\) with a basis \((1, 1), (\beta, \beta')\). Denote by \(E^\circ\) the interior of a set \(E\).

**Lemma 2.2.** Let \(\beta\) be a quadratic Pisot unit, and let \(K\) be the region in Figure 1 associated with \(\beta\). Then the collection \(\{K + v ; v \in \mathcal{J}\}\) is a translation tiling of \(\mathbb{R}^2\). That is, \(\mathbb{R}^2 = \bigcup_{v \in \mathcal{J}}(K + v)\) and \((K + v_1)^\circ \cap (K + v_2)^\circ = \emptyset\) whenever \(v_1 \neq v_2, v_1, v_2 \in \mathcal{J}\).

**Proof.** First we note that \((1, 1)/\beta\) is a basis of \(\mathbb{Z}[\beta]\) and thus \((1, 1), (1/\beta, 1/\beta')\) is a basis of \(\mathcal{J}\) when \(N(\beta) = -1\). Likewise \(1, 1 - \beta^{-1}\) is a basis of \(\mathbb{Z}[\beta]\) and thus \((1, 1), (1 - \beta^{-1}, 1 - (\beta')^{-1})\) is a basis of \(\mathcal{J}\) when \(N(\beta) = 1\).

From Figure 2 we see clearly that \(K\) tiles the plane by translation, and the translation set is a lattice with a basis \(\vec{p}\alpha, \vec{p}\beta\). Since \(\vec{p}\alpha = (1, 1), \vec{p}\beta = (1/\beta, 1/\beta')\) when \(N(\beta) = -1\), and \(\vec{p}\alpha = (1, 1), \vec{p}\beta = (1 - \beta^{-1}, 1 - (\beta')^{-1})\) when \(N(\beta) = 1\), we conclude that the translation set is \(\mathcal{J}\) and the lemma is proved. ■

**Lemma 2.3.** Let \(\beta\) be a quadratic Pisot unit. Let \(x, y \in \mathbb{Q}(\beta) \cap [0, 1]\), \(x, y \neq 0\) and \(x \neq y\). If \(x - y \in \mathbb{Z}[\beta]\), then at most one of \(x, y\) has strictly periodic \(\beta\)-expansion.

**Proof.** Suppose one of \((x, x'), (y, y')\), say \((x, x')\), is an inner point of the region \(K\). Since \(K + \mathcal{J}\) is a tiling of \(\mathbb{R}^2\), we infer that \((y, y')\) is an inner point of the tile \(K + (y - x, (y - x'))\). Hence \((y, y')\) is not in \(K\) and thus the \(\beta\)-expansion of \(y\) is not strictly periodic. The lemma holds in this case.

Now we consider the case that both \((x, x'), (y, y')\) are on the boundary of \(K\). It is easy to check that
\[
\{x \in \mathbb{Q}(\beta) ; (x, x') \in \partial K\} = \begin{cases} 
\{0, \beta^{-1}, 1\} & \text{when } N(\beta) = -1, \\
\{0, 1 - \beta^{-1}\} & \text{when } N(\beta) = 1.
\end{cases}
\]
When $N(\beta) = -1$, only $0$ belongs to $\text{Pur}(\beta)$, while $\beta^{-1}$ and $1$ belong to $\text{Pur}'(\beta)$ but not to $\text{Pur}(\beta)$. When $N(\beta) = 1$, we have $0, 1 - \beta^{-1} \in \text{Pur}(\beta)$. So there is at most one $x \neq 0$ such that $(x, x')$ is on the boundary of $K$ and $x \in \text{Pur}(\beta)$. The lemma is hence proved in this case. ■

Remark 2.4. By the above discussion, we see that $\mathbb{Z}[\beta] \cap \text{Pur}(\beta) = \{0\}$ when $N(\beta) = -1$, while $\mathbb{Z}[\beta] \cap \text{Pur}(\beta) = \{0, 1 - \beta^{-1}\}$ when $N(\beta) = 1$. Since $1 - \beta^{-1} = 0.(n-2)^\infty$ when $N(\beta) = 1$, one checks directly that Theorem 1.1 holds when $q = 1$.

2.3. Carry sequence. Let
\begin{equation}
(2.1) \quad P(x) = x^2 - a_1 x - a_0
\end{equation}
be the minimal polynomial of $\beta$. Let $q \geq 1$ be the smallest integer such that $qx \in \mathbb{Z}[\beta]$. Then $x$ can be written uniquely as
\begin{equation}
(2.2) \quad x = \frac{u_0(a_0 \beta^{-1}) + u_1}{q}
\end{equation}
with $u_0, u_1$ integers and $\gcd\{u_0, u_1, q\} = 1$.

We define a sequence $\tilde{u}_k$ as follows. Set $\tilde{u}_0 = u_0$, $\tilde{u}_1 = u_1$. Supposing $\tilde{u}_0, \tilde{u}_1, \ldots, \tilde{u}_k$ are defined, we define $\tilde{u}_{k+1}$ to be the unique integer such that
\begin{equation}
(2.3) \quad \tilde{u}_{k+1} = a_1 \tilde{u}_k + a_0 \tilde{u}_{k-1} \pmod{q}, \quad 0 \leq \tilde{u}_k(a_0 \beta^{-1}) + \tilde{u}_{k+1} < q.
\end{equation}
Let us call $\{\tilde{u}_k\}_{k \geq 0}$ the carry sequence of $x$.

The carry sequence was first introduced by Hollander [Hol] in the case $q = 1$, i.e., for $x \in \mathbb{Z}[\beta]$; it has been used in [AR, ARS]. Here we generalize it to all $x \in \mathbb{Q}(\beta)$. The carry sequence is closely related to the $\beta$-expansion.

Let $x = 0.x_1x_2 \ldots$ be the $\beta$-expansion of $x$. Then by (2.1)–(2.3), one has
\begin{equation}
T_\beta(x) = \beta x - x_1 = \frac{\tilde{u}_1(a_0 \beta^{-1}) + (a_1 u_1 + a_0 u_0 - x_1 q)}{q} = \frac{\tilde{u}_1(a_0 \beta^{-1}) + \tilde{u}_2}{q}.
\end{equation}
In general, it is easy to show by induction that
\begin{equation}
T_\beta^k(x) = \frac{\tilde{u}_k(a_0 \beta^{-1}) + \tilde{u}_{k+1}}{q}.
\end{equation}
Therefore $x$ has strictly periodic $\beta$-expansion if and only if its carry sequence $\tilde{u}_k$ is strictly periodic. Moreover, $L_\beta(x)$ equals the minimal period of the sequence $\tilde{u}_k$.

Proof of Theorem 1.1. Let $\{u_k(u_0, u_1)\}_{k \geq 0}$ be the linear recurrent sequence defined by (1.1). We claim that
\begin{equation}
(2.4) \quad u_k \equiv \tilde{u}_k \pmod{q}
\end{equation}
for all $k \geq 0$. For suppose (2.4) holds for $1, \ldots, k$; then
\begin{equation}
\tilde{u}_{k+1} = a_1 \tilde{u}_k + a_0 \tilde{u}_{k-1} \equiv a_1 u_k + a_0 u_{k-1} = u_{k+1} \pmod{q}.
\end{equation}
It remains to show that the sequences \( \tilde{u}_k \) and \( u_k \) (mod \( q \)) have the same periods, which completes the proof of the theorem.

Let \( h \) be a period of the sequence \( \tilde{u}_k \). Then \( \tilde{u}_0 = \tilde{u}_h, \tilde{u}_1 = \tilde{u}_{h+1} \). Thus by (2.4), we have \( u_0 \equiv u_h, u_1 \equiv u_{h+1} \) (mod \( q \)). Therefore \( h \) is a period of the sequence \( u_k \) modulo \( q \) since \( u_k \) is completely determined by \( u_k \) and \( u_{k-1} \).

Conversely, suppose \( h \) is a period of \( u_k \) (mod \( q \)). Again by (2.4), we have \( \tilde{u}_0 \equiv \tilde{u}_h, \tilde{u}_1 \equiv \tilde{u}_{h+1} \) (mod \( q \)). Let \( y = T^h_\beta(x) \). Then

\[
x - y = \left( \tilde{u}_0 - \tilde{u}_h \right)(a_0 \beta^{-1}) + \left( \tilde{u}_1 - \tilde{u}_{h+1} \right) \in \mathbb{Z}[\beta].
\]

Since both \( x \) and \( y \) have strictly periodic \( \beta \)-expansions, we have \( x = y \) by Lemma 2.3. Hence \( h \) is a period of the \( \beta \)-expansion of \( x \) as well as a period of \( \tilde{u}_k \).

3. Proof of Theorem 1.2. To prove Theorem 1.2, we need three easy lemmas. Lemma 3.1 gives a formula for the general term of the sequence \( u_k \) (see for example [Eng, W]).

**Lemma 3.1.** The general term of \( u_k \) is given by

\[
(3.1) \quad u_k = c_1 \beta^k + c_2 (\beta')^k
\]

where

\[
c_1 = \frac{u_1 + a_0 \beta^{-1} u_0}{\beta - \beta'}, \quad c_2 = (c_1)' = \frac{u_1 + a_0 (\beta')^{-1} u_0}{\beta' - \beta}.
\]

**Proof.** One can check that the initial value of (3.1) is \( u_0, u_1, \) and \( u_k \) in (3.1) satisfies the recurrence relation (1.1). ■

Let \( H(q) \) be the minimal period of the sequence \( u_k \) modulo \( q \). Then we have

**Lemma 3.2.** If \( q = p_1^{e_1} \cdots p_k^{e_k} \), then

\[
(3.2) \quad H(q) = \text{lcm}\{H(p_1^{e_1}), \ldots, H(p_k^{e_k})\}
\]

where lcm denotes the least common multiple.

Lemma 3.2 can be found in [Eng, W]. We leave the easy proof to the reader.

Let \( \mathfrak{R} \) be an ideal in \( \mathbb{Q}(\beta) \). Denote by \( G(x, \mathfrak{R}) \) the minimal period of the sequence \( x, x\beta, x\beta^2, \ldots \) modulo \( \mathfrak{R} \). Then similar to Lemma 3.2, we have

**Lemma 3.3.** If \( q = p_1^{e_1} \cdots p_k^{e_k} \), then

\[
G(x, q) = \text{lcm}\{G(x, p_1^{e_1}), G(x, p_2^{e_2}), \ldots, G(x, p_k^{e_k})\}.
\]

**Theorem 3.4.** Let \( x_0 = u_0(a_0 \beta^{-1}) + u_1 \). If \( q \) is prime to \( D/D_0 \), then the periods of the sequence \( \{u_k \text{ (mod } q)\} \) coincide with the periods of the sequence

\[
x_0, x_0\beta, x_0\beta^2, \ldots \text{ (mod } q)\)
Proof. Since \( a_0 = \pm 1 \), it is easy to see that both \( \{ x_0 \beta^k \pmod{q} \} \) and \( \{ u_k \pmod{q} \} \) are strictly periodic.

According to Lemmas 3.2 and 3.3, we need only show that the assertion is valid for \( q = p^m \) where \( p \) is prime to \( D/D_0 \).

Set \( x_k = u_k(a_0\beta^{-1}) + u_{k+1}, k \geq 0 \). Then \( x_{k+1} = \beta x_k \) and so \( x_k = x_0\beta^k \). Hence \( x_k \in \mathbb{Z}[^{\beta}] \) are algebraic integers in \( \mathbb{Q}(\beta) \).

Clearly if \( h \) is a period of \( \{ u_k \pmod{q} \} \), then it is a period of \( \{ x_k \pmod{q} \} \).

Conversely, suppose \( h \) is a period of \( \{ x_k \pmod{q} \} \). Then \( x_0(\beta^h - 1) \) is divisible by \( q = p^m \) and so the algebraic conjugate \( (x_0(\beta^h - 1))' \) is also divisible by \( p^m \). By Lemma 3.1, we have

\[
    u_k = \frac{(u_1 + a_0\beta^{-1}u_0)\beta^k - (u_1 + a_0\beta^{-1}u_0)'(\beta')^k}{\beta - \beta'}.
\]

Hence

\[
    (3.3) \quad u_{k+h} - u_k = \frac{x_0(\beta^h - 1)\beta^k - x_0'((\beta')^h - 1)(\beta')^k}{\beta - \beta'}.
\]

By the assumption of \( h \), the numerator of the right side of (3.3) is divisible by \( p^m \). Notice that \( \beta - \beta' = \sqrt{D} = I\sqrt{D_0} \).

If \( p \) is prime to \( D \), then the denominator \( D \) is prime to \( p^m \). Hence \( u_{k+h} - u_k \) is divisible by \( p^m \) for all \( k \geq 0 \), and \( h \) is a period of \( \{ u_k \pmod{p^m} \} \).

If \( p \) is a factor of \( D_0 \), then \( p = \mathfrak{R}^2 \) where \( \mathfrak{R} \) is a prime ideal in \( \mathbb{Q}(\beta) \). We divide the discussion into two cases: \( p \neq 2 \) and \( p = 2 \). Recall that \( D_0 = d_0 \) or \( 4d_0 \) where \( d_0 \) is square-free.

If \( p \neq 2 \), then \( p^2 \nmid D_0 \) and so the power of \( \mathfrak{R} \) contained in the denominator of (3.3) is 1. Since the power of \( \mathfrak{R} \) contained in the numerator of (3.3) is at least \( 2m \), we find that \( (u_{k+h} - u_k)/p^{m-1} \) is an integer and it is divisible by \( p \), the norm of \( \mathfrak{R} \). Therefore \( u_{k+h} - u_k \) is divisible by \( q = p^m \) for all \( k \geq 0 \).

If \( p = 2 \), then \( D_0 \) is an even number and hence \( D_0 = 4d_0 \). Moreover \( 1, \sqrt{d_0} \) is a basis of \( \mathbb{Q}(\beta) \). Let \( x_0(\beta^h - 1)\beta^k = X + Y\sqrt{d_0} \). Then \( q = 2^m \) dividing \( X + Y\sqrt{d_0} \) implies that \( 2^m | Y \). Formula (3.3) becomes

\[
    u_{k+h} - u_k = \frac{2Y\sqrt{d_0}}{\sqrt{D}} = \frac{2Y\sqrt{d_0}}{I\sqrt{D_0}} = \frac{2Y\sqrt{d_0}}{2I\sqrt{d_0}} = \frac{Y}{I}.
\]

Since \( p = 2 \) is coprime to \( I \), we conclude that \( u_{k+h} - u_k \) is divisible by \( 2^m \) for all \( k \geq 0 \). This completes the proof the theorem. ■

Theorem 1.2 follows immediately from Theorems 1.1 and 3.4.

References


Periods of $\beta$-expansions


Department of Mathematics
Tsinghua University
100084 Beijing, China
E-mail: jyh02@mails.tsinghua.edu.cn
hrao@math.tsinghua.edu.cn
nancy_yym@163.com

Received on 24.9.2004
and in revised form on 22.6.2005 (4854)