On some problems of the arithmetical theory of continued fractions II

by

A. Schinzel (Warszawa)

To Professor Wacław Sierpiński on his 80th birthday

§ 1. In the preceding paper [5], I considered the following two problems

P. Decide for a given integer-valued polynomial \( f(n) \) whether

\[
\lim_{n \to \infty} p(f(n)) < \infty.
\]

(\( p(f(n)) \) denotes the length of the shortest period of the expansion of \( \sqrt{f(n)} \) into an arithmetic continued fraction).

\( P_1 \). Decide whether for a given polynomial \( f(n) \) of the form

\[
a_n n^\mu + a_{n-1} n^{\mu-1} + \ldots + a_0, \quad (\mu, a_0, a_1, \ldots, a_n \text{ integers, } \mu \geq 2, a_0 \neq 0)
\]

there exist polynomials \( u_i \) of positive degree with rational coefficients such that

\[
\sqrt{f(n)} = u_1(n) \cdot \frac{1}{u_2(n)} + \frac{1}{u_3(n)} + \ldots + \frac{1}{u_k(n)}
\]

(the dash denotes the period).

I indicated a connection between them. Now I prove (in § 2) that for polynomials \( f \) of form (1) problem \( P \) can be completely reduced to problem \( P_1 \). The proof follows the ideas of H. Schmidt [6] rather than those of paper [5]. Since for polynomials \( f \) not of form (1) problem \( P \) is solved (negatively) by Theorem 3 [5], one can limit oneself to the investigation of problem \( P_1 \). In § 3 I show how problem \( P_1 \) can be reduced to the case where the polynomial \( f(n) \) has no multiple factors. Finally (§ 4), I discuss the results concerning problem \( P_1 \) which I have found in papers about pseudo-elliptic integrals (they contain in fact a complete solution of problem \( P_1 \) for polynomials \( f \) of degree 4 without multiple factors)

* This paper was written when the author was Rockefeller Foundation Fellow at Uppsala University.
and I generalise some of them to the hyperelliptic case ($\mu > 2$). The connection between problem \( P \) and the theory of Abelian integrals was already established by Abel [1], who also proved that the answer to \( P \) is positive if and only if the equation

\[
X^2 - fY^2 = \text{const}
\]

is solvable in polynomials \( X, Y \) where \( Y \neq 0 \). Furthermore, if \( X, Y \) is a solution of the above equation and \( X = Y(\infty) = \infty \), then \( X = Y \) is necessarily equal to one of the reducible solutions of expansion (2). I shall make frequent use of these theorems.

As to notation, I shall follow [5]; in particular, I shall denote throughout by \([h_0(n), h_1(n), \ldots]\) the expansion of \( f(n) \) into an arithmetic continued fraction, by \( A_{\ell}(n)R_{\ell}(n) \) the corresponding reduceds. Besides, I shall put LP \( \sqrt{f} = K \) if \( K \) is the smallest number \( \geq 0 \) for which (2) holds, and LP \( \sqrt{f} = \infty \) if such a number does not exist. Putting

\[
\sqrt{f} = u_0 + \frac{1}{u_1 + \frac{1}{u_2 + \ldots}}
\]

I shall assume simultaneously

\[
T_{-4} = 1, \quad T_0 = u_0, \quad T_i = u_iT_{i-1} + T_{-4}, \\
U_{-4} = 0, \quad U_0 = 1, \quad U_i = u_iU_{i-1} + U_{-4}.
\]

\( [g] \) and \( (g) \) will denote the integral and the fractional part of \( g \), respectively, \( \Phi_{n}(g) \) the \( n \)-th cyclotomic polynomial.

§ 2. Lemma 1. For every polynomial \( f \) of form (1) which is not a perfect square and every \( k \geq 0 \) there exists a finite set of \( s_k \) systems of polynomials with rational coefficients \([b_0^k, b_1^k, \ldots, b_{s_k}^k] \) \((1 \leq j \leq s_k) \) such that integers \( > n_k(k) \) can be divided into \( s_k \) classes \( K_1, K_2, \ldots, K_{s_k} \), so that if \( n < K_j \) then \( b_i(n) = b_i^k(n) \) \((0 \leq i < k, 1 \leq j \leq s_k) \). Proof by induction with respect to \( k \). To avoid the repetition of the argument, we shall start the induction from \( k = 1 \), where for all \( n \) we can assume \( b_i(n) = 0 \) and no division into classes is necessary. Suppose now that the theorem is proved for \( k-1 \) \((k \geq 0) \), and let \( K_1, K_2, \ldots, K_{s_{k-1}} \) be corresponding classes and \([b_0^{k-1}, b_1^{k-1}, \ldots, b_{s_{k-1}}] \) \((j < s) \) corresponding systems of polynomials. For \( n < K_j \) we have

\[
\sqrt{f(n)} = [b_0^k(n), b_1^k(n), \ldots, b_{i-1}^k(n), \xi_i(n)],
\]

where evidently \( \xi_i(n) = [\sqrt{f(n)} + r(n)]b_i(n) \), \( r(n) \) and \( s(n) \) being polynomials with rational coefficients completely determined by the class \( K_j \) (this is true also for \( k = 0 \)). Now

\[
\frac{\sqrt{f(n)} + r(n)}{s(n)} = g(n) + q(n),
\]

where \( g(n) \) is a polynomial with rational coefficients, \( q(n) = o(1) \) and, for sufficiently large \( n \), \( g(n) \) has a fixed sign. Therefore for \( n > n_k(k) \)

\[
b_i(n) = \begin{cases} 
q(n) - 1 & \text{if } q(n) \text{ integral and } 
\frac{1}{q(n)} \left(\frac{1}{q(n)}\right) = -\infty, \\
[q(n)] & \text{otherwise.}
\end{cases}
\]

Put \( q(n) = Q(n) \mod m \), where \( Q(n) \) is a polynomial with integral coefficients and \( m \) an integer. If \( n = r \mod m \), we have \( [q(n)] = q(n) - [q(r)] \). Therefore, putting for \( 0 \leq r < m \)

\[
b_i^r(n) = \begin{cases} 
q(n) - 1 & \text{if } (q(r)) = 0 \text{ and } 
\frac{1}{q(n)} \left(\frac{1}{q(n)}\right) = -\infty, \\
q(n) - [q(r)] & \text{otherwise,}
\end{cases}
\]

we have for \( n < K_j, n > n_k(k), n = r \mod m \)

\[
b_i^r(n) = b_i^r(n).
\]

This determines the required subdivision of the class \( K_j \) into a finite number of classes and completes the proof.

Theorem 1. If \( \sqrt{f} = \infty \), then \( \lim_{n \to \infty} f(n) = \infty \).

Proof. Let \( k \) be an arbitrary integer \( \geq 0 \). For all classes \( K_1, K_2, \ldots, K_{s_k} \), whose existence is stated in Lemma 1, we form polynomials \( A_{\ell}(n), B_{\ell}(n) \) defined by the formulae \((0 \leq i < k, 1 \leq j \leq s_k) \)

\[
A_{-1}(n) = 1, \quad A_{\ell}(r) = b_0^k(n), \quad A_{\ell}(n) = b_i^k(n)A_{\ell-1}(n) + A_{\ell-2}(n), \\
B_{-1}(n) = 0, \quad B_{\ell}(r) = b_0^k(n), \quad B_{\ell}(n) = b_i^k(n)B_{\ell-1}(n) + B_{\ell-2}(n).
\]

Since \( \sqrt{f} = \infty \), among the polynomials \( A_{\ell}(n), B_{\ell}(n) \) there is no pair satisfying identically the equation

\[
A_{\ell}(n) - f(n)B_{\ell}(n) = \text{const}.
\]

It follows that if \( n > n_k(k) \), we have for all \( i < k, j < s_k \):

\[
A_{\ell}(n) - f(n)B_{\ell}(n) \neq \pm 1.
\]

On the other hand, by Lemma 1, for \( n > n_k(k), b_i(n) = b_i^k(n) \) for some \( j < s_k \) and all \( i < k \), and thus \( A_{\ell}(n) = A_{\ell}(n) \) and \( B_{\ell}(n) = B_{\ell}(n) \). The last inequality implies therefore that for all \( n > \max(m_k(k), n_k(k)) \)

\[
A_{\ell}(n) - f(n)B_{\ell}(n) \neq \pm 1 \quad (0 \leq i < k),
\]

whence \( \lim_{n \to \infty} f(n) > k \).

Lemma 2. If \( R(n) \) is any rational function with rational coefficients, then

\[
\lim_{n \to \infty} R(n) < \infty.
\]
Proof. We shall prove it by induction with respect to the degree \( d \) of the denominator of \( R(n) \) in its irreducible form. If \( d = 0 \), we have \( R(n) = P(n)/m \), where \( P(n) \) is a polynomial with integral coefficients and \( m \) is an integer. Obviously
\[
\text{lap} R(n) \leq \max_{0 < \epsilon < \infty} \text{lap} R(r).
\]
Suppose now that the lemma is valid for all rational functions with denominators of degree \( d < d \) and let \( R(n) = P(n)/Q(n) \) where \( P, Q \) are polynomials and the degree of \( Q \) is equal to \( d \). We have
\[
R(n) = q(n)/Q(n),
\]
where \( q, r \) are polynomials and \( r \) is of degree \( < d \). Putting \( q(n) = q_{k}n/m \), where \( q_{k} \) is a polynomial with integral coefficients and \( m \) is an integer, we have for \( n \equiv r (mod \ m) \)
\[
\text{lap} R(n) = \text{lap} \left( \frac{q(r)}{m} + \frac{r(n)}{Q(n)} \right) = \text{lap} \left( \frac{q(r) \xi(n) + m}{mQ(n)} \right),
\]
where \( \xi(n) = Q(n)/r(n) \). Since by the inductive assumption: \( \lim \text{lap} \xi(n) < \infty \), it follows immediately from Theorem 1 [5] that \( \text{lap} R(n) < \infty \), which completes the proof.

Theorem 2. If \( LP \sqrt{f} = K > 0 \) and
\[
\sqrt{f} = u_{0} + \frac{1}{u_{1} + \frac{1}{u_{2} + \ldots + \frac{1}{u_{k}}}}
\]
denote by \( E \) the set of all integers \( n \) such that \( 2T_{K-1}(n) \) is integral, and by \( CE \) its complement. Then
\begin{align*}
\lim_{n \to \infty} \text{lap} \sqrt{n}(n) & = \infty, \quad n \in E, \\
\lim_{n \to \infty} \text{lap} \sqrt{n}(n) & < \infty, \quad n \notin E.
\end{align*}

Proof. We begin with a proof of equation (4). Let \( k \) be an arbitrary integer \( > 0 \), and define \( K_{j}, A_{k}(n), B_{k}(n) \) \( 0 \leq j \leq k \) as in the proof of Theorem 1. Suppose that for some \( i, j \) we have \( K_{i} \notin E \) and similarly
\[
A_{k}(n) - f(n)B_{k}(n) = \pm 1.
\]
Since the continued fraction expansion furnishes the fundamental solution \( T_{K-1}(n), U_{K-1}(n) \) of the Pell equation \( X^{2} - f(n)Y^{2} = \pm 1 \), we must have, for some \( i \) and suitably chosen signs, identically
\[
\pm A_{k}(n) \pm f(n)B_{k}(n) = T_{K-1} + \sqrt{f(n)}U_{K-1} = [T_{K-1} + \sqrt{f(n)}]^{2}.
\]

The proof of this is completely analogous to the corresponding proof for the ordinary Pell equation and will be omitted.

Now let \( n_{E} \in K_{E}. \) Since \( n_{E} \in K_{i}. \) \( \sqrt{f(n_{E})} \) is irrational; \( A_{k}(n_{E}) = A_{k}(n_{E}) \), \( B_{k}(n_{E}) = B(n_{E}) \) are integers, whence \( \pm A_{k}(n_{E}) \pm \sqrt{f(n_{E})}B_{k}(n_{E}) \) is an integer of the field \( \mathbb{K} \sqrt{f(n_{E})} \). On the other hand, since \( 2T_{K-1}(n_{E}) \) is not a rational integer, \( T_{K-1}(n_{E}) + \sqrt{f(n_{E})}U_{K-1}(n_{E}) \) and therefore also \( T_{K-1}(n_{E}) + \sqrt{f(n_{E})}U_{K-1}(n_{E}) \) cannot be an integer of the field \( \mathbb{K} \sqrt{f(n_{E})} \).

The contradiction obtained proves that for all \( f \) such that \( K_{E} \notin E, \) and all \( i \leq k, \)
\[
A_{k}(n) - f(n)B_{k}(n) = \pm 1
\]
does not hold identically. There exists therefore a number \( n_{E}(k) \) such that for all \( n > n_{E}(k) \)
\[
A_{k}(n) - f(n)B_{k}(n) \neq \pm 1.
\]
Thus if \( n > \max(n_{E}(k), n_{E}(k)) \), \( n \notin E, \) then
\[
A_{k}(n) - f(n)B_{k}(n) \neq \pm 1
\]
for all \( i \leq k, \) whence \( \sqrt{f(n_{E})} > k, \) which completes the proof of (4).

To prove inequality (5) put \( U_{K-1}(n) = W(n)/m \), where \( W(n) \) is an integer-valued polynomial and \( m \) is an integer and consider all rational functions
\[
\frac{T_{K-1}}{U_{K-1}}, \quad \frac{a_{K-1}}{U_{K-1}}.
\]
By Lemma 2, there exists a number \( M \) such that for all \( i \leq m \)
\[
\text{lap} \frac{T_{K-1}(n)}{U_{K-1}(n)} < M \quad (i = 1 \text{ or } -1).
\]
We shall prove (5) by showing that for all \( n \in E \)
\[
\text{lap} \sqrt{f(n)} < M + 2.
\]
In fact, if \( n \in E, \) \( 2T_{K-1}(n) \) is an integer. If \( T_{K-1}(n) \) itself is an integer, then it follows from the equation
\[
T_{K-1} - f(n)U_{K-1} = (-1)^{K}
\]
that \( f(n)U_{K-1}(n) \) is also an integer. Therefore if \( m_{n}m \) is the denominator of \( U_{K-1}(n) \) represented as an irreducible fraction, the number \( f(n)/m_{n} \) must be integral. The equation
\[
T_{K-1} - f(n)U_{K-1} = \left( T_{K-1} + \sqrt{f(n)}U_{K-1} \right)\sqrt{f(n)}
\]
implies that \( T_{K-1}(n) + \sqrt{f(n)}U_{K-1}(n) \) and \( m_{n}U_{K-1}(n) \) are integers and, a fortiori, \( T_{K-1}(n) \) and \( m_{n}U_{K-1}(n) \) are integers.
Consider therefore all systems \((T_{k-1}(n), mU_{k-1}(n))\) reduced mod. \(m\). Since the number of all systems \((a, b)\) different mod. \(m\) is \(m^2\), we have for some \(1 \leq i < j \leq m^2 + 1\),
\[
T_{k-1}(n) = T_{k-1}(n) \pmod{m},
\]
\[
mU_{k-1}(n) = mU_{k-1}(n) \pmod{m}.
\]
Hence
\[
T_{k-1}(n) + \sqrt{f(n)}U_{k-1}(n) = f(n) U_{k-1} + T_{k-1} \cdot m U_{k-1} + \sqrt{f(n)} m U_{k-1} - T_{k-1} \cdot m U_{k-1}.
\]
Since
\[
T_{k-1}mU_{k-1} - T_{k-1}m U_{k-1} = 0 \pmod{m},
\]
the number \(U_{k-1}(n)\) is an integer.
Since the numbers \(T_{k-1}(n)\) and \(U_{k-1}(n)\) form an integral solution of the equation
\[
a^2 - f(n)b^2 = \pm 1,
\]
the number
\[
\frac{T_{k-1}(n)}{U_{k-1}(n)}
\]
must be a reducible arithmetic continued fraction for \(\sqrt{f(n)}\), and if \(hp\sqrt{f(n)} = k\), we must have
\[
\frac{T_{k-1}(n)}{U_{k-1}(n)} = \frac{A_{k-1}}{B_{k-1}},
\]
whence
\[
k \leq M \leq \log \frac{T_{k-1}(n)}{U_{k-1}(n)} + 2 \leq M + 2.
\]
If \(2T_{k-1}(n)\) is an integer but \(T_{k-1}(n)\) is not, then it is evident from the formula
\[
T_{k-1} = T_{k-1}4T_{k-1}^2 - 3(1)^2
\]
that \(T_{k-1}(n)\) is an integer. \textit{Mutatis mutandis}, the whole previous argument applies.

Theorem 2 immediately implies

\textbf{Theorem 3.} If \(LP/\sqrt{f(n)} = K < \infty\) and formula (2) holds, then \(\lim npl\sqrt{f(n)} < \infty\) if and only if \(2T_{k-1}(n)\) is an integer-valued polynomial.

Theorems 2 and 3 generalise Theorems 4 and 5 of [5]. Their proofs furnish also independent proofs of the latter theorems. In view of Theorem 3 [5], problem \(P\) is now completely reduced to problem \(P_1\).
By comparing the degrees we obtain
\[ \prod_{\alpha \in \mathcal{A}} (x^2 - 2T(r)x + 1) = G(x) \Phi(x)^{v(r)} \]
i.e. the first part of condition (ii).

Further it follows from (9) that
\[ X_0^{(j)}(r) = 0 \quad (j = 1, 2, \ldots, \alpha_0 - 1), \]
and since \( g^{(j)}(r) = 0 \quad (j = 1, 2, \ldots, \alpha_0 - 1), \) \( h(r) \neq 0, \) we have
\[ \frac{d}{dx} \left[ \pm X_0(x) \pm \sqrt{h(x)g(x)} X_0(x) \right] \bigg|_{x=r} = 0 \quad (j = 1, 2, \ldots, \alpha_0 - 1). \]

It follows from (8) by easy induction that
\[ \frac{d}{dx} \left[ T(x) + \sqrt{h(x)} U(x) \right] \bigg|_{x=r} = 0 \quad (j = 1, 2, \ldots, \alpha_1 - 1), \]
and hence \( T^{(j)}(r) = 0 \quad (j = 1, 2, \ldots, \alpha_1 - 1), \) i.e.
\[ T'(r) = 0 \quad (mod \, (x-r)^{\alpha_1 - 1}). \]

Since the last divisibility holds for each root \( r \) of \( g \), we have
\[ T' = 0 \quad (mod \, g^{\alpha_1 - 1}), \]
i.e. the second part of condition (ii).

It remains to prove that conditions (i)-(ii) are sufficient. Suppose therefore that they are fulfilled.

If \( g(r) \neq 0 \), denote by \( n(t) \) the index of the cyclotomic polynomial that occurs in condition (ii) and let \( n \) be the least common multiple of all numbers \( n(t) \). Define polynomials \( V, W \) by the identity
\[ V + \sqrt{h} W = (T + \sqrt{h} U)^n. \]

In view of (ii) we have for each root \( r \) of \( g(r) \neq 0 \)
\[ (T(r) \pm \sqrt{h(r)} U(r))^n = 1, \]
and thus for each root of each \( g(r) \neq 0 \):
\[ V(r) \pm \sqrt{h(r)} W(r) = 1, \quad W(r) = 0 \]
and
\[ W(x) = 0 \quad (mod \, \prod_{\alpha \in \mathcal{A}} g_\alpha), \]

On the other hand, it follows from condition (i) and identity (10) that
\[ W(x) = 0 \quad (mod \, \prod_{\alpha \in \mathcal{A}} g_\alpha), \]
so that \( W(x) = 0 \quad (mod \, g(x)) \) and equation (7) has the solution \( V(x), \)
\[ W(x) = 0 \quad (mod \, g(x)), \]
which completes the proof.

**Corollary.** If \( h \neq 0 \), \( LP(s-a) \sqrt{s-a} > 0 \) holds if and only if \( a = 0 \) or \( h = \frac{1}{2} a^2, 2a^2 \text{ or } 4a^2 \).

**Proof.** We have here \( T(x) = 1 - \frac{2a^2}{h} U(x) = -2s/h. \) Conditions (i)-(ii) take the shape
\[ h \neq a^3 \]
and
\[ a = 0 \text{ or } x^2 - 2s \left( 1 - \frac{2a^2}{h} \right) x + 1 = \Phi_1(x), \Phi_2(x) \text{ or } \Phi_1(x), \Phi_2(x), \Phi_3(x). \]

The last identity gives \( 1 - 2a^2/h \pm t = \pm 1, \pm \frac{1}{2} \text{ or } 0, \) which leads to the four cases stated in the corollary.

**§ 4.** Now we shall make some remarks about problem \( P_1 \), the really important case where the polynomial \( f \) has no multiple factors. Suppose that \( LPf = k \) and (2) holds, so that
\[ T^{K-1}_{K-1}(f) U_{K-1} = (-1)^{K}, \]
and let \( T_{K-1} \) be of degree \( \lambda \).
Applying the theorem of Abel to the function

$$T_{k-1}(x) + yU_{k-1}(x)$$

on the Riemann surface $S$ defined by equation $y^2 = f(x)$, we find

$$\lambda \int_A \omega dx - \lambda \int_A \omega dx = a \text{ period},$$

where $\int_A \omega dx$ is any integral of the first kind on $S$, $A$ is an arbitrary place and $P_1, P_2$ are two places in infinity on $S$. Taking $A = P_1$ we get

$$\lambda \int_{P_1} \omega dx = a \text{ period},$$

which means that

If $\text{LP} \sqrt{f} < \infty$, then the value of $\int_{P_1} \omega dx$ is commensurable with the periods of the integral $\int_A \omega dx$, $\omega$ being any integrand of the first kind.

For polynomials $f$ of degree $4$, the inverse of the above statement is also true, which has been known for a very long time ([2], Vol. II, p. 590). Furthermore, if $r$ is the smallest integer such that

$$r \int_{P_1} \frac{dx}{\sqrt{f(x)}} = a \text{ period},$$

then $\text{LP} \sqrt{f} = r - 1$ or $2(r-1)$. More precisely, $r$ is the smallest integer $\geq 2$ such that

$$T_{r-1}^r(x) - f(x)U_{r-1}^r(x) - C = \text{ constant}$$

and $\text{LP} \sqrt{f} = r - 1$ or $2(r-1)$ if $C = (-1)^{r-1}$ or not, respectively. According to Abel ([1], p. 213), if $r$ is odd, we have necessarily $C = 1$ and $\text{LP} \sqrt{f} = r - 1$.

These statements in themselves do not form a solution of problem $P_1$ for polynomials of degree $4$, since they do not supply any method of deciding whether the value of $\int_{P_1} \frac{dx}{\sqrt{f(x)}}$ is commensurable with the periods or not.

A method of deciding that was given by Tchebicheff [8], and its justification was later furnished by Zolotareff [9].

Now, after the theory of rational points on curves of genus $1$ has been developed, another method can be indicated, actually based on the same idea but leading to the end more rapidly. Without loss of generality we can assume that

$$f(x) = x^2 + 6a_2x^2 + 4a_4x + a_4.$$
Über die Normalität von Zahlen zu verschiedenen Basen

von

WOLFGANG M. SCHMIDT (New York)


Wir konstruieren Zahlen mit den erwähnten Eigenschaften explizit, und geben daher mehr als einen reinen Existenzbeweis. Am Ende der Arbeit skizzieren wir einen Beweis dafür, daß die Menge $M(E, S)$ dieser Zahlen die Mächtigkeit $\mathfrak{c}$ des Kontinuums hat. Da die Menge der Klasseneinteilungen $E, S$ ebenfalls kontinuierliche Mächtigkeit hat, ergibt dies eine nette (freilich komplizierte!) Illustration der Gleichung $\mathfrak{c} = \mathfrak{c}$.

Der Bequemlichkeit halber nehmen wir im folgenden an, $S$ sei nicht leer. Für leeres $S$ ist der Satz wohlbekannt. Außerdem werden wir am Ende zeigen, wie sich unsere Konstruktion auf diesen Fall übertragen läßt.

2. Hilfssätze. Wir schreiben $[r]$ für die ganze Zahl $a$, die $n < r < n+1$ leistet, und $[r]$ für $r - [r]$. In diesem Abschnitt sind $r, s$ feste ganze Zahlen größer als 1, die $r \sim s$ erfüllen, und $a_1, a_2, \ldots$ sind positive Konstanten, die nur von $r$ und $s$ abhängen.

Sind

$$r = p_1^{a_1} \ldots p_k^{a_k}, \quad s = p_1^{b_1} \ldots p_k^{b_k}$$

($d_i + a_i \neq 0$)

die Primzerlegungen von $r$ und $s$, dann dürfen wir

$$d_i/a_i \gg \gg d_i/e_i$$