ACTA ARITHMETICA
VII (1962)

On some problems of the arithmetical theory of continued fractions II *

by

A. SCHINZEL (Warszawa)

To Professor Wacław Sierpiński on his 80-th birthday

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

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

$$\overline{\lim} \operatorname{lp} \sqrt{f(n)} < \infty .$$

($\operatorname{lp} \sqrt{f(n)}$ 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*

(1) $\quad a^2 n^{2\mu} + a_1 n^{2\mu-1} + \ldots + a_{2\mu} \quad (\mu, a, a_i$—integers, $\mu \geqslant 2, \ a \neq 0)$

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

$$\sqrt{f(n)} = u_0(n) + \overline{\frac{1}{|u_1(n)|} + \frac{1}{|u_2(n)|} + \ldots + \frac{1}{|u_K(n)|}} \tag{2}$$

(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_1 and the theory of Abelian integrals was already established by Abel [1], who also proved that the answer to P_1 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 $\frac{X}{Y}(\infty) = \infty$, then $\frac{X}{Y}$ is necessarily equal to one of the reducts 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 $[b_0(n), b_1(n), \ldots]$ the expansion of $\sqrt{f(n)}$ into an arithmetic continued fraction, by $A_i(n)/B_i(n)$ the corresponding reducts. Besides, I shall put $\mathrm{LP}\sqrt{f} = K$ if K is the smallest number $\geqslant 0$ for which (2) holds, and $\mathrm{LP}\sqrt{f} = \infty$ 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

$$T_{-1} = 1\,, \quad T_0 = u_0\,, \quad T_\nu = u_\nu T_{\nu-1} + T_{\nu-2}\,,$$
$$U_{-1} = 0\,, \quad U_0 = 1\,, \quad U_\nu = u_\nu U_{\nu-1} + U_{\nu-2}\,.$$

$[q]$ and (q) will denote the integral and the fractional part of q, respectively, $\Phi_n(x)$—the n-th cyclotomic polynomial.

§ 2. LEMMA 1. *For every polynomial f of form* (1) *which is not a perfect square and every $k \geqslant 0$ there exists a finite set of s_k systems of polynomials with rational coefficients $[b_0^{(j)}, b_1^{(j)}, \ldots, b_k^{(j)}]$ $(1 \leqslant j \leqslant s_k)$ such that integers $> n_0(k)$ can be divided into s_k classes $K_1, K_2, \ldots, K_{s_k}$ so that if $n \in K_j$ then $b_i(n) = b_i^{(j)}(n)$ $(0 \leqslant i \leqslant k,\ 1 \leqslant j \leqslant s_k)$.*

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 $b_{-1}(n) = 0$ and no division into classes is necessary. Suppose now that the theorem is proved for $k-1$ $(k \geqslant 0)$, and let $K_1, K_2, \ldots, K_s$ be corresponding classes and $[b_0^{(j)}, b_1^{(j)}, \ldots, b_{k-1}^{(j)}]$ $(j \leqslant s)$ corresponding systems of polynomials. For $n \in K_j$ we have

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

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

$$\frac{\sqrt{f(n)} + r(n)}{s(n)} = q(n) + \varrho(n)\,,$$

where $q(n)$ is a polynomial with rational coefficients, $\varrho(n) = o(1)$ and, for sufficiently large n, $\varrho(n)$ has a fixed sign. Therefore for $n > n_0(k)$

$$b_k(n) = \begin{cases} q(n) - 1 & \text{if } q(n) \text{ is integral and } \frac{1}{\varrho}(\infty) = -\infty\,, \\ [q(n)] & \text{otherwise}\,. \end{cases}$$

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

$$b_k^{(j,r)}(n) = \begin{cases} q(n) - 1 & \text{if } (q(r)) = 0 \text{ and } \frac{1}{\varrho}(\infty) = -\infty\,, \\ q(n) - (q(r)) & \text{otherwise}\,, \end{cases}$$

we have for $n \in K_j$, $n > n_0(k)$, $n \equiv r \pmod m$

$$b_k(n) = b_k^{(j,r)}(n)\,.$$

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

THEOREM 1. *If $\mathrm{LP}\sqrt{f} = \infty$, then $\overline{\lim}\,\mathrm{lp}\sqrt{f(n)} = \infty$.*

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

$$A_{-1,j}(n) = 1\,, \quad A_{0,j}(n) = b_0^{(j)}(n)\,, \quad A_{i,j}(n) = b_i^{(j)}(n) A_{i-1,j}(n) + A_{i-2,j}(n)\,,$$

(3)

$$B_{-1,j}(n) = 0\,, \quad B_{0,j}(n) = 1\,, \quad B_{i,j}(n) = b_i^{(j)}(n) B_{i-1,j}(n) + B_{i-2,j}(n)\,.$$

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

$$A_{i,j}^2(n) - f(n) B_{i,j}^2(n) = \text{const}\,.$$

It follows that if $n > n_1(k)$, we have for all $i \leqslant k$, $j \leqslant s_k$:

$$A_{i,j}^2(n) - f(n) B_{i,j}^2(n) \neq \pm 1\,.$$

On the other hand, by Lemma 1, for $n > n_0(k)$, $b_i(n) = b_i^{(j)}(n)$ for some $j \leqslant s_k$ and all $i \leqslant k$, and thus $A_i(n) = A_{i,j}(n)$ and $B_i(n) = B_{i,j}(n)$. The last inequality implies therefore that for all $n > \max(n_0(k), n_1(k))$

$$A_i^2(n) - f(n) B_i^2(n) \neq \pm 1 \quad (0 \leqslant i \leqslant k)\,,$$

whence $\mathrm{lp}\sqrt{f(n)} > k$.

LEMMA 2. *If $R(n)$ is any rational function with rational coefficients, then*

$$\overline{\lim}\,\mathrm{lap}\,R(n) < \infty\,.$$

Proof. We shall prove it by induction with respect to the degree d of the denominator of $R(n)$ in its irreducible from. 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

$$\operatorname{lap} R(n) \leqslant \max_{0 \leqslant r < m} \operatorname{lap} R(r) .$$

Suppose now that the lemma is valid for all rational functions with denominators of degree $< d$ and let $R(n) = P(n)/Q(n)$ where P, Q are polynomials and the degree of Q is equal to d. We have

$$R(n) = q(n) + \frac{r(n)}{Q(n)} ,$$

where q, r are polynomials and r is of degree $< d$. Putting $q(n) = q_1(n)/m$, where $q_1(n)$ is a polynomial with integral coefficients and m is an integer, we have for $n \equiv r \pmod m$

$$\operatorname{lap} R(n) = \operatorname{lap}\left(\frac{q_1(r)}{m} + \frac{r(n)}{Q(n)}\right) = \operatorname{lap}\left(\frac{q_1(r)\,\xi(n) + m}{m\xi(n)}\right) ,$$

where $\xi(n) = Q(n)/r(n)$. Since by the inductive assumption: $\overline{\lim}\operatorname{lap}\xi(n) < \infty$, it follows immediately from Theorem 1 [5] that $\overline{\lim}\operatorname{lap} R(n) < \infty$, which completes the proof.

THEOREM 2. *If* $\operatorname{LP}\sqrt{f} = K > 0$ *and*

$$\sqrt{f} = u_0 + \cfrac{1}{|u_1| + \cfrac{1}{|u_2| + \ldots + \cfrac{1}{|u_K|}}} ,$$

denote by E *the set of all integers* n *such that* $2\,T_{K-1}(n)$ *is integral, and by* CE *its complement. Then*

$$\lim_{\substack{n\to\infty \\ n \in CE}} \operatorname{lp}\sqrt{f(n)} = \infty , \tag{4}$$

$$\overline{\lim_{\substack{n\to\infty \\ n \in E}}} \operatorname{lp}\sqrt{f(n)} < \infty . \tag{5}$$

Proof. We begin with a proof of equation (4). Let k be an arbitrary integer > 0, and define K_j, $A_{i,j}(n)$, $B_{i,j}(n)$ $(0 \leqslant i \leqslant k,\ 0 \leqslant j \leqslant s_k)$ as in the proof of Theorem 1. Suppose that for some i, j we have $K_j CE \neq 0$ and identically

$$A_{i,j}^2(n) - f(n) B_{i,j}^2(n) = \pm 1 .$$

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 l and suitably chosen signs, identically

$$\pm A_{i,j}(n) \pm \sqrt{f(n)}\, B_{i,j}(n) = T_{lK-1} + \sqrt{f(n)}\, U_{lK-1} = \left(T_{K-1} + \sqrt{f(n)}\, U_{K-1}\right)^l$$

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

Now let $n_0 \in K_j CE$. Since $n_0 \in K_j$, $\sqrt{f(n_0)}$ is irrational; $A_{i,j}(n_0) = A_i(n_0)$, $B_{i,j}(n_0) = B_i(n_0)$ are integers, whence $\pm A_{i,j}(n_0) \pm \sqrt{f(n_0)}\, B_{i,j}(n_0)$ is an integer of the field $K\left(\sqrt{f(n_0)}\right)$. On the other hand, since $2\,T_{K-1}(n_0)$ is not a rational integer, $T_{K-1}(n_0) + \sqrt{f(n_0)}\, U_{K-1}(n_0)$ and therefore also $\left(T_{K-1}(n_0) + \sqrt{f(n_0)}\, U_{K-1}(n_0)\right)^l$ cannot be an integer of the field $K\left(\sqrt{f(n_0)}\right)$.

The contradiction obtained proves that for all j such that $K_j CE \neq 0$, and all $i \leqslant k$.

$$A_{i,j}^2(n) - f(n) B_{i,j}^2(n) = \pm 1$$

does not hold identically. There exists therefore a number $n_1(k)$ such that for all $n > n_1(k)$

$$A_{i,j}^2(n) - f(n) B_{i,j}^2(n) \neq \pm 1 .$$

Thus if $n > \max\left(n_0(k), n_1(k)\right)$, $n \in CE$, then

$$A_i^2(n) - f(n) B_i^2(n) \neq \pm 1$$

for all $i \leqslant k$, whence $\operatorname{lp}\sqrt{f(n)} > k$, 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

$$\frac{T_{lK-1}}{U_{lK-1}} , \quad \frac{T_{3lK-1}}{U_{3lK-1}} \qquad (l = 1, 2, \ldots, m^2) .$$

By Lemma 2, there exists a number M such that for all $i \leqslant 3m^2$

$$\operatorname{lap}\varepsilon \frac{T_{iK-1}(n)}{U_{iK-1}(n)} \leqslant M \qquad (\varepsilon = 1 \text{ or } -1) .$$

We shall prove (5) by showing that for all $n \in E$

$$\operatorname{lp}\sqrt{f(n)} \leqslant M + 2 .$$

In fact, if $n \in E$, $2\,T_{K-1}(n)$ is an integer. If $T_{K-1}(n)$ is itself an integer, then it follows from the equation

$$T_{K-1}^2 - f(n)\, U_{K-1}^2 = (-1)^K$$

that $f(n)\, U_{K-1}^2(n)$ is also an integer. Therefore if $m_n | m$ is the denominator of $U_{K-1}(n)$ represented as an irreducible fraction, the number $f(n)/m_n^2$ must be integral. The equation

$$T_{lK-1}(n) + \sqrt{\frac{f(n)}{m_n^2}}\, m_n U_{lK-1}(n) = \left(T_{K-1}(n) + \sqrt{\frac{f(n)}{m_n^2}}\, m_n U_{K-1}(n)\right)^l$$

implies that $T_{lK-1}(n)$ and $m_n U_{lK-1}(n)$ are integers and, *a fortiori*, $T_{lK-1}(n)$ and $m U_{lK-1}(n)$ are integers.

Consider therefore all systems $(T_{lK-1}(n), mU_{lK-1}(n))$ reduced mod m. Since the number of all systems (a, b) different mod m is m^2, we have for some $1 \leqslant i < j \leqslant m^2+1$

$$T_{iK-1}(n) \equiv T_{jK-1}(n) \pmod m,$$
$$mU_{iK-1}(n) \equiv mU_{jK-1}(n) \pmod m.$$

Hence

$$T_{K(j-i)-1}(n)+\sqrt{f(n)}\,U_{K(j-i)-1} = \left(T_{Kj-1}(n)T_{Ki-1}(n)-f(n)\,U_{Kj-1}U_{Ki-1}\right)+$$
$$+\frac{\sqrt{f(n)}}{m}\left(T_{Kj-1}mU_{Kj-1}-T_{Ki-1}mU_{Kj-1}\right).$$

Since

$$T_{Kj-1}mU_{Ki-1}-T_{Ki-1}mU_{Kj-1} \equiv 0 \pmod m,$$

the number $U_{K(j-i)-1}$ is an integer.

Since the numbers $T_{K(j-i)-1}(n)$ and $U_{K(j-i)-1}(n)$ form an integral solution of the equation

$$x^2-f(n)y^2 = \pm 1,$$

the number $\left|\frac{T_{K(j-i)-1}(n)}{U_{K(j-i)-1}(n)}\right|$ must be a reduct of the arithmetic continued fraction for $\sqrt{f(n)}$, and if $\operatorname{lp}\sqrt{f(n)} = k$, we must have

$$\left|\frac{T_{K(j-i)-1}(n)}{U_{K(j-i)-1}(n)}\right| = \frac{A_{kt-1}}{B_{kt-1}},$$

whence

$$k \leqslant kt \leqslant \operatorname{lap}\left|\frac{T_{K(j-i)-1}(n)}{U_{K(j-i)-1}(n)}\right|+2 \leqslant M+2.$$

If $2T_{K-1}(n)$ is an integer but $T_{K-1}(n)$ is not, then it is evident from the formula

$$T_{3K-1} = T_{K-1}\left(4T_{K-1}^2-3(-1)^K\right)$$

that $T_{3K-1}(n)$ is an integer. *Mutatis mutandis*, the whole previous argument applies.

Theorem 2 immediately implies

THEOREM 3. *If* $\operatorname{LP}\sqrt{f} = K < \infty$ *and formula* (2) *holds, then* $\lim \operatorname{lp}\sqrt{f(n)} < \infty$ *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.

§ 3. THEOREM 4. *If* $f(x) = g^2(x)h(x)$ *where* $h(x)$ *has no multiple roots, then* $\operatorname{LP}\sqrt{f} < \infty$ *implies* $\operatorname{LP}\sqrt{h} < \infty$. *Furthermore, if* $g(x) = g_1^{a_1}(x)g_2^{a_2}(x)\dots g_s^{a_s}(x)$, *where* g_i *are distinct irreducible polynomials of degree* γ_i *respectively,* $\operatorname{LP}\sqrt{h} < \infty$ *and* T, U *is the fundamental solution of the Pell equation*

$$X^2-h(x)Y^2 = 1, \tag{6}$$

then $\operatorname{LP}\sqrt{f} < \infty$ *if and only if for each* $i \leqslant s$ *we have*

(i) $U \equiv 0 \pmod{g_i^{a_i}}$ *if* $g_i \mid hU$,

(ii) $\prod_{g_i(r)=0} [x^2-2T(r)x+1] = \Phi_n(x)^{2\gamma_i/\varphi(n)}$ *for some* n *satisfying* $\varphi(n) \mid 2\gamma_i$

and $T' \equiv 0 \pmod{g_i^{a_i-1}}$ *if* $g_i \nmid hU$.

Proof. If polynomials X_0, Y_0 satisfy the equation

$$X^2-f(x)Y^2 = 1, \tag{7}$$

then polynomials X_0, $g(x)Y_0$ satisfy equation (6) and thus $\operatorname{LP}\sqrt{f} < \infty$ implies $\operatorname{LP}\sqrt{h} < \infty$.

In order to prove that conditions (i)-(ii) are necessary, let us observe that for some l and suitably chosen signs we must have

$$\pm X_0 \pm \sqrt{h}gY_0 = \left(T+\sqrt{h}U\right)^l. \tag{8}$$

If $g_i \mid hU$, we have $(T, g_i) = 1$ because polynomials T, U satisfy (6). On the other hand,

$$\pm gY_0 = \sum_{i \geqslant 0} \binom{l}{2i+1} T^{l-2i-1}h^iU^{2i+1},$$

and thus g_i divides gY_0 in exactly the same power as it divides lT^lU. Hence condition (i).

If $g_i \nmid hU$, let r be any of the roots of g_i. Since polynomials X_0, Y_0 satisfy (7),

$$X_0^2 \equiv 1 \left(\bmod (x-r)^{2a_i}\right),$$

whence for some $\varepsilon = \pm 1$ we have

$$X_0 \equiv \varepsilon \left(\bmod (x-r)^{a_i}\right). \tag{9}$$

From (8) and (9) it follows first of all that $T(r)+\sqrt{h(r)}\,U(r) = \zeta$ satisfies the cyclotomic equation $\Phi_n(x) = 0$ for some $n \mid 2l$. Since $T^2-hU^2 = 1$, $T(r)-\sqrt{h(r)}\,U(r) = \zeta^{-1}$ satisfies the same equation. Therefore

$$(x-\zeta)(x-\zeta^{-1}) = x^2-2T(r)x+1 \mid \Phi_n(x)$$

and the same divisibility holds for each root r of g_i. Since both polynomials g_i and Φ_n are irreducible, $\prod_{g_i(r)=0} \left(x^2-2T(r)x+1\right)$ must be a power of $\Phi_n(x)$.

By comparing the degrees we obtain

$$\prod_{\substack{r\\ g_i(r)=0}} (x^2-2T(r)x+1) = \Phi_n(x)^{2\gamma_i/\varphi(n)},$$

i.e. the first part of condition (ii).

Further it follows from (9) that

$$X_0^{(j)}(r) = 0 \quad (j = 1, 2, \ldots, 2\alpha_i-1),$$

and since $g^{(j)}(r) = 0$ $(j = 1, 2, \ldots, \alpha_i-1)$, $h(r) \neq 0$, we have

$$\left[\frac{d^j}{dx^j}\left(\pm X_0(x) \pm \sqrt{h(x)}\, g(x)\, Y_0(x)\right)\right]_{x=r} = 0 \quad (j = 1, 2, \ldots, \alpha_i-1).$$

It follows from (8) by easy induction that

$$\left[\frac{d^j}{dx^j}\left(T(x)+\sqrt{h(x)}\, U(x)\right)\right]_{x=r} = 0 \quad (j = 1, 2, \ldots, \alpha_i-1),$$

and hence $T^{(j)}r) = 0$ $(j = 1, 2, \ldots, \alpha_i-1)$, i.e.

$$T'(x) \equiv 0 \pmod{(x-r)^{\alpha_i-1}}.$$

Since the last divisibility holds for each root r of g_i, we have

$$T' \equiv 0 \pmod{g_i^{\alpha_i-1}},$$

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 $g_i \nmid hU$, denote by $n(i)$ the index of the cyclotomic polynomial that occurs in condition (ii) and let m be the least common multiple of all numbers $n(i)$. Define polynomials V, W by the identity

$$V+\sqrt{h}W = (T+\sqrt{h}U)^m. \tag{10}$$

In view of (ii) we have for each root r of $g_i \nmid hU$

$$\left(T(r) \pm \sqrt{h(r)}\, U(r)\right)^{n(i)} = 1,$$

and thus for each root of each $g_i \nmid hU$:

$$V(r) \pm \sqrt{h(r)}\, W(r) = 1, \qquad W(r) = 0$$

and

$$W(x) \equiv 0 \pmod{\prod_{g_i \nmid hU} g_i}. \tag{11}$$

Now since for all $g_i \nmid hU$, $T' \equiv 0 \pmod{g_i^{\alpha_i-1}}$, we have $T^{(j)}(r) = 0$ for each root r of g_i $(g_i \nmid hU$, $1 \leqslant j \leqslant \alpha_i-1)$. This, in view of $T^2-hU^2 = 1$, gives also

$$\left[\frac{d^j}{dx^j}\left(h(x)\, U^2(x)\right)\right]_{x=r} = 0 \quad (j = 1, 2, \ldots, \alpha_i-1),$$

and since $h(r)\, U(r) \neq 0$,

$$\left[\frac{d^j}{dx^j}\left(\sqrt{h(x)}\, U(x)\right)\right]_{x=r} = 0 \quad (j = 1, 2, \ldots, \alpha_i-1).$$

By identity (10) we get

$$\left[\frac{d^j}{dx^j}\left(\sqrt{h(x)}\, W(x)\right)\right]_{x=r} = 0 \quad (j = 1, 2, \ldots, \alpha_i-1),$$

which, in view of (11) and since $h(r) \neq 0$, gives

$$W(x) \equiv 0 \pmod{\prod_{g_i \nmid hU} g_i^{\alpha_i}}.$$

On the other hand, it follows from condition (i) and identity (10) that

$$W(x) \equiv 0 \pmod{\prod_{g_i \mid hU} g_i^{\alpha_i}},$$

so that $W(x) \equiv 0 \pmod{g(x)}$ and equation (7) has the solution $V(x)$, $W(x)/g(x)$, which completes the proof.

COROLLARY. *If* $h \neq 0$, $\mathrm{LP}(x-a)\sqrt{x^2-h} < \infty$ *holds if and only if* $a = 0$ *or* $h = \frac{4}{3}a^2$, $2a^2$ *or* $4a^2$.

Proof. We have here $T(x) = 1-\dfrac{2x^2}{h}$, $U(x) = -2x/h$. Conditions (i)-(ii) take the shape

$$h \neq a^2$$

and

$$a = 0 \quad \text{or} \quad x^2-2\left(1-\frac{2a^2}{h}\right)x+1 = \Phi_1^2(x),\ \Phi_2^2(x) \quad \text{or} \quad \Phi_3(x),\ \Phi_4(x),\ \Phi_6(x).$$

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

§ 4. Now we shall make some remarks about problem P_1 in the really important case where the polynomial f has no multiple factors. Suppose that $\mathrm{LP}\sqrt{f} = K$ and (2) holds, so that

$$T_{K-1}^2 - f(x)\, U_{K-1}^2 = (-1)^K,$$

and let T_{K-1} be of degree λ.

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

$$\lambda\int_A^{P_2} w\,dx-\lambda\int_A^{P_1} w\,dx=\text{a period},$$

where $\int w\,dx$ 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

$$\lambda\int_{P_1}^{P_2} w\,dx=\text{a period},$$

which means that

If $\mathrm{LP}\sqrt{f}<\infty$, *then the value of* $\int_{P_1}^{P_2} w\,dx$ *is commensurable with the periods of the integral* $\int w\,dx$, *w 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. 592). Furthermore, if r is the smallest integer such that

$$r\int_{P_1}^{P_2}\frac{dx}{\sqrt{f(x)}}=\text{a period},$$

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

$$T_{r-2}^2(x)-f(x)U_{r-2}^2(x)=\mathrm{C}=\text{const}$$

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

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 $\int_{P_1}^{P_2}\frac{dx}{\sqrt{f(x)}}$ 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

$$f(x)=x^4+6a_2x^2+4a_3x+a_4.$$

According to Halphen ([2], Vol. I, p. 120 and Vol. II, p. 591),

$$r\int_{P_1}^{P_2}\frac{dx}{\sqrt{f(x)}}=\text{a period}$$

if and only if

$$rv=\text{a period},$$

where if $\wp$ is the function of Weierstrass,

$$g_2=3a_2^2+a_4,\quad g_3=a_2a_4-a_2^3-a_3^2;\quad \wp(v;g_2,g_3)=-a_2,\quad \wp'(v;g_1,g_3)=a_3.$$

This means that the point $(-a_2, a_3)$ is exceptional of the order r on the cubic $y^2=4x^3-g_2x-g_3$. Now, a method has been given by T. Nagell [3] which permits us not only to decide whether a given point is exceptional or not but also to find all exceptional points on a given cubic of Weierstrass. This method seems to work more rapidly than the method of Tchebicheff, however, it is noteworthy that, with the use of completely different terminology, the first problem concerning exceptional points mentioned above was already solved by Tchebicheff.

From known results regarding exceptional points further conclusions may be drawn regarding the functional $\mathrm{LP}\sqrt{f}$, f of degree 4. It follows in particular that $\mathrm{LP}\sqrt{f}$ can take the values 1, 2, 3, 4, 6, 8, 10, 14, 18, 22 and possibly also 5, 7, 9, 11 (I have not verified this) and, if the conjecture of Nagell [4] is true, no other values.

For polynomials f of degree >4 I do not know any method which would always lead to the solution of problem P_1. However, the following rule solves the problem for almost all (in an adequate sense) polynomials f.

If $\mathrm{LP}\sqrt{f}<\infty$, *then* f *is reducible in a certain quadratic field.*

The proof given below does not differ essentially from Tchebicheff's proof [7] of an analogous theorem for polynomials f of degree 4.

Suppose that $\mathrm{LP}\sqrt{f}<\infty$, (2) holds and s is the smallest integer $\geqslant 0$ such that

$$T_s^2-f(x)U_s^2=\mathrm{C}.$$

Since T_s, U_s have rational coefficients, C is rational. We have

$$f(x)U_s^2=T_s^2-\mathrm{C}=(T_s-\sqrt{\mathrm{C}})(T_s+\sqrt{\mathrm{C}}).$$

If $f(x)$ were irreducible in the field $K(\sqrt{\mathrm{C}})$, we should have

$$\text{(12)}\qquad \begin{aligned} &f(x)\mid T_s-\varepsilon\sqrt{\mathrm{C}}\quad(\varepsilon=1\text{ or }-1),\quad\text{whence}\\ &T_s-\varepsilon\sqrt{\mathrm{C}}=f(x)W^2,\quad T_s+\varepsilon\sqrt{\mathrm{C}}=V^2\quad\text{and}\\ &V^2-f(x)W^2=2\varepsilon\sqrt{\mathrm{C}}. \end{aligned}$$

In virtue of the theorem quoted in § 1, one of the fractions V/W and $-V/W$ must be a reduct of expansion (2), and thus we have, for some $r \geqslant 0$: $\pm V/W = T_r/U_r$,

$$T_r^2 - f U_r^2 = \text{const},$$

and the degree of T_r, equal to the degree of V, is less than the degree of T_s by (12). Since this is incompatible with the definition of s, $f(x)$ must be reducible in the field $K(\sqrt{C})$, which completes the proof.

References

[1] N. H. Abel, *Über die Integration der Differential-Formel $\varrho\,dx/\sqrt{R}$, wenn R und ϱ ganze Funktionen sind*, Journal f. d. r. u. a. Math. 1 (1826), pp. 185-221.

[2] G. H. Halphen, *Traité des fonctions elliptiques et de leurs applications*, Paris 1886-1891.

[3] T. Nagell, *Solution de quelques problèmes dans la théorie arithmétique des cubiques planes du premier genre*, Vid. Akad. Skrifter Oslo I, 1935, Nr. 1.

[4] — *Problems in the theory of exceptional points on plane cubics of genus one*, Den 11te Skandinaviske Matematikerkongress, Trondheim 1949, pp. 71-76.

[5] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, Acta Arithm. 6 (1961), pp. 393-413.

[6] H. Schmidt, *Zur Approximation und Kettenbruchentwicklung quadratischer Zahlen*, Math. Z. 52 (1950), pp. 168-192.

[7] P. Tchebicheff, *Sur l'intégration des différentielles qui contiennent une racine carrée d'un polynome du troisième ou du quatrième degré*, Journal des math. pures et appl. (2) 2 (1857), pp. 1-42.

[8] — *Sur l'integration de la differentielle* $\dfrac{x+A}{\sqrt{x^4+\alpha x^3+\beta x^2+\gamma x+\delta}}\,dx$, Journal des math. pures et appl. (2) 9 (1864), pp. 225-246.

[9] G. Zolotareff, *Sur la méthode d'intégration de M. Tchebicheff*, Journal des math. pures et appl. (2) 19 (1874), pp. 161-188.

Reçu par la Rédaction le 7. 10. 1961

ACTA ARITHMETICA
VII (1962)

Über die Normalität von Zahlen zu verschiedenen Basen

von

WOLFGANG M. SCHMIDT (New York)

1. Einleitung. Cassels [1] zeigte die Existenz reeller Zahlen, die zwar nicht zur Basis 3, jedoch zu jeder Basis r normal sind, die keine Potenz von 3 ist. Unabhängig davon bewies der Author [2] kurz darauf: *Normalität zur Basis r impliziert Normalität zur Basis s genau dann, wenn s rationale Potenz von r ist.* Wir bezeichnen daher natürliche Zahlen r, s äquivalent und setzen $r \sim s$, falls jede der beiden Zahlen rationale Potenz der anderen ist. In dieser Arbeit beweisen wir den folgenden

SATZ. *Gegeben sei eine Einteilung der Zahlen $2, 3, \ldots$ in zwei fremde Klassen R, S derart, daß äquivalente Zahlen in dieselbe Klasse fallen. Dann gibt es reelle Zahlen, die normal zu jeder Basis aus R und anormal zu jeder Basis aus S sind.*

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 $M(R, S)$ dieser Zahlen die Mächtigkeit $\mathfrak{c}$ des Kontinuums hat. Da die Menge der Klasseneinteilungen R, S ebenfalls kontinuierliche Mächtigkeit hat, ergibt dies eine nette (freilich komplizierte!) Illustration der Gleichung $\mathfrak{c} \cdot \mathfrak{c} = \mathfrak{c}$.

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 $[\nu]$ für die ganze Zahl n, die $n \leqslant \nu < n+1$ leistet, und $\{\nu\}$ für $-[-\nu]$. In diesem Abschnitt sind r, s feste ganze Zahlen größer als 1, die $r \not\sim s$ erfüllen, und $\alpha_1, \alpha_2, \ldots$ sind positive Konstanten, die nur von r und s abhängen.

Sind

$$r = p_1^{d_1} \ldots p_h^{d_h}, \quad s = p_1^{e_1} \ldots p_h^{e_h} \quad (d_i + e_i \neq 0)$$

die Primzerlegungen von r und s, dann dürfen wir

$$d_1/e_1 \geqslant \ldots \geqslant d_h/e_h$$