COLLOQUIUM MATHEMATICUM

VOL. 98 2003 NO. 2

TOWARDS BAUER'S THEOREM FOR LINEAR RECURRENCE SEQUENCES

BY

MARIUSZ SKAŁBA (Warszawa)

Abstract. Consider a recurrence sequence $(x_k)_{k\in\mathbb{Z}}$ of integers satisfying $x_{k+n} = a_{n-1}x_{k+n-1}+\ldots+a_1x_{k+1}+a_0x_k$, where $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ are fixed and $a_0 \in \{-1, 1\}$. Assume that $x_k > 0$ for all sufficiently large k. If there exists $k_0 \in \mathbb{Z}$ such that $x_{k_0} < 0$ then for each negative integer $-D$ there exist infinitely many rational primes q such that $q \mid x_k$ for some $k \in \mathbb{N}$ and $(\frac{-D}{q}) = -1$.

Let $P(K)$ denote the set of those rational primes which have a prime ideal factor of the first degree in the algebraic number field K. A classical theorem of M. Bauer [1] states that:

If K is normal, then $P(\Omega) \subset P(K)$ implies $\Omega \supset K$.

This can be reformulated in the language of polynomial congruences ([3]). For instance, take $K = \mathbb{Q}(\sqrt{-D})$, a quadratic imaginary field, and $f(x) \in \mathbb{Q}[x]$, a monic irreducible polynomial taking negative values. If $\Omega = \mathbb{Q}(\alpha)$, where $\alpha \in \mathbb{R}$ and $f(\alpha) = 0$, then $K \not\subset \Omega$, and the above theorem of Bauer has the following corollary:

There exist infinitely many rational prime numbers q such that $q \mid f(x)$ for some $x \in \mathbb{Z}$ and $(\frac{-D}{q}) = -1$ (cf. also [5, pp. 168–169]).

The main goal of the present paper is the proof of the following theorem:

THEOREM. *Let $(x_k)_{k\in\mathbb{Z}}$ be a recurrence sequence of integers which satisfies the relation*

$$x_{k+n} = a_{n-1}x_{k+n-1} + a_{n-2}x_{k+n-2} + \ldots + a_1x_{k+1} + a_0x_k, \tag{1}$$

where $a_0, a_1, \ldots, a_{n-1} \in \mathbb{Z}$ are fixed and $a_0 \in \{-1, 1\}$. Assume further that $x_k > 0$ for all sufficiently large k. If there exists $k_0 \in \mathbb{Z}$ such that $x_{k_0} < 0$ then for each negative integer $-D$ there exist infinitely many rational primes q such that $q \mid x_k$ for some $k \in \mathbb{N}$ and $\left(\frac{-D}{q}\right) = -1$.

The set of recurrence sequences to which the above theorem applies contains all polynomials because the condition $a_0 \in \{-1, 1\}$ is fulfilled for polynomials in a trivial way. Hence the above theorem is the extension of

2000 *Mathematics Subject Classification*: 11A05, 11A41, 11B37.

a restricted version of Bauer's theorem (restricted to quadratic imaginary fields K) to a wider class of linear recurrence sequences.

The next result is of a very technical nature, but the proof of the Theorem relies heavily on it.

LEMMA. *Assume that a recurrence sequence $(x_k)_{k\in\mathbb{Z}}$ of rational numbers satisfies* (1), *where $a_j \in \mathbb{Z}$, $a_0 \neq 0$. Let there be given s positive definite binary quadratic forms $f_j(x,y) = c_j x^2 + b_j y^2$, where c_j, b_j are squarefree natural numbers for $j = 1, \ldots, s$. Assume that there exists $k_0 \in \mathbb{Z}$ such that $x_{k_0} < 0$ and for each rational prime p the following implication holds*:

$$p \mid a_0 \ \Rightarrow\ \left(\frac{c_j}{x_{k_0}}, \frac{b_j}{x_{k_0}}\right)_p = 1 \text{ for } j = 1, \ldots, s, \tag{2}$$

where $(\ ,\ )_p$ is the p-adic Hilbert symbol. Then there exists a natural number M such that for each $l \geq 0$,

$$x_{k_0+lM} \neq f_j(x,y)$$

for all $j = 1, \ldots, s$ and $x, y \in \mathbb{Q}$.

Proof of Lemma. By the quadratic reciprocity law in Hilbert's form,

$$\prod_{p\in P\cup\{\infty\}} \left(\frac{c_j}{x_{k_0}}, \frac{b_j}{x_{k_0}}\right)_p = 1$$

for each $j = 1, \ldots, s$. Since $x_{k_0} < 0$ we obtain

$$\left(\frac{c_j}{x_{k_0}}, \frac{b_j}{x_{k_0}}\right)_\infty = -1$$

and therefore there exist $p_j \in P$ such that

$$\left(\frac{c_j}{x_{k_0}}, \frac{b_j}{x_{k_0}}\right)_{p_j} = -1, \qquad j = 1, \ldots, s. \tag{3}$$

By the assumption (2) we obtain

$$\gcd(p_1 \ldots p_s, a_0) = 1. \tag{4}$$

This implies that for each $j = 1, \ldots, s$ and any natural number t, the sequence $(x_k \bmod p_j^t)$ is periodic (say, by "prolonging-to-the-left" reasoning). Moreover, after multiplying (x_k) by a number of the form $p_1^{2l_1} p_2^{2l_2} \cdots p_s^{2l_s}$ we can assume that $0 \leq v_{p_j}(x_{k_0}) \leq 1$ for $j = 1, \ldots, s$. Let M_j be a period of $(x_k \bmod p_j^2)$ for $p_j \neq 2$, and of $(x_k \bmod 16)$ for $p_j = 2$. By the well known calculation rules for the Hilbert symbol ([2, Theorem 7 of Ch. 1]), from (3) we obtain

$$\left(\frac{c_j}{x_{k_0+lM_j}}, \frac{b_j}{x_{k_0+lM_j}}\right)_{p_j} = -1$$

for $j = 1, \dots, s$ and any $l \geq 0$. Now we put $M = \prod_{j=1}^{s} M_j$ and the assertion follows.

Proof of Theorem. Without loss of generality we restrict ourselves to fundamental discriminants $-D$. Let

$$f_j(x, y) = c_j x^2 + b_j y^2, \quad c_j, b_j \in \mathbb{N} \text{ squarefree}, \ j = 1, \dots, s,$$

represent all equivalence classes of primitive integral positive definite binary quadratic forms of discriminant $-D$ over $\mathbb{Q}$ (by the Gauss theory of genera we can take $s = 2^{\omega(D)-1}$, but what we actually need is just $s < \infty$). We can apply the Lemma because the condition (2) is satisfied in a trivial way. Define

$$x_{k_0}^- = \prod_{q^a \| x_{k_0}, \, (\frac{-D}{q}) = -1} q^a, \quad \mathcal{N} = \prod_{q^a \| x_{k_0}, \, (\frac{-D}{q}) = -1} q^{a+1}$$

(in case $x_{k_0}^- = 1$ we put $\mathcal{N} = 1$ as well).

By periodicity there exists M_0 such that for $l \in \mathbb{Z}$,

$$x_{k_0 + lM_0} \equiv x_{k_0} \pmod{\mathcal{N}}.$$

Now, we define

$$\widetilde{x}_l = x_{k_0 + lM_0} / x_{k_0}^- \quad \text{for } l \in \mathbb{Z}.$$

The sequence $(\widetilde{x}_l)$ is also a recurrence sequence, consists of integers and satisfies $\widetilde{a}_0 \in \{-1, 1\}$ and $\widetilde{x}_0 < 0$. By the above construction,

$$q \in P \text{ and } \left(\frac{-D}{q}\right) = -1 \ \Rightarrow \ q \nmid \widetilde{x}_0. \tag{5}$$

Now, take any finite set Q of prime numbers q satisfying

$$\left(\frac{-D}{q}\right) = -1.$$

Let

$$\mathcal{M} = \prod_{q \in Q} q.$$

By periodicity there exists $S \in \mathbb{N}$ such that

$$\widetilde{x}_{lS} \equiv \widetilde{x}_0 \pmod{\mathcal{M}} \quad \text{for } l \in \mathbb{Z}.$$

Hence, by property (5),

$$\gcd(\widetilde{x}_{lS}, \mathcal{M}) = 1 \quad \text{for } l \in \mathbb{Z}. \tag{6}$$

If we define

$$\widetilde{\widetilde{x}}_l = \widetilde{x}_{lS}, \quad l \in \mathbb{Z},$$

then $(\widetilde{\widetilde{x}}_l)$ is again a recurrence sequence and it satisfies the assumptions of the Lemma. Hence there exists a natural number M such that for each $l \geq 0$,

$$\widetilde{\widetilde{x}}_{lM} \neq f_j(x, y)$$

for $j = 1, \ldots, s$, $x, y \in \mathbb{Q}$. Now take $l \geq 0$ such that $\widetilde{\widetilde{x}}_{lM} > 0$. By a classical theorem ([2, Theorem 3 of Ch. 3]) we obtain in particular

$$\exists q \in P,\ k \geq 0, \qquad \left(\frac{-D}{q}\right) = -1,\ q^{2k+1} \parallel \widetilde{\widetilde{x}}_{lM}.$$

By property (6) we infer that $q \notin Q$. So we have constructed a prime divisor q of $(x_k)_k$ with $\left(\frac{-D}{q}\right) = -1$, lying outside a given finite set of such primes. The proof of the Theorem is finished.

Now, we deduce a corollary which states in part (ii) that in the case of linear recurrence sequences of the second order the assumption that $x_{k_0} < 0$ for some $k_0 \in \mathbb{Z}$ is crucial.

COROLLARY 1. *Let $(x_k)_{k\in\mathbb{Z}}$ be a non-constant recurrence sequence of integers satisfying*

$$x_{k+2} = a_1 x_{k+1} + a_0 x_k, \qquad k \in \mathbb{Z},$$

where $a_0, a_1 \in \mathbb{Z}$, $a_0 \in \{-1, 1\}$ and $x_k > 0$ for k sufficiently large.

(i) *If there exists $k_0 \in \mathbb{Z}$ such that $x_{k_0} < 0$ then for each negative integer $-D$ there exist infinitely many rational primes q such that $q \mid x_k$ for some $k \in \mathbb{N}$ and $\left(\frac{-D}{q}\right) = -1$.*

(ii) *If $x_k > 0$ for each $k \in \mathbb{Z}$ then there exists a negative integer $-D$ such that for each k and each prime p,*

$$p \mid x_k \ \Rightarrow\ \left(\frac{-D}{p}\right) = 1 \ \text{or}\ p \mid 2D.$$

Proof. Case (i) is an immediate consequence of the Theorem.

For the proof of (ii) assume that

$$x_k > 0 \quad \text{for each } k \in \mathbb{Z}. \tag{7}$$

It follows easily that

$$a_0 = -1, \qquad a_1 \geq 3. \tag{8}$$

For convenience of notation put $g = a_1$. Let us work with the explicit formula for x_k,

$$x_k = \alpha\gamma^k + \overline{\alpha}\,\overline{\gamma}^k,$$

where

$$\gamma = \frac{g + \sqrt{g^2 - 4}}{2} \in K := \mathbb{Q}(\sqrt{g^2 - 4}), \qquad \alpha \in K,$$

and the bar denotes the non-trivial automorphism of K. The property (7) forces that

$$\alpha > 0, \qquad \overline{\alpha} > 0. \tag{9}$$

Now, define $u_k, v_k \in \mathbb{Q}$ by

$$\frac{u_k + v_k\sqrt{g^2-4}}{2} = \gamma^k. \tag{10}$$

If we put $\alpha = \frac{h+j\sqrt{g^2-4}}{2}$ then

$$\begin{aligned} x_{2k} &= \operatorname{Tr}\left[\left(\frac{h+j\sqrt{g^2-4}}{2}\right)\left(\frac{u_k+v_k\sqrt{g^2-4}}{2}\right)^2\right] \\ &= \frac{h}{4}\,u_k^2 + \frac{j(g^2-4)}{2}\,u_kv_k + \frac{h(g^2-4)}{4}\,v_k^2. \end{aligned}$$

The binary quadratic form

$$f(x,y) = \frac{h}{4}\,x^2 + \frac{j(g^2-4)}{2}\,xy + \frac{h(g^2-4)}{4}\,y^2$$

is positive definite because by (9),

$$f(1,0) = \frac{h}{4} = \frac{1}{4}\operatorname{Tr}(\alpha) > 0,$$

$$\Delta_f = \frac{j^2(g^2-4)^2}{4} - \frac{h^2(g^2-4)}{4} = (4-g^2)N(\alpha) < 0.$$

Now define $-D = \Delta_f$. Then $-D$ is a negative integer and for each $k \in \mathbb{Z}$ and prime p we have

$$p \mid x_{2k} \;\Rightarrow\; f(u_k, v_k) \equiv 0 \pmod{p}.$$

In view of (10), $\gcd(u_k, v_k) \in \{1, 2\}$, hence

$$2 \neq p \mid x_{2k} \;\Rightarrow\; f(u_k/v_k, 1) = 0 \text{ or } f(1, v_k/u_k) = 0 \text{ in } F_p.$$

Hence the discriminant of the relevant quadratic trinomial ($f(x,1)$ or $f(1,x)$) must be a square in F_p, thus

$$\left(\frac{-D}{p}\right) = 1 \text{ or } p \mid D. \tag{11}$$

In a similar way

$$\begin{aligned} x_{2k+1} = {} & \operatorname{Tr}\left[\left(\frac{h+j\sqrt{g^2-4}}{2}\right)\left(\frac{g+\sqrt{g^2-4}}{2}\right)\left(\frac{u_k+v_k\sqrt{g^2-4}}{2}\right)^2\right] \\ &= g(u_k, v_k), \end{aligned}$$

where

$$\begin{aligned} g(x,y) = {} & \frac{hg+jg^2-4j}{8}\,x^2 + \frac{(h+gj)(g^2-4)}{4}\,xy \\ & + \frac{(hg+jg^2-4j)(g^2-4)}{8}\,y^2. \end{aligned}$$

In view of (8),

$$\gamma > 0, \qquad \overline{\gamma} > 0,$$

and therefore

$$\alpha' := \gamma\alpha > 0, \qquad \overline{\alpha'} > 0.$$

Hence $g(x,y)$ is positive definite for similar reasons as $f(x,y)$,

$$\Delta_g = (4-g^2)N(\alpha') = \Delta_f,$$

and the characterization (11) of odd prime divisors p of x_{2k+1} can be obtained in the same way as for prime divisors of x_{2k}, above.

The next corollary illustrates that our approach is more general than it seems to be—in many specific situations we can dispense with the assumption $a_0 \in \{-1,1\}$.

COROLLARY 2. *Let A,B be positive odd integers, $C = 2^c$ with $c \geq 1$, and consider the sequence $x_k = AC^k - B$. For each prime number $r \equiv 3 \pmod 4$ there exist infinitely many prime numbers q such that*

$$q \mid x_k \quad \textit{for some } k \quad \textit{and} \quad \left(\frac{-r}{q}\right) = -1$$

(*or equivalently $\left(\frac{q}{r}\right) = -1$, by the quadratic reciprocity law*).

Sketch of proof. The proof goes along the same lines as the proof of the Theorem. In order to apply the Lemma we now consider just one form $f_1(x,y) = x^2 + ry^2$. We will only verify that the assumption (2) of the Lemma is fulfilled. The unique prime divisor p of a_0 is $p = 2$. Hence, the verification of (2) will be brief. Choose $k_0 = -2l$ where $l > 0$ is such that $x_{k_0} < 0$. Then

$$\left(\frac{1}{x_{k_0}}, \frac{r}{x_{k_0}}\right)_2 = (x_{k_0}, -r)_2 = (A - BC^{2l}, -r)_2 = (-1)^{\frac{A-1}{2}\frac{-r-1}{2}} = 1.$$

As an immediate application of the above corollary we obtain for instance:

There exist infinitely many primes q such that $q \mid 4^x - 5$ for some $x \in \mathbb{N}$ and simultaneously $q \nmid 4^y + 7$ for each $y \in \mathbb{N}$.

But we have not been able to handle the following more general problem. What can be said about positive integers a,b,c,d, where $a,c > 1$, if for each prime number q, q divides a number of the form $a^x - b$ if and only if q divides a number of the form $c^y - d$?

Our method of proving the infinitude of relevant primes is in essence that of Euclid. Despite of this we venture to formulate

CONJECTURE. *Let g be an integer, $|g| \geq 3$ and consider a recurrence sequence $(x_k)_{k\in\mathbb{Z}}$ of integers satisfying*

$$x_{k+2} = gx_{k+1} - x_k, \qquad k \in \mathbb{Z}. \tag{12}$$

Assume that x_k *is a sum of two integral squares for all sufficiently large* k*. Then there exist two recurrence sequences* u_k, v_k *of integers such that* $x_k = u_k^2 + v_k^2$.

It seems doubtful that one can make real progress without any density results concerning prime divisors of linear recurrence sequences. The situation is much more satisfactory in the case of polynomials ([4], [6]).

Acknowledgments. This paper was presented at Prof. A. Schinzel's seminar. I want to thank him for giving me this opportunity. It has resulted in some improvements of presentation.

REFERENCES

[1] M. Bauer, *Zur Theorie der algebraischen Zahlkörper*, Math. Ann. 77 (1916), 353–356.
[2] Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Nauka, Moscow, 1985 (in Russian).
[3] J. Brillhart and I. Gerst, *On the prime divisors of polynomials*, Amer. Math. Monthly 78 (1971), 250–266.
[4] H. Davenport, D. J. Lewis and A. Schinzel, *Polynomials of certain special types*, Acta Arith. 9 (1964), 107–116.
[5] T. Nagell, *Introduction to Number Theory*, Almqvist & Wiksell, Stockholm, 1951.
[6] A. Schinzel, *On a theorem of Bauer and some of its applications*, *I*, *II*, Acta Arith. 11 (1966), 333–344; 22 (1973), 221–231.

Department of Mathematics, Computer Science and Mechanics
University of Warsaw
Banacha 2
02-097 Warszawa, Poland
E-mail: skalba@mimuw.edu.pl
skalba@impan.gov.pl

Received 16 June 2003 (4355)