COLLOQUIUM MATHEMATICUM
VOL. LIX 1990 FASC. 1

SCHINZEL'S CONJECTURE H AND DIVISIBILITY IN ABELIAN LINEAR RECURRING SEQUENCES

BY

F. MARKO (BRATISLAVA)

1. Many divisibility properties of special recurring sequences (such as the Fibonacci, Lucas, Lehmer sequences and others) are known, but little is known about divisibility properties in general linear recurring sequences.

One example of this is Perrin's question [6] and problems connected with it. The question is stated as follows:

Does there exist a composite index n with $a_n \equiv 0 \pmod{n}$ in the linear recurring sequence $\{a_n\}$ of integers defined by $a_{n+3} = a_{n+1} + a_n$ and the initial conditions $a_0 = 3$, $a_1 = 0$, $a_2 = 2$?

Plainly, if p is a prime, then $a_p \equiv 0 \pmod{p}$, and therefore the negative answer to this question yields a strong primality test. Unfortunately, Adams and Shanks [1] and independently Jakubec and Nemoga [3] proved that Perrin's question can be answered affirmatively. This fact was surely known sooner to many others but the only other reference we find is an unpublished work [4], kindly suggested by Professor Schinzel.

Although Perrin's question can be answered affirmatively, it is not clear whether there are infinitely many composite numbers satisfying the mentioned condition. From the point of view of primality testing it may be interesting to answer the question of the existence of infinitely many composite numbers satisfying simultaneously the conditions of the above type for a finite system of linear recurring sequences. We conjecture (**P 1379**) that the answer is affirmative for an arbitrary finite system of simple linear recurring sequences. This problem seems to be very difficult even for special sequences. However, we show that the answer to this question is affirmative provided that every sequence of the system is simple and Abelian and Conjecture H holds. Namely, we prove the following:

Let $\{a_n\}$ be a linear recurring sequence of integers and $g(x)$ be its characteristic polynomial. Suppose that $g(x)$ has only simple roots over Q and the splitting field of the polynomial $g(x)$ has an Abelian Galois group over Q. Schinzel's Conjecture H implies that there exist infinitely many composite integers n of the form $n = pq$, where p and q are primes, such that $a_{ns} \equiv a_s \pmod{n}$ holds for every nonnegative integer s.

The celebrated *Schinzel's Conjecture* H says:

If $f_1(x), \ldots, f_k(x)$ are irreducible polynomials with integral coefficients and positive leading coefficient such that the product $f_1(x)\ldots f_k(x)$ has no constant factor greater than 1, *then there exist infinitely many positive integers x for which $f_1(x), \ldots, f_k(x)$ are primes.*

We notice that Perrin's sequence $\{a_n\}$ does not satisfy our assumptions, hence we say nothing about it. However, Perrin's question was the motivation for our work.

2. A sequence $\{a_n\}$ of rational numbers will be called a *linear recurring sequence with characteristic polynomial*

$$g(x) = b_m x^m - b_{m-1}x^{m-1} - \ldots - b_0$$

if coefficients of $g(x)$ are rational integers and a_n's fulfil the relation

$$b_m a_{n+m} = b_{m-1}a_{n+m-1} + \ldots + b_0 a_n$$

for every nonnegative integer n. (It is natural to require that $b_0 \neq 0$.) If the polynomial $g(x)$ has only simple roots, then the linear recurring sequence $\{a_n\}$ will be called *simple.*

Let $\{a_n\}$ be a simple linear recurring sequence and $\alpha_1, \ldots, \alpha_m$ be roots of its characteristic polynomial $g(x)$. It is well known that the terms of the sequence $\{a_n\}$ can be written in the form

$$a_n = c_1\alpha_1^n + \ldots + c_m\alpha_m^n \tag{1}$$

for some $c_1, \ldots, c_m \in Q(\alpha_1, \ldots, \alpha_m)$. The numbers $c_1, \ldots, c_m$ are determined by the system of linear equations

$$\sum_{j=1}^{m} c_j\alpha_j^s = a_s, \quad \text{where } s = 0, \ldots, m-1.$$

Since $g(x)$ has only simple roots, the determinant D of this system is nonvanishing. Cramer's rule gives

$$c_j = d_j/D, \tag{2}$$

where d_j belongs to the field $Q(\alpha_1, \ldots, \alpha_m)$. Then for some integer e all numbers ed_j will be algebraic integers of the field $Q(\alpha_1, \ldots, \alpha_m)$. For further reasons fix one such e and set

$$E = eD. \tag{3}$$

Now let $g(x)$ be a monic integral polynomial with simple roots $\alpha_1, \ldots, \alpha_m$. The sequence $a_n = \alpha_1^n + \ldots + \alpha_m^n$ is a linear recurring sequence of integers. If p is a prime, then we have

$$a_{ps} = \alpha_1^{ps} + \ldots + \alpha_m^{ps} \equiv (\alpha_1^s + \ldots + \alpha_m^s)^p = a_s^p \equiv a_s \pmod{p}$$

for every nonnegative integer s.

The property $a_{ns} \equiv a_s \pmod{n}$ can be seen as a generalization of that given in Perrin's question (see [1]).

DEFINITION 1. Let $\{a_n\}$ be a simple linear recurring sequence. An integer n which satisfies the congruences $a_{ns} \equiv a_s \pmod{n}$ for every nonnegative integer s is called a *pseudoprime with respect to the sequence* $\{a_n\}$.

We restrict ourselves only to simple linear recurring sequences $\{a_n\}$, because in the other case there may exist only finitely many (even none) primes satisfying the congruences $a_{ns} \equiv a_s \pmod{n}$ for every nonnegative integer s.

The notion of pseudoprime with respect to simple linear recurring sequences is similar to that defined in [8].

At the present time one can find a lot of different definitions of pseudoprimes (see, e.g., [7]). Questions concerning pseudoprimes are important in some primality tests.

We remark that generally it is not true that every prime is a pseudoprime with respect to a simple linear recurring sequence. However, this is true for the special sequences of type $a_n = \alpha_1^n + \ldots + \alpha_m^n$ (as is the case considered in [1] and [3]).

The following lemma says that every prime which splits completely in the splitting field of the characteristic polynomial $g(x)$ of a simple linear recurring sequence $\{a_n\}$ is a pseudoprime with respect to $\{a_n\}$.

LEMMA 1. *Let $\{a_n\}$ be a simple linear recurring sequence and $\alpha_1, \ldots, \alpha_m$ be the roots of its characteristic polynomial $g(x)$. Then for E from* (3) *and every prime p coprime to E, which splits completely in $Q(\alpha_1, \ldots, \alpha_m)$, we have $a_{ps} \equiv a_s \pmod{p}$.*

Proof. Let k be the degree of the field $Q(\alpha_1, \ldots, \alpha_m)$ over Q. Then

$$p = \mathfrak{p}_1 \ldots \mathfrak{p}_k$$

for some prime ideals $\mathfrak{p}_i$ of degree 1 in $Q(\alpha_1, \ldots, \alpha_m)$.

From (1)–(3) we infer that every c_j belongs to the valuation ring of the ideal $\mathfrak{p}_l$ for $l = 1, \ldots, k$ because $(\mathfrak{p}_l, E) = 1$. For every l the residue field mod $\mathfrak{p}_l$ has p elements, and therefore

$$a_{ps} = c_1\alpha_1^{sp} + \ldots + c_m\alpha_m^{sp} \equiv (c_1\alpha_1^s + \ldots + c_m\alpha_m^s)^p$$

$$= (a_s)^p \equiv a_s \pmod{\mathfrak{p}_l} \quad \text{for every } l = 1, \ldots, k.$$

Hence $a_{ps} \equiv a_s \pmod{p}$.

Remark 1. According to the Tschebotarev theorem the set of primes which split completely in a given algebraic field of finite degree has positive Dirichlet density.

Perrin's question gives rise to the question of the existence of composite pseudoprimes with respect to various simple linear recurring sequences.

DEFINITION 2. A simple linear recurring sequence $\{a_n\}$ is called *Abelian* if the

Galois group of the splitting field of its characteristic polynomial $g(x)$ over Q is Abelian.

3. The aim of the paper is to prove the following theorem:

THEOREM. *Let* $\{a_n^i\}$, $i = 1, \ldots, r$, *be a finite system of linear recurring sequences. If every* $\{a_n^i\}$ *is simple and Abelian, then Conjecture* H *implies the existence of infinitely many common composite pseudoprimes with respect to every sequence* $\{a_n^i\}$, $i = 1, \ldots, r$.

First we prove the following lemma:

LEMMA 2. *Let* $g(x)$ *be the characteristic polynomial of a simple linear recurring sequence* $\{a_n\}$. *Then for some positive integer* M *and every positive integer* s *we have:*

If a prime $q \equiv 1 \pmod{Ms}$ *splits completely in the splitting field* L *of the polynomial* $g(x^{2^s})$, *then the period of the sequence* $\{a_n\} \bmod q$ *is a divisor of* $(q-1)/s$.

Proof. Decompose $g(x)$ into the product of two polynomials $g_1(x)$ and $g_2(x)$ such that the roots of $g_2(x)$ are just the roots of unity. It is clear that for some positive integer N the polynomial $g_2(x)$ divides $x^N - 1$. We claim that $M = 2NE$, where E is defined in (3), satisfies the requirement of the lemma.

In view of formula (1) it suffices to show that for every root α of $g(x)$ and every n one has

$$\alpha^{n+M} \equiv \alpha^n \pmod{q}.$$

For the roots of $g_2(x)$ this is obvious, so we may assume that α is a root of $g_1(x)$.

Write $s = 2^t v$, where v is odd. Let D be the greatest divisor of v such that there is some $\beta \in Q(\alpha)$ such that $\alpha = \beta^D$ and let 2^u be the greatest divisor of 2^t such that

$$\alpha^2 = \gamma^{2^{u+1}} \quad \text{for some } \gamma \in Q(\alpha)$$

(for finding D and u we may use the decomposition law of ideals or the Dirichlet theorem on units). Capelli's theorem (see Theorem 21 of [9]) implies that the polynomials $x^{v/D} - \beta$ and $x^{2^{t-u}} - \gamma$ are irreducible over $Q(\alpha)$ which contains both $Q(\beta)$ and $Q(\gamma)$.

Let $h_1(x)$ and $h_2(x)$ be minimal polynomials for β, resp. γ, over Q. Then another theorem of Capelli (see Theorem 20 of [9]) implies that

$$f_1(x) = h_1(x^{v/D}) \quad \text{and} \quad f_2(x) = h_2(x^{2^{t-u}})$$

are irreducible over Q.

For some root β_1 of $f_1(x)$ and γ_1 of $f_2(x)$ we have

$$\beta_1^{v/D} = \beta \quad \text{and} \quad \gamma_1^{2^{t-u}} = \gamma,$$

and hence

$$\beta_1^v = \beta^D = \alpha \quad \text{and} \quad \gamma_1^{2^{t+1}} = \gamma^{2^{u+1}} = \alpha^2.$$

Since β_1 and γ_1 belong to L and L is normal, it is clear that L contains the splitting fields of the polynomials $f_1(x)$ and $f_2(x)$. If q splits completely in L, then q splits completely in both latter fields, which means according to [2] (Theorem 3, Chapter IV, Section 2) that $f_1(x)$ and $f_2(x)$ decompose into distinct linear factors over the field Q_q of q-adic numbers.

Therefore β is a (v/D)-th power and γ is a 2^{t-u}-th power of integral elements from Q_q. (Here we use the fact that q is coprime to E.) Hence for some rational integers b and c we have

$$\beta \equiv b^{v/D} \pmod{q} \quad \text{and} \quad \gamma \equiv c^{2^{t-u}} \pmod{q}$$

and, consequently,

$$\alpha \equiv \beta^D \equiv b^v \pmod{q} \quad \text{and} \quad \alpha^2 \equiv c^{2^{t+1}} \pmod{q}.$$

Since v and 2^{t+1} are coprime, we obtain $\alpha^2 \equiv d^{2s} \pmod{q}$ for some rational integer d.

If now $e = (q-1)/s$, then for all n we have

$$\alpha^{n+e} = \alpha^{n+2(e/2)} \equiv d^{q-1}\alpha^n \equiv \alpha^n \pmod{q}$$

and the truth of the lemma results from (1).

From the proof of Lemma 2 it is clear that in the notation of that lemma the following is also true:

LEMMA 3. *If a prime* $q \equiv 1 \pmod{Ms}$ *splits completely in the splitting field* K *of the polynomial* $g(x)$, *then the period of the sequence* $\{a_n\}$ *is a divisor of* $q-1$.

Our main tool for the utilization of Conjecture H is the following lemma:

LEMMA 4. *Let* $k > 1$ *be an integer,* θ *an algebraic integer such that* $L = Q(\theta)$ *is normal over* Q, *and* $g(x)$ *the minimal polynomial of* θ, *of degree* N_1, *say. If* F *is a positive integer divisible by* $k(2N_1)!$, *then there exists a polynomial* $f_1(x)$ *such that the polynomials* $f_1(x)$ *and* $f_2(x) = (f_1(x)-1)/k+1$ *satisfy the assumptions of Conjecture* H. *Moreover, if* $f_1(x) = q$ *is a prime for some positive integer* x, *then* q *splits in* L *and* $q \equiv 1 \pmod{kF}$.

Proof. Since the proof differs only a little from that of Lemma 4 in [10], we state only the needed modifications.

Let $f_0(x) = x^{N_1} - 1 + k$. Using a similar argument to that in the proof of Lemma 4 in [10] we prove the existence of an arbitrarily large prime l which splits completely in L and such that

$$f(x) = f_0 + l \equiv \prod_{i=1}^{n} (x - z_i') \pmod{l^2}.$$

Let $l = \mathfrak{l}_1 \ldots \mathfrak{l}_{N_1}$ be the splitting of l in L. By the Chinese remainder theorem for L there exists an integer $\gamma \in L$ satisfying the system of congruences

$$\gamma \equiv 1 \pmod{kF},$$
$$\gamma \equiv -z_i' \pmod{\mathfrak{l}_i^2}, \quad i = 1, \ldots, N_1.$$

Let w be a rational integer different from all the numbers

$$\frac{\sigma\gamma-\gamma}{kFr^2(\theta-\sigma\theta)},$$

where σ is an arbitrary nonunit element of the Galois group of L/Q.

Put

$$\Gamma = \gamma + kFl^2\theta w \quad \text{and} \quad f_1(x) = N(kFx+\Gamma).$$

Since k divides $N(\Gamma)-1$, the polynomial $f_2(x)$ has rational integral coefficients. The leading coefficient of $f_1(x)f_2(x)$ is $k^{2N_1-1}F^{2N_1}$. Because of

$$f_1(0) = N(\Gamma) \equiv 1 \pmod{kF},$$

$$f_2(0) = (N(\Gamma)-1)/k+1 \equiv 1 \pmod{F}$$

we have $(f_1(0)f_2(0), kF) = 1$ since k divides F.

At this point we can use the argument in the proof of Lemma 4 of [10]. The last part of the proof looks as follows:

$$\begin{aligned} f_1(x)-1+k &= \prod_{i=1}^{N_1}(kFx+\sigma_i\Gamma)-1+k \equiv \prod_{i=1}^{N_1}(kFx-z_i')-1+k \\ &\equiv f(kFx)-1+k \equiv ((kF)^{N_1}x^{N_1}+l+1-k)-1+k \\ &\equiv (kF)^{N_1}x^{N_1}+l \pmod{l_1^2}. \end{aligned}$$

Thereby

$$f_1(x)-1+k \equiv (kF)^{N_1}x^{N_1}+l \pmod{l^2}$$

since l splits completely in L.

The condition $q \equiv 1 \pmod{kF}$ is satisfied because of the definition of the polynomial $f_1(x)$.

Proof of the Theorem. Let $g_i(x)$ be the characteristic polynomial of the simple linear recurring sequence $\{a_n^i\}$. Using Lemma 2 we may choose an integer k greater than 1 such that for some M the following holds: If a prime q splits in the splitting field L of the product of polynomials $g_i(x^{2k})$, then the period of all sequences $\{a_n^i\}$ modulo q is a divisor of $(q-1)/k$.

Now we take an integer F such that $fkM(2N_1)!$ divides F, where N_1 is the degree of L over Q and f is the conductor of the splitting field K of the product of polynomials $g_i(x)$. According to Lemma 4, Conjecture H implies that for the chosen k there are infinitely many primes p, q such that

$$p = (q-1)/k+1 \equiv 1 \pmod{kF}$$

and q splits completely in L. Since f divides F, we infer that p splits completely in K.

Using Lemma 2 for q and L, resp. Lemma 3 for p and K, we have

$$a^i_{pqm} = a^i_{p(q-1)m+pm} \equiv a^i_{pm} = a^i_{(q-1/k+1)m} \equiv a^i_m \pmod q,$$

resp.

$$a^i_{pqm} = a^i_{q(p-1)m+qm} \equiv a^i_{qm} = a^i_{(k(p-1)+1)m} \equiv a^i_m \pmod p.$$

Hence

$$a^i_{(pq)m} \equiv a^i_m \pmod{pq}.$$

This completes the proof of the Theorem.

At the end we remark that for a fixed algebraic number field L_0 the Theorem above remains valid for linear recurring sequences of algebraic numbers from L_0 whose characteristic polynomial has coefficients from L_0 provided the splitting field K over L_0 of the product of $g_i(x)$ is Abelian over Q.

We conjecture that the analogous theorem holds also for nonabelian simple linear recurring sequences but in this case the decomposition of ideals (splitting) does not depend only on the congruence class of conductor f. Therefore our method cannot be applied to this case.

Acknowledgement. I would like to thank the referee for useful comments.

REFERENCES

[1] W. Adams and D. Shanks, *Strong primality tests that are not sufficient*, Math. Comp. 39 (1982), pp. 255–300.

[2] Z. Borevich and I. R. Shafarevich, *Number Theory* (in Russian), Moscow 1964. English translation: Academic Press, New York 1966.

[3] S. Jakubec and K. Nemoga, *On a conjecture concerning sequences of the third order*, Math. Slovaca 36 (1986), pp. 85–89.

[4] J. C. P. Miller, G. Spencer Brown and D. J. Spencer Brown, *The identification of prime numbers*, unpublished.

[5] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, PWN–Polish Scientific Publishers, Warszawa 1974.

[6] R. Perrin, *Item 1484*, L'Intermédiaire des Math., Vol. 6, 1899, pp. 76–77.

[7] A. Rotkiewicz, *Pseudoprime numbers and their generalizations*, Student Association of the Faculty of Sciences, University of Novi Sad, Novi Sad 1972.

[8] — *On Euler Lehmer pseudoprimes and strong Lehmer pseudoprimes with parameters L, Q in arithmetic progressions*, Math. Comp. 39 (1982), pp. 239–247.

[9] A. Schinzel, *Selected Topics on Polynomials*, University of Michigan Press, Ann Arbor 1982.

[10] J. Wójcik, *On the composite Lehmer numbers with prime indices, III*, Colloq. Math. 45 (1981), pp. 81–90.

MATHEMATICAL INSTITUTE OF THE SLOVAK ACADEMY OF SCIENCES
OBRANCOV MIERU 49
814 73 BRATISLAVA, CZECHOSLOVAKIA

Reçu par la Rédaction le 28.1.1988;
en version définitive le 27.10.1988