František Marko

Polynomials of the form $g(x^k)$ and pseudoprimes with respect to linear recurring sequences

Mathematica Slovaca, Vol. 42 (1992), No. 5, 621--639

Persistent URL: http://dml.cz/dmlcz/131568

Mathematica Slovaca
©1992
Mathematical Institute
Slovak Academy of Sciences

Math. Slovaca, **42** (1992), No. 5, 621–639

POLYNOMIALS OF THE FORM $g(x^k)$ AND PSEUDOPRIMES WITH RESPECT TO LINEAR RECURRING SEQUENCES

FRANTIŠEK MARKO[1)]

ABSTRACT. The degree of the splitting field of the polynomial $g(x^k)$ over the composition of the splitting field of the polynomial $g(x)$ and the k th cyclotomic field is investigated and the result is then used in heuristic argument about the existence of pseudoprimes with respect to simple linear recurring sequence which are the product of two different primes.

1. Introduction

In [5] the notion of pseudoprime with respect to a linear recurring sequence of integers is defined and the existence of infinitely many pseudoprimes with respect to any finite system of simple abelian linear recurrences is derived from Schinzel's conjecture H. Pseudoprimes constructed there are products of two different primes.

The above mentioned pseudoprimes form a type which is important in actual searching for pseudoprimes (see [1] and [4]).

At the end of this paper we present a certain heuristic arguments which enable us to classify linear recurrences according to the expected "density" of the pseudoprimes n of the type $n = pq$, where p and q are primes.

Heuristic considerations led us to the formulation of the following problem, which is the main topic of this paper. It is the investigation of the degree of the splitting field of the polynomial $g(x^k)$ over the composition of the splitting field of the polynomial $g(x)$ and the k th cyclotomic field.

Suppose that the polynomial $g(x) = x^r - b_{r-1}x^{r-1} - \cdots - b_0$ has only simple roots, namely $\alpha_1, \ldots, \alpha_r$. Denote by K the splitting field of the polynomial

AMS Subject Classification (1991): Primary 11B37, 12F05.

Key words: Kummer extension, Degree of an extension, Multiplicative dependence over a field, Pseudoprimes with respect to linear recurring sequence.

[1)] Research supported by Slovak Academy of Sciences Grant 363.

$g(x)$ over the field Q of rationals. Then the splitting field Ω of the polynomial $g(x^k)$ over Q is $\Omega = K(\zeta_k, \sqrt[k]{\alpha_1}, \ldots, \sqrt[k]{\alpha_r})$, where ζ_k is a primitive kth root of unity.

Let $L = K(\zeta_k)$ and $s(k) = [\Omega : L]$. Our main result states the following:

THEOREM. *There are positive integers M and h such that if k is prime to M then $s(k) = k^h$.*

2. k-dependence over number field

We start with the definition of k-dependence (see also [3] and[9]).

DEFINITION 1. *Numbers $\{\alpha_i \in F;\ i \in I\}$ are called k-dependent over a number field F if there are integers $x_i;\ 0 \leq x_i < k$, not all equal to zero such that*

$$\prod_{i \in I} \alpha_i^{x_i} = \beta^k$$

for some $\beta \in K$.

Numbers α_i which are not k-dependent over F are called k-independent over F.

It follows straight from the definition that numbers which are k-dependent over F are kl-dependent over any extension F' of F for every natural l.

DEFINITION 2. *Numbers $\{\alpha_i \in F;\ i \in I\}$ are called dependent over F if for some integers $x_i;\ i \in I$ not all equal to zero*

$$\prod_{i \in I} \alpha_i^{x_i} = 1.$$

The previous notions are connected in the following way:

LEMMA 1. *Dependent numbers over F are k-dependent over F for every k which does not divide all exponents x_i in the relation of dependence.*

P r o o f. It is sufficient to raise the equality from the definition of dependence to the kth power. □

The field $\Omega = L(\sqrt[k]{\alpha_1}, \ldots, \sqrt[k]{\alpha_r})$ can be obtained from the field L by multiple cyclic extensions, whose degrees are divisors of k. Every of these extensions is a Kummer extension of the preceding one.

We will use the following result about Kummer extensions which can be found in [3, §9] and [9, Chap. 17]).

PROPOSITION 1. *Suppose that a number field L contains a primitive k th root of unity.*

If the numbers $\{\alpha_i;\ i \in I\}$ are k-independent over L, then the degree $[L(\sqrt[k]{\alpha_i};\ i \in I) : L]$ equals k^s, where s denotes the cardinality of the index set I.

Moreover, the fields $L(\sqrt[k]{\alpha_i})$ are linearly disjoint over L, i.e. the intersection of every two such fields which do not coincide is the field L.

If the numbers $\alpha_1, \ldots, \alpha_r$ are k-dependent over L, then the determination of the degree $[\Omega : L]$ can be a more complicated task.

LEMMA 2. *Let $k>1$ be a prime. Suppose that a number field L contains a primitive k th root of unity, the numbers $\{\alpha_1, \ldots, \alpha_r\}$ belong to L and $\{\alpha_i;\ i \in I\}$ is a maximal subset of elements of the previous set such that its elements are k-independent over L. If h is the number of elements in I, then $[L(\sqrt[k]{\alpha_1}, \ldots, \sqrt[k]{\alpha_r}) : L] = k^h$.*

P r o o f. If $r = h$ the claim follows from Proposition 1. Otherwise we enlarge the index set I by adding an arbitrary element $j_0 \notin I$ and we denote the emerged set by J_0. It is possible to create $r - h$ sets of this kind.

The elements $\{\alpha_j;\ j \in J_0\}$ are k-dependent over L and therefore there exist integers z_j not all equal to zero such that $0 \leq z_j < k$ and

$$\prod_{j \in J_0} \alpha_j^{z_j} = \beta^k,$$

for some $\beta \in L$. From the choice of the set I it follows that $z_{j_0} \neq 0$, consequently one can find integers t, u such that $z_{j_0} t = 1 + ku$. If we raise the equation of the k-dependence to the t th power, then we infer

$$\alpha_{j_0} = \prod_{i \in I} \alpha_i^{-z_i t} \alpha_{j_0}^{-ku} \beta^{kt}.$$

Therefore $\sqrt[k]{\alpha_{j_0}} \in L(\sqrt[k]{\alpha_i};\ i \in I)$, because L contains a primitive k th root of unity. Since the last relation holds for every $j_0 \notin I$, the claim of the lemma follows from Proposition 1. □

LEMMA 3. *If*

$$k = \prod_{j \in J} p_j^{e_j}$$

is the canonical decomposition of the number k, *then*

$$[\Omega : L] = \prod_{j \in J} \left[L\left(\sqrt[p_j^{e_j}]{\alpha_1}, \ldots, \sqrt[p_j^{e_j}]{\alpha_r} \right) : L \right]$$

is the canonical decomposition of the number $[\Omega : L]$.

The degree s_j *of the extension* $L\left(\sqrt[p_j^{e_j}]{\alpha_1}, \ldots, \sqrt[p_j^{e_j}]{\alpha_r} \right)$ *over* L *is the product of the degrees* $s_{j,l}$ *of the field* $L\left(\sqrt[p_j^{l}]{\alpha_1}, \ldots, \sqrt[p_j^{l}]{\alpha_r} \right)$ *over* $L\left(\sqrt[p_j^{l-1}]{\alpha_1}, \ldots, \sqrt[p_j^{l-1}]{\alpha_r} \right)$ *for* $l = 1, \ldots, e_j$.

Proof.

For every index j the field $L\left(\sqrt[p_j^{e_j}]{\alpha_1}, \ldots, \sqrt[p_j^{e_j}]{\alpha_r} \right)$ is a subfield of the field Ω. The degree of the multiple Kummer extension $L\left(\sqrt[p_j^{e_j}]{\alpha_1}, \ldots, \sqrt[p_j^{e_j}]{\alpha_r} \right)$ over L is a power of the prime p_j.

This number divides the number $[\Omega : L]$. Since the field Ω is a multiple Kummer extension of the field $L\left(\sqrt[p_j^{e_j}]{\alpha_1}, \ldots, \sqrt[p_j^{e_j}]{\alpha_r} \right)$ and $p_j^{e_j}$ is the greatest power of the prime p_j which divides k, the degree $\left[\Omega : L\left(\sqrt[p_j^{e_j}]{\alpha_1}, \ldots, \sqrt[p_j^{e_j}]{\alpha_r} \right) \right]$ is prime to p_j. The first part of the lemma follows from this and the second one is obvious. □

If we denote $\sqrt[p_j^{l-1}]{\alpha_h}$ by symbols $\beta_{h,j,l}$, then the number $s_{j,l}$ equals the degree of the extension $L\left(\sqrt[p_j]{\beta_{1,j,l}}, \ldots, \sqrt[p_j]{\beta_{r,j,l}} \right)$ over $L(\beta_{1,j,l}, \ldots, \beta_{r,j,l})$. According to Lemma 2 this number equals the power of the prime p_j with the exponent, which is equal to the cardinality of a maximal index set $I \subset \{1, \ldots, r\}$ such that the numbers $\beta_{i,j,l}$, $i \in I$, are p_j-independent over $L(\beta_{1,j,l}, \ldots, \beta_{r,j,l})$.

Now we will discuss the mutual relation of k-dependence over the field K and over the field $L = K(\zeta_k)$.

LEMMA 4. *Numbers* $\{\alpha_j ;\ j \in J\}$ *from the number field* K *are* k*-dependent over the field* L *which is the composition of the field* K *and the* k *th cyclothomic field* Q_k *if and only if they are* p*-dependent over the field* L *for some prime* p *which divides* k.

Proof. Suppose that the numbers $\{\alpha_j ;\ j \in J\}$ are k-dependent over L, i.e. for suitable integers $\{x_j ;\ 0 \leq x_j < k,\ j \in J\}$ not all equal to zero and some $\beta \in L$

$$\prod_{j \in J} \alpha_j^{x_j} = \beta^k.$$

If we denote by d the greatest common divisor of the numbers $\{x_j;\ j \in J\}$ and k, then for a suitable integer t and a prime p which divides $\frac{k}{d}$ we have the relation

$$\prod_{j\in J} \alpha_j^{\frac{x_j}{d}} = \left(\zeta_k^t \beta\right)^{\frac{k}{d}} = \left(\zeta_k^{\frac{tk}{pd}} \beta^{\frac{k}{pd}}\right)^p,$$

where ζ_k is a primitive kth root of unity.

From this relation we infer that the numbers $\{\alpha_j;\ j \in J\}$ are p-dependent over L because some x_j is not divisible by the prime p.

The converse implication is obvious. □

Although we can take into consideration the previous reduction, the task to gain insight into the degrees $s(k) = s\big(g(x), k\big)$ of the fields Ω over L for all k and fixed $\alpha_1, \ldots, \alpha_r$ (and fixed field K) remains difficult.

However, for a number k such that $\big(k, \varphi(k)\big) = 1$ or k prime to certain integer R it is possible to determine the number $s(k)$ only from the properties of the base field K.

LEMMA 5. *If the numbers $\{\alpha_j;\ j \in J\}$ from the field K are k-dependent over L and $\big(k, \varphi(k)\big) = 1$, then they are k-dependent over K.*

Proof. Using Lemma 4 it is possible to find such prime divisor p of the number k that the numbers $\{\alpha_j;\ j \in J\}$ are p-dependent over $L = KQ_k$, that is for some $\{x_j;\ 0 \le x_j < p,\ j \in J\}$ not all equal to zero and some $\beta \in L$ we have

$$\prod_{j\in J} \alpha_j^{x_j} = \beta^p.$$

If we take norms to the field K in the above equality, then we obtain

$$\prod_{j\in J} \alpha_j^{x_j \deg(L/K)} = N_{L/K}(\beta)^p.$$

Since $\deg(L/K)$ divides the number $\varphi(k)$ and prime p divides k, the assumption $\big(k, \varphi(k)\big) = 1$ implies that some $x_j \deg(L/K)$ is not divisible by p. This means that the numbers $\{\alpha_j;\ j \in J\}$ are p-dependent over K and that is why they are k-dependent over K. □

Suppose that R is the highest possible order of a root of unity contained in the field K.

The following proposition is a consequence of Theorem 3 from [10].

PROPOSITION 2. *Suppose that k is a positive integer prime to R. If $\alpha \in K$ is such that $\alpha = \beta^k$ for some $\beta \in K(\zeta_k)$ then $\alpha = \gamma^k$ for some $\gamma \in K$. Consequently, if $\{\alpha_j ;\ j \in J\}$ are elements of the field K which are k-dependent over $L = K(\zeta_k)$ then they are k-dependent over K.*

DEFINITION 3. *For arbitrary prime p we define the number $d(p)$ as the cardinality of such maximal index set $J \subseteq \{1, \ldots, r\}$ that the numbers $\{\alpha_j ;\ j \in J\}$ are p-independent over K.*

The numbers $d(p)$, where p divides k, are strongly connected with the number $s(k)$.

In the next part we will give a certain lower bound for the numbers $d(p)$.

For the sake of simplicity we will suppose from now on that the polynomial $g(x)$ is irreducible.

First we will deal with the case when the numbers $\alpha_1, \ldots, \alpha_r$ are algebraic units of the field K.

3. Sequences with $b_0 = \pm 1$

a) Lower bound for $d(p)$.

The case when some (and hence every) number α_i is a root of unity is trivial and therefore in the sequel we will suppose that none of the numbers α_i are a root of unity.

Suppose that the constant term b_0 of the polynomial $g(x)$ equals ± 1, hence the roots $\alpha_1, \ldots, \alpha_r$ of the polynomial $g(x)$ are units of the field K. Further, let fundamental units $\varepsilon_1, \ldots, \varepsilon_u$ of the field K ($u = s + t - 1$, where s is a number of real embeddings and t is a number of pairs of conjugate complex embeddings of the field K in the field $\mathbb{C}$ of complex numbers) and the number ζ which is the root of unity of the highest possible order R in K be given.

Let

$$\alpha_i = \zeta^{E_i} \varepsilon_1^{e_{i1}} \ldots \varepsilon_u^{e_{iu}} \qquad \text{for} \quad i = 1, \ldots, r$$

be the expressions for the roots of the polynomial $g(x)$, whose existence follows from the Dirichlet theorem about units.

Denote by $\mathbf{E}$ the matrix of the dimension $r \times u$ consisting of the numbers e_{ij} and by $\mathbf{E}'$ the matrix obtained from $\mathbf{E}$ by adding the row determined by the vector $\mathbf{e}' = (E_1, \ldots, E_r)$.

Using this notation we can state the following lemma:

LEMMA 6. *Let R be the order of ζ. Then there is a number D such that:*

(i) *For all primes p which do not divide the number DR we have the inequality $d(p) \geq h$, where h is the rank of the matrix $\mathbf{E}$.*

(ii) *For primes* p *which divide* D *but do not divide* R *we have the inequality* $d(p) \geq h_p$, *where* h_p *is the rank of the matrix* $\mathbf{E}$ *modulo* p.

(iii) *For primes* p *which divide* R *we have the inequality* $d(p) \geq h'_p$, *where* h'_p *is the rank of the matrix* $\mathbf{E}'$ *modulo* p.

P r o o f. Suppose that the numbers $\{\alpha_i;\ i \in I\}$ are p-dependent over K, this means that

$$\prod_{i \in I} \alpha_i^{x_i} = \beta^p, \tag{$*$}$$

where $\beta \in K$, $0 \leq x_i < p$ for $i \in I$ and some x_i is not divisible by prime p.

Since all numbers $\alpha_1, \ldots, \alpha_r$ are algebraic units of the field K, the number β must be an algebraic unit of the field K too.

According to the Dirichlet theorem about units it is possible to write every number $\alpha_1, \ldots, \alpha_r$ and β in the form of the product of a root of unity and the integral powers of fundamental units of the field K.

Let

$$\alpha_i = \zeta^{E_i} \varepsilon_1^{e_{i1}} \ldots \varepsilon_u^{e_{iu}}$$

for $i = 1, \ldots, r$ and

$$\beta = \zeta^{Y} \varepsilon_1^{y_1} \ldots \varepsilon_u^{y_u}$$

be the corresponding decompositions.

The equality $(*)$ can be rewritten in the form

$$\zeta^{\sum_{i \in I} E_i x_i} \varepsilon_1^{\sum_{i \in I} e_{i1} x_i} \ldots \varepsilon_u^{\sum_{i \in I} e_{iu}} = \zeta^{Yp} \varepsilon_1^{y_1 p} \ldots \varepsilon_u^{y_u p},$$

in which some number x_i is not divisible by the prime p.

Since the units ε_j are fundamental, the last equality is equivalent to the following system of linear equations (L_I) and the congruence $(**)$

$$\begin{aligned} &\sum_{i \in I} e_{i1} x_i = y_1 p \\ &\qquad \ldots \qquad\qquad (L_I) \\ &\sum_{i \in I} e_{iu} x_i = y_u p \\ &\sum_{i \in I} E_i x_i \equiv Yp \pmod{R}, \qquad (**) \end{aligned}$$

where some x_i is not divisible by p.

If the prime p does not divide the number R, then the congruence $(**)$ is solvable for arbitrary $\{x_i;\ i \in I\}$. Otherwise the congruence $(**)$ is reduced to the equation

$$\sum_{i \in I} E_i x_i = Yp.$$

Denote by symbols $\mathbf{E}_I$ and $\mathbf{E}'_I$ matrices which are obtained from the matrices $\mathbf{E}$ and $\mathbf{E}'$, respectively, in such a way that we choose the rows whose indices belong to the set I or we choose these rows and add the last row determined by the vector $\boldsymbol{e}'$, respectively. Hence the rows of the matrix $\mathbf{E}_I$ are the vectors $\{\boldsymbol{e}_i = (e_{i1}, \ldots, e_{iu});\ i \in I\}$ and the rows of the matrix $\mathbf{E}'_I$ are the vectors $\{\boldsymbol{e}_i;\ i \in I\}$ and the vector $\boldsymbol{e}'$.

We can regard the system (L_I) and the congruence $(**)$ as a homogeneous system of linear equations over the field $\mathbb{Z}/p\mathbb{Z}$ with unknowns $\{x_i;\ i \in I\}$ determined by the matrix $\mathbf{E}_I$ or $\mathbf{E}'_I$, respectively.

The numbers $\{\alpha_i;\ i \in I\}$ are p-dependent over K if and only if the homogeneous system of linear equations determined by the matrix $\mathbf{E}_I$ in the case when p does not divide R or by the matrix $\mathbf{E}'_I$ otherwise has a non-trivial solution $\{x_i;\ i \in I\}$ in the field $\mathbb{Z}/p\mathbb{Z}$.

We can infer from this that the numbers $\{\alpha_i;\ i \in I\}$ are p-independent over K if and only if there is a submatrix $\mathbf{M}$ of the dimension $l \times l$ of the matrix $\mathbf{E}$ or of the dimension $(l+1) \times (l+1)$ of the matrix $\mathbf{E}'$, respectively, where l is the cardinality of the index set I, such that the determinant D of $\mathbf{M}$ is invertible in the field $\mathbb{Z}/p\mathbb{Z}$.

Let h be the rank of the matrix $\mathbf{E}$. Then there is a submatrix $\mathbf{M}$ of the matrix $\mathbf{E}$ of the dimension $h \times h$, whose determinant D is a nonzero integer. With the matrix $\mathbf{M}$ we can uniquely associate an index set $\bar{I}$ of its rows. For arbitrary prime p which does not divide D, the system $L_{\bar{I}}$ has only the trivial solution in $\mathbb{Z}/p\mathbb{Z}$.

Therefore for all primes p which do not divide DR the numbers $\{\alpha_i;\ i \in \bar{I}\}$ are p-independent over K. Hence $d(p) \geq h$ and this proves (i).

It remains to determine the bound for $d(p)$ for those primes which divide DR. Again it is sufficient to determine the maximal index set I such that the numbers $\{\alpha_i;\ i \in I\}$ are p-independent over K for prime divisors p of the number DR. This can be done if for index sets $J \subseteq \{1, \ldots, r\}$ we know the ranks of the matrices $\mathbf{E}_J$ over the fields $\mathbb{Z}/p\mathbb{Z}$, where p divides D but does not divide R and the ranks of the matrices $\mathbf{E}'_J$ over the fields $\mathbb{Z}/p\mathbb{Z}$, where p divides R.

The statements (ii) and (iii) can be proved in the same way as the statement (i). □

We remark that there could be more maximal index sets. However, since we consider the rank of the matrix over the field, the numbers of elements in these maximal index sets are the same.

From the proof of the last lemma it follows that $h = 0$ if and only if all roots α_i of the polynomial $g(x)$ are roots of unity. Moreover, $h_p = 0$ if and only if all numbers $\{\alpha_i\,;\ i \in I\}$ are the pth powers of numbers δ_i from the field K or products of such powers by powers the multiple of the pth root of unity which belongs to K. This case is possible only for a finite number of primes p and we can gain further information about the degree $[\Omega : L]$ by considering the numbers δ_i instead of α_i.

b) Bound for the number $s(k,p)$.

Let

$$k = \prod_{j \in J} p_j^{e_j}$$

be the canonical decomposition of the number k. We denote by $s(k,p)$ the highest power of the prime p which divides the number $s(k)$. Then

$$s(k) = \prod_{p \setminus s(k)} s(k,p).$$

Using this notation we can state the next lemma.

LEMMA 7. *Let h be the rank of the matrix $\mathbf{E}$. There is some integer M such that for every prime p not dividing M we have $s(k,p_j) \leq p_j^{he_j}$.*

P r o o f. Add to the index set $\bar{I}$ defined in the proof of Lemma 6 an arbitrary element $j_0 \notin \bar{I}$ and denote the obtained index set by the symbol J_0. We can create $r - h$ sets of this kind. Rows $\{\boldsymbol{e}_j\,;\ j \in J_0\}$ are linearly dependent over $\mathbb{Q}$ and therefore there are some rational numbers $\{z_j\,;\ j \in J_0\}$ and z such that $z_{j_0} \neq 0$ and

$$\prod_{j \in J_0} \alpha_j^{z_j} = \zeta^z.$$

We can raise the last equality to the suitable integer power C_{j_0} and we obtain an analogous equality, where the exponents of the numbers α_j are integers whose greatest common divisor is F_{j_0} and therefore the exponent of ζ must be an integer too.

After the subsequent raising to the Rth power we obtain the equality

$$\prod_{j \in J_0} \alpha_j^{z_j'} = 1, \qquad (***)$$

hence the numbers α_j are dependent and the greatest common divisor of all exponents z'_j divides $F_{j_0}R$.

The exponent z'_{j_0} in $(***)$ can not be divisible by a prime which does not divide $F_{j_0}DR$ because for such a prime p_j the numbers $\{\alpha_i\,;\ i \in \bar{I}\}$ are p_j-independent over K according to the choice of the index set $\bar{I}$.

For such p_j it is possible to find a natural t which fulfils the congruence $z'_{j_0}t \equiv 1 \pmod{p_j^{e_j}}$.

After the raising of $(***)$ to the power t we obtain

$$\alpha_{j_0} = \prod_{i \in \bar{I}} \alpha_i^{-z'_i t} \alpha_{j_0}^{-p_j^{e_j} u}$$

for a suitable natural u. If we take the roots of the degree $p_j^{e_j}$ in this equality, we obtain that the number $\sqrt[p_j^{e_j}]{\alpha_{j_0}} \in L\left(\sqrt[p_j^{e_j}]{\alpha_i}\,;\ i \in \bar{I}\right)$, because L contains a primitive $p_j^{e_j}$ th root of unity.

If we put $M = DR \prod_{j_0 \notin \bar{I}} F_{j_0}$ then the last result holds for every index $j_0 \notin \bar{I}$ and therefore we obtain the equality

$$L\left(\sqrt[p_j^{e_j}]{\alpha_1}, \ldots, \sqrt[p_j^{e_j}]{\alpha_r}\right) = L\left(\sqrt[p_j^{e_j}]{\alpha_i}\,;\ i \in \bar{I}\right).$$

According to Lemma 3 and Lemma 2 this means that if p_j is prime to M then $s(k, p_j) \leq p_j^{he_j}$. □

If we compare the statement of Lemma 6 and Lemma 7, the natural question arises whether it is possible to derive the upper bound for the number $s(k, p_j)$ also in the case when p divides M. In this respect we have only the following partial result.

LEMMA 8. *If a prime p does not divide R, then*

$$\left[L\left(\sqrt[p_j]{\alpha_1}, \ldots, \sqrt[p_j]{\alpha_r}\right) : L\right] = p_j^{h_{p_j}}$$

otherwise

$$\left[L\left(\sqrt[p_j]{\alpha_1}, \ldots, \sqrt[p_j]{\alpha_r}\right) : L\right] = p_j^{h'_{p_j}}$$

P r o o f . Lemma follows from the definition of the numbers h_{p_j} and h'_{p_j}, respectively, and from Lemma 2. □

On the other hand the degrees

$$\left[L\left(\sqrt[p_j^c]{\alpha_1},\ldots,\sqrt[p_j^c]{\alpha_r}\right):L\left(\sqrt[p_j^{c-1}]{\alpha_1},\ldots,\sqrt[p_j^{c-1}]{\alpha_r}\right)\right]$$

for $c>1$ do not depend only on h_{p_j} and h'_{p_j}, respectively.

LEMMA 9. *Suppose that* $(k,R)=1$ *or* $\big(k,\varphi(k)\big)=1$. *Then for primes* p_j *which do not divide* DR *it holds that* $s(k,p_j)\geq p_j^{he_j}$. *For primes which divide* D *but do not divide* R *it holds that* $s(k,p_j)\geq p_j^{h_{p_j}e_j}$ *and for primes* p_j *which divide* R *it holds that* $s(k,p_j)\geq p_j^{h'_{p_j}e_j}$.

P r o o f . The lemma follows from Lemma 6, Lemma 5, Proposition 2 and Proposition 1. □

4. Sequences with $b_0\neq\pm1$

Now we will deal with the case when $b_0\neq\pm1$, i.e. when none of the numbers $\alpha_1,\ldots,\alpha_r$ is an algebraic unit in the field K.

Till now we did not practically use the assumption that $g(x)$ is an irreducible polynomial. However, in this part the last assumption will play an important role.

If $g(x)$ is irreducible, then $N_{K/\mathbb{Q}}(\alpha_1)=\cdots=N_{K/\mathbb{Q}}(\alpha_r)=N=\pm b_0$ and N is different from ±1 as it follows from our assumption.

We denote by d the greatest natural number such that the number N is a dth power of some integer: $N=N_0^d$.

Using the introduced notation we can state the following lemma.

LEMMA 10. *Choose the index set* I *and some element* i_0 *of this set. If the numbers* $\{\alpha_i;\ i\in I\}$ *are* k*-dependent over* K, *then the numbers* $\left\{\gamma_{i,i_0}=\dfrac{\alpha_i}{\alpha_{i_0}};\ i\neq i_0\right\}$ *are* k*-dependent over* K *or* $D=(k,d)\geq1$ *and the numbers* $\{\alpha_i;\ i\in I\}$ *are* D*-dependent over* L.

P r o o f . Suppose that the numbers $\{\alpha_i;\ i\in I\}$ are k-dependent over K, that is for some $\beta\in K$ and integers $x_i;\ 0\leq x_i<k$ not all equal to zero we have

$$\prod_{i\in I}\alpha_i^{x_i}=\beta^k. \tag{+}$$

We divide the last equality by the number $\alpha_{i_0}^{\sum_{i\in I} x_i}$ and obtain the equality

$$\prod_{i\in I,\ i\neq i_0} \left(\frac{\alpha_i}{\alpha_{i_0}}\right)^{x_i} = \frac{\beta^k}{\alpha_{i_0}^{\sum_{i\in I} x_i}}. \qquad (++)$$

If we take norms of both sides of (+), we obtain

$$N_{K/\mathbb{Q}}(\beta)^k = N^{\sum_{i\in I} x_i}.$$

The last equality implies the congruence

$$d\sum_{i\in I} x_i \equiv 0 \pmod{k},$$

which is equivalent to

$$\sum_{i\in I} x_i \equiv 0 \pmod{\tfrac{k}{D}}.$$

If $x_i \not\equiv 0 \pmod{\frac{k}{D}}$ for some $i \in I$, then it follows from the last congruence that this index i could be chosen different from i_0. After the raising of the equality (++) to the Dth power we have

$$\prod_{i\in I,\ i\neq i_0} \left(\frac{\alpha_i}{\alpha_{i_0}}\right)^{x_i D} = \frac{\beta^{kD}}{\alpha_{i_0}^{\left(\sum_{i\in I} x_i\right)D}} = \gamma^k,$$

where $\gamma \in K$ and $x_i D \not\equiv 0 \pmod{k}$ for some $i \neq i_0$. This means that the numbers $\left\{\frac{\alpha_i}{\alpha_{i_0}};\ i \in I - \{i_0\}\right\}$ are k-dependent over K.

If $x_i \equiv 0 \pmod{\frac{k}{D}}$ for all $i \in I$, then after taking roots of both sides in the equality (+), we obtain

$$\prod_{i\in I} \alpha_i^{x_i \frac{D}{k}} = \zeta_{\frac{k}{D}}^{z} \beta^D = (\zeta_k^z \beta)^D.$$

This equality means that the numbers $\{\alpha_i;\ i \in I\}$ are D-dependent over $L = KQ_k$, because we know that some $x_i \not\equiv 0 \pmod{k}$ and this implies $x_i \frac{D}{k} \not\equiv 0 \pmod{D}$. □

The following converse of the previous lemma will also be important for us. Here we use the previous notation.

LEMMA 11. *If the numbers* $\{\gamma_{i,i_0};\ i \in I - \{i_0\}\}$ *are* k*-dependent over* K *and in the case* $D > 1$ *they are not* D*-dependent over* L*, then the numbers* $\{\alpha_i;\ i \in I\}$ *are* k*-dependent over* K.

Proof. If the numbers $\{\gamma_{i,i_0};\ i \in I - \{i_0\}\}$ are k-dependent over K, then there are some $\gamma \in K$ and integers $\{x_i;\ 0 \leq x_i < k;\ i \in I - \{i_0\}\}$ not all equal to zero such that

$$\prod_{i \in I, i \neq i_0} \left(\frac{\alpha_i}{\alpha_{i_0}}\right)^{x_i} = \gamma^k.$$

Choose the number x_{i_0} in such a way that the following congruence is fulfilled

$$d \sum_{i \in I} x_i \equiv 0 \pmod{k}.$$

If we multiply the last equality by the number $\alpha_{i_0}^{\sum_{i \in I} x_i}$, then

$$\prod_{i \in I} \alpha_i^{x_i} = \gamma^k \alpha_{i_0}^{\sum_{i \in I} x_i}.$$

After the raising to the Dth power we have

$$\prod_{i \in I} \alpha_i^{x_i D} = \gamma^{kD} \alpha_{i_0}^{\left(\sum_{i \in I} x_i\right) D} = \delta^k,$$

where $\delta \in K$. If $D = 1$ or for some $i \in I$ we have $x_i \not\equiv 0 \pmod{\frac{k}{D}}$, then this x_i satisfies $x_i D \not\equiv 0 \pmod{k}$ and the last equality implies that the numbers $\{\alpha_i;\ i \in I\}$ are k-dependent over K. If $D > 1$ and each x_i is divisible by the number $\frac{k}{D}$, then we take the $\frac{k}{D}$ th roots of both sides of the last equality, which lie in L. From the resulting equality we see that the numbers $\{\alpha_i;\ i \in I\}$ are D-dependent over L, which contradicts the assumption of the lemma. Hence this case is not possible. □

We remark that the above results do not actually depend on the choice of the element i_0 from the index set I, provided that the number k is prime to d. In this case the equality

$$\prod_{i \in I} \left(\frac{\alpha_i}{\alpha_{i_0}}\right)^{x_i} = \beta^k$$

and the congruence

$$\sum_{i\in I} x_i \equiv 0 \pmod{k}$$

imply that

$$\prod_{i\in I}\left(\frac{\alpha_i}{\alpha_{i_1}}\right)^{x_i} = \beta^k\left(\frac{\alpha_{i_0}}{\alpha_{i_1}}\right)^{\sum_{i\in I} x_i} = \delta^k,$$

where $\delta \in K$.

5. Proof of Theorem

Proof of Theorem. First suppose that $b_0 = \pm 1$. In this case the theorem follows from Lemma 7 and 9.

In the case when $b_0 \neq \pm 1$ we will use Lemma 10 and 11.

The numbers γ_{i,i_0} from Lemma 11 are not necessarily algebraic integers, but they become algebraic integers when they are multiplied by a suitable natural number. Denote by S the set of those valuations of the field K, which correspond to the prime divisors of K that divide the principal divisor generated by the element α_{i_0}. Then all numbers γ_{i,i_0} are S-units of the field K.

Using the generalized Dirichlet theorem about S-units (see [7]) we can decompose the number γ_{i,i_0} into a product of a root of unity and integral powers of the fundamental S-units in the field K. The problem of k-dependence of these numbers over K could be solved in the same way as in the case when all $\alpha_1, \ldots, \alpha_r$ were supposed to be algebraic units of the field K.

If the number k is chosen to be prime to a suitable integer M, then we can again compute the degree $[\Omega : L]$ as before. □

6. Heuristic considerations

In this part we will apply the above result to the case of pseudoprimes with respect to simple linear recurring sequences. We will concentrate on such pseudoprimes which are the products of two different primes.

First we recall some definitions from [5].

Suppose that $\{a_n\}$ is a linear recurring sequence of integers of the r th order whose characteristic polynomial is $g(x)$. If all roots of $g(x)$ are simple, then the linear recurring sequence $\{a_n\}$ is called *simple*.

If $\{a_n\}$ is a simple linear recurring sequence, then an integer n which satisfies the congruence $a_{ns} \equiv a_s \pmod{n}$ for every natural number s is called *pseudoprime with respect to the sequence* $\{a_n\}$.

If for some composite n the sequence $\{a_n\}$ modulo n is periodic with the period $n-1$, then n is a pseudoprime with respect to $\{a_n\}$. Pseudoprimes of

this kind are called regular. Regular pseudoprimes which are the products of two different primes were considered in [5] and later investigated in [6].

LEMMA 12. *There is some natural number M such that if primes p and q satisfy the following properties:*

$p \equiv 1 \pmod{M}$, p splits completely in the splitting field of the polynomial $g(x)$,

q does not divide M, $q = k(p-1)+1$ for some natural k, q splits completely in the splitting field of the polynomial $g(x^{2k})$ if k is divisible by four or $g(x^k)$ otherwise,

then the number $t = pq$ is a pseudoprime with respect to the simple linear recurring sequence $\{a_n\}$.

P r o o f. Using Lemma 2 from [5] for q and p respectively we obtain that

$$a_{pqm} = a_{p(q-1)m+pm} \equiv a_{pm} = a_{(\frac{q-1}{k}+1)m} \equiv a_m \pmod{q},$$

resp.

$$a_{pqm} = a_{q(p-1)m+qm} \equiv a_{qm} = a_{(k(p-1)+1)m} \equiv a_m \pmod{p}.$$

Hence

$$a_{(pq)m} \equiv a_m \pmod{pq}.$$

□

We will base our heuristic arguments on statements about the density of primes of a certain splitting type in a given number field. We will also use the statement about the density of prime divisors in a generalized arithmetic progression and theorem about the degree of the splitting field of the polynomial $g(x^k)$ proved in the preceding section.

PROPOSITION 3. (see [2]) *Let K be a normal number field of the degree n over the field $\mathbb{Q}$ and let $\overline{M}$ be the class of primes p which split completely in the field K. Then*

$$d(\overline{M}) = \lim_{s\to 1} \frac{\sum\limits_{p\in\overline{M}} \frac{1}{p^s}}{\log \frac{1}{s-1}} = \lim_{s\to 1} \frac{\sum\limits_{p\in\overline{M}} \frac{1}{p^s}}{\sum\limits_{p} \frac{1}{p^s}} = \frac{1}{n},$$

i.e. the class $\overline{M}$ has the Dirichlet density $\frac{1}{n}$.

LEMMA 13. *Let K be a normal number field of the degree n over the field $\mathbb{Q}$. For arbitrary integer $m > 1$ we have: The number of primes p which do not exceed an integer x, satisfy the congruence $p \equiv 1 \pmod{m}$ and which split completely in the field K is asymptotically equale to $\left(1/[K(\zeta_m) : \mathbb{Q}]\right) \cdot \left(x/\log x\right)$.*

P r o o f. According to [2] a prime p satisfies $p \equiv 1 \pmod{m}$ if and only if p splits completely in $\mathbb{Q}(\zeta_m)$. Hence using [3] we see that $p \equiv 1 \pmod{m}$ splits completely in K if and only if p splits completely in $K(\zeta_m)$. Therefore the required statement follows from Proposition 3. □

The following definition will be useful in the later heuristic considerations.

DEFINITION 4. *The number h corresponding to the characteristic polynomial $g(x)$ and uniquely determined by Theorem is called the characteristic of a simple linear recurrent sequence $\{a_n\}$.*

Now we try to give the heuristic reason for the existence of pseudoprimes n which are the product of two different primes p, q.

Let M be the natural number from Lemma 12. According to Lemma 13 there are infinitely many primes $p \equiv 1 \pmod{M}$ which split completely in the splitting field of the polynomial $g(x)$. For almost all such p this is equivalent with the splitting of the polynomial $g(x)$ into linear factors over $\mathbb{Z}/p\mathbb{Z}$.

Firstly, suppose that positive integers k are bounded by k_0 or even suppose that $k = k_0$ is fixed. Consider p as a variable taking only values which are primes $p \equiv 1 \pmod{M}$ splitting completely in the field K. Then consider the expressions $q = 1 + k(p-1)$, where $k \leq k_0$ or even $k = k_0$. We may expect that for infinitely many primes p and integers k as above the expression q is a prime. If $k = k_0$ is fixed this would follow from Schinzel's conjecture H. If k is bounded by k_0 then by the choice of sufficiently large k_0 we can obtain arbitrary large number of primes q even if the prime p is fixed because the density of primes in the arithmetic progression $1 + k(p-1)$ is positive according to the Dirichlet theorem.

The density of primes which split completely in the splitting field of the polynomial $g(x^{2k})$ with k bounded as above is positive according to Proposition 3. Therefore we may require not only that q is a prime but also that it splits completely in the splitting field of the polynomial $g(x^{2k})$.

This heuristic arguments together with Lemma 12 lead to the expectation that there are infinitely many regular pseudoprimes $t = pq$ with respect to any simple linear recurring sequence.

The above heuristic arguments give also a method of actual searching for pseudoprimes in general situation.

Secondly, suppose that a prime $p \equiv 1 \pmod{M}$ which splits completely in K is fixed and positive integer k is variable (Here again M is a number from Lemma 12). According to Lemma 13 the primes $q \equiv 1 \pmod{p-1}$ which split completely in K form a $1/[K(\zeta_{p-1}) : \mathbb{Q}]$th part of all primes. Moreover a prime $q = 1 + k(p-1)$ splits completely in the field K if and only if it splits completely in the field $K(\zeta_k)$. We want to determine the density of primes $q = 1 + k(p-1)$, where $(k, M) = 1$ which split completely in the field $K(\zeta_k)$. Let $\{p_1, \ldots, p_s\}$ be the set of all prime divisors of M and $u = \prod_{i=1}^{s} p_i^{d_i}$ for some positive integers d_i's. Then $\left[K(\zeta_{(p-1)u}) : K(\zeta_{p-1})\right] = u$ for every integer u as above (recall that M is supposed to be even). Using this together with arguments analogous to previous ones and the inclusion – exclusion principle we compute that density is equal to $\dfrac{C}{[K(\zeta_{p-1}) : \mathbb{Q}]}$, where the constant $C = \prod_{i=1}^{s} \left(1 - \dfrac{1}{p_i}\right)$.

Our theorem implies that the probability of the fact that such a prime q splits completely in the field $\Omega = K\left(\zeta_k, \sqrt[k]{\alpha_1}, \ldots, \sqrt[k]{\alpha_r}\right)$ is equal to $\dfrac{1}{k^h}$.

Therefore the total probability of the fact that for a given prime q the following conditions are fulfilled:

(i) $q = 1 + k(p-1)$ for some integer $k > 1$ such that $(k, M) = 1$

(ii) q splits completely in the field Ω

equals $\dfrac{C}{[K(\zeta_{p-1}) : \mathbb{Q}]} \dfrac{1}{k^h}$.

Since a fixed prime $p \equiv 1 \pmod{M}$ is supposed to split completely in the field K, Lemma 12 implies that the probability that for a certain prime q the number $t = pq$ is a regular pseudoprime with respect to the sequence $\{a_n\}$ is not smaller than $\dfrac{C}{[K(\zeta_{p-1}) : \mathbb{Q}]} \dfrac{1}{k^h} \geq \dfrac{C}{n\varphi(p-1)} \dfrac{1}{k^h} \geq \dfrac{C}{nqk^{h-1}}$.

Suppose for the moment that $h = 1$. Then the last expression equals $\dfrac{C}{nq}$. Since the numbers C and n are constant and $\sum_{q \text{ prime}} \dfrac{1}{q} = \infty$, the sum of these probabilities for all q diverges to infinity. Therefore for any simple linear recurring sequence with characteristic $h = 1$ we expect the existence of infinitely many regular pseudoprimes of the form $t = pq$, where p is fixed.

If $h > 1$ then the sum of the reciprocals of the hth powers of primes converges and we therefore cannot expect that the analogous statement is valid for such sequences.

This observation together with the properties of the sequences with $h = 0$ justify the division of linear recurrent sequences into classes with respect to their characteristics.

Thirdly, the considerations in the second part allow us to make the following conclusion. For any prime p as above the probability that there exists some prime q such that $t = pq$ is a regular pseudoprime is bounded uniformly from below by positive constant independent of p. Since we can use infinitely many primes p we would expect for any simple linear recurring sequence the existence of infinitely many pseudoprimes of the form $t = pq$.

Finally let us make some comments which provide examples of linear recurring sequences of characteristic 1.

Recall that by u we have denoted the rank of the torsion-free part of the group of units in K.

We remark that $u = 0$ only if $g(x)$ is a cyclotomic polynomial.

If for some linear recurring sequence we have $u = 1$ for the corresponding polynomial $g(x)$, then $h = 1$ and according to heuristic arguments given above we expect that for a prime p which splits completely in K and fulfils the congruence $p \equiv 1 \pmod{M}$ for a certain M there are infinitely many pseudoprimes n, which are the product of the prime p and of an other prime q for which $q \equiv 1 \pmod{p-1}$.

The examples of such sequences are linear recurring sequences for which $b_0 = \pm 1$ and the splitting field K of the characteristic polynomial $g(x)$ is a real quadratic field or a cubic field, which is not totally real or a biquadratic totally imaginary field.

Acknowledgement

I would like to thank Professor Schinzel for calling my attention to Theorem 3 of the paper [10].

REFERENCES

[1] ADAMS, W.—SHANKS, D.: *Strong primality tests that are not sufficient*, Math. Comp. **39** (1982), 255-300.

[2] CASSELS, J. W. S.—FRÖHLICH, A.: *Algebraic Number Theory*, Academic Press, London, 1967.

[3] HASSE, H.: *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Jahresber. Deutsch. Math.-Verein. **35** (1926), 1–55, (Addendum, ibid. **36** (1927), 233-311).

[4] JAKUBEC, S.—NEMOGA, K.: *On a conjecture concerning sequences of the third order*, Math. Slovaca **36** (1986), 85-89.

[5] MARKO, F.: *Schinzel's conjecture H and divisibility in abelian linear recurring sequences*, Colloq. Math. **LIX** (1990), 1-7.

[6] MARKO, F.: *Pseudoprimes with respect to linear recurring sequences.* (Slovak), Thesis, Bratislava, 1991.

[7] NARKIEWICZ, W.: *Elementary and Analytic Theory of Algebraic Numbers*, Polish Scientific Publishers, Warszawa, 1974.

[8] PRACHAR, K.: *Primzahlverteilung*, Springer Verlag, Berlin-Göttingen-Heidelberg, 1957.

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

[10] SCHINZEL, A.: *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), 245–274, (Addendum, ibid. **36** (1980), pp.101-104).

Received November 12, 1991

Institute of Mathematics
Slovak Academy of Science
Štefánikova 49
814 73 Bratislava
Czecho-Slovakia