BULLETIN OF THE POLISH
ACADEMY OF SCIENCES
MATHEMATICS
Vol. 52, No. 2, 2004

NUMBER THEORY

On Alternatives of Polynomial Congruences

by

Mariusz SKAŁBA

Presented by Andrzej SCHINZEL

Summary. What should be assumed about the integral polynomials $f_1(x),\dots,f_k(x)$ in order that the solvability of the congruence $f_1(x)f_2(x)\cdots f_k(x)\equiv 0 \pmod p$ for sufficiently large primes p implies the solvability of the equation $f_1(x)f_2(x)\cdots f_k(x)=0$ in integers x? We provide some explicit characterizations for the cases when $f_j(x)$ are binomials or have cyclic splitting fields.

Let K be a number field and consider the following situation. The given polynomials $f_1(x),\dots,f_k(x)\in\mathcal{O}_K[x]$ have the property that for each prime ideal $\mathfrak{p}$ of $\mathcal{O}_K$ with sufficiently large norm (abbreviated: with s.l.n.), at least one of the congruences

$$(1)\qquad f_j(x)\equiv 0 \pmod{\mathfrak{p}},\qquad j=1,\dots,k,$$

is solvable in $x\in\mathcal{O}_K$. What can be said about $f_1,\dots,f_k$?

Essentially this question has been put and answered in terms of Galois theory by M. Fried in [3, Theorem 1]. Although the condition is quite simple it requires the explicit computation of relevant Galois groups, which is not easy. On the other hand, if one restricts to some classes of polynomials then it is possible to give a more explicit characterization in terms of the coefficients of the relevant polynomials. For example the case of binomials (which can be naturally called the case of power residues) is studied very thoroughly in [7].

Our main goal is to provide generalizations of the following beautiful result of D. Richman:

THEOREM 1 (D. Richman, unpublished manuscript [5], for $K=\mathbb{Q}$). *Let S denote a subset of a number field K such that $|S|\le q$, where q is a given*

2000 *Mathematics Subject Classification*: 11R20, 11A15.

Key words and phrases: polynomial congruences, power residues, Galois groups.

rational prime. Assume that for almost every prime ideal $\mathfrak{p}$ of K there is an element of S which is congruent modulo $\mathfrak{p}$ to a qth power. Then S contains a qth power of a number from K.

The first generalization allows the degrees q of power residues to be nonconstant.

Theorem 2. *Let Q be a finite set of odd primes and K a number field satisfying*

$$\{\zeta_q : q \in Q\} \cap K = \emptyset, \tag{2}$$

where ζ_q denotes a qth primitive root of unity. Moreover, for each $q \in Q$ let $A_q \subset K^*$ be a finite set satisfying $|A_q| \le q$. Assume that for each prime ideal $\mathfrak{p}$ of K with s.l.n. there exist $q \in Q$ and $a \in A_q$ such that the congruence

$$x^q \equiv a \pmod{\mathfrak{p}}$$

is solvable in $x \in \mathcal{O}_K$. Then there exist $q_0 \in Q$, $a \in A_{q_0}$ and $b \in K^*$ such that $a = b^{q_0}$.

This is an immediate consequence of Theorem 1 (Theorem 5 for $k = 1$) and the following more general theorem.

Theorem 3. *Let Q be a finite set of odd primes and K a number field satisfying* (2). *Moreover, for each $q \in Q$ let $A_q \subset K^*$ be a finite set. Assume that for each prime ideal $\mathfrak{p}$ of K with s.l.n. there exist $q \in Q$ and $a \in A_q$ such that the congruence*

$$x^q \equiv a \pmod{\mathfrak{p}}$$

is solvable in $x \in \mathcal{O}_K$. Then there exists $q_0 \in Q$ which is universal in the following sense. For each prime ideal $\mathfrak{p}$ of K with s.l.n. there exists $a \in A_{q_0}$ such that the congruence

$$x^{q_0} \equiv a \pmod{\mathfrak{p}}$$

is solvable in $x \in \mathcal{O}_K$.

Remark. The condition (2) excludes obviously $q = 2$ from the set Q. This exclusion is necessary as shown by the following example, due in principle to van der Waerden [9]:

$$Q = \{2, 3\}, \quad A_2 = \{-3\}, \quad A_3 = \{-5\}.$$

The main ingredient in the proof of the above theorem will be the next theorem which (we hope) is of some independent interest.

Theorem 4. *Assume that all the polynomials $g_1, \ldots, g_k, h_1, \ldots, h_l \in \mathcal{O}_K[x]$ have Abelian splitting fields over a number field K and that the congruence*

$$\prod_{i=1}^{k} g_i(x) \prod_{j=1}^{l} h_j(x) \equiv 0 \pmod{\mathfrak{p}}$$

is solvable for all prime ideals $\mathfrak{p}$ *of* K *with s.l.n. Moreover assume that*

$$\gcd\Big(\prod_{i=1}^{k}\deg g_i, \prod_{j=1}^{l}\deg h_j\Big) = 1.$$

Then either the congruence

$$\prod_{i=1}^{k} g_i(x) \equiv 0 \pmod{\mathfrak{p}}$$

is solvable for all prime ideals $\mathfrak{p}$ *of* K *with s.l.n., or the congruence*

$$\prod_{j=1}^{l} h_j(x) \equiv 0 \pmod{\mathfrak{p}}$$

is solvable for all prime ideals $\mathfrak{p}$ *of* K *with s.l.n.*

Another generalization of Richman's result can be obtained if we allow for more general "testing" modules. First recall a definition: for $I \lhd \mathcal{O}_K$ let $\Omega(I)$ denote the number of all prime ideal factors of I, counted with multiplicities.

THEOREM 5. *Let* q *be a rational prime and* K *a number field. Let* S *denote a subset of* K *such that* $|S| \le q^k + q^{k-1} + \dots + q$ *where* k *is a given natural number. Assume that for almost every ideal* I *of* K *with* $\Omega(I) \le k$ *there is an element of* S *which is congruent modulo* I *to a* q*th power. Then* S *contains a* q*th power of a number from* K*.*

Here the phrase "for almost every ideal I of K" means that possible exceptions are I such that $\gcd(I, J) \ne \mathcal{O}_K$, for a fixed $J \lhd \mathcal{O}_K$.

Our last theorem and corollaries concern the alternative of congruences (1) where the f_j are polynomials with cyclic Galois groups. We transfer some result on binomials, contained in [7], to the cyclic case.

THEOREM 6. *Let* K *be a number field*, $n \in \mathbb{N}$, *and assume that*

$$\gcd(n, [K(\zeta_n) : K]) = 1.$$

Consider k *polynomials* $f_1, \dots, f_k \in \mathcal{O}_K[x]$, *irreducible over* K, *with splitting fields cyclic of degrees* $n_j = \deg f_j \mid n$*. Then the following two conditions are equivalent*:

(i) *For almost all prime ideals* $\mathfrak{p}$ *of* K *there exists* $j = j(\mathfrak{p})$ *such that the congruence*

$$f_j(x) \equiv 0 \pmod{\mathfrak{p}}$$

is solvable in $x \in \mathcal{O}_K$*.*

(ii) *There exists an involution σ of the family of all subsets of $\{1,\ldots,k\}$ such that for each $A\subset\{1,\ldots,k\}$,*

$$|\sigma(A)|\equiv|A|+1 \pmod 2$$

and

$$\prod_{j\in\sigma(A)}\mathcal{L}_j^n=\gamma_A^n\prod_{j\in A}\mathcal{L}_j^n, \tag{3}$$

where $\gamma_A\in K(\zeta_n)$ and

$$\mathcal{L}_j=\sum_{l=0}^{n_j-1}\zeta_{n_j}^l\sigma_j^l(b_j)$$

are Lagrange resolvents of f_j, $j=1,\ldots,k$ (b_j and σ_j are a fixed root of f_j and a fixed generator of the Galois group of its splitting field, respectively).

Corollary 1 (M. Fried [3], M. A. Filaseta and D. R. Richman [2]). *Let $f_j(x)=x^2+b_jx+c_j\in\mathbb{Z}[x]$ and $\Delta_j=b_j^2-4c_j$ for $j=1,\ldots,k$. The following two conditions are equivalent:*

(i) *For each sufficiently large prime p there exists $j\in\{1,\ldots,k\}$ such that the congruence*

$$f_j(x)\equiv 0 \pmod p$$

is solvable in integers x.

(ii) *There exists $J\subset\{1,\ldots,k\}$ of odd cardinality and $d\in\mathbb{Z}$ such that*

$$\prod_{j\in J}\Delta_j=d^2.$$

Remark. The most general assertion concerning the above situation is contained in Corollary 2 of [7].

On the other hand we have not found any reference to the following theorem.

Corollary 2. *Let $f_j(x)=x^3+p_jx+q_j\in\mathbb{Z}[x]$ for $j=1,\ldots,k$ and assume that for each j, $\Delta_j:=-4p_j^3-27q_j^2=d_j^2$ with $d_j\in\mathbb{Z}$. The following two conditions are equivalent:*

(i) *For each sufficiently large prime p there exists $j\in\{1,\ldots,k\}$ such that the congruence*

$$x^3+p_jx+q_j\equiv 0 \pmod p$$

is solvable in integers x.

(ii) *There exists an involution σ of the family of all subsets of $\{1,\ldots,k\}$ such that for each $A\subset\{1,\ldots,k\}$,*

$$|\sigma(A)|\equiv|A|+1 \pmod 2$$

and

$$\prod_{j\in\sigma(A)}\Big(-\frac{27}{2}q_j+\frac{3}{2}d_j\sqrt{-3}\Big)=\gamma_A^3\prod_{j\in A}\Big(-\frac{27}{2}q_j+\frac{3}{2}d_j\sqrt{-3}\Big), \tag{4}$$

where $\gamma_A\in\mathbb{Q}(\sqrt{-3})^*$.

Example. The following polynomials are irreducible over $\mathbb{Q}$ and their discriminants are squares (so their splitting fields over $\mathbb{Q}$ are cyclic):

$$f_1(x)=x^3-7x+7,\qquad f_3(x)=x^3-91x+273,$$
$$f_2(x)=x^3-13x+13,\qquad f_4(x)=x^3-91x+182.$$

For a suitable choice of $\mathcal{L}_j$ for $j=1,2,3,4$ we can write

$$\mathcal{L}_1^3=7\Big(-\frac{27}{2}+\frac{3}{2}\sqrt{-3}\Big),\qquad \mathcal{L}_3^3=91\Big(-\frac{81}{2}-\frac{33}{2}\sqrt{-3}\Big),$$
$$\mathcal{L}_2^3=13\Big(-\frac{27}{2}+\frac{15}{2}\sqrt{-3}\Big),\qquad \mathcal{L}_4^3=91(-27+24\sqrt{-3}).$$

For $\alpha,\beta\in\mathbb{Q}(\sqrt{-3})$ we write $\alpha\sim\beta$ if $\alpha=\beta\gamma^3$ for some $\gamma\in\mathbb{Q}(\sqrt{-3})$. We have

$$\mathcal{L}_3^3\sim\mathcal{L}_1^3\mathcal{L}_2^3,\qquad \mathcal{L}_4^3\sim\mathcal{L}_1^3(\mathcal{L}_2^3)^2$$

so we can take the following σ:

$$\{1\}\mapsto\{2,4\},\quad \{2\}\mapsto\{1,2,3,4\},\quad \{3\}\mapsto\{1,2\},\quad \{4\}\mapsto\{2,3\},$$
$$\{2,3,4\}\mapsto\{1,3\},\quad \{1,2,3\}\mapsto\{1,4\},\quad \{1,2,4\}\mapsto\{3,4\},\quad \{1,3,4\}\mapsto\emptyset.$$

By Corollary 2 our polynomials have the crucial property that the congruence

$$f_1(x)f_2(x)f_3(x)f_4(x)\equiv 0 \pmod p$$

is solvable for all primes p.

The proofs are based on six lemmas.

Lemma 1. *If* $G_1,\dots,G_k,H_1,\dots,H_l$ *are normal subgroups of a group* G *and* $((G:G_i),(G:H_j))=1$ *for all* i,j, *then either* $G=\bigcup G_i$ *or* $G=\bigcup H_j$ *or* $G\neq\bigcup G_i\cup\bigcup H_j$.

Remark. The assumption that $G_1,\dots,G_k,H_1,\dots,H_l$ are normal is essential as the following example shows: $G=S_3$, G_1,G_2,G_3 are all its subgroups of index 3, and H_1 is the unique subgroup of index 2.

Proof. The following short proof is due to A. Schinzel. Let

$$r=\operatorname{lcm}(G:G_i),\qquad s=\operatorname{lcm}(G:H_j)$$

and assume that

$$x\notin\bigcup_{i=1}^{k}G_i,\qquad y\notin\bigcup_{j=1}^{l}H_j. \tag{5}$$

Then $x^s \in \bigcap_{j=1}^{l} H_j$ and $y^r \in \bigcap_{i=1}^{k} G_i$. Hence $x^s y^r \in G_i$ would give $x^s \in G_i$, and $x^s y^r \in H_j$ would give $y^r \in H_j$. On the other hand, there exist integers t and u such that

$$st \equiv 1 \pmod{r}, \qquad ru \equiv 1 \pmod{s}.$$

Hence $x^s \in G_i$ would give $x^{st} \in G_i$ and since $x^r \in G_i$, we would obtain $x \in G_i$, contrary to (5). Similarly $y^r \in H_j$ would give $y \in H_j$, contrary to (5).

LEMMA 2 (M. Fried, Theorem 1 of [3]). *Let M be a number field and consider a finite family F of polynomials $f(x) \in \mathcal{O}_M[x]$. Assume that all the splitting fields M_f, $f \in F$, are Abelian over M. Let L be their compositum. Then the following two conditions are equivalent*:

(i) *For each prime ideal $\mathfrak{p}$ of $\mathcal{O}_M$ with s.l.n. there exist $f \in F$ and $x \in \mathcal{O}_M$ such that $f(x) \equiv 0 \pmod{\mathfrak{p}}$*,

(ii) $\mathrm{Gal}(L/M) = \bigcup_{f \in F} \mathrm{Gal}(L/M_f)$.

Theorem 1 of [3] is much more general, but we have adapted it above to the Abelian case.

LEMMA 3. *Let $w_n(M)$ be the number of nth roots of unity contained in a number field M and assume that*

$$(w_n(M), \mathrm{lcm}[M(\zeta_q) : M]) = 1, \tag{6}$$

where the least common multiple is over all prime divisors q of n and additionally $q = 4$ if $4 \mid n$. Let $\beta_1, \ldots, \beta_l \in M^*$. Then the following two conditions are equivalent:

(i) *For each prime ideal $\mathfrak{p}$ of M with s.l.n. there exists $1 \le j \le l$ such that the congruence*

$$x^n \equiv \beta_j \pmod{\mathfrak{p}}$$

is solvable in M.

(ii) *There exists an involution σ of the family of all subsets of $\{1, \ldots, l\}$ such that for each $A \subset \{1, \ldots, l\}$*,

$$|\sigma(A)| \equiv |A| + 1 \pmod{2}$$

and

$$\prod_{j \in \sigma(A)} \beta_j = \gamma_A^n \prod_{j \in A} \beta_j, \tag{7}$$

where $\gamma_A \in M^*$.

Proof. This is a special case of Corollary 1 of [7], for $k = 0$.

LEMMA 4 (A. Schinzel, Theorem 2 of [6]). *Let K be a field*, *m a positive integer not divisible by* char K, *and w the number of mth roots of unity in K.*

Let M be the splitting field of $x^m - a$ over K for some $a \in K$. Then

$$M/K \text{ is Abelian } \Leftrightarrow a^w \in K^m.$$

For a simple proof of the above classical result see also [10].

LEMMA 5. *Let M be a number field and assume that $\zeta_q \in M$, where q is a fixed rational prime. Let $\beta_1, \ldots, \beta_l \in M^*$ and let V be the subgroup of M^*/M^{*q} generated by $\beta_j M^*$, $j = 1, \ldots, l$. Then for each character $\chi \in \widehat{V}$ one can find infinitely many prime ideals $\mathfrak{p}$ of M of degree one over $\mathbb{Q}$ for which*

$$\chi(\beta) = (\beta \,|\, \mathfrak{p})_q \quad \text{for } \beta \in V,$$

where the symbol on the right hand side is the qth power residue symbol.

Proof. We choose a maximal F_q-independent subset $a_1, \ldots, a_n$ of $\beta_1, \ldots, \beta_l$ and apply the Chebotarev theorem ([1], also [4, Theorem 7.13]).

LEMMA 6. *Let $n > k$ be positive integers and V an n-dimensional vector space over a finite field F_q. If a set $S \subset V - \{0\}$ intersects each linear subspace W of V satisfying $\dim V/W = k$ then*

$$|S| \geq q^k + q^{k-1} + \cdots + q + 1. \tag{8}$$

Proof. The proof is given in [8].

Proof of Theorem 4. We apply Lemma 2 for $M = K$ and the family $F = \{g_1, \ldots, g_k, h_1, \ldots, h_l\}$ to infer that

$$\mathrm{Gal}(L/M) = \bigcup_{f \in F} \mathrm{Gal}(L/M_f).$$

Now we apply Lemma 1 for $G := \mathrm{Gal}(L/M)$, $G_i = \mathrm{Gal}(L/M_{g_i})$, $i = 1, \ldots, k$, $H_j = \mathrm{Gal}(L/M_{h_j})$, $j = 1, \ldots, l$. Because

$$(G : G_i) = |\mathrm{Gal}(M_{g_i}/M)| = \deg g_i, \qquad (G : H_j) = |\mathrm{Gal}(M_{h_j}/M)| = \deg h_j,$$

the assumption of Lemma 1 is satisfied. Hence the assertion follows by applying first Lemma 1, and then Lemma 2 again, but now in the opposite direction.

Proof of Theorem 3. Let $n = \prod_{q \in Q} q$ and consider $M := K(\zeta_n)$. Moreover, for each pair $(q, a^{(q)})$ with $q \in Q$ and $a^{(q)} \in A_q$ let $M_{q,a^{(q)}} := M(\sqrt[q]{a^{(q)}})$ be the splitting field of $x^q - a^{(q)}$ over M. Obviously, $M_{q,a^{(q)}}$ is Abelian of exponent dividing q. Applying Theorem 4 to the system of polynomials $f_{q,a^{(q)}}(x) := x^q - a^{(q)}$ we find that there exists $q_0 \in Q$ such that the alternative of congruences

$$x^{q_0} \equiv a^{(q_0)} \pmod{\mathfrak{p}}, \qquad a^{(q_0)} \in A_{q_0},$$

is solvable for all prime ideals $\mathfrak{p}$ of M with s.l.n. Now we use Lemma 3 for $n = q_0$ and $(\beta_j)_{j=1}^{l}$ being all the elements $a^{(q_0)} \in A_{q_0}$, so $l = |A_{q_0}|$. Using the implication (i)⇒(ii) of Lemma 3 we deduce that for each $A \subset \{1,\dots,l\}$,

$$\gamma_A^{q_0} = \prod_{j\in\sigma(A)} \beta_j \prod_{j\in A} \beta_j^{-1} \in M^{*q_0},$$

where $\gamma_A \in M = K(\zeta_n)$. On the other hand, all factors β_j belong to K^* and therefore $\gamma_A^{q_0} \in K^*$. The field $K(\gamma_A)$ is an Abelian extension of K as a subextension of $M = K(\zeta_n)$. By Lemma 4 we obtain $(\gamma_A^{q_0})^1 \in K^{*q_0}$. The proof is finished by referring to the implication (ii)⇒(i) of Lemma 3.

Proof of Theorem 5. Put $M := K(\zeta_q)$. Let $S = \{\beta_1,\dots,\beta_l\}$ and adopt the notation from Lemma 5 and its proof. We will now verify that the assumptions of Lemma 6 are satisfied for the set S, with the convention that its elements are now considered mod M^{*q}, and assuming that $S \subset V - \{0\}$. Consider a subspace W of V with $\dim V/W = k$. Such a subspace W can be described by a system of k "linear" equations:

$$\chi_1(v) = \chi_2(v) = \dots = \chi_k(v) = 1 \tag{9}$$

with properly chosen $\chi_1,\dots,\chi_k \in \widehat{V}$. Now we use Lemma 5 and for each $j = 1,\dots,k$ we choose a prime ideal $\mathfrak{p}_j$ such that

$$\chi_j(v) = (v \mid \mathfrak{p}_j)_q \quad \text{for } v \in V.$$

Put $I := \prod_{j=1}^k \mathfrak{p}_j$. By the assumption of the theorem there is a $v \in S$ such that v is a qth power residue mod I. Hence this v satisfies the system (9) and it belongs to W by definition. Using Lemma 6 we obtain the inequality (8), which contradicts the assumption of the theorem. Therefore $S \subset V - \{0\}$ is impossible. This means that $M^{*q} \cap S \neq \emptyset$. If $\zeta_q \in K$, then $M = K$ and we are done. In the case $\zeta_q \notin K$ we use Lemma 4 and infer again that $K^{*q} \cap S \neq \emptyset$.

Proof of Theorem 6. Let $L_1,\dots,L_k$ be splitting fields of $f_1,\dots,f_k$ over K. Let $M_1,\dots,M_k$ be splitting fields of $f_1,\dots,f_k$ over $M := K(\zeta_n)$. By the classical Galois theory

$$M_j = M(\mathcal{L}_j), \quad \mathcal{L}_j^{n_j} \in K(\zeta_{n_j}) \subset M.$$

Elementary considerations (using the assumption $\zeta_n \in M$) lead to the equivalence of two conditions:

(a) For a prime ideal $\mathfrak{p}$ of M there exists $j = j(\mathfrak{p})$ such that the congruence

$$x^{n_j} \equiv \mathcal{L}^{n_j} \pmod{\mathfrak{p}}$$

has a solution in $x \in M$.

(b) For a prime ideal $\mathfrak{p}$ of M there exists $j = j(\mathfrak{p})$ such that the congruence

$$x^n \equiv \mathcal{L}^n \pmod{\mathfrak{p}}$$

has a solution in $x \in M$.

By the construction of Lagrange resolvent condition (a) is equivalent to:

(c) For a prime ideal $\mathfrak{p}$ of M there exists $j = j(\mathfrak{p})$ such that the congruence

$$f_j(x) \equiv 0 \pmod{\mathfrak{p}}$$

has a solution in $x \in M$.

What is left is to prove the equivalence of the following two set-theoretic equalities:

(iii) $\mathrm{Gal}(L'/M) = \bigcup_{j=1}^{k} \mathrm{Gal}(L'/M_j)$,

(iv) $\mathrm{Gal}(L/K) = \bigcup_{j=1}^{k} \mathrm{Gal}(L/L_j)$,

where L is the compositum of $L_1, \ldots, L_k$ and L' is the compositum of $M_1, \ldots, M_k$.

Indeed, then (i) is equivalent to (iv) (by Lemma 2), (iv) is equivalent to (iii), and (iii) to (ii) (by Lemmas 2 and 3).

The reasoning which will establish the equivalence of (iii) and (iv) will be purely field-theoretical. The implication (iv)⇒(iii) is obvious. For the proof of (iii)⇒(iv) assume that (iii) holds and consider an arbitrary $\sigma \in \mathrm{Gal}(L/K)$.

Since $\mathrm{Gal}(L/K) \hookrightarrow \prod_{j=1}^{k} \mathrm{Gal}(L_j/K)$ we see that the exponent of $\mathrm{Gal}(L/K)$ divides n, hence

$$p \mid (L : K) \;\Rightarrow\; p \mid n. \tag{10}$$

L', being the compositum of $M_1, \ldots, M_k$ is of the form $L' = L(\zeta_n) = LM$.

Using (10) and the assumption $\gcd(n, [M : K]) = 1$ we obtain

$$L \cap M = K.$$

This equality enables us to extend $\sigma \in \mathrm{Gal}(L/K)$ to $\widetilde{\sigma} \in \mathrm{Gal}(LM/M) = \mathrm{Gal}(L'/M)$. Because of (iii) there exists j such that $\widetilde{\sigma}|_{M_j} = \mathrm{id}$. Hence $\sigma|_{L_j} = \mathrm{id}$ as well, and we have proved (iv).

Acknowledgements. I am greatly indebted to Prof. J. Browkin and Prof. A. Schinzel for their kind interest in this paper and many valuable suggestions.

References

[1] N. G. Chebotarev, *Der Hilbertsche Satz*, Visti VUAN 1923, 3–7; Russian translation: Collected Works, Vol. 1, Moscow–Leningrad, 1949, Vol. 1, 14–17.

[2] M. Filaseta and D. R. Richman, *Sets which contain a quadratic residue mod p for almost all p*, Math. J. Okayama Univ. 31 (1989), 1–8.

[3] M. Fried, *Arithmetical properties of value sets of polynomials*, Acta Arith. 15 (1969), 91–115.

[4] W. Narkiewicz, *Elementary and Analytic Theory of Algebraic Numbers*, PWN, Warszawa, 1990.

[5] D. R. Richman, *On q-th power residues*, unpublished manuscript, 1987.

[6] A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. 32 (1977), 245–274; Addendum and corrigendum, 36 (1980), 101–104.

[7] A. Schinzel and M. Skałba, *On power residues*, ibid. 108 (2003), 77–94.

[8] M. Skałba, *Power residue problem on elliptic curves*, Manuscripta Math. 114 (2004), 37–43.

[9] B. L. van der Waerden, *Noch eine Bemerkung zu der Arbeit "Zur Arithmetik der Polynome" von U. Wegner in Math. Ann. 105, 628–631*, Math. Ann. 109 (1934), 679–680.

[10] J. Wójcik, *Contributions to the theory of Kummer extensions*, Acta Arith. 40 (1982), 155–174.

Mariusz Skałba
Institute of Mathematics
Polish Academy of Sciences
P.O. Box 21
00-956 Warszawa, Poland
E-mail: skalba@impan.gov.pl

Received November 5, 2003;
received in final form December 12, 2003 (7357)