ACTA ARITHMETICA
108.1 (2003)

On power residues

by

A. Schinzel and M. Skałba (Warszawa)

Let n be a positive integer, K a number field, $\alpha_i \in K$ $(1 \le i \le k)$, $\beta \in K$. A simple necessary and sufficient condition was given in [7] in order that, for almost all prime ideals $\mathfrak{p}$ of K, solubility of the k congruences $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$ should imply solubility of the congruence $x^n \equiv \beta \pmod{\mathfrak{p}}$, where $n_i \mid n$. The aim of this paper is to extend that result to the case where the congruence $x^n \equiv \beta \pmod{\mathfrak{p}}$ is replaced by the alternative of l congruences $x^n \equiv \beta_j \pmod{\mathfrak{p}}$. The general result is quite complicated, but it simplifies if n or K satisfy some restrictions. Here are precise statements, in which ζ_n denotes a primitive nth root of unity, $|A|$ is the cardinality of a set A, $K^n = \{x^n : x \in K\}$ and $\mathcal{F}$ is the family of all subsets of $\{1, \ldots, l\}$.

Theorem 1. *Let n and n_i be positive integers with $n_i \mid n$ $(1 \le i \le k)$, K be a number field and $\alpha_i, \beta_j \in K^*$ $(1 \le i \le k,\ 1 \le j \le l)$. Consider the implication*

(i) *solubility in K of the k congruences $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$ implies solubility in K of at least one of the l congruences $x^n \equiv \beta_j \pmod{\mathfrak{p}}$.*

Then (i) *holds for almost all prime ideals $\mathfrak{p}$ of K if and only if*

(ii) *for every unitary divisor $m > 1$ of n and, if $n \equiv 0 \pmod 4$, for every $m = 2m^*$, where m^* is a unitary divisor of the odd part of n, there exists an involution σ_m of $\mathcal{F}$ such that for all $A \subset \{1, \ldots, l\}$,*

$$|\sigma_m(A)| \equiv |A| + 1 \pmod 2, \tag{1}$$

$$\prod_{j \in \sigma_m(A)} \beta_j = \prod_{j \in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i m/(m,n_i)} \Gamma^m, \tag{2}$$

where $a_i \in \mathbb{Z}$, $\Gamma \in K(\zeta_m)^*$.

Corollary 1. *Let $w_n(K)$ be the number of nth roots of unity contained in K and assume that*

$$(w_n(K), \operatorname{lcm}[K(\zeta_q) : K]) = 1, \tag{3}$$

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

where the least common multiple is over all prime divisors q of n and additionally $q = 4$ if $4 \mid n$. The implication (i) *holds for almost all prime ideals $\mathfrak{p}$ of K if and only if there exists an involution σ of $\mathcal{F}$ such that for all $A \subset \{1, \ldots, l\}$,*

$$|\sigma(A)| \equiv |A| + 1 \pmod 2 \tag{4}$$

and

$$\prod_{j \in \sigma(A)} \beta_j = \prod_{j \in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i n/n_i} \gamma^n, \tag{5}$$

where $a_i \in \mathbb{Z}$, $\gamma \in K^*$.

The condition (3) holds for every K if $n = 2$ or $n = l^e$, where l is an odd prime, and for $K = \mathbb{Q}$ if n is odd.

Corollary 2. *For $n = n_i = 2$ $(1 \le i \le k)$,* (i) *holds for almost all prime ideals $\mathfrak{p}$ of K if and only if*

(iii) *there exists a subset A_0 of $\{1, \ldots, l\}$ such that*

$$|A_0| \equiv 1 \pmod 2 \tag{6}$$

and

$$\prod_{j \in A_0} \beta_j = \prod_{i=1}^{k} \alpha_i^{a_i} \gamma_0^2, \tag{7}$$

where $a_i \in \mathbb{Z}, \gamma_0 \in K^*$.

Corollary 2 contains as a special case ($K = \mathbb{Q}$, $k = 0$) a theorem of Fried [3], rediscovered by Filaseta and Richman [2].

The case $n = 2^e$ $(e \ge 2)$ is covered by the following corollary, in which τ denotes the greatest integer such that $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$. This corollary is of interest only if $\zeta_4 \notin K$, otherwise (3) holds.

Corollary 3. *For $n = 2^e$ $(e \ge 2)$ and $n_i > 1$ $(1 \le i \le k)$,* (i) *holds for almost all prime ideals $\mathfrak{p}$ of K if and only if simultaneously* (iii) *holds and*

(iv) *there exists an involution σ of $\mathcal{F}$ such that for all $A \subset \{1, \ldots, l\}$ we have* (4) *and*

$$\prod_{j \in \sigma(A)} \beta_j = \varepsilon \prod_{j \in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i n/n_i} \gamma^n, \tag{8}$$

where $a_i \in \mathbb{Z}$, $\gamma \in K^*$ and

$$\varepsilon \in \begin{cases} \{1, -1\} & \text{if } e < \tau, \\ \{1, (-1)^{n/2^\tau} (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2}\} & \text{if } e \ge \tau. \end{cases} \tag{9}$$

The case $K = \mathbb{Q}$, n odd is covered by Corollary 1. The case $K = \mathbb{Q}$, n even is covered by the following

THEOREM 2. *Let* $n = 2^\nu n^*$, $\nu > 0$, n^* *odd*, $n_i \mid n$ $(1 \le i \le k)$, $K = \mathbb{Q}$. *The implication* (i) *holds for almost all prime ideals* $\mathfrak{p}$ *of* K *if and only if*

(v) *for every* $m = 2^\nu m^*$ *and, if* $\nu = 2$, *for every* $m = 2m^*$, *where* m^* *is a unitary divisor of* n^*, *there exists an involution* σ_m *of* $\mathcal{F}$ *such that for all* $A \subset \{1, \ldots, l\}$ *we have* (1) *and*

$$\prod_{j \in \sigma_m(A)} \beta_j = \varepsilon \prod_{j \in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i m/(m,n_i)} \delta^{m/2} \gamma^m,$$

where $a_i \in \mathbb{Z}$, $\gamma \in \mathbb{Q}^*$, δ *is a fundamental discriminant dividing* m *and*

$$\varepsilon \in \begin{cases} \{1, -2^{m/2}\} & \text{if } m \equiv 4 \pmod 8, \\ \{1\} & \text{otherwise.} \end{cases}$$

COROLLARY 4. *Let* $n = 2^\nu n^*$, $\nu \ge 0$, n^* *odd*, $\beta_1, \beta_2 \in \mathbb{Q}^*$. *The alternative of congruences*

$$x^n \equiv \beta_j \pmod p \qquad (1 \le j \le 2)$$

is soluble for almost all primes p, *if and only if either*

$$\beta_i \in \mathbb{Q}^n \tag{10}$$

for some $i \le 2$, *or there is a* $j \le 2$, *a prime* $q \mid n^*$ *with* $q^e \parallel n^*$ *and some* $\gamma_1, \gamma_2 \in \mathbb{Q}$ *such that one of the following holds*:

- $\nu = 1$ *and*

$$\beta_j = ((-1)^{(q-1)/2} q)^{n/2} \gamma_1^n, \qquad \beta_{3-j} = \gamma_2^{n/q^e}, \tag{11}$$

- $\nu = 2$ *and either*

$$\beta_j = -2^{n/2} \gamma_1^n, \qquad \beta_{3-j} = \gamma_2^{n/2} \tag{12}$$

or

$$\beta_j = q^{n/2} \gamma_1^n, \qquad \beta_{3-j} \in \{\gamma_2^{n/q^e}, -2^{n/2q^e} \gamma_2^{n/q^e}\}, \tag{13}$$

- $\nu \ge 3$ *and either*

$$\beta_j = 2^{n/2} \gamma_1^n \tag{14}$$

or

$$\beta_j \in \{q^{n/2} \gamma_1^n, 2^{n/2} q^{n/2} \gamma_1^n\}, \qquad \beta_{3-j} \in \{\gamma_2^{n/q^e}, 2^{n/2q^e} \gamma_2^{n/q^e}\}. \tag{15}$$

The proofs are based on eight lemmas and use the *nth power residue symbol*, which is defined as follows. If a number field K contains ζ_n, then for every prime ideal $\mathfrak{p}$ of K prime to n and every $\mathfrak{p}$-adic unit α of K, $(\alpha|\mathfrak{p})_n$ is the unique number ζ_n^j that satisfies the congruence

$$\alpha^{(N\mathfrak{p}-1)/n} \equiv \zeta_n^j \pmod{\mathfrak{p}},$$

where $N\mathfrak{p}$ is the absolute norm of $\mathfrak{p}$. Moreover, $\operatorname{ind} \alpha$ is the index of α with respect to a fixed primitive root modulo the relevant prime ideal.

We give two proofs of Corollary 2, one short using Theorem 1 and the other longer, but using neither Theorem 1 nor the lemmas bellow, except the classical Lemma 3.

At the end of the paper we give a deduction of the more difficult necessity part of Theorem 1 of [7] from Theorem 1 above.

We thank Professor J. Browkin for some helpful suggestions.

LEMMA 1. *Let G be a finite abelian group, $\widehat{G}$ its group of characters and $g_j \in G$ $(1 \le j \le l)$. If*

$$\prod_{j=1}^{l}(\chi(g_j)-1)=0 \tag{16}$$

for every $\chi \in \widehat{G}$ then there exists an involution σ of $\mathcal{F}$ such that for all $A \subset \{1,\ldots,l\}$ we have (4) *and*

$$\prod_{j\in\sigma(A)} g_j = \prod_{j\in A} g_j.$$

Proof. For $g \in G$ let

$$c(g) = \sum_{\substack{A\subset\{1,\ldots,l\}\\ \prod_{j\in A} g_j = g}} (-1)^{|A|}.$$

The equality (16) can be written in the form

$$\sum_{g\in G} c(g)\chi(g) = 0$$

or, if h is any fixed element of G,

$$\sum_{g\in G} c(g)\chi(gh^{-1}) = 0.$$

Summing over all characters χ gives $|G|c(h) = 0$, hence $c(h) = 0$, and h being arbitrary, $c(g) = 0$ for all $g \in G$. It follows that for all $g \in G$ the number of subsets A of $\{1,\ldots,l\}$ with $\prod_{j\in A} g_j = g$ and $|A|$ odd equals the corresponding number with $|A|$ even, hence there is an involution σ_g of the family of subsets A of $\{1,\ldots,l\}$ with $\prod_{j\in A} g_j = g$ such that

$$|\sigma_g(A)| \equiv |A| + 1 \pmod 2.$$

The involution σ is obtained by combining all involutions σ_g.

LEMMA 2. *Let n be a positive integer, K and L be number fields, $K(\zeta_n) \subset L$, $\beta_j \in K^*$ $(1 \le j \le l)$. Let H be the multiplicative group generated by $\beta_1,\ldots,\beta_l$, and H_1 the intersection of H with L^n. For every $\chi \in \widehat{H/H_1}$ there exists a set $\mathcal{P}$, with positive Dirichlet density, of prime ideals $\mathfrak{P}$ of L such* *that*

$$\chi([x]) = (x|\mathfrak{P})_n, \tag{17}$$

where $[x]$ *is the coset of* H_1 *in* H *containing* x.

Proof. By a theorem of Skolem [9] the field L has a multiplicative basis $\zeta_w, \pi_1, \pi_2, \ldots$, where ζ_w is a root of unity and $\pi_1, \pi_2, \ldots$ are generators of infinite order. Let π_s be the last generator that occurs in the representation of $\alpha_1, \ldots, \alpha_k, \beta_1, \ldots, \beta_l$. We have

$$H/H_1 < J/J^n,$$

where J is the group generated by $\zeta_w, \pi_1, \ldots, \pi_s$. Indeed, $H < J$ and the relations $h_1 \in H$, $h_2 \in H$ and $h_1 h_2^{-1} \in J^n$ together imply $h_1 h_2^{-1} \in H_1$. Hence for every $\chi \in \widehat{H/H_1}$ there exists $\chi_1 \in \widehat{J/J^n}$ such that

$$\chi(y) = \chi_1(y) \quad \text{for } y \in H/H_1. \tag{18}$$

Clearly $\chi_1(y)^n = 1$ for all $y \in J/J^n$. On the other hand, by Theorem 4 of [8] with $\sigma = 1$, for any integers $c_0, \ldots, c_s$ there exist infinitely many prime ideals $\mathfrak{P}$ of L such that

$$(\zeta_w|\mathfrak{P})_n = \zeta_n^{c_0}, \quad (\pi_r|\mathfrak{P})_n = \zeta_n^{c_r} \quad (1 \le r \le s).$$

Since the proof is via the Chebotarev density theorem (see [8, p. 263]), the infinite set of prime ideals in question has a positive Dirichlet density. Hence for every $\chi_1 \in \widehat{J/J^n}$ there exists a set $\mathcal{P}$ of positive Dirichlet density such that for $\mathfrak{P} \in \mathcal{P}$,

$$\chi_1(\overline{x}) = (x|\mathfrak{P})_n \quad \text{for } x \in J, \tag{19}$$

where $\overline{x}$ is the coset of J^n in J containing x. Since by (18),

$$\chi([x]) = \chi_1(\overline{x}) \quad \text{for } x \in H,$$

(17) follows from (19).

LEMMA 3. *Let* $n \in \mathbb{N}$, K *be a number field*, $\zeta_n \in K$, *and* $\alpha_1, \ldots, \alpha_k, \beta$ *elements of* K^*. *If*

$$\sqrt[n]{\beta} \in K(\sqrt[n]{\alpha_1}, \ldots, \sqrt[n]{\alpha_k}),$$

then

$$\beta = \prod_{i=1}^{k} \alpha_i^{a_i} \gamma^n,$$

where $a_i \in \mathbb{Z}$, $\gamma \in K^*$.

Proof. See [5, p. 222, formula (2)].

LEMMA 4. *The condition* (i) *for almost all prime ideals* $\mathfrak{p}$ *of* K *implies the existence of an involution* σ *of* $\mathcal{F}$ *such that*, *for all* $A \subset \{1, \ldots, l\}$, (4) *holds and*

$$\prod_{j\in\sigma(A)} \beta_j = \prod_{j\in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i n/n_i} \Gamma^n \quad \textit{for some } a_i \in \mathbb{Z},\ \Gamma \in K(\zeta_n)^*. \tag{20}$$

Proof. Let χ be a character of the group H/H_1 described in Lemma 2 with $L = K(\zeta_n, \xi_1, \ldots, \xi_k)$, where $\xi_i^{n_i} = \alpha_i$ $(1 \le i \le k)$. By Lemma 2 there exists a set $\mathcal{P}$, with positive Dirichlet density, of prime ideals $\mathfrak{P}$ of L such that

$$(x|\mathfrak{P})_n = \chi([x]) \quad \text{for } x \in H, \tag{21}$$

where $[x]$ is the coset of H_1 in H containing x. Since the prime ideals of degree greater than 1 have Dirichlet density 0 and the relative norms of prime ideals from $\mathcal{P}$ have positive Dirichlet density, there is $\mathfrak{P} \in \mathcal{P}$ such that $\mathfrak{p} = N_{L/K}\mathfrak{P}$ has the property that solubility in K of the k congruences $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$ implies solubility of at least one of the l congruences $x^n \equiv \beta_j \pmod{\mathfrak{p}}$. Moreover, the congruence $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{P}}$ has the solution $x = \xi_i$ in L, hence, $\mathfrak{P}$ being of relative degree 1, the congruence $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$ has a solution in K and, by (i),

$$\prod_{j=1}^{l}((\beta_j|\mathfrak{P})_n - 1) = 0.$$

By (21) we have

$$\prod_{j=1}^{l}(\chi([\beta_j]) - 1) = 0$$

and, χ being arbitrary, it follows by Lemma 1 that there exists an involution σ of $\mathcal{F}$ such that (4) holds and

$$\prod_{j\in\sigma(A)} [\beta_j] = \prod_{j\in A} [\beta_j].$$

The last formula means that

$$\prod_{j\in\sigma(A)} \beta_j \prod_{j\in A} \beta_j^{-1} = \Gamma_1^n \quad \text{for some } \Gamma_1 \in L. \tag{22}$$

Since $\Gamma_1^n \in K(\zeta_n)$, by Lemma 3 we have

$$\Gamma_1^n = \prod_{i=1}^{k} \alpha_i^{a_i n/n_i} \Gamma^n \quad \text{for some } a_i \in \mathbb{Z}, \Gamma \in K(\zeta_n),$$

which together with (22) gives (20).

LEMMA 5. *If there exists an involution σ of $\mathcal{F}$ such that, for all $A \subset \{1,\ldots,l\}$,* (4) *holds and*

$$\prod_{j\in\sigma(A)} \beta_j = \prod_{j\in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i m/(m,n_i)} \Gamma^m \tag{23}$$

for some $a_i \in \mathbb{Z}$ and $\Gamma \in K(\zeta_m)$, then the implication (i) *holds for all prime ideals $\mathfrak{p}$ of K such that all α_i, β_j are $\mathfrak{p}$-adic units and $(N\mathfrak{p}-1, n) = m$.*

Proof. Let $\mathfrak{p}$ satisfy the assumptions of the lemma and assume that the k congruences $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$, hence also $x^{(m,n_i)} \equiv \alpha_i \pmod{\mathfrak{p}}$, are soluble in K. Let g be a primitive root mod $\mathfrak{p}$ and Φ_m the mth cyclotomic polynomial. We have

$$\Phi_m(x) \equiv \prod_{(k,m)=1} (x - g^{\frac{N\mathfrak{p}-1}{m}k}) \pmod{\mathfrak{p}},$$

hence, by Dedekind's theorem, $\mathfrak{p}$ has a prime ideal factor $\mathfrak{P}$ in $K(\zeta_m)$ of relative degree 1. Solubility in K of the congruences in question implies

$$(\alpha_i^{a_i m/(m,n_i)}|\mathfrak{P})_m = 1 \qquad (1 \le i \le k)$$

and, since $(\Gamma^m|\mathfrak{P})_m = 1$, by (23) we have

$$\Big(\prod_{j\in\sigma(A)} \beta_j\Big|\mathfrak{P}\Big)_m = \Big(\prod_{j\in A} \beta_j\Big|\mathfrak{P}\Big)_m,$$

hence

$$\begin{aligned} 2\prod_{j=1}^{l}&(1-(\beta_j|\mathfrak{P})_m) \\ &= \sum_{A\subset\{1,\ldots,l\}} \Big((-1)^{|A|}\Big(\prod_{j\in A}\beta_j\Big|\mathfrak{P}\Big)_m + (-1)^{|\sigma(A)|}\Big(\prod_{j\in\sigma(A)}\beta_j\Big|\mathfrak{P}\Big)_m\Big) \\ &= \sum_{A\subset\{1,\ldots,l\}} ((-1)^{|A|} + (-1)^{|\sigma(A)|})\Big(\prod_{j\in A}\beta_j\Big|\mathfrak{P}\Big)_m = 0. \end{aligned}$$

Thus $(\beta_j|\mathfrak{P})_m = 1$ for at least one $j \le l$. Since $\mathfrak{P}$ is of relative degree 1, this means that the congruence

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

is soluble in K. Choosing an integer t such that $(N\mathfrak{p}-1)t \equiv m \pmod{n}$ we have, for every $\mathfrak{p}$-adic unit x of K,

$$x^{(N\mathfrak{p}-1)t} \equiv 1 \pmod{\mathfrak{p}},$$

hence the congruence $x^n \equiv \beta_j \pmod{\mathfrak{p}}$ is soluble in K.

LEMMA 6. *Let $m, n_i \in \mathbb{N}$ $(1 \le i \le k)$ and $n_i = n_i' n_i''$, where $(n_i'', m) = 1$. Let $\alpha_i, \beta_j \in K^*$ $(1 \le i \le k,\ 1 \le j \le l)$. If there exists a prime ideal $\mathfrak{p}_0$ of K*

such that $m, n_i, \alpha_i, \beta_j$ *are* $\mathfrak{p}_0$*-adic units, the congruences*

$$x^{n_i'} \equiv \alpha_i \pmod{\mathfrak{p}_0} \quad (1 \le i \le k) \tag{24}$$

are soluble in K *and the congruences*

$$x^{m} \equiv \beta_j \pmod{\mathfrak{p}_0} \quad (1 \le j \le l) \tag{25}$$

are insoluble in K, *then there exists a set* $\mathcal{P}$, *with positive Dirichlet density, of prime ideals of* K *such that for* $\mathfrak{p} \in \mathcal{P}$ *the congruences*

$$x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}} \quad (1 \le i \le k) \tag{26}$$

are soluble in K *and the congruences*

$$x^{m} \equiv \beta_j \pmod{\mathfrak{p}} \quad (1 \le j \le l) \tag{27}$$

are insoluble in K.

Proof. Assume first that all n_i are prime powers, $n_i = l_i^{\nu_i}$, where l_i are primes, and let

$$I_0 = \{1 \le i \le k : l_i \mid m\},$$
$$I_1 = \{1 \le i \le k : l_i \mid N\mathfrak{p}_0 - 1\} \setminus I_0,$$
$$I_2 = \{1 \le i \le k\} \setminus I_0 \setminus I_1.$$

Let further $(N\mathfrak{p}_0 - 1, m) = m'$. We set

$$L = K(\zeta_{n_i}, \sqrt[n_i]{\alpha_i}\ (1 \le i \le k), \zeta_{m'}, \sqrt[m']{\beta_j}\ (1 \le j \le l)),$$

take $\mathfrak{P}_0$ to be a prime ideal factor of $\mathfrak{p}_0$ in L, and let S be the element of the Galois group of L/K such that

$$\vartheta^S \equiv \vartheta^{N\mathfrak{p}_0} \pmod{\mathfrak{P}_0}$$

for all $\mathfrak{P}_0$-adic units ϑ of L.

By the assumption about the congruences (24) the congruence

$$x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}_0}$$

has a solution $x_i \in K$ for $i \in I_0$, hence there exists a zero A_i of $x^{n_i} - \alpha_i$ such that $A_i \equiv x_i \pmod{\mathfrak{P}_0}$ and then

$$A_i^S = A_i. \tag{28}$$

For $i \in I_1 \cup I_2$ and $1 \le j \le l$, we choose A_i and B_j to be arbitrary zeros of $x^{n_i} - \alpha_i$ and $x^{m'} - \beta_j$, respectively.

By the assumption about the congruences (25) also the congruences

$$x^{m'} \equiv \beta_j \pmod{\mathfrak{p}_0} \quad (1 \le j \le l) \tag{29}$$

are insoluble in K. We have

$$\begin{gathered} \zeta_{m'}^S = \zeta_{m'}^{N\mathfrak{p}_0} = \zeta_{m'}, \qquad \zeta_{n_i}^S = \zeta_{n_i}^{N\mathfrak{p}_0} \quad (1 \le i \le k), \\ A_i^S = \zeta_{n_i}^{a_i} A_i \quad (i \in I_1 \cup I_2), \qquad B_j^S = \zeta_{m'}^{b_j} B_j \quad (1 \le j \le l), \end{gathered} \tag{30}$$

where $a_i, b_j \in \mathbb{Z}$. Since the congruences (25) are insoluble in K we have

$$(31) \qquad b_j \not\equiv 0 \pmod{m'} \quad (1 \le j \le l).$$

Put now

$$n_0 = \operatorname{lcm}\{n_i : i \in I_1\}.$$

We have

$$1 + N\mathfrak{p}_0 + \ldots + N\mathfrak{p}_0^{n_0-1} = (N\mathfrak{p}_0^{n_0} - 1)/(N\mathfrak{p}_0 - 1) \equiv 0 \pmod{n_i} \quad (i \in I_1),$$

$$1 + N\mathfrak{p}_0 + \ldots + N\mathfrak{p}_0^{n_0-1} \equiv n_0 \pmod{m'}.$$

It follows from (28) that

$$(32) \qquad A_i^{S^{n_0}} = A_i \quad (i \in I_0)$$

and from (30) and (31) that

$$(33) \quad A_i^{S^{n_0}} = \zeta_{n_i}^{a_i(1+N\mathfrak{p}_0+\ldots+N\mathfrak{p}_0^{n_0-1})} A_i = A_i \quad (i \in I_1 \cup I_2),$$

$$(34) \quad B_j^{S^{n_0}} = \zeta_{m'}^{b_j(1+N\mathfrak{p}_0+\ldots+N\mathfrak{p}_0^{n_0-1})} B_j = \zeta_{m'}^{b_j n_0} B_j \ne B_j \quad (1 \le j \le l),$$

$$(35) \quad \zeta_{m'}^{S^{n_0}} = \zeta_{m'}.$$

If now $\mathfrak{P}$ is a prime ideal of L such that the Frobenius symbol

$$\left[\frac{L/K}{\mathfrak{P}}\right] = S^{n_0}$$

and $\mathfrak{p}$ is the prime ideal of K divisible by $\mathfrak{P}$ we infer from (32)–(35) that the congruences (26) are soluble in K and the congruences

$$x^{m'} \equiv \beta_j \pmod{\mathfrak{p}} \quad (1 \le j \le l),$$

hence also the congruences (27), are insoluble in K. However, by Chebotarev's density theorem the set of relevant prime ideals $\mathfrak{p}$ has a positive Dirichlet density.

Consider now the general case. Let

$$(36) \qquad n_i = \prod_{j=1}^{h_i} q_{ij}$$

where for each i, q_{ij} $(1 \le j \le h_i)$ are powers of distinct primes. Since the congruences (24) are soluble in K, for each $i \le k$ and each j such that $(q_{ij}, m) \ne 1$ the congruence

$$x^{q_{ij}} \equiv \alpha_i \pmod{\mathfrak{p}_0}$$

is soluble in K. Now, by the already proved case of the lemma, there exists a set $\mathcal{P}$, with positive Dirichlet density, of prime ideals of K such that for each $\mathfrak{p} \in \mathcal{P}$ the congruences

$$x^{q_{ij}} \equiv \alpha_i \pmod{\mathfrak{p}} \quad (1 \le i \le k,\ 1 \le j \le h_i)$$

are soluble, but the congruences (27) are insoluble. Thus for all i, j we have

$$\operatorname{ind}\alpha_i \equiv 0 \pmod{(N\mathfrak{p}-1, q_{ij})}.$$

It now follows from (36) that for all i,

$$\operatorname{ind}\alpha_i \equiv 0 \pmod{(N\mathfrak{p}-1, n_i)},$$

hence the congruences (26) are soluble.

LEMMA 7. *Suppose that* (i) *holds for almost all prime ideals* $\mathfrak{p}$ *of* K.

(vi) *If* m *is a unitary divisor of* n, *then for almost all prime ideals* $\mathfrak{p}$ *of* K, *solubility in* K *of the* k *congruences*

$$x^{(m,n_i)} \equiv \alpha_i \pmod{\mathfrak{p}} \tag{37}$$

implies solubility in K *of at least one congruence*

$$x^m \equiv \beta_j \pmod{\mathfrak{p}} \quad (1 \le j \le l). \tag{38}$$

(vii) *If* $n \equiv 0 \pmod 4$ *and* $m = 2m^*$, *where* m^* *is a unitary divisor of the odd part of* n, *then for almost all prime ideals* $\mathfrak{p}$ *of* K, *solubility in* K *of the* k *congruences*

$$x^{(m,n_i)} \equiv \alpha_i \pmod{\mathfrak{p}}$$

implies solubility in K *of at least one congruence*

$$x^m \equiv -1 \pmod{\mathfrak{p}}, \quad x^m \equiv \beta_j \pmod{\mathfrak{p}} \quad (1 \le j \le l).$$

Proof. In order to prove statement (vi) assume to the contrary that there exists a prime ideal $\mathfrak{p}_0$ of K such that m, n_i, α_i and β_j are $\mathfrak{p}_0$-adic units, the congruences (37) are soluble and the congruences (38) are insoluble. We apply Lemma 6 with

$$n_i' = (m, n_i), \quad n_i'' = \frac{n_i}{(m, n_i)}.$$

The assumptions of the lemma are satisfied, since with our choice of m

$$(m, n_i'') = \frac{(m^2, n_i)}{(m, n_i)} = 1$$

and the assertion of the lemma contradicts the assumption of Lemma 7.

A similar argument shows that if statement (vii) were false, there would exist a set $\mathcal{P}$, with positive Dirichlet density, of prime ideals of K such that for $\mathfrak{p} \in \mathcal{P}$ the congruences

$$x^{n_i^*} \equiv \alpha_i \pmod{\mathfrak{p}} \quad (1 \le i \le k) \tag{39}$$

would be soluble and the congruences

$$x^m \equiv -1 \pmod{\mathfrak{p}}, \quad x^m \equiv \beta_j \pmod{\mathfrak{p}} \quad (1 \le j \le l) \tag{40}$$

insoluble, where n_i^* is the greatest divisor of n_i not divisible by 4. However, insolubility of $x^m \equiv -1 \pmod{\mathfrak{p}}$ implies

$$\frac{N\mathfrak{p}-1}{2} = \operatorname{ind}(-1) \not\equiv 0 \pmod{(N\mathfrak{p}-1, m)},$$

hence for $m \equiv 2 \pmod 4$, $N\mathfrak{p} \equiv 3 \pmod 4$ and then solubility of (39) implies solubility of (26), while (40) is insoluble, contrary to the assumption of the lemma.

Proof of Theorem 1. *Necessity.* The existence of an involution σ_m satisfying (1) and (2) for m being a unitary divisor of n follows at once from Lemma 4 and (vi). In order to prove the same for m of the form $2m^*$, where m^* is a unitary divisor of the odd part of n, denote by $\overline{m}$ the least unitary divisor of n divisible by m. Let G_m, resp. $G_{\overline{m}}$, be the multiplicative subgroup of K^* generated by $\alpha_i^{m/(m,n_i)}$ $(1 \le i \le k)$ and $K(\zeta_m)^{*m}$, resp. by $\alpha_i^{\overline{m}/(\overline{m},n_i)}$ $(1 \le i \le k)$ and $K(\zeta_{\overline{m}})^{*\overline{m}}$.

If $G_{\overline{m}} \subset G_m$, then it suffices to take $\sigma_m = \sigma_{\overline{m}}$.

If $G_{\overline{m}} \not\subset G_m$, let $\delta \in G_{\overline{m}} \setminus G_m$. We have

$$\delta = \prod_{i=1}^{k} \alpha_i^{a_i\overline{m}/(\overline{m},n_i)} \Gamma^{\overline{m}}, \tag{41}$$

where $a_i \in \mathbb{Z}$, $\Gamma \in K(\zeta_{\overline{m}})^*$. By Theorem 3 of [8] we have $\Gamma^{\overline{m}} = \Gamma_0^{\overline{m}}$ for some $\Gamma_0 \in K(\zeta_{4m^*})$. Taking norms of both sides of (41) with respect to $K(\zeta_m)$ and denoting the norm of Γ_0 by Γ_1 we obtain

$$\delta^2 = \prod_{i=1}^{k} \alpha_i^{2a_i\overline{m}/(\overline{m},n_i)} \Gamma_1^{\overline{m}},$$

hence

$$\delta = \pm \prod_{i=1}^{k} \alpha_i^{a_i\overline{m}/(\overline{m},n_i)} \Gamma_1^{\overline{m}/2},$$

and, since

$$\frac{m}{(m,n_i)} \,\Big|\, \frac{\overline{m}}{(\overline{m},n_i)}, \qquad m \,\Big|\, \frac{\overline{m}}{2}, \qquad \Gamma_1 \in K(\zeta_m), \qquad \delta \notin G_m,$$

the plus sign is excluded and we have

$$-1 \notin G_m \quad \text{and} \quad \delta \equiv -1 \ (\operatorname{mod}{}^{\times} G_m).$$

Since $\delta \equiv 1 \ (\operatorname{mod}{}^{\times} G_{\overline{m}})$ it follows that

$$[G_{\overline{m}} : G_m \cap G_{\overline{m}}] = 2, \qquad G_{\overline{m}} = (G_m \cap G_{\overline{m}}) \cup \delta(G_m \cap G_{\overline{m}}).$$

From the existence of $\sigma_{\overline{m}}$ satisfying (1) and (2) it follows that for each

$B \in K^*$,

$$\sum_{A\in V(B)} (-1)^{|A|} + \sum_{A\in V(\delta B)} (-1)^{|A|} = 0, \tag{42}$$

where

$$V(B) = \Big\{A \in \mathcal{F} : \prod_{j\in A} \beta_j \equiv B \ (\operatorname{mod}{}^\times G_m \cap G_{\overline{m}})\Big\}.$$

Let $S = \{\prod_{j\in A} \beta_j : A \in \mathcal{F}\}$ and let $\{B_1, \ldots, B_r\}$ be a subset of S maximal with respect to the property that

$$B_i \equiv B \ (\operatorname{mod}{}^\times G_m), \quad B_j \not\equiv B_i \ (\operatorname{mod}{}^\times G_m \cap G_{\overline{m}}) \quad \text{for } j \neq i.$$

Set

$$U(B) = \Big\{A \in \mathcal{F} : \prod_{j\in A} \beta_j \equiv B \ (\operatorname{mod}{}^\times G_m)\Big\}.$$

Replacing B by B_i in (42) and summing with respect to i we obtain

$$\sum_{A\in U(B)} (-1)^{|A|} + \sum_{A\in U(-B)} (-1)^{|A|} = 0.$$

However, from (vii) and Lemma 4 it follows that

$$\sum_{A\in U(B)} (-1)^{|A|} + \sum_{A\in U(-B)} (-1)^{|A|+1} = 0.$$

Adding the last two equalities we obtain

$$2 \sum_{A\in U(B)} (-1)^{|A|} = 0,$$

hence there exists an involution ϱ_B of the family of all subsets A of $\{1, \ldots, l\}$ with $\prod_{j\in A} \beta_j = B$, such that

$$|\varrho_B(A)| \equiv |A| + 1 \ (\operatorname{mod} 2).$$

The involution σ_m is obtained by combining all involutions ϱ_B.

Sufficiency. Consider a prime ideal $\mathfrak{p}$ of K such that α_i, β_j are all $\mathfrak{p}$-adic units and let

$$(N\mathfrak{p} - 1, n) = m_1. \tag{43}$$

If $m_1 = 1$ the implication (i) is obvious.

If $m_1 > 1$, $m_1 \not\equiv 0 \ (\operatorname{mod} 2)$ or $m_1 \equiv 0 \ (\operatorname{mod} 4)$, let m be the least unitary divisor of n divisible by m_1. By condition (ii) we have (1) and (2) where $\Gamma \in K(\zeta_m)$. However, $\Gamma^m \in K$, hence also

$$\Gamma^m \in K(\zeta_q : q \mid m, q \text{ prime or } q = 4) =: K_0.$$

It now follows from Theorem 3 of [8] that $\Gamma^m = \Gamma_0^m$, where $\Gamma_0 \in K_0$. However, by the definition of m, we have $K_0 \subset K(\zeta_{m_1})$ and also

$$\frac{m_1}{(m_1, n_i)} \,\Big|\, \frac{m}{(m, n_i)}.$$

The implication (i) now follows from Lemma 5.

If $m_1 \equiv 2 \pmod 4$, we take $m = 2m^*$, where m^* is the least unitary divisor of n divisible by $m_1/2$, and argue as before.

Proof of Corollary 1. Under the assumption (3) the conditions $\Gamma^n \in K$, $\Gamma \in K(\zeta_n)$ imply, by Theorem 3 of [8], that $\Gamma^n = \gamma^n$, $\gamma \in K$, hence for $\sigma = \sigma_n$, (1) implies (4) and (2) implies (5).

First proof of Corollary 2. The necessity of condition (iii) follows from Corollary 1 on taking $A_0 = \sigma(\emptyset)$. Conversely, if (iii) holds, then we define the involution σ in Corollary 1 by $\sigma(A) = A \div A_0$ ($\div$ denotes the symmetric difference) and notice that

$$\prod_{j\in\sigma(A)} \beta_j = \prod_{j\in A} \beta_j \prod_{i=1}^{k} \alpha_i^{a_i} \Big(\gamma_0 \prod_{j\in A\cap A_0} \beta_j\Big)^2,$$

hence (4) and (5) are satisfied and, by Corollary 1, (i) holds for almost all prime ideals $\mathfrak{p}$ of K.

Second (*direct*) *proof of Corollary* 2. In order to prove the necessity of the condition, choose a maximal subset $\{i_1, \ldots, i_s\}$ of $\{1, \ldots, l\}$ such that

$$\prod_{r=1}^{s} \beta_{i_r}^{e_r} \in L^2, \quad \text{where} \quad L = K(\sqrt{\alpha_1}, \ldots, \sqrt{\alpha_k}),$$

implies $e_r \equiv 0 \pmod 2$ $(1 \le r \le s)$.

By the theorem of Chebotarev [1] there exists a set $\mathcal{P}$, with positive Dirichlet density, of prime ideals $\mathfrak{P}$ of L of degree 1 such that

$$(\beta_{i_r}|\mathfrak{P})_2 = -1 \quad (1 \le r \le s). \tag{44}$$

Let $\mathfrak{p}$ be the prime ideal of K divisible by $\mathfrak{P}$. Since $\mathfrak{P}$ is of degree 1 and the k congruences $x^2 \equiv \alpha_i \pmod{\mathfrak{P}}$ are soluble in L, they are soluble in K and, by the implication,

$$(\beta_j|\mathfrak{p})_2 = 1 \quad \text{for at least one } j \le k. \tag{45}$$

On the other hand, for each $j \le l$, by the maximality of $\{i_1, \ldots, i_s\}$ we have

$$\beta_j = \prod_{r=1}^{s} \beta_{i_r}^{e_{jr}} \gamma_j^2, \quad e_{jr} \in \{0, 1\},\ \gamma_j \in L. \tag{46}$$

If for each j we have

$$\sum_{r=1}^{s} e_{jr} \equiv 1 \pmod 2,$$

then the formulae (44) and (46) imply $(\beta_j|\mathfrak{P})_2 = -1$, contrary to (45). If for a certain j_0 we have

$$\sum_{r=1}^{s} e_{j_0 r} \equiv 0 \pmod 2,$$

then taking $A_0 = \{i_r : e_{j_0 r} = 1\} \div \{j_0\}$ we get (6) and

$$\prod_{j\in A_0} \beta_j = \begin{cases} \beta_{j_0}^2 \gamma_{j_0}^{-2} & \text{if } j_0 \in A_0, \\ \gamma_{j_0}^{-2} & \text{if } j_0 \notin A_0. \end{cases} \tag{47}$$

However, since $\gamma_{j_0}^{-2} \in K$, it follows by Lemma 3 that

$$\gamma_{j_0}^{-2} = \prod_{i=1}^{k} \alpha_i^{a_i} \gamma^2 \quad \text{for some } a_i \in \mathbb{Z},\ \gamma \in K,$$

which together with (47) implies (7).

In order to prove the sufficiency of the condition, let $\mathfrak{p}$ be a prime ideal of K such that α_i and β_j are $\mathfrak{p}$-adic units and the k congruences $x^2 \equiv \alpha_i \pmod{\mathfrak{p}}$ are soluble in K. Then (7) gives

$$\prod_{j\in A_0} (\beta_j|\mathfrak{p})_2 = 1 \neq (-1)^{|A_0|},$$

hence $(\beta_j|\mathfrak{p})_2 = 1$ for at least one $j \in A_0$.

Proof of Corollary 3. *Necessity.* For $n = 2^e$, by a theorem of Hasse [4] (see also Lemma 6 in [8]), $\Gamma^n \in K$ with $\Gamma \in K(\zeta_n)$ implies $\Gamma^n = \varepsilon\gamma^n$, where ε is given by (9) and $\gamma \in K$, hence (iv) follows from (ii) for $\sigma = \sigma_n$. Also (iii) follows from (ii), on taking $m = 2$ and $A_0 = \sigma_2(\emptyset)$.

Sufficiency. There is only one unitary divisor $m > 1$ of $n = 2^e$, namely $m = n$, and for this m, (ii) follows from (iv) by the theorem of Hasse quoted above, used in the opposite direction. For $m = 2$, (ii) follows from (iii) on taking $\sigma_2(A) = A \div A_0$.

LEMMA 8. *Let m be even and $\alpha \in \mathbb{Q}^*$. Then $\alpha \in \mathbb{Q}(\zeta_m)^m$ if and only if*

$$\alpha = \varepsilon\delta^{m/2}\gamma^m,$$

where $\gamma \in \mathbb{Q}^*$, δ is a fundamental discriminant dividing m and

$$\varepsilon \in \begin{cases} \{1, -2^{m/2}\} & \textit{if } m \equiv 4 \pmod 8, \\ \{1\} & \textit{otherwise.} \end{cases}$$

Proof. This is a reformulation of a lemma of Mills [6].

Proof of Theorem 2. The necessity of the conditions follows at once from Theorem 1 and Lemma 8. In order to prove the sufficiency we consider the cases $\nu \le 2$ and $\nu \ge 3$ separately. If $\nu \le 2$, then (ii) follows from (v) and Lemma 8 for every even unitary divisor m of n. For an odd unitary divisor m of n it suffices to take $\sigma_m = \sigma_{2m}$.

For $\nu \ge 3$ and $m \not\equiv 2 \pmod 4$, (ii) follows as before, while for $m \equiv 2 \pmod 4$ it suffices to take $\sigma_m = \sigma_n$. Indeed, for $\nu \ge 3$ we have $\varepsilon = 1$ and every number of the form $\varepsilon\delta^{n/2}\gamma^n$ with $\delta, \gamma \in \mathbb{Q}$ belongs to $\mathbb{Q}^m$.

Proof of Corollary 4. *Necessity.* In the case $\nu = 0$ the assertion follows at once from Corollary 1. We shall consider in detail only the case $\nu = 1$; the proof in the other cases is similar and will be only indicated briefly.

Applying Theorem 2 for $\nu = 1$ and $m = n$ we infer that for $\{j\} = \sigma_n(\emptyset)$,

$$\beta_j = \delta_n^{n/2}\gamma_n^n \quad \text{for some } \gamma_n \in \mathbb{Q}, \tag{48}$$

where δ_n is a fundamental discriminant dividing n. If $\delta_n = 1$ we have $\beta_j \in \mathbb{Q}^n$, hence (10) with $i = j$.

If $\delta_n = (-1)^{(q-1)/2}q$, where q is an odd prime, we have β_j as in (11). Now we apply Theorem 2 for $m_0 = 2$ and $m_1 = n/q^e$. If $\sigma_{m_i}(\emptyset) = \{j\}$ then

$$\beta_j = \delta_{m_i}^{m_i/2}\gamma_i^{m_i} \quad \text{for some } \gamma_i \in \mathbb{Q} \quad (i = 0, 1), \tag{49}$$

where δ_{m_i} is a fundamental discriminant dividing m_i. Now the equations (48) and (49) are incompatible, since denoting by $k(x)$ the squarefree kernel of an integer x, we have

$$k(\delta_{m_i}^{m_i/2}\gamma_i^{m_i}) = \delta_{m_i} \ne \delta_n = k(\delta_n^{n/2}\gamma_n^n).$$

Therefore, $\sigma_{m_i}(\emptyset) = \{3 - j\}$ $(i = 0, 1)$ and we obtain

$$\beta_{3-j} = \delta_{m_i}^{m_i/2}\gamma_i^{m_i} \quad (i = 0, 1).$$

We have $\delta_{m_0} = 1$, hence $\beta_{3-j} \in \mathbb{Q}^{[2, n/2q^e]} = \mathbb{Q}^{n/q^e}$, which proves (11).

Suppose now that δ_n has at least two distinct prime factors q_1 and q_2 and $q_i^{e_i} \,\|\, n$. Applying Theorem 2 for $m_0 = 2$, $m_i = n/q_i^{e_i}$ $(i = 1, 2)$ we obtain, as before, $\sigma_{m_i}(\emptyset) = \{3 - j\}$ $(i = 0, 1, 2)$. Then

$$\beta_{3-j} \in \mathbb{Q}^2 \cap \bigcap_{i=1}^{2} \mathbb{Q}^{n/2q_i^{e_i}},$$

hence $\beta_{3-j} \in \mathbb{Q}^n$, which gives (10) with $i = 3 - j$.

For $\nu = 2$, let $\sigma_n(\emptyset) = \{j\}$.

If $\varepsilon = 1$ and $\delta_n = 1$ or -4 we obtain (10) with $i = j$.

If $\varepsilon = -2^{n/2}$ and $\delta_n = 1$ or -4 we consider $m_0 = 2$, $m_1 = n/2$ and obtain (12).

If $\varepsilon = -2^{n/2}$ and $\delta_n \ne 1, -4$ we consider $m_0 = 4$, $m_1 = n/2$ and obtain (10) with $i = 3 - j$.

If $\varepsilon = 1$ and δ_n has one odd prime factor q we consider $m_0 = 4$, $m_1 = n/q^e$ and obtain (13).

If $\varepsilon = 1$ and δ_n has at least two odd prime factors q_1, q_2 we consider $m_0 = 4$, $m_i = n/q_i^{e_i}$ $(i = 1, 2)$ and obtain (12) with j and $3-j$ interchanged.

For $\nu \geq 3$ let $\sigma_n(\emptyset) = \{j\}$ and

$$\beta_j = \delta_n^{n/2}\gamma_n^n.$$

If $\delta_n = 1$ or -4 we obtain the case (10) with $i = j$.

If $\delta_n = \pm 8$ we obtain the case (14). If δ_n has one odd prime factor q we consider $m_0 = 2^\nu$, $m_1 = n/q^e$ and obtain (15). If δ_n has at least two odd prime factors q_1 and q_2 we consider $m_0 = 2^\nu$, $m_i = n/q_i^{e_i}$ $(i = 1, 2)$ and obtain (10) with $i = 3 - j$ or (14) with $3 - j$ in place of j.

Sufficiency. If (10) holds then for each relevant divisor m of n we take $\sigma_m = c_i d_i$, where c_i, d_i are the cycles $(\emptyset \to \{i\})$ and $(\{3-i\} \to \{1, 2\})$, respectively.

If (11) holds, we take

$$\sigma_m = \begin{cases} c_j d_j & \text{if } q \mid m, \\ c_{3-j} d_{3-j} & \text{if } q \nmid m. \end{cases}$$

If (12) holds, we take

$$\sigma_m = \begin{cases} c_j d_j & \text{if } 4 \mid m, \\ c_{3-j} d_{3-j} & \text{if } 4 \nmid m. \end{cases}$$

If (13) holds, we take

$$\sigma_m = \begin{cases} c_j d_j & \text{if } q \mid m, \text{ or } 4 \nmid m, \\ c_{3-j} d_{3-j} & \text{if } q \nmid m \text{ and } 4 \mid m. \end{cases}$$

If (14) holds, we take

$$\sigma_m = c_j d_j.$$

If (15) holds, we take

$$\sigma_m = \begin{cases} c_j d_j & \text{if } q \mid m, \\ c_{3-j} d_{3-j} & \text{if } q \nmid m. \end{cases}$$

Deduction of Theorem 1 *of* [7] (necessity part) from Theorem 1 (above). Let $n = \prod_{j=0}^{l} p_j^{e_j}$, where $p_0 = 2$, p_j are distinct odd primes and $e_j > 0$ for $j > 0$. Applying Theorem 1 above with $m = p_j^{e_j}$ we infer that

$$\beta = \prod_{i=1}^{k} \alpha_i^{a_{ij} p_j^{e_j}/(n_i, p_j^{e_j})} \Gamma_j^{p_j^{e_j}} \tag{50}$$

for some $a_{ij} \in \mathbb{Z}$ and $\Gamma_j \in K(\zeta_{p_j^{e_j}})$ (for $m = 1$ the conclusion is trivial). By the theorem of Hasse [4] (see [8, Lemma 6])

$$\Gamma_j^{p_j^{e_j}} = \varepsilon_j \gamma_j^{p_j^{e_j}} \quad \text{for some } \gamma_j \in K,\ \varepsilon_j = 1 \text{ for } j > 0 \tag{51}$$

and

$$\begin{aligned} \varepsilon_0 &\in \{1\} && \text{if } e_0 \le 1,\\ \varepsilon_0 &\in \{1,-1\} && \text{if } 1 < e_0 < \tau,\\ \varepsilon_0 &\in \{1, (-1)^{2^{e_0-\tau}} (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{2^{e_0-1}}\} && \text{if } e_0 \ge \tau. \end{aligned} \tag{52}$$

We take integers $u_0, \ldots, u_l$ satisfying the linear equation

$$\sum_{j=0}^{l} \frac{n}{p_j^{e_j}}\, u_j = 1$$

and set

$$\gamma = \prod_{j=0}^{l} \gamma_j^{u_j}.$$

By (50) and (51) we have

$$\gamma^n = \prod_{j=0}^{n} (\gamma_j^{p_j^{e_j}})^{\frac{n}{p_j^{e_j}} u_j} = \beta \varepsilon_0^{-\frac{n}{2^{e_0}} u_0} \prod_{j=0}^{l} \prod_{i=1}^{k} \alpha_i^{-a_{ij} \frac{n u_j}{(n_i, p_j^{e_j})}},$$

hence

$$\beta \prod_{i=1}^{k} \alpha_i^{m_i n / n_i} = \varepsilon^{\frac{n}{2^{e_0}} u_0} \gamma^n \tag{53}$$

for some $m_i \in \mathbb{Z}$, $\gamma \in K^*$.

If $e_0 \le 1$, or $e_0 > \tau$, or $\varepsilon_0 = 1$, or u_0 is even, we obtain, by (51), condition (i) or (iv) of Theorem 1 of [7]. If $1 < e_0 \le \tau$, $\varepsilon \ne 1$ and u_0 is odd we apply Theorem 1 above with $m = 2$. We obtain

$$\beta = \prod_{2 \mid n_i} \alpha_i^{a_i} \gamma^2,$$

which combined with (53) gives, by (52),

$$\prod_{2 \mid n_i} \alpha_i^{l_i} = -\delta^2$$

and

$$\beta \prod_{i=1}^{k} \alpha_i^{m_i n / n_i} = \begin{cases} -\gamma^n & \text{if } 1 < e_0 < \tau,\\ -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2} \gamma_1^n & \text{if } e_0 = \tau, \end{cases}$$

for some $\delta, \gamma_1 \in K^*$. These are just conditions (ii) and (iii) of Theorem 1 of [7]. The proof that conditions (i)–(iv) are sufficient is easy.

References

[1] N. G. Chebotarev, *Der Hilbertsche Satz*, Visti VUAN 1923, 3–7; Russian translation: Collected Works, Vol. 1, Moscow–Leningrad, 1949, 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] H. Hasse, *Zum Existenzsatz von Grunwald in der Klassenkörpertheorie*, J. Reine Angew. Math. 188 (1950), 40–64.

[5] —, *Vorlesungen über Klassenkörpertheorie*, Physica-Verlag, Würzburg, 1967.

[6] W. H. Mills, *Characters with preassigned values*, Canad. J. Math. 15 (1963), 179–181.

[7] A. Schinzel, *On power residues and exponential congruences*, Acta Arith. 27 (1975), 397–420.

[8] —, *Abelian binomials, power residues and exponential congruences*, ibid. 32 (1977), 245–274; Addendum and corrigendum 36 (1980), 101–104.

[9] T. Skolem, *On the existence of a multiplicative basis for an arbitrary algebraic field*, Norske Vid. Selsk. Forh. (Trondheim) 20 (1947), no. 3.

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

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

Received on 9.7.2002 (4329)