by our choice of d. We have

$$\begin{aligned} M(\log d - \log 2) &= \big(M/(Mk+1)\big)|\log \Delta| - M\log 2 \\ &\geqslant |\log \Delta|\big((1/k) - (1/k^2 M)\big) - M\log 2 \\ &\geqslant (1/k)\,|\log \Delta| - (2/k)\,|\log \Delta|^{1/2}(\log 2)^{1/2} - \log 2 \end{aligned}$$

by (22), so that by (23),

$$2^M r_M + \Delta r_M \leqslant 4\Delta^{1/k}\exp\big(2\,(\log 2)^{1/2}k^{-1}\,|\log \Delta|^{1/2}\big).$$

This in conjunction with (21) gives

$$z(S) \geqslant N\big(\mu(S) - c_1(A, \sigma)\,\Delta^{1/k}\exp(\ldots)\big).$$

The same inequality holds with S replaced by S'. Both inequalities together yield

$$|z(S) - N\mu(S)| \leqslant N\Big(c_1(A, \sigma)\,\Delta^{1/k}\exp\big(2\,(\log 2)^{1/2}k^{-1}\,|\log \Delta|^{1/2}\big)\Big).$$

Since this holds for every $S \in \mathfrak{S}(\sigma)$, Theorem 3 is proved.

References

[1] E. Hlawka, *Discrepancy and uniform distribution of sequences*, Compositio Math. 16 (1964), pp. 83–91. (Nijenrode lecture 1962).

[2] — *Zur Definition der Diskrepanz*, Acta Arith. 18 (1971), pp. 233–241.

[3] Rudolf Mück and Walter Philipp, *Distances of probability measures and uniform distribution* mod 1, Math. Zeitschr. (to appear).

[4] F. K. Roth, *On irregularities of distribution*, Mathematika 7 (1954), pp. 73–79.

[5] W. M. Schmidt, *Irregularities of distribution. IV*, Invent. Math. 7 (1969), pp. 55–82.

[6] — *Irregularities of distribution. VII*, Acta Arith. 21 (1972), pp. 45–50.

[7] C. J. Smyth, *Inequalities relating different definitions of discrepancy*, J. Australian Math. Soc. 17 (1974), pp. 81–87.

[8] — Thesis, University of Cambridge, England.

[9] S. K. Zaremba, *La discrépance isotrope et l'intégration numerique*, Ann. di Mat. pura et appl. (IV) 87 (1970), pp. 125–136.

UNIVERSITY OF COLORADO
Boulder, Colorado

Received on 6. 12. 1973 (501)

ACTA ARITHMETICA
XXVII (1975)

On power residues and exponential congruences

by

A. Schinzel (Warszawa)

In memory of Yu. V. Linnik

The main aim of this paper is to extend the results of [6] to algebraic number fields. We shall prove

Theorem 1. *Let K be an algebraic number field, ζ_q a primitive qth root of unity and τ the greatest integer such that $\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K$. Let $n_1, \ldots, n_k, n$ be positive integers, $n_i | n$; $\alpha_1, \ldots, \alpha_k, \beta$ be non-zero elements of K. The solubility of the k congruences $x^{n_i} \equiv \alpha_i \bmod \mathfrak{p}$ $(1 \leqslant i \leqslant k)$ implies the solubility of the congruence $x^n \equiv \beta \bmod \mathfrak{p}$ for almost all prime ideals $\mathfrak{p}$ of K if and only if at least one of the following four conditions is satisfied for suitable rational integers $l_1, \ldots, l_k, m_1, \ldots, m_k$ and suitable $\gamma, \delta \in K$:*

(i) $\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = \gamma^n$;

(ii) $n \not\equiv 0 \bmod 2^\tau$, $\prod_{2|n_i} \alpha_i^{l_i} = -\delta^2$ *and* $\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = -\gamma^n$;

(iii) $n \equiv 2^\tau \bmod 2^{\tau+1}$, $\prod_{2|n_i} \alpha_i^{l_i} = -\delta^2$ *and*

$$\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2}\gamma^n;$$

(iv) $n \equiv 0 \bmod 2^{\tau+1}$ *and* $\beta \prod_{i=1}^{k} \alpha_i^{nm_i/n_i} = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2}\gamma^n$.

If $\zeta_4 \in K$, the conditions (ii), (iii), (iv) *imply* (i); *if $\tau = 2$,* (ii) *implies* (i) *for not necessarily the same $m_1, \ldots, m_k$ and γ.*

Almost all prime ideals means all but for a set of Dirichlet density zero or all but finitely many. In this context it comes to the same in virtue of Frobenius density theorem.

Corollary 1. *If each of the fields $K(\xi_1, \xi_2, \ldots, \xi_k)$, where $\xi_i^{n_i} = \alpha_i$ contains at least one η satisfying $\eta^n = \beta$ then at least one of the conditions* (i)–(iv) *holds.*

This corollary may be regarded as a generalization of the well known result concerning Kummer fields (see [3], p. 42). As one can see from Lemmata 6 and 7 below it holds for arbitrary fields K of characteristic not dividing n (with $\tau = \infty$, if necessary).

COROLLARY 2. *The congruences* $x^n \equiv a \bmod \mathfrak{p}$ *and* $x^n \equiv \beta \bmod \mathfrak{p}$ *are simultaneously soluble or insoluble for almost all prime ideals* $\mathfrak{p}$ *of* K *if and only if either*

$$\beta a^u = \gamma^n,$$

or $n \equiv 0 \bmod 2^{\tau+1}$ *and*

$$\beta a^u = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2} \gamma^n$$

where $(u, n) = 1$ *and* $\gamma \in K$.

This is a simultaneous refinement of the theorems of Flanders [1] and Gerst [2] concerning $a = 1$ and $K = Q$, respectively.

We shall prove further

THEOREM 2. *If* $a_1, \ldots, a_k, \beta$ *are non-zero elements of* K *and the congruence*

$$a_1^{x_1} a_2^{x_2} \ldots a_k^{x_k} \equiv \beta \bmod \mathfrak{p}$$

is soluble for almost all prime ideals $\mathfrak{p}$ *of* K *then the corresponding equation in soluble in rational integers.*

This is a refinement of a theorem of Skolem [7], in which he assumes that the congruence is soluble for all moduli (also composite). Skolem's proof is defective but it can be amended.

On the lines indicated by Skolem we prove

THEOREM 3. *Let* a_{ij}, β_i $(i = 1, \ldots, h,\ j = 1, \ldots, k)$ *be non-zero elements of* K, D *a positive integer. If the system of congruences*

$$\prod_{j=1}^{k} a_{ij}^{x_j} \equiv \beta_i \bmod \mathfrak{m} \qquad (i = 1, \ldots, h)$$

is soluble for all moduli $\mathfrak{m}$ *prime to* D *then the corresponding system of equations is soluble in integers.*

We show on an example that already for $h = 2$, $k = 3$ one cannot replace here "all moduli prime to D" by "all prime moduli".

On the other hand, the present approach gives no clue to Skolem's very interesting conjecture:

If the congruence

$$\sum_{i=1}^{h} a_{i0} a_{i1}^{x_1} \ldots a_{ik}^{x_k} \equiv 0 \bmod \mathfrak{m}$$

is soluble for all moduli $\mathfrak{m}$ *then the corresponding equation is soluble in rational integers.*

The proof of Theorem 1 is based on nine lemmata. In formulating and proving them we use as much as possible the matrix notation. Integral matrices are denoted by bold face capital letters, integral vectors are treated as matrices with one row and denoted by bold face lower case letters. A^T is the transpose of A. A congruence $\boldsymbol{a} \equiv \boldsymbol{b} \bmod \boldsymbol{M}$ or $\boldsymbol{a}^T \equiv \boldsymbol{b}^T \bmod \boldsymbol{M}$ means that for a certain $\boldsymbol{x}$, $\boldsymbol{a} - \boldsymbol{b} = \boldsymbol{x}\boldsymbol{M}$, a congruence $\boldsymbol{a} \equiv \boldsymbol{b} \bmod (\boldsymbol{M}, \boldsymbol{N})$ means that $\boldsymbol{a} - \boldsymbol{b} = \boldsymbol{x}\boldsymbol{M} + \boldsymbol{y}\boldsymbol{N}$. Instead of mod $n\boldsymbol{I}$ or mod $(n\boldsymbol{I}, \boldsymbol{N})$, where $\boldsymbol{I}$ is the identity matrix we write mod n or mod$(n, \boldsymbol{N})$, respectively. The congruence $\boldsymbol{a} \equiv \boldsymbol{b} \bmod (n, \boldsymbol{N})$ implies $\boldsymbol{a}\boldsymbol{R} \equiv \boldsymbol{b}\boldsymbol{R} \bmod (n, \boldsymbol{N}\boldsymbol{R})$ for any $\boldsymbol{R}$ and $\boldsymbol{a} \equiv \boldsymbol{b} \bmod (n, \boldsymbol{R}\boldsymbol{N})$ for any unimodular $\boldsymbol{R}$.

LEMMA 1. *For every integral matrix* $\boldsymbol{A}$ *there exist two unimodular matrices* $\boldsymbol{P}$ *and* $\boldsymbol{Q}$ *such that all elements of* $\boldsymbol{P}\boldsymbol{A}\boldsymbol{Q}$ *outside the diagonal are zero.*

Proof, see [8], p. 13.

LEMMA 2. *Let* $\boldsymbol{A}$ *be an integral matrix,* $\boldsymbol{b}$ *an integral vector. If for all integral vectors* $\boldsymbol{x}$ *the congruence* $\boldsymbol{x}\boldsymbol{A} \equiv \boldsymbol{0} \bmod n$ *implies* $\boldsymbol{x}\boldsymbol{b}^T \equiv \boldsymbol{0} \pmod n$ *then* $\boldsymbol{b}^T \equiv \boldsymbol{A}\boldsymbol{c}^T \bmod n$ *for an integral vector* $\boldsymbol{c}$.

Proof. Let $\boldsymbol{A} = [a_{ij}]_{\substack{i \leqslant r \\ j \leqslant s}}$, $\boldsymbol{b} = [b_1, \ldots, b_r]$. If $a_{ij} = 0$ for $i \neq j$ then the congruence $\boldsymbol{x}\boldsymbol{A} \equiv 0 \bmod n$ is satisfied by

$$\boldsymbol{x}_i = \begin{cases} \Big(\underbrace{0, \ldots, 0, \frac{n}{(n, a_{ii})}}_{i}, \ldots, 0\Big) & (1 \leqslant i \leqslant q = \min(r, s)), \\ (\underbrace{0, \ldots, 0, 1}_{i}, 0, \ldots, 0) & (q < i \leqslant r). \end{cases}$$

It follows that $\boldsymbol{x}_i \boldsymbol{b}^T \equiv 0 \bmod n$ $(1 \leqslant i \leqslant r)$ and hence

$$b_i \equiv \begin{cases} 0 \bmod (n, a_{ii}) & (1 \leqslant i \leqslant q), \\ 0 \bmod n & (q < i \leqslant r). \end{cases}$$

Thus $b_i \equiv a_{ii} c_i \bmod n$ for suitable c_i $(1 \leqslant i \leqslant q)$ and setting $\boldsymbol{c} = [c_1, \ldots, c_q, 0, \ldots, 0]$ we get $\boldsymbol{b}^T \equiv \boldsymbol{A}\boldsymbol{c}^T \bmod n$.

In the general case let $\boldsymbol{P}, \boldsymbol{Q}$ have the property asserted in Lemma 1. If $\boldsymbol{x}\boldsymbol{P}\boldsymbol{A}\boldsymbol{Q} \equiv 0 \bmod n$ then $\boldsymbol{x}\boldsymbol{P}\boldsymbol{A} \equiv 0 \bmod n$ hence $\boldsymbol{x}\boldsymbol{P}\boldsymbol{b}^T \equiv 0 \bmod n$. By the already proved case of our lemma $\boldsymbol{P}\boldsymbol{b}^T \equiv \boldsymbol{P}\boldsymbol{A}\boldsymbol{Q}\boldsymbol{d}^T \bmod n$ for a suitable integral $\boldsymbol{d}$ and since $\boldsymbol{P}$ is unimodular $\boldsymbol{b}^T \equiv \boldsymbol{A}\boldsymbol{Q}\boldsymbol{d}^T \bmod n$. Thus we can take $\boldsymbol{c} = \boldsymbol{d}\boldsymbol{Q}^T$.

LEMMA 3. *Let* $\boldsymbol{A}$ *and* $\boldsymbol{b}$ *satisfy the assumptions of Lemma 2, let besides* $\boldsymbol{a} \equiv \boldsymbol{0} \bmod np^{-1}$ *and* $\boldsymbol{b} \equiv \boldsymbol{0} \bmod np^{-1}$, *where* p *is a prime and* $p \| n$. *If for all integral vectors* $\boldsymbol{x}$ *the congruence* $\boldsymbol{x}\boldsymbol{A} \equiv \boldsymbol{a} \bmod n$ *implies* $\boldsymbol{x}\boldsymbol{b}^T$

$\equiv b \bmod n$ *then*

$$\boldsymbol{b}^T \equiv \boldsymbol{A}\boldsymbol{d}^T \bmod n \quad \text{and} \quad b \equiv \boldsymbol{a}\boldsymbol{d}^T \bmod n$$

for an integral vector $\boldsymbol{d}$.

Proof. Let $\boldsymbol{A} = [a_{ij}]_{\substack{i\leqslant r\\ j\leqslant s}}$, $\boldsymbol{a} = (a_{01}, \ldots, a_{0s})$. As in the proof of Lemma 2 it is enough to consider the case, where $a_{ij} = 0$ for $i \neq 0, j$. In virtue of that lemma we have $\boldsymbol{b}^T \equiv \boldsymbol{A}\boldsymbol{c}^T \bmod n$, for a certain $\boldsymbol{c}$.

If the congruence $\boldsymbol{x}\boldsymbol{A} \equiv \boldsymbol{a} \bmod n$ is soluble then we take $\boldsymbol{d} = \boldsymbol{c}$. Indeed, we have for a suitable $\boldsymbol{x}_0$

$$b \equiv \boldsymbol{x}_0\boldsymbol{b}^T \equiv \boldsymbol{x}_0\boldsymbol{A}\boldsymbol{c}^T \equiv \boldsymbol{a}\boldsymbol{c}^T \bmod n.$$

If the congruence $\boldsymbol{x}\boldsymbol{A} \equiv \boldsymbol{a} \bmod n$ is insoluble we have for a certain $j \leqslant \min(r, s)$ $(n, a_{jj}) \nmid a_{0j}$, hence in view of $a_{0j} \equiv 0 \bmod np^{-1}$

$$p \mid a_{jj} \quad \text{and} \quad p \nmid a_{0j}. \tag{1}$$

We determine d from the system of congruences

$$d \equiv 0 \bmod np^{-1}, \tag{2}$$

$$a_{0j}d \equiv (b - \boldsymbol{a}\boldsymbol{c}^T) \bmod p \tag{3}$$

and set $\boldsymbol{d} = \boldsymbol{c} + (\underbrace{0, \ldots, 0, d}_{j}, 0, \ldots, 0)$.

It follows from (1) and (2) that $\boldsymbol{A}\boldsymbol{d}^T \equiv \boldsymbol{A}\boldsymbol{c}^T \equiv \boldsymbol{b}^T \bmod n$ and by (3) $\boldsymbol{a}\boldsymbol{d}^T \equiv b \bmod n$.

LEMMA 4. *Let* $\mathscr{A}_n$ *be a subgroup of the multiplicative group of residues* mod n *and* B *the set of all integers* $b \equiv 1 \bmod (4, n)$, *the residues of which belong to* $\mathscr{A}_n$. *Let* d *be the greatest common factor of all numbers* $b-1$, *where* $b \in B$; $n = n_1 n_2$, *where each prime factor of* n_1 *divides* d *and* $(n_2, d) = 1$. *If an integer valued function* h *on* B *satisfies the congruences*

$$h(ab) \equiv ah(b) + h(a) \bmod n, \tag{4}$$

$$h(b) \equiv 0 \bmod n_1 \quad \text{if} \quad b \equiv 1 \bmod n_1 \tag{5}$$

then

$$h(b) \equiv c(b-1) \bmod n$$

for a suitable c *and all* $b \in B$.

Proof. Let $n = p_1^{\nu_1} p_2^{\nu_2} \ldots p_s^{\nu_s}$ be the factorization of n into primes. Assume that $p_i \mid n_1$ for $i \leqslant r$, $p_i \mid n_2$ for $i > r$. Let b_i be an element of B such that $\operatorname{ord}_{p_i}(b_i - 1)$ is minimal, equal, say μ_i. We have

$$d = p_1^{\mu_1} p_2^{\mu_2} \ldots p_r^{\mu_r}, \quad 1 \leqslant \mu_i \leqslant \nu_i \ (i \leqslant r), \ \mu_i = 0 \ (i > r).$$

For $i \leqslant r$ let g_i be a primitive root mod $p_i^{\nu_i+1}$ or if $p_i = 2$, $\nu_i \geqslant 2$: $g_i = 5$.

Let $\operatorname{ind}_i a$ be defined by the congruence

$$g_i^{\operatorname{ind}_i a} \equiv a \bmod p_i^{\nu_i+1}$$

and set

$$\varphi'(p^\nu) = \begin{cases} 2^{\nu-2} & \text{if } p = 2, \nu \geqslant 2, \\ p^{\nu-1}(p-1) & \text{otherwise.} \end{cases} \tag{6}$$

$\operatorname{ind}_i a$ is determined $\bmod \varphi'(p_i^{\nu_i+1})$, moreover for $\mu \leqslant \nu_i + 1$

$$a \equiv 1 \bmod p_i^\mu \text{ if and only if } \operatorname{ind}_i a \equiv 0 \bmod \varphi'(p_i^{\nu_i}). \tag{7}$$

Since $\operatorname{ind}_i a^\nu \equiv \nu \operatorname{ind}_i a \bmod \varphi'(p_i^{\nu_i+1})$ it follows from (6) and (7) that

$$\min\bigl(\nu_i + 1, \operatorname{ord}_{p_i}(a^\nu - 1)\bigr) = \min\bigl(\nu_i + 1, \operatorname{ord}_{p_i}\nu + \operatorname{ord}_{p_i}(a-1)\bigr)$$

and since ν_i can be arbitrarily large

$$\operatorname{ord}_{p_i}(a^\nu - 1) = \operatorname{ord}_{p_i}\nu + \operatorname{ord}_{p_i}(a-1). \tag{8}$$

Since for all $a \in B$

$$\operatorname{ord}_{p_j}(a-1) \geqslant \mu_j, \tag{9}$$

we have in particular

$$\operatorname{ord}_{p_j}(b_i^{n_1 d^{-1}} - 1) \geqslant \nu_j \quad (1 \leqslant j \leqslant r)$$

and hence $b_i^{n_1 d^{-1}} \equiv 1 \bmod n_1$. By (5)

$$h(b_i^{n_1 d^{-1}}) \equiv 0 \bmod n_1. \tag{10}$$

On the other hand, by (6)

$$h(b^e) \equiv \frac{b^e - 1}{b-1} h(b) \bmod n. \tag{11}$$

The formula (8) gives $\operatorname{ord}_{p_i}(b_i^{n_1 d^{-1}} - 1) = \nu_i$ and we infer from (10) and (11) that $p_i^{\mu_i} \mid h(b_i)$ for all $i \leqslant r$. The same holds clearly for $i > r$. We now choose c to satisfy the system of congruences

$$c \equiv \frac{h(b_i) p_i^{-\mu_i}}{(b_i - 1) p_i^{-\mu_i}} \bmod p_i^{\nu_i} \quad (1 \leqslant i \leqslant s). \tag{12}$$

For every $b \in B$ we have by (6), (7) and (9)

$$\bigl(\operatorname{ind}_i b_i, \varphi'(p_i^{\nu_i})\bigr) \mid \operatorname{ind}_i b.$$

Choosing x_i so that

$$x_i \operatorname{ind}_i b_i + \operatorname{ind}_i b \equiv 0 \bmod \varphi'(p_i^{\nu_i})$$

we get

$$b_i^{x_i} b \equiv 1 \bmod p_i^{\gamma_i}. \tag{13}$$

It follows from (8) and (9) with $a = b_i^{x_i} b$ that

$$\operatorname{ord}_{p_j}\left((b_i^{x_i} b)^{n_1 p_i^{-\gamma_i}} - 1\right) \geqslant \nu_j \quad (1 \leqslant j \leqslant r)$$

and thus

$$(b_i^{x_i} b)^{n_1 p_i^{-\gamma_i}} \equiv 1 \bmod n_1.$$

Hence by (4) and (11)

$$h\left((b_i^{x_i} b)^{n_1 p_i^{-\gamma_i}}\right) \equiv \frac{(b_i^{x_i} b)^{n_1 p_i^{-\gamma_i}} - 1}{b_i^{x_i} b - 1}\, h(b_i^{x_i} b) \equiv 0 \bmod n_1.$$

However by (8) the cofactor of $h(b_i^{x_i} b)$ above is prime to p_i, thus

$$h(b_i^{x_i} b) \equiv b\,\frac{b_i^{x_i} - 1}{b_i - 1}\, h(b_i) + h(b) \equiv 0 \bmod p_i^{\gamma_i}$$

and by (12) and (13)

$$h(b) \equiv c(b-1) \bmod p_i^{\gamma_i} \quad (1 \leqslant i \leqslant r). \tag{14}$$

On the other hand, for $i > r$ we have by (4)

$$h(bb_i) \equiv b h(b_i) + h(b) \equiv b_i h(b) + h(b_i) \bmod p_i^{\gamma_i},$$

hence by (12)

$$h(b) \equiv \frac{h(b_i)}{b_i - 1}(b-1) \equiv c(b-1) \bmod p_i^{\gamma_i} \quad (r < i \leqslant s), \tag{15}$$

and the lemma follows from (14) and (15).

LEMMA 5. *Let $\mathscr{A}_n$ be a subgroup of the multiplicative group of residues mod n and A the set of all integers the residues of which belong to $\mathscr{A}_n$. Let $\boldsymbol{M}$ be a non-singular square matrix such that $n\boldsymbol{M}^{-1}$ is integral. Let $\boldsymbol{f}$ and g be functions on A into set of integral vectors or integers respectively, satisfying the conditions*

$$\boldsymbol{f}(a) \equiv \boldsymbol{f}(b), \quad g(a) \equiv g(b) \bmod n \quad \text{if} \quad a \equiv b \bmod n, \tag{16}$$

$$\boldsymbol{f}(ab) \equiv a\boldsymbol{f}(b) + \boldsymbol{f}(a) \bmod \boldsymbol{M}, \tag{17}$$

$$g(ab) \equiv a g(b) + g(a) \bmod n. \tag{18}$$

If for all $a \in A$ the congruence

$$\boldsymbol{f}(a) \equiv 0 \bmod (a-1, \boldsymbol{M})$$

implies the congruence

$$g(a) \equiv 0 \bmod (a-1, n)$$

then there exist vectors $\boldsymbol{u}_1$ and $\boldsymbol{u}_2$ and an integer c such that for all $a \equiv 1 \bmod (4, n)$

$$g(a) \equiv c(a-1) + \boldsymbol{f}(a) n \boldsymbol{M}^{-1} \boldsymbol{u}_1^T \bmod n$$

and for all $a \in A$

$$g(a) \equiv \boldsymbol{f}(a)\boldsymbol{u}_2^T \bmod (2, n), \quad \boldsymbol{M}\boldsymbol{u}_2^T \equiv \boldsymbol{0} \bmod (2, n).$$

Proof. By Lemma 1 there exist unimodular matrices $\boldsymbol{P}$ and $\boldsymbol{Q}$ such that

$$\boldsymbol{PMQ} = \begin{bmatrix} e_1 & 0 & \dots & 0 \\ 0 & e_2 & \dots & 0 \\ 0 & 0 & \dots & e_k \end{bmatrix}. \tag{19}$$

Since $\boldsymbol{M}$ is non-singular the entries e_i are non-zero and since $n\boldsymbol{M}^{-1}$ is integral we have $e_i | n$ $(1 \leqslant i \leqslant k)$. Any congruence $\boldsymbol{x} \equiv \boldsymbol{0} \bmod (m, \boldsymbol{PMQ})$ where $\boldsymbol{x} = [x_1, \dots, x_k]$ is equivalent to the system of congruences $x_i \equiv 0 \bmod (m, e_i)$ $(1 \leqslant i \leqslant k)$, which will be frequently used in the sequel.

Let n_1, n_2 have the meaning defined in Lemma 4.

For each prime $p_i | n_2$ there exists $b_i \in A$ such that $b_i \not\equiv 1 \bmod p_i$. If $p_i^{\gamma_i} || n_2$ we get by (17) for all $a \in A$

$$\begin{aligned} \boldsymbol{f}(a)(b_i - 1) &\equiv \boldsymbol{f}(b_i)(a-1) \bmod \boldsymbol{M}, \\ \boldsymbol{f}(a)(b_i - 1)\boldsymbol{Q} &\equiv \boldsymbol{0} \bmod (a-1, \boldsymbol{PMQ}), \\ \boldsymbol{f}(a)\boldsymbol{Q} &\equiv \boldsymbol{0} \bmod \left((a-1, p_i^{\gamma_i}), \boldsymbol{PMQ}\right), \\ \boldsymbol{f}(a)\boldsymbol{Q} &\equiv \boldsymbol{0} \bmod \left((a-1, n_2), \boldsymbol{PMQ}\right). \end{aligned} \tag{20}$$

Let $a_1, \dots, a_r$ represent all residue classes of $\mathscr{A}_n$ congruent to $1 \bmod n_1$.

If $x_1, \dots, x_r$ are integers not necessarily positive and

$$a \equiv a_1^{x_1} \dots a_r^{x_r} \bmod n$$

we have by (16), (17) and (18)

$$\boldsymbol{f}(a) \equiv x_1 \boldsymbol{f}(a_1) + \dots + x_r \boldsymbol{f}(a_r) \bmod (n_1, \boldsymbol{M}), \tag{21}$$

$$g(a) \equiv x_1 g(a_1) + \dots + x_r g(a_r) \bmod n_1. \tag{22}$$

Let us set

$$\boldsymbol{F} = \begin{bmatrix} \boldsymbol{f}(a_1) \\ \boldsymbol{f}(a_2) \\ \vdots \\ \boldsymbol{f}(a_r) \end{bmatrix}, \quad \boldsymbol{g} = [g(a_1), \dots, g(a_r)].$$

By (21)

$$f(a) \equiv \boldsymbol{x}\boldsymbol{F} \bmod (n_1, \boldsymbol{PM})$$

and

$$f(a)\boldsymbol{Q} \equiv \boldsymbol{x}\boldsymbol{F}\boldsymbol{Q} \bmod (n_1, \boldsymbol{PMQ}). \tag{23}$$

Now suppose that for a vector $\boldsymbol{x}$ we have

$$\boldsymbol{x}\boldsymbol{F}n\boldsymbol{M}^{-1} \equiv \boldsymbol{0} \bmod n_1. \tag{24}$$

Then

$$n_2\boldsymbol{x}\boldsymbol{F}\boldsymbol{Q} \equiv \boldsymbol{0} \bmod \boldsymbol{PMQ}$$

and in view of (19)

$$\boldsymbol{x}\boldsymbol{F}\boldsymbol{Q} \equiv \boldsymbol{0} \bmod (n_1, \boldsymbol{PMQ}).$$

By (23) we can write the above congruence in the form

$$f(a)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod (n_1, \boldsymbol{PMQ}).$$

This together with (20) gives

$$f(a)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod \big((a-1, n), \boldsymbol{PMQ}\big)$$

and since $e_i \mid n$ we infer that

$$f(a)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod (a-1, \boldsymbol{PMQ}),$$

$$f(a) \equiv \boldsymbol{0} \bmod (a-1, \boldsymbol{M}).$$

By the assumption

$$g(a) \equiv 0 \bmod (a-1, n)$$

and by (22)

$$\boldsymbol{x}\boldsymbol{g}^T \equiv 0 \bmod n_1. \tag{25}$$

Thus (24) implies (25) and by Lemma 2 we get

$$\boldsymbol{g}^T \equiv \boldsymbol{F}n\boldsymbol{M}^{-1}\boldsymbol{u}_1^T \bmod n_1$$

for a suitable $\boldsymbol{u}_1$. On comparing the components it follows

$$g(a_i) \equiv \boldsymbol{f}(a_i)n\boldsymbol{M}^{-1}\boldsymbol{u}_1^T \bmod n_1 \quad (1 \leqslant i \leqslant r).$$

However every $a \equiv 1 \bmod n_1$ satisfies $a \equiv a_i \bmod n$ for a suitable $i \leqslant r$, thus by (16) the function

$$h(a) = g(a) - \boldsymbol{f}(a)n\boldsymbol{M}^{-1}\boldsymbol{u}_1^T$$

satisfies $h(a) \equiv 0 \bmod n_1$ for all $a \equiv 1 \bmod n_1$. By (17) and (18) it satisfies also $h(ab) \equiv ah(b)+h(a) \bmod m$ and by Lemma 4 we infer that for all $a \in A$, $a \equiv 1 \bmod (4, n)$

$$h(a) \equiv c(a-1) \bmod n$$

for a suitable c. This gives the first assertion of the lemma.

In order to prove the second one it is enough to consider the case, where $4 \mid n$ and A contains an integer $\bar{a}_0 \equiv -1 \bmod 4$. Let n_0 be the greatest odd factor of n_1 and $a_0 = \bar{a}_0^{n_0}$. Clearly $a_0 \equiv -1 \bmod 4$ and by (8)

$$a_0 \equiv 1 \bmod n_0(\bar{a}_0-1).$$

Hence by (17) and (18)

$$\boldsymbol{f}(a_0) \equiv \frac{a_0-1}{\bar{a}_0-1}\boldsymbol{f}(\bar{a}_0) \equiv \boldsymbol{0} \bmod (n_0, \boldsymbol{M}), \tag{26}$$

$$g(a_0) \equiv \frac{a_0-1}{\bar{a}_0-1}g(\bar{a}_0) \equiv 0 \bmod n_0. \tag{27}$$

Let $a_1, \ldots, a_s$ represent all residue classes of A congruent to $1 \bmod 4n_0$. If

$$a \equiv a_0 a_1^{x_1} \ldots a_s^{x_s} \bmod n \tag{28}$$

we have by (16), (17) and (18)

$$\begin{aligned} \boldsymbol{f}(a) &\equiv \boldsymbol{f}(a_0) + \boldsymbol{f}(a_1^{x_1} \ldots a_s^{x_s}) \\ &\equiv \boldsymbol{f}(a_0) + x_1\boldsymbol{f}(a_1) + \ldots + x_s\boldsymbol{f}(a_s) \bmod (4n_0, \boldsymbol{M}), \end{aligned} \tag{29}$$

$$g(a) \equiv g(a_0) + g(a_1^{x_1} \ldots a_s^{x_s}) \equiv g(a_0) + x_1 g(a_1) + \ldots + x_s g(a_s) \bmod 4n_0. \tag{30}$$

Let us set

$$\boldsymbol{F}_0 = \begin{bmatrix} \boldsymbol{f}(a_1) \\ \vdots \\ \boldsymbol{f}(a_s) \end{bmatrix}, \quad \boldsymbol{g}_0 = [g(a_1), \ldots, g(a_s)].$$

By (29)

$$\boldsymbol{f}(a) \equiv \boldsymbol{f}(a_0) + \boldsymbol{x}\boldsymbol{F}_0 \bmod (4n_0, \boldsymbol{PM})$$

and

$$\boldsymbol{f}(a)\boldsymbol{Q} \equiv \boldsymbol{f}(a_0)\boldsymbol{Q} + \boldsymbol{x}\boldsymbol{F}\boldsymbol{Q} \bmod (4n_0, \boldsymbol{PMQ}).$$

Now suppose that for a vector $\boldsymbol{x}$ we have

$$\boldsymbol{x}\boldsymbol{F}_0\boldsymbol{R} + \boldsymbol{f}(a_0)\boldsymbol{R} \equiv \boldsymbol{0} \bmod 2n_0, \tag{31}$$

where

$$\boldsymbol{R} = \boldsymbol{Q}\begin{bmatrix} \dfrac{2n_0}{(2n_0, e_1)} & \ldots & 0 \\ \ldots\ldots\ldots\ldots & & \\ 0 & \ldots & \dfrac{2n_0}{(2n_0, e_k)} \end{bmatrix}.$$

Then

$$\boldsymbol{x}\boldsymbol{F}_0\boldsymbol{Q} + \boldsymbol{f}(a_0)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod (2n_0, \boldsymbol{PMQ})$$

and since by (28) $(2n_0, e_i) = (a-1, n_1, e_i)$ we have by (27)

$$f(a)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod \big((a-1, n_1), \boldsymbol{PMQ}\big).$$

This together with (20) gives

$$f(a)\boldsymbol{Q} \equiv \boldsymbol{0} \bmod (a-1, \boldsymbol{PMQ}),$$

$$f(a) \equiv \boldsymbol{0} \bmod (a-1, \boldsymbol{M}).$$

By the assumption

$$g(a) \equiv 0 \bmod (a-1, n)$$

and by (30)

$$\boldsymbol{x}\boldsymbol{g}_0^T + g(a_0) \equiv 0 \bmod 2n_0. \tag{32}$$

Thus (31) implies (32). On the other hand, by the already proved part of the lemma and since $a-1 \equiv 0 \bmod 2n_0$,

$$\boldsymbol{g}_0^T = \boldsymbol{F}_0 n \boldsymbol{M}^{-1} \boldsymbol{u}_1^T \bmod 2n_0.$$

Also

$$n\boldsymbol{M}^{-1} = \boldsymbol{R}\begin{bmatrix} \dfrac{n(2n_0, e_1)}{2n_0 e_1} & \dots & 0 \\ \vdots & & \vdots \\ 0 & \dots & \dfrac{n(2n_0, e_k)}{2n_0 e_k} \end{bmatrix}\boldsymbol{P}$$

and finally by (26) and (27)

$$f(a_0)\boldsymbol{R} \equiv \boldsymbol{0} \bmod n_0, \qquad g(a_0) \equiv 0 \bmod n_0.$$

The assumptions of Lemma 3 are satisfied with $p = 2$ and we infer that for a suitable vector $\boldsymbol{d}$

$$\boldsymbol{g}_0^T \equiv \boldsymbol{F}_0 \boldsymbol{R}\boldsymbol{d}^T \bmod 2n_0, \qquad g(a_0) \equiv f(a_0)\boldsymbol{R}\boldsymbol{d}^T \bmod 2n_0.$$

Setting $\boldsymbol{u}_2 = \boldsymbol{d}\boldsymbol{R}^T$ we get

$$\boldsymbol{M}\boldsymbol{u}_2^T = \boldsymbol{M}\boldsymbol{R}\boldsymbol{d}^T = \boldsymbol{P}^{-1}\begin{bmatrix} \dfrac{2n_0 e_1}{(2n_0, e_1)} & & \\ & \ddots & \\ & & \dfrac{2n_0 e_k}{(2n_0, e_k)} \end{bmatrix}\boldsymbol{d}^T \equiv \boldsymbol{0} \bmod 2. \tag{33}$$

On the other hand, for each $i \leqslant s$

$$g(a_i) \equiv f(a_i)\boldsymbol{u}_2^T \bmod 2n_0$$

and since every $a \equiv 1 \bmod 2n_0$ is congruent to a_i or to $a_0 a_i \bmod n$ we infer from (16), (29) and (30) that

$$g(a) \equiv f(a)\boldsymbol{u}_2^T \bmod 2n_0$$

for all $a \equiv 1 \bmod 2n_0$. By (8) for any $a \in A$, $a^{n_0} \equiv 1 \bmod n_0$ and hence

$$g(a^{n_0}) - f(a^{n_0})\boldsymbol{u}_2^T \equiv 0 \bmod 2n_0.$$

On the other hand by (17), (18) and (33)

$$g(a^{n_0}) - f(a^{n_0})\boldsymbol{u}_2^T \equiv \frac{a^{n_0}-1}{a-1}\big(g(a) - f(a)\boldsymbol{u}_2^T\big) \bmod 2$$

and since $\dfrac{a^{n_0}-1}{a-1}$ is odd

$$g(a) \equiv f(a)\boldsymbol{u}_2^T \bmod 2.$$

LEMMA 6. *Let K be an arbitrary field, n a positive integer not divisible by the characteristic of K, n_i divisors of n and $\alpha_1, \dots, \alpha_k$, β non-zero elements of K. Let $\mathcal{G}$ be the Galois group of the field $K(\zeta_n, \sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_k]{\alpha_k})$ and assume that every element of $\mathcal{G}$ which fixes one of the fields $K(\xi_1, \dots, \xi_k)$, where $\xi_i^{n_i} = \alpha_i$ fixes at least one η with $\eta^n = \beta$. Then for any choice of numbers ξ_i and η and for suitable exponents $m_0, m_1, \dots, m_k, q_1, \dots, q_k$*

$$\zeta_n^{m_0}\eta\xi_1^{m_1} \dots \xi_k^{m_k} \in K(\zeta_4),$$

and if $n \equiv 0 \bmod 2$,

$$\eta^{n/2}\xi_1^{q_1} \dots \xi_k^{q_k} \in K, \qquad 2q_i \equiv 0 \bmod n_i \qquad (1 \leqslant i \leqslant k).$$

Proof. Let us choose some ξ_i and η. It is clear that

$$\eta \in K(\zeta_m, \xi_1, \dots, \xi_k) = L.$$

The elements σ of $\mathcal{G}$ act on L in the following way

$$\sigma(\zeta_n) = \zeta_n^a, \qquad \sigma(\xi_i) = \zeta_{n_i}^{t_i}\xi_i.$$

$\mathcal{G}$ contains a normal subgroup $\mathcal{H} = \{\sigma\colon \sigma(\zeta_n) = \zeta_n\}$. The vectors $[t_1, \dots, t_k]$ such that for a $\sigma \in \mathcal{H}$

$$\sigma(\xi_i) = \zeta_{n_i}^{t_i}\xi_i \qquad (1 \leqslant i \leqslant k)$$

constitute a lattice Λ. The fundamental vectors of Λ written horizontally form a matrix, say $\boldsymbol{M}$. Since the vectors $[n_1, 0, \dots, 0]$, $[0, n_2, 0 \dots, 0], \dots,$ $[0, 0, \dots, n_k]$ belong to Λ, $\boldsymbol{M}$ is non-sigular and

$$n\boldsymbol{M}^{-1} = \boldsymbol{S}\boldsymbol{N} \quad \text{for} \quad \boldsymbol{S} = \begin{bmatrix} n/n_1 & \dots & 0 \\ & \ddots & \\ 0 & \dots & n/n_k \end{bmatrix} \tag{34}$$

and a certain integral matrix $\boldsymbol{N}$.

Let A be the set of all integers a such that for a $\sigma \in \mathcal{G}$: $\sigma(\zeta_n) = \zeta_n^a$. The residues of $a \in A$ mod n form a subgroup $\mathcal{A}_n$ of the multiplicative group of residues mod n, isomorphic to $\mathcal{G}/\mathcal{H}$, and every integer the residue of which belongs to $\mathcal{A}_n$ is in A. Let $\boldsymbol{f}(1) = \boldsymbol{0}$, for an $a \in A$, $1 < a < n$, $\boldsymbol{f}(a) = [f_1(a), \ldots, f_k(a)]$ be any vector such that for a $\sigma \in \mathcal{G}$:

$$\sigma(\zeta_n) = \zeta_n^a, \quad \sigma(\xi_i) = \zeta_{n_i}^{f_i(a)}\xi_i \quad (1 \leqslant i \leqslant k)$$

and for all the other a let $\boldsymbol{f}(a) = \boldsymbol{f}\left(a - n\left[\frac{a}{n}\right]\right)$. Thus $\boldsymbol{f}(a) = \boldsymbol{f}(b)$ for $a \equiv b \bmod n$. On the other hand, for every $\sigma \in \mathcal{G}$ we have

$$\sigma(\zeta_n) = \zeta_n^a, \quad \sigma(\xi_i) = \zeta_{n_i}^{f_i(a)+t_i}\xi_i \tag{35}$$

for a suitable $a \in A$ and a suitable $[t_1, \ldots, t_k] \equiv \boldsymbol{0} \bmod \boldsymbol{M}$. Since $\mathcal{G}$ is a group with respect to superposition we get for all $a, b \in A$

$$\boldsymbol{f}(ab) \equiv a\boldsymbol{f}(b) + \boldsymbol{f}(a) \bmod \boldsymbol{M}.$$

Now for every pair $a, \boldsymbol{t}$ where $a \in A$, $\boldsymbol{t} \equiv \boldsymbol{0} \bmod \boldsymbol{M}$ we define σ by (35) and $\varphi(a, \boldsymbol{t})$ by the condition

$$\sigma(\eta) = \zeta_n^{\varphi(a,\boldsymbol{t})}\eta, \quad 0 \leqslant \varphi(a, \boldsymbol{t}) < n. \tag{36}$$

Since $\sigma_2\sigma_1(\eta) = \sigma_2\big(\sigma_1(\eta)\big)$ we get

$$\varphi\big(a_1a_2, a_2\big(\boldsymbol{t}_1 + \boldsymbol{f}(a_1)\big) + \boldsymbol{t}_2 + \boldsymbol{f}(a_2) - \boldsymbol{f}(a_1a_2)\big) \equiv a_2\varphi(a_1, \boldsymbol{t}_1) + \varphi(a_2, \boldsymbol{t}_2) \bmod n \tag{37}$$

and in particular

$$\varphi(1, \boldsymbol{t}_1 + \boldsymbol{t}_2) \equiv \varphi(1, \boldsymbol{t}_1) + \varphi(1, \boldsymbol{t}_2) \bmod n \quad \text{for} \quad \boldsymbol{t}_1 \equiv \boldsymbol{t}_2 \equiv 0 \bmod \boldsymbol{M}.$$

It follows that $\varphi(1, \boldsymbol{0}) \equiv 0 \bmod n$ and if $\boldsymbol{t} = \boldsymbol{x}\boldsymbol{M}$, $\boldsymbol{M} = \begin{bmatrix} \boldsymbol{m}_1 \\ \boldsymbol{m}_2 \\ \vdots \\ \boldsymbol{m}_k \end{bmatrix}$ then

$$\varphi(1, \boldsymbol{t}) = x_1\varphi(1, \boldsymbol{m}_1) + \ldots + x_k\varphi(1, \boldsymbol{m}_k).$$

Since $\boldsymbol{t}\boldsymbol{S} \equiv \boldsymbol{0} \bmod n$ implies $\varphi(1, \boldsymbol{t}) = \varphi(1, \boldsymbol{0}) = 0 \bmod n$ we infer by Lemma 2 that for an integral vector $\boldsymbol{c}$

$$\begin{bmatrix} \varphi(1, \boldsymbol{m}_1) \\ \vdots \\ \varphi(1, \boldsymbol{m}_k) \end{bmatrix} \equiv \boldsymbol{M}\boldsymbol{S}\boldsymbol{c}^T \bmod n$$

and thus $\varphi(1, \boldsymbol{t}) \equiv \boldsymbol{t}\boldsymbol{S}\boldsymbol{c}^T \bmod n$. Hence by (37) with $a_2 = 1$, $\boldsymbol{t}_1 = \boldsymbol{0}$

$$\varphi(a, \boldsymbol{t}) \equiv \varphi(a, \boldsymbol{0}) + \boldsymbol{t}\boldsymbol{S}\boldsymbol{c}^T \bmod n. \tag{38}$$

The condition (37) takes the form

$$\varphi(a_1a_2, \boldsymbol{0}) + (a_2\boldsymbol{t}_1 + \boldsymbol{t}_2)\boldsymbol{S}\boldsymbol{c}^T + \big(a_2\boldsymbol{f}(a_1) + \boldsymbol{f}(a_2) - \boldsymbol{f}(a_1a_2)\big)\boldsymbol{S}\boldsymbol{c}^T \equiv a_2\varphi(a_1, \boldsymbol{0}) + a_2\boldsymbol{t}_1\boldsymbol{S}\boldsymbol{c}^T + \varphi(a_2, \boldsymbol{0}) + \boldsymbol{t}_2\boldsymbol{S}\boldsymbol{c}^T \bmod n.$$

It follows that the function

$$g(a) = \varphi(a, \boldsymbol{0}) - \boldsymbol{f}(a)\boldsymbol{S}\boldsymbol{c}^T \tag{39}$$

satisfies the conditions $g(a) \equiv g(b) \bmod n$ for $a \equiv b \bmod n$ and

$$g(ab) \equiv ag(b) + g(a) \bmod n.$$

Now suppose that for an $a \in A$ we have

$$\boldsymbol{f}(a) \equiv \boldsymbol{0} \bmod (a-1, \boldsymbol{M}). \tag{40}$$

It follows that for a suitable $\boldsymbol{v} = [v_1, \ldots, v_k]$

$$\boldsymbol{f}(a) - (a-1)\boldsymbol{v} \equiv \boldsymbol{0} \bmod \boldsymbol{M}$$

and $\mathcal{G}$ contains σ such that

$$\sigma(\zeta_n) = \zeta_n^a, \quad \sigma(\xi_i) = \zeta_{n_i}^{(a-1)v_i}\xi_i^{v_i} \quad (1 \leqslant i \leqslant k).$$

We have

$$\sigma(\zeta_{n_i}^{-v_i}\xi_i) = \zeta_{n_i}^{-v_i}\xi_i \quad (1 \leqslant i \leqslant k),$$

thus by the assumption

$$\sigma(\zeta_n^{-v_0}\eta) = \zeta_n^{-v_0}\eta$$

for a suitable v_0. We obtain from (36), (38) and (39)

$$-v_0a + \varphi\big(a, (a-1)\boldsymbol{v} - \boldsymbol{f}(a)\big) \equiv -v_0 \bmod n,$$

$$\varphi(a, \boldsymbol{0}) + \big((a-1)\boldsymbol{v} - \boldsymbol{f}(a)\big)\boldsymbol{S}\boldsymbol{c}^T \equiv (a-1)v_0 \bmod n,$$

$$g(a) \equiv 0 \bmod (a-1, n). \tag{41}$$

Thus (40) implies (41) and we infer by Lemma 5 that for all $a \equiv 1 \bmod (4, n)$

$$g(a) \equiv -m_0(a-1) + \boldsymbol{f}(a)n\boldsymbol{M}^{-1}\boldsymbol{u}_1^T \bmod n \tag{42}$$

and for all a

$$g(a) \equiv \boldsymbol{f}(a)\boldsymbol{u}_2^T \bmod (2, n), \quad \boldsymbol{M}\boldsymbol{u}_2^T \equiv 0 \bmod (2, n). \tag{43}$$

Set $\boldsymbol{m} = [m_1, \ldots, m_k] = -\boldsymbol{c} - \boldsymbol{u}_1\boldsymbol{N}^T$, where $\boldsymbol{N}$ is defined by (34). If $a \equiv 1 \bmod (4, n)$ and σ is defined by (35) we get

$$\sigma(\zeta_n^{m_0}\eta\xi_1^{m_1}\ldots\xi_k^{m_k}) = \zeta_n^{e_1}\eta\,\xi_1^{m_1}\ldots\xi_k^{m_k},$$

where by (36), (38), (39) and (42)

$$\begin{aligned} e_1 &= am_0+\varphi(a,\boldsymbol{t})+(\boldsymbol{f}(a)+\boldsymbol{t})\boldsymbol{S}\boldsymbol{m}^T \\ &\equiv am_0+g(a)+(\boldsymbol{f}(a)+\boldsymbol{t})\boldsymbol{S}\boldsymbol{c}^T+(\boldsymbol{f}(a)+\boldsymbol{t})\boldsymbol{S}\boldsymbol{m}^T \\ &\equiv am_0-m_0(a-1)+f(a)n\boldsymbol{M}^{-1}\boldsymbol{u}_1^T-(\boldsymbol{f}(a)+\boldsymbol{t})\boldsymbol{S}\boldsymbol{N}\boldsymbol{u}_1^T \\ &\equiv m_0-tn\boldsymbol{M}^{-1}\boldsymbol{u}_1^T \equiv m_0 \bmod n. \end{aligned}$$

Thus $\sigma(\zeta_4)=\zeta_4$ implies

$$\sigma(\zeta_n^{m_0}\eta\xi_1^{m_1}\dots\xi_k^{m_k}) = \zeta_n^{m_0}\eta\xi_1^{m_1}\dots\xi_k^{m_k}$$

and the first assertion of the lemma follows. In order to prove the second one assume $2\mid n$ and set

$$\boldsymbol{q}=[q_1,\dots,q_k]=\frac{n}{2}\boldsymbol{c}+\frac{n}{2}\boldsymbol{u}_2\boldsymbol{S}^{-1}. \tag{44}$$

$\boldsymbol{q}$ is integral since by (34) and (43)

$$(n\boldsymbol{u}_2\boldsymbol{S}^{-1})^T = n\boldsymbol{S}^{-1}\boldsymbol{u}_2^T = \boldsymbol{N}\boldsymbol{M}\boldsymbol{u}_2^T \equiv \boldsymbol{0} \bmod 2.$$

If σ is defined by (35) we get

$$\sigma(\eta^{n/2}\xi_1^{q_1}\dots\xi_k^{q_k}) = \zeta_n^{e_2}\eta^{n/2}\xi_1^{q_1}\dots\xi_k^{q_k},$$

where by (36), (38), (39) and (43)

$$e_2=\frac{n}{2}\varphi(a,\boldsymbol{t})+(\boldsymbol{f}(a)+\boldsymbol{t})\boldsymbol{S}\boldsymbol{q}^T$$

$$\equiv\frac{n}{2}g(a)+\frac{n}{2}(\boldsymbol{f}(a)+\boldsymbol{t})\boldsymbol{S}\boldsymbol{c}^T+(\boldsymbol{f}(a)+\boldsymbol{t})\frac{n}{2}\boldsymbol{S}\boldsymbol{c}^T+(\boldsymbol{f}(a)+\boldsymbol{t})\frac{n}{2}\boldsymbol{u}_2^T \equiv 0 \bmod n.$$

It follows that

$$\eta^{n/2}\xi_1^{q_1}\dots\xi_k^{q_k}\in K.$$

Also, by (44) $2q_i\equiv 0 \bmod n_i$.

LEMMA 7. *Let K be an arbitrary field of characteristic different from 2 and τ the greatest integer such that $\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}\in K$ if there are only finitely many of them, otherwise $\tau=\infty$. If $\vartheta\in K(\zeta_4)$, $\vartheta^n\in K$, then at least one of the following four conditions is satisfied for a suitable $\gamma\in K$*

(i) $\vartheta^n=\gamma^n$,

(ii) $n\not\equiv 0 \bmod 2^\tau$, $\vartheta^n=-\gamma^n$,

(iii) $n\equiv 2^\tau \bmod 2^{\tau+1}$, $\vartheta^n=-(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)^{n/2}\gamma^n$,

(iv) $n\equiv 0 \bmod 2^{\tau+1}$, $\vartheta^n=(\zeta_{2^\tau}+\zeta_{2^\tau}^{-1}+2)^{n/2}\gamma^n$.

Remark. If n is a power of 2 the lemma is contained in Satz 2 of [4].

Proof. Set $\zeta_4=i$, $\vartheta=\alpha+\beta i$, $\alpha,\beta\in K$. If $i\in K$ we have (i); if $i\notin K$ then $(\alpha+\beta i)^n=\varkappa\in K$ implies $(\alpha-\beta i)^n=\varkappa$ hence

$$\alpha+\beta i=\zeta_n^\nu(\alpha-\beta i), \tag{45}$$

$$\zeta_n^\nu+\zeta_n^{-\nu}=\frac{\alpha+\beta i}{\alpha-\beta i}+\frac{\alpha-\beta i}{\alpha+\beta i}=\frac{2(\alpha^2-\beta^2)}{\alpha^2+\beta^2}\in K.$$

It follows that the only conjugate of ζ_n^ν over K is $\zeta_n^{-\nu}$ and the only possible conjugates of ζ_{2n}^ν are

$$\varepsilon_1\zeta_{2n}^{\varepsilon_2\nu} \quad (\varepsilon_1=\pm1,\ \varepsilon_2=\pm1).$$

(ζ_{2n} is chosen so that $\zeta_{2n}^2=\zeta_n$.)

Let

$$\mu=\operatorname{ord}_2 2n/(2n,\nu). \tag{46}$$

Then

$$\zeta_{2^\mu}=\zeta_{2n}^{\nu\varrho}, \quad \varrho\equiv 1 \bmod 2. \tag{47}$$

If σ is an automorphism of $K(\zeta_{2n}^\nu)$ and

$$\sigma(\zeta_{2n}^\nu)=\varepsilon_1\zeta_{2n}^{\varepsilon_2\nu} \tag{48}$$

we get

$$\sigma(\zeta_{2^\mu})=\varepsilon_1\zeta_{2^\mu}^{\varepsilon_2}. \tag{49}$$

If $\mu=2$ we have $\zeta_n^\nu\neq 1$, by (45)

$$\alpha=\beta i\frac{\zeta_n^\nu+1}{\zeta_n^\nu-1},$$

$$\vartheta^n=\beta^n\left(\frac{2i}{\zeta_n^\nu-1}\right)^n=\beta^n(-1)^\nu\left(\frac{2i}{\zeta_{2n}^\nu-\zeta_{2n}^{-\nu}}\right)^n \tag{50}$$

and by (48) and (49) for all automorphisms σ of $K(\zeta_{2n}^\nu)$ over K

$$\sigma\left(\frac{2i}{\zeta_{2n}^\nu-\zeta_{2n}^{-\nu}}\right)=\frac{2i}{\zeta_{2n}^\nu-\zeta_{2n}^{-\nu}}.$$

Thus $\dfrac{2i}{\zeta_{2n}^\nu-\zeta_{2n}^{-\nu}}\in K$ and by (46) and (50) we get (i) if ν is even and (ii) if ν is odd.

If $\mu\neq 2$, $\zeta_n^\nu\neq -1$ and by (45)

$$\beta i=\alpha\frac{\zeta_n^\nu-1}{\zeta_n^\nu+1},$$

$$\vartheta^n=\alpha^n\left(\frac{2}{\zeta_n^\nu+1}\right)^n=\alpha^n(-1)^\nu\left(\frac{2}{\zeta_{2n}^\nu+\zeta_{2n}^{-\nu}}\right)^n. \tag{51}$$

If σ is an automorphism of $K(\zeta_{2n}^{\nu})$,

$$\delta = (\zeta_{2n}^{\nu}+\zeta_{2n}^{-\nu})(\zeta_{2^{\mu}}+\zeta_{2^{\mu}}^{-1})$$

we have by (48) and (49)

$$\sigma(\delta) = \delta.$$

Thus $\delta \in K$ and since $\zeta_{2^{\mu}}+\zeta_{2^{\mu}}^{-1} \neq 0$ we get from (51)

$$\vartheta^n = (-1)^{\nu}(\zeta_{2^{\mu}}+\zeta_{2^{\mu}}^{-1})^n\left(\frac{2a}{\delta}\right)^n. \tag{52}$$

On the other hand, $\mu \leqslant \tau+1$. This is clear if $\mu = 0$ and if $\mu > 0$ it follows from (47) that

$$\zeta_{2^{\mu-1}}+\zeta_{2^{\mu-1}}^{-1} = \zeta_n^{\nu\varrho}+\zeta_n^{-\nu\varrho} = \left(\frac{\alpha+\beta i}{\alpha-\beta i}\right)^{\varrho}+\left(\frac{\alpha-\beta i}{\alpha+\beta i}\right)^{\varrho} \in K$$

thus $\mu-1 \leqslant \tau$.

Denoting by γ a suitable element of K we can draw from (46) and (52) the following conclusions:

If $\mu \leqslant \tau$, $\nu \equiv 0 \bmod 2$ then $\vartheta^n = \gamma^n$;

if $\mu \leqslant \tau$, $\nu \equiv 1 \bmod 2$ then $\vartheta^n = -\gamma^n$, $n \not\equiv 0 \bmod 2^{\tau}$;

if $\mu = \tau+1$, $\nu \equiv 1 \bmod 2$, then $\vartheta^n = -(\zeta_{2^{\tau}}+\zeta_{2^{\tau}}^{-1}+2)^{n/2}\gamma^n$ and $n \equiv 2^{\tau} \bmod 2^{\tau+1}$;

if $\mu = \tau+1$, $\nu \equiv 0 \bmod 2$, then $\vartheta^n = (\zeta_{2^{\tau}}+\zeta_{2^{\tau}}^{-1}+2)^{n/2}\gamma^n$,

which correspond to the conditions (i), (ii), (iii), (iv), respectively.

LEMMA 8. *Let K be an algebraic number field, $f_i(x)$ polynomials over K with integral coefficients and discriminants D_i and $\mathfrak{p}$ a prime ideal of K not dividing $D_1 \dots D_k$. The k congruences $f_i(x) \equiv 0 \bmod \mathfrak{p}$ $(1 \leqslant i \leqslant k)$ are soluble $\bmod \mathfrak{p}$ if and only if $\mathfrak{p}$ has a prime factor of degree one in at least one field $K(\xi_1, \dots, \xi_k)$, where $f_i(\xi_i) = 0$.*

Proof. The sufficiency of the condition is obvious. In order to prove the necessity we proceed by induction. For $k = 1$ the condition follows from Dedekind's theorem applied to a suitable irreducible factor of f. Suppose that the condition holds for less than k polynomials and that the k congruences $f_i(x) \equiv 0 \bmod \mathfrak{p}$ are soluble. Then $\mathfrak{p}$ has a prime factor $\mathfrak{P}$ of degree one in $K(\xi_1, \dots, \xi_{k-1})$, where ξ_i is a certain zero of $f_i(x)$. The congruence $f_k(x) \equiv 0 \bmod \mathfrak{P}$ being soluble it follows by Dedekind's theorem that $\mathfrak{P}$ has a prime factor of relative degree one in at least one field $K(\xi_1, \dots, \xi_k)$ where $f_k(\xi_k) = 0$. This factor is of degree one over K, which completes the proof.

LEMMA 9. *If K is an algebraic number field, τ is defined as in Theorem 1 and $\nu > \tau$ then the congruence $x^{2^{\nu}} \equiv (\zeta_{2^{\tau}}+\zeta_{2^{\tau}}^{-1}+2)^{2^{\nu-1}} \bmod \mathfrak{p}$ is soluble for all prime ideals $\mathfrak{p}$ of K.*

Proof, see [5], p. 156.

Proof of Theorem 1. Necessity. Suppose that the Galois group $\mathcal{G}$ of the extension $L = K(\zeta_n, \sqrt[n_1]{\alpha_1}, \dots, \sqrt[n_k]{\alpha_k})$ of K contains an element σ, which fixes one of the fields $K(\xi_1, \dots, \xi_k)$, where $\zeta_i^{n_i} = \alpha_i$ but does not fix any η with $\eta^n = \beta$. By Frobenius density theorem prime ideals $\mathfrak{p}$ of K belonging to the division of σ in $\mathcal{G}$ have a positive density. Every such prime ideal $\mathfrak{p}$ has a prime factor of degree one in $K(\xi_1, \dots, \xi_k)$ $(1 \leqslant i \leqslant k)$ where $\xi_1, \dots, \xi_k$ are suitably chosen roots of $\xi_i = \alpha_i$, but it has no prime factor of degree one in any of the fields $K(\eta)$, where $\eta^n = \beta$. By Lemma 8, for almost all $\mathfrak{p}$'s the congruences $x^{n_i} \equiv \alpha_i \pmod{\mathfrak{p}}$ are soluble and the congruence $x^n \equiv \beta \pmod{\mathfrak{p}}$ is insoluble. The obtained contradiction shows that the assumptions of Lemma 6 are satisfied. Let us choose some values of $\xi_1, \dots, \xi_k$ and η. By Lemma 6 there exist integers $m_0, m_1, \dots, m_k$, $q_1, \dots, q_k$ such that

$$\vartheta = \zeta_n^{m_0}\eta\xi_1^{m_1} \dots \xi_k^{m_k} \in K(\zeta_4)$$

and if $n \equiv 0 \bmod 2$

$$\varkappa = \eta^{n/2}\xi_1^{q_1} \dots \xi_k^{q_k} \in K, \quad 2q_i \equiv 0 \bmod n_i \quad (1 \leqslant i \leqslant k). \tag{53}$$

Since

$$\vartheta^n = \beta\prod_{i=1}^{k}\alpha_i^{nm_i/n_i} \in K$$

we have by Lemma 7 for a suitable $\gamma \in K$ either

$$\beta\prod_{i=1}^{k}\alpha_i^{nm_i/n_i} = \gamma^n, \tag{54}$$

or $n \not\equiv 0 \bmod 2^{\tau}$

$$\beta\prod_{i=1}^{k}\alpha_i^{nm_i/n_i} = -\gamma^n \tag{55}$$

or $n \equiv 2^{\tau} \bmod 2^{\tau+1}$

$$\beta\prod_{i=1}^{k}\alpha_i^{nm_i/n_i} = -(\zeta_{2^{\tau}}+\zeta_{2^{\tau}}^{-1}+2)^{n/2}\gamma^n \tag{56}$$

or $n \equiv 0 \bmod 2^{\tau+1}$

$$\beta\prod_{i=1}^{k}\alpha_i^{nm_i/n_i} = (\zeta_{2^{\tau}}+\zeta_{2^{\tau}}^{-1}+2)^{n/2}\gamma^n. \tag{57}$$

(54) and (57) correspond to the conditions (i) and (iv), respectively.

If $n \not\equiv 0 \bmod 2$ (55) reduces to (54). If $n \equiv 0 \bmod 2$ we get from (53)

$$\beta\prod_{i=1}^{k}\alpha_i^{2q_i/n_i} = \varkappa^2, \quad \varkappa \in K.$$

This together with (55) and (56) gives on division

$$\prod_{i=1}^{k} a_i^{l_i} = -\lambda^2, \quad \text{where} \quad l_i = \frac{nm_i - 2q_i}{n_i},\ \lambda \in K.$$

However if n_i is odd, l_i is even, thus

$$\prod_{n_i \text{ even}} a_i^{l_i} = -\delta^2, \quad \delta \in K.$$

Sufficiency. The sufficiency of the condition (i) is obvious. To show that (ii) and (iii) are sufficient we argue as follows. The equality

$$\prod_{n_i \text{ even}} a_i^{l_i} = -\delta^2$$

implies that for any choice of ξ_i satisfying $\xi_i^{n_i} = a_i$

$$\zeta_4 \in K(\xi_1, \ldots, \xi_k).$$

Since

$$\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} \in K, \quad 2\zeta_{2^\tau} = \zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + \zeta_4(\zeta_{2^\tau}^{1-2^{\tau-2}} + \zeta_{2^\tau}^{-1+2^{\tau-2}})$$

we have $K(\zeta_4) = K(\zeta_{2^\tau})$. Hence $\zeta_{2^\tau} \in K(\xi_1, \ldots, \xi_k)$.

Let $\nu = \operatorname{ord}_2 n$. The conditions

$$\beta \prod_{i=1}^{k} a_i^{nm_i/n_i} = -\gamma^n, \quad \nu < \tau,$$

and

$$\beta \prod_{i=1}^{k} a_i^{nm_i/n_i} = -(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2}\gamma^n, \quad \nu = \tau,$$

can be rewritten for a suitable η and ϱ as

$$\eta \prod_{i=1}^{k} \xi_i^{m_i} = \zeta_{2^\tau}^{\varrho}\gamma$$

and

$$\eta \prod_{i=1}^{k} \xi_i^{m_i} = (\zeta_{2^\tau} + 1)\gamma,$$

respectively.

It follows that $\eta \in K(\xi_1, \ldots, \xi_k)$ and any ideal $\mathfrak{p}$ which has a prime factor of degree one in $K(\xi_1, \ldots, \xi_k)$ has a prime factor of degree one in $K(\eta)$. Since this is valid for any choice of ξ_i and a suitable η, we infer

by Lemma 8 that the solubility of $x^n \equiv a_i$ $(1 \leqslant i \leqslant k)$ implies the solubility of $x^n \equiv \beta \bmod \mathfrak{p}$.

The sufficiency of condition (iv) follows from Lemma 9, since the solubility of the congruence

$$x^{2^\nu} \equiv (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{2^{\nu-1}} \bmod \mathfrak{p}$$

clearly implies the solubility of the congruence

$$x^n \equiv (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2} \bmod \mathfrak{p}.$$

If $\zeta_4 \in K$ then $\zeta_{2^\tau} \in K$ and the equalities

$$-1 = \zeta_{2^{\nu+1}}^{n} \quad \text{if} \quad \nu < \tau,$$

$$(-1)^{n/2^\tau}(\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2} = (\zeta_{2^\tau} + 1)^n, \quad \text{if} \quad \nu \geqslant \tau$$

show that the conditions (ii), (iii), (iv) imply (i).

If $\tau = 2$ and $n \not\equiv 0 \bmod 2^\tau$ we have either $n \equiv 1 \bmod 2$ in which case $-\gamma^n = (-\gamma)^n$ or $n \equiv 2 \bmod 4$. In the latter case we get from (ii)

$$\beta \prod_{i=1}^{k} a_i^{nm_i/n_i} \prod_{n_i \text{ even}} a_i^{l_i n/2} = (\gamma\delta)^n,$$

which leads to (i). The proof is complete.

Proof of Corollary 1 follows at once from Lemma 8.

Proof of Corollary 2. If the congruences $x^n \equiv \alpha \bmod \mathfrak{p}$ and $x^n \equiv \beta \bmod \mathfrak{p}$ are for almost all $\mathfrak{p}$ simultaneously soluble or insoluble, we have by Theorem 1 the following seven possibilities:

(58) $$\alpha \overset{n}{=} \beta^t, \quad \beta \overset{n}{=} \alpha^s;$$

(59) $$n \not\equiv 0 \bmod 2^\tau, \quad \alpha \overset{n}{=} \beta^t = -\delta^2, \quad \beta \overset{n}{=} -\alpha^s;$$

(60) $$n \equiv 2^\tau \bmod 2^{\tau+1}, \quad \alpha \overset{n}{=} \beta^t = -\delta^2, \quad \beta \overset{n}{=} -\omega\alpha^s;$$

(61) $$n \equiv 0 \bmod 2^{\tau+1}, \quad \alpha \overset{n}{=} \beta^t, \quad \beta \overset{n}{=} \omega\alpha^s;$$

(62) $$n \not\equiv 0 \bmod 2^\tau, \quad \alpha \overset{n}{=} -\beta^t = -\delta_1^2, \quad \beta \overset{n}{=} -\alpha^s = -\delta_2^2;$$

(63) $$n \equiv 2^\tau \bmod 2^{\tau+1}, \quad \alpha \overset{n}{=} -\omega\beta^t = -\delta_1^2, \quad \beta \overset{n}{=} -\omega\alpha^s = -\delta_2^2;$$

(64) $$n \equiv 0 \bmod 2^{\tau+1}, \quad \alpha \overset{n}{=} \omega\beta^t, \quad \beta \overset{n}{=} \omega\alpha^s$$

and three other possibilities obtained by the permutation of α and β in (59), (60) and (61). Here $\gamma \overset{n}{=} \delta$ means that γ/δ is an nth power in K and $\omega = (\zeta_{2^\tau} + \zeta_{2^\tau}^{-1} + 2)^{n/2}$. Moreover, in (59) to (64) it is assumed that $\zeta_4 \notin K$. Let us choose an integer x such that $u = s + (st-1)x$ is prime to n. If s is even or t is odd x will be chosen odd, which is possible because then $(s + st - 1, 2(st-1)) = 1$.

Now, (58) gives $\alpha \overset{n}{=} \alpha^{st}$, $\alpha^{st-1} \overset{n}{=} 1$, $\beta \overset{n}{=} \alpha^{u}$;

(59) gives $t \equiv 1 \bmod 2$, $\alpha \overset{n}{=} -\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} -1$, $\beta \overset{n}{=} \alpha^{u}$;

(60) gives $t \equiv 1 \bmod 2$, $\alpha \overset{n}{=} -\omega\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} -\omega$, $\beta \overset{n}{=} \alpha^{u}$;

(61) gives $\alpha \overset{n}{=} \omega^{t}\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} \omega^{t}$, $\beta \overset{n}{=} \omega^{t+1}\alpha^{u}$;

(62) gives $s \equiv t \equiv 0 \bmod 2$. Indeed, if for instance $t \equiv 1 \bmod 2$ then $-\delta_1^2 = -\beta^t = \delta_2^{2t}$ and $\zeta_4 \in K$. If $s \equiv t \equiv 0 \bmod 2$ then $\alpha \overset{n}{=} -\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} -1$, $\beta \overset{n}{=} \alpha^{u}$.

(63) gives like (62) that $s \equiv t \equiv 0 \bmod 2$. In that case $\alpha \overset{n}{=} -\omega\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} -\omega$, $\beta \overset{n}{=} \alpha^{u}$.

Finally (64) gives $\alpha \overset{n}{=} \omega^{t+1}\alpha^{st}$, $\alpha^{st-1} \overset{n}{=} \omega^{t+1}$, $\beta \overset{n}{=} \omega^{t+x+1}\alpha^{u}$.

On the other hand, if $\beta \overset{n}{=} \alpha^{u}$ or $n \equiv 0 \bmod 2^{r+1}$ and $\beta \overset{n}{=} \omega\alpha^{u}$, where $(u, n) = 1$ then also $\alpha \overset{n}{=} \beta^{v}$ or $\alpha \overset{n}{=} \omega\beta^{v}$, respectively and by Theorem 1 the congruences $x^n \equiv \alpha \bmod \mathfrak{p}$ and $x^n \equiv \beta \bmod \mathfrak{p}$ are simultaneously soluble or insoluble for almost all prime ideals $\mathfrak{p}$ of K.

To prove Theorem 2 we need two lemmata both due to Skolem.

LEMMA 10. *In every algebraic number field K there exists an infinite sequence of elements π_j such that every element of K is represented uniquely in the form $\zeta \prod_{j=1}^{l} \pi_j^{d_j}$, where ζ is a root of unity and d_j are rational integers.*

Proof, see [9].

LEMMA 11. *If a system of linear congruences is soluble for all moduli, then the corresponding system of equations is soluble in rational integers.*

Proof, see [7].

Proof of Theorem 2. Let

$$\alpha_i = \zeta_w^{a_{i0}} \prod_{j=1}^{l} \pi_j^{a_{ij}}, \qquad \beta = \zeta_w^{b_0} \prod_{j=1}^{l} \pi_j^{b_j},$$

where w is the number of roots of unity contained in K, π_j have the property asserted in Lemma 10 and a_{ij}, b_j are rational integers. If the congruence

$$\alpha_1^{x_1} \dots \alpha_k^{x_k} \equiv \beta \pmod{\mathfrak{p}}$$

is soluble for almost all $\mathfrak{p}$ then for every positive integer n the solubility of the k congruences $x^n \equiv \alpha_i \pmod{\mathfrak{p}}$ $(1 \leqslant i \leqslant k)$ implies the solubility of $x^n \equiv \beta \pmod{\mathfrak{p}}$. It follows hence by Theorem 1 with $n = 2^{r+1}m$ that for every positive integer n there exist $\gamma \in K$ and rational integers $m_1, \dots, m_k$ such that

$$\beta\alpha_1^{m_1} \dots \alpha_k^{m_k} = \gamma^m.$$

By Lemma 10 the last equality implies for a suitable m_0

$$b_0 + \sum_{i=1}^{k} a_{i0}m_i + wm_0 \equiv 0 \bmod m,$$

$$b_j + \sum_{i=1}^{k} a_{ij}m_i \equiv 0 \bmod m \qquad (1 \leqslant j \leqslant l).$$

By Lemma 11 there exist rational integers $m_0, \dots, m_k$ such that

$$b_0 + \sum_{i=1}^{k} a_{i0}m_i + wm_0 = 0,$$

$$b_j + \sum_{i=1}^{k} a_{ij}m_i = 0 \qquad (1 \leqslant j \leqslant l)$$

and this gives

$$\beta = \prod_{i=1}^{k} \alpha_i^{m_i}.$$

The above proof is modelled on Skolem's proof ([7]) of his theorem that the solubility of the congruence $\alpha_1^{x_1} \dots \alpha_k^{x_k} \equiv \beta \bmod \mathfrak{m}$ for all moduli implies the solubility of the corresponding equation. That proof uses instead of Theorem 1 the case $D = 1$ of the following

LEMMA 12. *Let $\xi_0 = \zeta_w, \xi_1, \dots, \xi_t$ be any t distinct terms of the sequence π_j. For any positive integer m there exists $\mu \in K$ prime to D such that the congruence*

$$\xi_0^{y_0}\xi_1^{y_1} \dots \xi_t^{y_t} \equiv 1 \bmod \mu$$

implies $y_0 \equiv 0 \bmod w$, $y_1 \equiv \dots \equiv y_t \equiv 0 \bmod m$.

Skolem's proof of the above lemma given only in the case of fields with class number one is defective because he claims the existence of prime ideals $\mathfrak{p}_0, \dots, \mathfrak{p}_t$ of K such that $x^m \equiv \xi_r \bmod \mathfrak{p}_s$ is soluble for $r \neq s$ and $x^m \equiv \xi_r^j \bmod \mathfrak{p}_r$ is insoluble for $j \not\equiv 0 \bmod m$, $r \neq 0$ and $j \not\equiv 0 \bmod (m, w)$, $r = 0$. The assertion is false for $K = Q$, $t = 1$, $\xi_1 = 2$, $m = 4$.

Proof of Lemma 12. We can assume without loss of generality that $m \equiv 0 \bmod 2^{r+1}w$. For every $p \mid m$ set $n = m(p, 2)$. Suppose that the solubility of

$$x^n \equiv \xi_i \bmod \mathfrak{p} \qquad (i \neq r \neq 0) \tag{65}$$

implies the solubility of

$$x^n \equiv \xi_r^{m/p} \bmod \mathfrak{p} \tag{66}$$

for almost all $\mathfrak{p}$. Then by Theorem 1

$$\xi_r^{m/p} \prod_{i \neq r} \xi_i^{m_i} = \gamma^{n/2}$$

for suitable $\gamma \in K$ and suitable exponents m_i. We get

$$\frac{m}{p} \equiv 0 \bmod \frac{n}{2}, \quad \frac{m}{p} \equiv 0 \bmod \frac{m(p,2)}{2},$$

which is impossible.

The obtained contradiction shows that for a certain prime ideal $\mathfrak{p}$ prime to D the congruences (65) are soluble, but (66) is insoluble. Denoting this prime ideal by $\mathfrak{p}_{p,r}$ we infer from

$$\xi_0^{x_0}\xi_1^{x_1}\dots\xi_t^{x_t} \equiv 1 \bmod \mathfrak{p}_{p,r}$$

that

$$(m(p,2), x_r) \nmid \frac{m}{p},$$

hence

$$\operatorname{ord}_p x_r \geqslant \operatorname{ord}_p m.$$

If $p \mid w$, suppose that the solubility of the congruences

$$x^n \equiv \xi_i \bmod \mathfrak{p} \quad (1 \leqslant i \leqslant t) \tag{67}$$

implies the solubility of the congruence

$$x^n \equiv \zeta_p \bmod \mathfrak{p} \tag{68}$$

for almost all $\mathfrak{p}$. Then by Theorem 1

$$\zeta_p \prod_{i=1}^{t} \xi_i^{m_i} = \gamma^{n/2}$$

for suitable $\gamma \in K$ and suitable exponents m_i. We get

$$\frac{w}{p} \equiv 0 \bmod \left(\frac{n}{2}, w\right), \quad \frac{w}{p} \equiv 0 \bmod \frac{w(p,2)}{2}.$$

The obtained contradiction shows that for a certain prime ideal $\mathfrak{p}$ prime to D the congruences (67) are soluble, but (68) is insoluble. Denoting this prime ideal by $\mathfrak{p}_{p,0}$ we infer from

$$\xi_0^{x_0}\xi_1^{x_1}\dots\xi_t^{x_t} \equiv 1 \bmod \mathfrak{p}_{p,0}$$

that

$$(x_0, w) \nmid \frac{w}{p}$$

hence $\operatorname{ord}_p x_0 \geqslant \operatorname{ord}_p w$.

For μ we can choose any number prime to D divisible by

$$\prod_{p \mid m} \prod_{r=1}^{k} \mathfrak{p}_{p,r} \prod_{p \mid w} \mathfrak{p}_{p,0}.$$

Proof of Theorem 3. Let for $i \leqslant h$, $j \leqslant k$

$$a_{ij} = \prod_{s=0}^{t} \xi_s^{a_{ijs}}, \quad \beta_i = \prod_{s=0}^{t} \xi_s^{a_{i0s}}$$

in the notation of Lemma 12 and let m, D be positive integers.

Let μ be a modulus with the property asserted in Lemma 12. Then the congruences

$$\prod_{j=1}^{k} a_{ij}^{x_j} \equiv \beta_i \bmod \mu \quad (i = 1, \dots, h)$$

imply

$$\sum_{j=1}^{k} a_{ij0} x_j \equiv a_{i00} \bmod w \quad (i = 1, \dots, h),$$

$$\sum_{j=1}^{k} a_{ijs} x_j \equiv a_{i0s} \bmod m \quad (i = 1, \dots, h;\ s = 1, \dots, t)$$

and by Lemma 11 there exist rational integers x_j $(j = 1, \dots, k)$ and y_i $(i = 1, \dots, h)$ satisfying the system of equations

$$\sum_{j=1}^{k} a_{ij0} x_j = a_{i00} + w y_i \quad (i = 1, \dots, h),$$

$$\sum_{j=1}^{k} a_{ijs} x_j = a_{i0s} \quad (i = 1, \dots, h;\ s = 1, \dots, t).$$

Hence

$$\prod_{j=1}^{k} a_{ij}^{x_j} = \beta_i \quad (i = 1, \dots, h).$$

The proof is complete.

We proceed to the example showing that Theorem 3 is no longer valid if the solubility for all moduli prime to D is replaced by the solubility for all prime moduli.

Let us consider the system

$$\begin{aligned} 2^x 3^y &\equiv 1 \bmod p, \\ 2^y 3^z &\equiv 4 \bmod p. \end{aligned} \tag{69}$$

For $p = 2, 3$ it has the solution $(x, y, z) = (0, 1, 0)$, $(0, 0, 0)$, respectively.

For other p it is equivalent to the system

$$\begin{aligned} x\operatorname{ind}2 + y\operatorname{ind}3 &\equiv 0 \bmod p-1, \\ y\operatorname{ind}2 + z\operatorname{ind}3 &\equiv 2\operatorname{ind}2 \bmod p-1, \end{aligned} \tag{70}$$

where indices are taken with respect to a fixed primitive root mod p. Now

$$((\operatorname{ind}2)^2, (\operatorname{ind}3)^2) \mid \operatorname{ind}2\operatorname{ind}3.$$

Hence

$$\left(\frac{(\operatorname{ind}2)^2}{(\operatorname{ind}2, \operatorname{ind}3)}, \operatorname{ind}3 \right) \mid \operatorname{ind}2$$

and the equation

$$t\frac{(\operatorname{ind}2)^2}{(\operatorname{ind}2, \operatorname{ind}3)} + z\operatorname{ind}3 = 2\operatorname{ind}2$$

is soluble in integers. The numbers $x = \dfrac{-t\operatorname{ind}3}{(\operatorname{ind}2, \operatorname{ind}3)}$, $y = \dfrac{t\operatorname{ind}2}{(\operatorname{ind}2, \operatorname{ind}3)}$ and z satisfy the system (70) and hence also (69).

References

[1] H. Flanders, *Generalization of a theorem of Ankeny and Rogers*, Ann. of Math. 57 (1953), pp. 392–400.

[2] I. Gerst, *On the theory of nth power residues and a conjecture of Kronecker*, Acta Arith. 17 (1970), pp. 121–139.

[3] H. Hasse, *Bericht über neuere Untersuchungen und Probleme aus der Theorie der algebraischen Zahlkörper*, Teil II, 1930; reprint Würzburg–Wien 1965.

[4] — *Zum Existenzsatz von Grunwald in der Klassenkörpertheorie*, J. Reine Angew. Math. 188 (1950), pp. 40–64.

[5] H. B. Mann, *Introduction to Algebraic Number Theory*, Columbus, Ohio 1955.

[6] A. Schinzel, *A refinement of a theorem of Gerst on power residues*, Acta Arith. 17 (1970), pp. 161–168.

[7] Th. Skolem, *Anwendung exponentieller Kongruenzen zum Beweis der Unlösbarkeit gewisser diophantischer Gleichungen*, Vid. akad. Avh. Oslo I 1937 nr 12.

[8] — *Diophantische Gleichungen*, Berlin 1938.

[9] — *On the existence of a multiplicative basis for an arbitrary algebraic field*, Norske Vid. Selsk. Forh. (Trondheim) 20 (1947) nr 2.

Received on 11. 12. 1973 (502)

ACTA ARITHMETICA
XXVII (1975)

The generalized Hardy-Littlewood's problem involving a quadratic polynomial with coprime discriminants

by

HENRYK IWANIEC (Warszawa)

Dedicated to the memory of Yu. V. Linnik

Introduction
(History of the problem and the principal ideas)

The problem to be treated in this paper has its origin in the third pape [4] of Hardy and Littlewood's famous series "*Some problems of partitio numerorum*". Having introduced in the analytic theory of numbers a new and powerful circle method the authors derived with its help many asymptotic formulae for the number of representation of a given positive integer as the sum of a fixed number of summands taken from prescribed sequences (prime numbers, squares and higher powers of positive integers). The method is applicable to problems involving a large number summands. Nevertheless Hardy and Littlewood using it in a formal way derived the asymptotic formula

$$\text{(HL)} \qquad \sum_{p+x^2+y^2=n} 1 \sim \pi \prod_{p>2} \left(1+\frac{\chi(p)}{p(p-1)}\right) \prod_{\substack{p\mid n \\ p\equiv 1 \pmod 4}} \left(1-\frac{p}{p^2-p+1}\right) \prod_{\substack{p\mid n \\ p\equiv 3 \pmod 4}} \left(1+\frac{p}{p^2-p-1}\right) \frac{n}{\log n}$$

and conjectured its validity (the first half of Conjecture J). In the fifth paper of the series [5] they expressed the opinion that the generalized Riemann hypothesis (GRH) implies the formula (HL) for almost all positive integers n. The implication was proved by Miss Stanley in 1928 ([12]). The problem of the validity of (HL) for almost all n unlike that for all n is ternary one and nowadays it can be easily solved without the generalized Riemann hypothesis by using Vinogradov's estimates for trigonometric sums with primes, which supplement the circle method in an essential way.