DEMONSTRATIO MATHEMATICA
Vol. XVIII No 1 1985

Andrzej Schinzel

SYSTEMS OF EXPONENTIAL CONGRUENCES

Dedicated to the memory of Professor Roman Sikorski

Some years ago I have proved the following theorem ([1], Theorem 2). Let K be an algebraic number field, $\alpha_1,\ldots,\alpha_k$, β non-zero elements of K. If for almost all prime ideals $\mathfrak{p}$ of K the congruence

$$\prod_{j=1}^{k} \alpha_j^{x_j} \equiv \beta \pmod{\mathfrak{p}}$$

is soluble in integers x_j then the equation

$$\prod_{j=1}^{k} \alpha_j^{x_j} = \beta$$

is soluble in integers. I have shown by an example that this theorem does not extend to systems of congruences of the form

$$(1)\qquad \prod_{j=1}^{k} \alpha_{ij}^{x_j} \equiv \beta_i \pmod{\mathfrak{p}} \qquad (i = 1,2,\ldots,h)$$

even for $h = 2$, $k = 3$.

Recently L. Somer [4] has considered systems of the form (1) for $k = 1$. The study of his work has suggested to me that the connection between the local and the global solubility of (1) may hold if for some $i \leq h$ the numbers α_{ij} are multiplicatively independent. The aim of this paper is to prove this assertion in the form of the following theorem.

Theorem 1. Let K be an algebraic number field, α_{ij}, β_i ($i = 1,2,\ldots,h$; $j = 1,2,\ldots,k$) non-zero elements of K and assume that for some $i \leq h$

$$\prod_{j=1}^{k} \alpha_{ij}^{x_j} = 1, \ x_j \in Z \quad \text{implies} \quad x_j = 0 \text{ for all } j \leq k.$$

If for almost all prime ideals $\mathfrak{p}$ of K in the sense of the Dirichlet density the system (1) is soluble in integers x_j then the system of equations

$$(2) \qquad \prod_{j=1}^{k} \alpha_{ij}^{x_j} = \beta_i \quad (i = 1,2,\ldots,h)$$

is soluble in integers.

The following corollary is almost immediate.

Corollary. If the system of congruences

$$\alpha_i^x \equiv \beta_i (\mathrm{mod}\ \mathfrak{p}) \quad (i = 1,2,\ldots,h)$$

is soluble in integers x for almost all prime ideals $\mathfrak{p}$ of K then the system of equations

$$\alpha_i^x = \beta_i \quad (i = 1,2,\ldots,h)$$

is soluble in integers.

Somer [4] has proved the above corollary under the assumption that either none of the α_i's is a root of unity or all the α_i's are roots of unity.

The next theorem shows that Theorem 1 cannot be extended further.

Theorem 2. For every $k \geq 2$ there exist non-zero rational integers α_{ij}, β_i ($i = 1,2$; $j = 1,2,\ldots,k$) such that $\alpha_{12},\ldots,\alpha_{1k}$ are multiplicatively independent, the system (1) with $h = 2$ is soluble for all rational primes $\mathfrak{p}$, but the system (2) is unsoluble in integers.

In the sequel ζ_q denotes a primitive q th root of unity.

For a rational matrix M den M denotes the least common denominator of the elements of M and M^T the transpose of M.

The proofs are based on eight lemmata.

L e m m a 1. For every rational square matrix A there exists a non-singular matrix U whose elements are integers in the splitting field of the characteristic polynomial of A such that

$$(3) \qquad U^{-1}AU = \begin{bmatrix} A_1 & & & & \\ & A_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \\ & & & & & A_n \end{bmatrix}$$

with A_ν a square matrix of degree ρ_ν:

$$(4) \qquad A_\nu = \begin{bmatrix} \lambda_\nu & 1 & & & \\ & \lambda_\nu & 1 & & \\ & & \ddots & \ddots & \\ & & & \lambda_\nu & 1 \\ & & & & \lambda_\nu \end{bmatrix} \quad (\nu=1,2,\dots,n)$$

where the empty places (not the dots) are zeros.

P r o o f (see [5], § 88). The elements of U can be made algebraic integers, since the left hand side of (3) is invariant with respect to the multiplication of U by a number.

L e m m a 2. Let $L_0, L_j, M_j \in Z[t_1,\dots,t_r]$ $(j=1,2,\dots,k)$ be homogeneous linear forms and M_j $(j=1,2,\dots,k)$ linearly independent. If the system of congruences

$$(5_1) \qquad \sum_{j=1}^{k} x_j L_j(t_1,\dots,t_r) \equiv L_0(t_1,\dots,t_r) \pmod{m}$$

$$(5_2) \qquad \sum_{j=1}^{k} x_j M_j(t_1,\ldots,t_r) \equiv 0 \pmod m$$

is soluble in x_j for all moduli m and all integer vectors $[t_1,\ldots,t_t]$, then $L_o = 0$.

P r o o f . Let $L_j = \sum_{s=1}^{r} l_{js} t_s$ $(0 \le j \le k)$, $M_j = \sum_{s=1}^{r} m_{js} t_s$ $(1 \le j \le k)$. Taking if necessary $l_{js} = m_{js} = 0$ for $s > k$ we can assume that $r > k$. Since M_j's are linearly independent we can assume also that the matrix

$$M = \left[m_{js}\right]_{j,s \le k}$$

is non-singular. Put

$$M^* = \left[m_{js}\right]_{\substack{j \le k \\ k < s \le r}},$$

$$L = \left[l_{js}\right]_{1 \le j,s \le k}, \quad L^* = \left[l_{js}\right]_{\substack{1 \le j \le k \\ k < s \le r}},$$

$$\ell_o = \left[l_{o1},\ldots,l_{ok}\right], \quad \ell_o^* = \left[l_{ok+1},\ldots,l_{or}\right].$$

Let K_o be the splitting field of the characteristic polynomial of LM^{-1}. In virtue of Lemma 1 there exists a matrix U whose elements are integers of K_o such that

$$(6) \qquad U^{-1}LM^{-1}U = \begin{bmatrix} A_1 & & & & \\ & A_2 & & & \\ & & \cdot & & \\ & & & \cdot & \\ & & & & \cdot \quad A_n \end{bmatrix}$$

where A_ν of degree ρ_ν is given by (3) $(\nu = 1,2,\ldots,n)$.

We proceed to show that $\ell_0 = 0$ and $\ell_0^* = 0$. Let us write

$$(7) \qquad \ell_0 M^{-1} U = [l_1, \dots, l_k].$$

Suppose that $\ell_0 \neq 0$ hence $\ell_0 M^{-1} U \neq 0$ and let the least $\varkappa \leq k$ for which $l_\varkappa \neq 0$ satisfy

$$(8) \qquad \sigma_\nu = \sum_{\mu<\nu} \varrho_\mu < \varkappa \leq \sum_{\mu\leq\nu} \varrho_\mu .$$

Let p be a prime which factorizes in K_0 into distinct prime ideals of degree one which divide neither den M^{-1} nor the numerators of $l_\varkappa$ and of λ_μ and l_k for $k > \varkappa$.

Take the modulus $m = p^{\varrho_\nu}$ and let $t := [t_1, \dots, t_k]^T \in Z^k$ satisfy the congruence

$$(9) \qquad U^{-1} M\, t \equiv \begin{bmatrix} 0 \\ \vdots \\ 0 \\ 1 \\ p \\ \vdots \\ p^{\varrho_\nu - 1} \\ 0 \\ \vdots \\ 0 \end{bmatrix} \begin{matrix} \left.\vphantom{\begin{matrix}0\\ \vdots\\ 0\end{matrix}}\right\} \sigma_\nu \\ \\ \\ \\ \\ \\ \\ \end{matrix} \pmod{\mathfrak{p}^{\varrho_\nu}},$$

where $\mathfrak{p}$ is a prime ideal factor of p in K_0. Since $\mathfrak{p}$ is unramified of degree one and does not divide den M^{-1} the congruence is soluble in rational integers. Take further

$$(10) \qquad t^* := [t_{k+1}, \dots, t_r]^T = 0 .$$

Setting $y = [y_1, \dots, y_k] = [x_1, \dots, x_k]U$ we can rewrite the system (5) in the form

$$y(U^{-1}LM^{-1}U)(U^{-1}Mt) \equiv l_0 M^{-1}U(U^{-1}Mt) \pmod{p^{\varrho_\nu}}$$

$$y(U^{-1}Mt) \equiv 0 \pmod{p^{\varrho_\nu}},$$

hence by (6) - (10)

$$(11_1) \qquad \sum_{j=\sigma_\nu+1}^{\sigma_{\nu+1}-1} y_j \left(\lambda_\nu p^{j-\sigma_\nu-1} + p^{j-\sigma_\nu}\right) + y_{\sigma_{\nu+1}} \lambda_\nu p^{\varrho_\nu-1} \equiv$$

$$\sum_{j=\sigma_\nu+1}^{\sigma_{\nu+1}} l_j p^{j-\sigma_\nu-1} \pmod{\mathfrak{p}^{\varrho_\nu}},$$

$$(11_2) \qquad \sum_{j=\sigma_\nu+1}^{\sigma_{\nu+1}} y_j p^{j-\sigma_\nu-1} \equiv 0 \pmod{\mathfrak{p}^{\varrho_\nu}}.$$

The left hand side of (11_1) is congruent mod $\mathfrak{p}^{\varrho_\nu}$ to the left hand side of (11_2) multiplied by $(\lambda_\nu+p)$. Since $\lambda_\nu^{-1} \not\equiv 0 \pmod{\mathfrak{p}}$ it follows that

$$\sum_{j=\sigma_\nu+1}^{\sigma_{\nu+1}} l_j p^{j-\sigma_\nu-1} \equiv 0 \pmod{\mathfrak{p}^{\varrho_\nu}},$$

hence $l_k \equiv 0 \pmod{\mathfrak{p}}$ contrary to the choice of $\mathfrak{p}$.

Therefore $l_0 = 0$ and it remains to prove that $l_0^* = 0$. Assume without loss of generality that

$$l_{0r} \neq 0.$$

Choose a rational integer $\lambda \neq \lambda_\nu$ $(\nu=1,2,\ldots,n)$ and take

$$(12) \qquad m = 2|l_{0r}| \operatorname{den}(L-\lambda M)^{-1} > 0,$$

$$t^* = [0,\ldots,0,\operatorname{den}(L-\lambda M)^{-1}]^T.$$

With this choice of t^* we can find a $t \in Z^k$ such that

$$(L-\lambda M)t = \lambda M^* t^* - L^* t^*$$

and then the system (5) gives for $x = [x_1, \dots, x_k]$

$$x\lambda(Mt + M^* t^*) \equiv l_{or}\ \mathrm{den}(L-\lambda M)^{-1} (\mathrm{mod}\ m),$$

$$x(Mt + M^* t^*) \equiv 0 (\mathrm{mod}\ m),$$

hence

$$l_{or}\ \mathrm{den}(L-\lambda M)^{-1} \equiv 0(\mathrm{mod}\ m).$$

The obtained contradiction with (12) completes the proof.

L e m m a 3. For every rational square matrix A there exists a non-singular integral matrix U such that (3) holds with A_ν a square matrix of degree ρ_ν (in general not the same as in Lemma 2),

$$A_\nu = \begin{bmatrix} -\alpha_{\nu 1} & 1 & & \\ -\alpha_{\nu 2} & & 1 & \\ \vdots & & & \ddots \\ -\alpha_{\nu \rho_\nu} & & & & 1 \end{bmatrix} \tag{13}$$

where $\alpha_{\nu j} \in Q$ and $x^{\rho_\nu} + \sum_{j=1}^{\rho_\nu} \alpha_{\nu j} x^{\rho_\nu - j}$ is a power of a polynomial irreducible over Q.

P r o o f (see [5], § 88). The form of the matrix A has been changed by applying central symmetry (matrices symmetric to each other with respect to the common centre are similar). U can be made integral via multiplication by a suitable integer.

L e m m a 4. Let $L_0, L_j, M_j \in Z[t_1, \dots, t_r]$ $(j=1,2,\dots,k)$ be homogeneous linear forms, M_j's linearly independent. Let $a_0, a_j, b_j \in Z$ $(j=1,2,\dots,k)$ and w be a fixed positive integer.

If for all moduli $m \equiv 0 (\mathrm{mod}\ w)$ and for all integer vectors $[t_1,\dots,t_r]$ the system of congruences

$$(14_1)\quad \sum_{j=1}^{k} x_j\left(L_j(t_1,\dots,t_r)+a_j \frac{m}{w}\right) \equiv L_0(t_1,\dots,t_r)+a_0 \frac{m}{w} \ (\mathrm{mod}\ m),$$

$$(14_2)\quad \sum_{j=1}^{k} x_j\left(M_j(t_1,\dots,t_r) + b_j \frac{m}{w}\right) \equiv 0 (\mathrm{mod}\ m)$$

is soluble in integers x_j then $L_0 = 0$ and $a_0 \equiv 0 (\mathrm{mod}\ w)$.

P r o o f . When m runs through all positive integers divisible by w, m/w runs through all positive integers, hence applying Lemma 2 we infer that $L_0 = 0$. In order to show $a_0 \equiv 0 \bmod w$ we adopt the meaning of L, L^*, M, M^* from the proof of Lemma 2.

In virtue of Lemma 3 there exists a non-singular integral matrix U such that

$$(15)\quad U^{-1}LM^{-1}U = \begin{bmatrix} A_1 & & & \\ & A_2 & & \\ & & \ddots & \\ & & & A_n \end{bmatrix},$$

where A_ν of degree ϱ_ν is given by (13). We can assume without loss of generality that $\alpha_{\nu\varrho_\nu} = 0$, $\varrho_1 \geqslant \varrho_\nu$ for $\nu \leqslant n_0$ and $\alpha_{\nu\varrho_\nu} \neq 0$ for $\nu > n_0$ (n_0 may be 0). It follows from the condition on $x^{\varrho_\nu} + \sum_{j=i}^{\varrho_\nu} \alpha_{\nu j} x^{\varrho_\nu - j}$ that

$$(16)\quad A_\nu = \begin{bmatrix} 1 & & & \\ & 1 & & \\ & & \ddots & \\ & & & 1 \end{bmatrix} \quad (1 \leqslant \nu \leqslant n_0),$$

where the empty places are zeros as before. Now put

$$(17)\qquad U^{-1}\begin{bmatrix} a_1 \\ \vdots \\ a_k \end{bmatrix} = \begin{bmatrix} \alpha_1 \\ \vdots \\ \alpha_n \end{bmatrix}, \quad U^{-1}\begin{bmatrix} b_1 \\ \vdots \\ b_k \end{bmatrix} = \begin{bmatrix} \beta_1 \\ \vdots \\ \beta_n \end{bmatrix},$$

where for $\nu = 1,2,\dots,n$

$$(18)\qquad \alpha_\nu = \begin{bmatrix} a_{\nu 1} \\ \vdots \\ a_{\nu \varrho_\nu} \end{bmatrix}, \quad \beta_\nu = \begin{bmatrix} b_{\nu 1} \\ \vdots \\ b_{\nu \varrho_\nu} \end{bmatrix}.$$

Take

$$(19)\qquad m_0 = w \text{ den } M^{-1} \text{ den } U^{-1} \underset{n_0<\nu\leq n}{\text{l.c.m.}} \text{ den } A_\nu^{-1}$$

and put

$$(20)\qquad m = m_0^{\varrho_1+1},$$

$$(21)\qquad t = \begin{bmatrix} t_1 \\ \vdots \\ t_k \end{bmatrix} = M^{-1}U \begin{bmatrix} u_1 \\ \vdots \\ u_n \end{bmatrix}, \quad t^* = \begin{bmatrix} t_{k+1} \\ \vdots \\ t_r \end{bmatrix} = 0,$$

where

$$(22)\qquad u_\nu = A^{-1}\alpha_\nu \frac{m_0^{\varrho_1+1}}{w} \quad (n_0 < \nu \leq n)$$

and for $\nu \leq n_0$ u_ν is a vector with ϱ_ν components and the j-th coordinate

$$u_{\nu j} = \frac{1}{w}\sum_{i=j}^{\varrho_\nu} m_0^{\varrho_1-i+j}(a_{\nu i} - m_0 b_{\nu i}) \qquad (1 \leq j \leq \varrho_\nu).$$

Since by (19) $u_\nu \equiv 0 \bmod \operatorname{den} M^{-1}$ $(1 \leqslant \nu \leqslant n)$ the vector f defined by (21) is integral. Moreover by (16), (18) and above we have

$$(23)\qquad A_\nu u_\nu + a_\nu \frac{m_0^{\varrho_\nu+1}}{w} = m_0\left(u_\nu + b_\nu \frac{m_0^{\varrho_1+1}}{w}\right) \quad (1 \leqslant \nu \leqslant n_0).$$

Setting

$$[x_1,\ldots,x_k]U = [x_1,\ldots,x_n],$$

where x_ν is a vector with ϱ_ν components and using (15), (17), (20) and (21) we can rewrite the system (14) in the form

$$\sum_{\nu=1}^{n} x_\nu\left(A_\nu u_\nu + a_\nu \frac{m_0^{\varrho_1+1}}{w}\right) \equiv a_0 \frac{m_0^{\varrho_1+1}}{w} \left(\bmod\ m_0^{\varrho_1+1}\right),$$

$$\sum_{\nu=1}^{n} x_\nu\left(u_\nu + b_\nu \frac{m_0^{\varrho_1+1}}{w}\right) \equiv 0 \left(\bmod\ m_0^{\varrho_1+1}\right).$$

In virtue of (22) this gives

$$(24_1)\qquad \sum_{\nu=1}^{n_0} x_\nu\left(A_\nu u_\nu + a_\nu \frac{m_0^{\varrho_1+1}}{w}\right) \equiv a_0 \frac{m_0^{\varrho_1+1}}{w} \left(\bmod\ m_0^{\varrho_1+1}\right),$$

$$(24_2)\qquad \sum_{\nu=1}^{n_0} x_\nu\left(u_\nu + b_\nu \frac{m_0^{\varrho_1+1}}{w}\right) \equiv$$

$$\equiv \sum_{\nu=n_0+1}^{n} x_\nu \left(A_\nu^{-1} a_\nu - b_\nu\right) \frac{m_0^{\varrho_1+1}}{w} \left(\bmod\ m_0^{\varrho_1+1}\right).$$

In virtue of (23) the left hand side of (24_1) equals the left hand side of (24_2) multiplied by m_0. Hence

$$a_0 \frac{m_0^{\varrho_1+1}}{w} \equiv m_0^{\varrho_1+1} \sum_{\nu=n_0+1}^{n} x_\nu \left(A_\nu^{-1} a_\nu - b_\nu \right) \frac{m_0}{w} \left(\bmod\ m_0^{\varrho_1+1} \right).$$

Since by (19) the vectors $\left(A_\nu^{-1} a_\nu - b_\nu\right) \frac{m_0}{w}$ are integral we get

$$a_0 \frac{m_0^{\varrho_1+1}}{w} \equiv 0 \left(\bmod\ m_0^{\varrho_1+1} \right), \quad a_0 \equiv 0 (\bmod\ w),$$

which completes the proof.

L e m m a 5. For every integral matrix A with all the k rows linearly independent there exist unimodular integral matrices B and C such that

$$(25) \qquad B^{-1} A C = \begin{bmatrix} e_1 & & & \\ & e_2 & & \\ & & \ddots & \\ & & & e_k \end{bmatrix},$$

where the elements outside the principal diagonal are zeros, $e_k \neq 0$ and $e_i | e_{i+1}$ $(1 \leq i < k)$.

P r o o f . Without the condition $e_k \neq 0$ the lemma is proved in [5], §85. The condition $e_k \neq 0$ follows from the linear independence of the rows of A.

L e m m a 6. Let $L_{ij} \in Z[t_1, \ldots, t_r]$ $(1 \leq i \leq h,\ 0 \leq j \leq k)$ be homogeneous linear forms and suppose L_{1j} $(1 \leq j \leq k)$ linearly independent. Let $l_{ij} \in Z$ $(1 \leq i \leq h,\ 0 \leq j \leq k)$. If the system of congruences

$$(26) \qquad \sum_{j=1}^{k} x_j \left(L_{ij}(t_1, \ldots, t_r) + l_{ij} \frac{m}{w}\right) \equiv$$

$$\equiv L_{i0}(t_1, \ldots, t_r) + l_{i0} \frac{m}{w} (\bmod\ m) \qquad (1 \leq i \leq h)$$

is soluble for all moduli $m \equiv 0 (\bmod\ w)$ and for all integer vectors $[t_1, \ldots, t_r]$ then there exist integers ξ_j $(1 \leq j \leq k)$ such that

$$(27)\qquad \sum_{j=1}^{k} \xi_j L_{ij} = L_{i0} \quad (1 \leqslant i \leqslant h)$$

and

$$(28)\qquad \sum_{j=1}^{k} \xi_j l_{ij} \equiv l_{i0} \pmod{w}.$$

P r o o f. Let

$$(29)\qquad L_{1j} = \sum_{s=1}^{r} a_{js} t_s \quad (0 \leqslant j \leqslant k), \quad A = [a_{js}]_{\substack{1 \leqslant j \leqslant k;\\ 1 \leqslant s \leqslant r.}}$$

In virtue of Lemma 5 there exist unimodular integral matrices B, C such that (25) holds. Let

$$(30)\qquad B^{-1}\begin{bmatrix} l_{11} \\ \cdot \\ \cdot \\ \cdot \\ l_{1k} \end{bmatrix} = \begin{bmatrix} b_1 \\ \cdot \\ \cdot \\ \cdot \\ b_k \end{bmatrix}, \quad C^{-1}\begin{bmatrix} t_1 \\ \cdot \\ \cdot \\ \cdot \\ t_r \end{bmatrix} = \begin{bmatrix} t'_1 \\ \cdot \\ \cdot \\ \cdot \\ t'_r \end{bmatrix},$$

$$[a_{01},\dots,a_{0r}]\, C = [c_1,\dots,c_r].$$

Setting $[y_1,\dots,y_k] = [x_1,\dots,x_k]\, B$ we get from (25), (26) and (30)

$$(31)\qquad \sum_{j=1}^{k} y_j\left(e_j t'_j + b_j \frac{m}{w}\right) \equiv \sum_{s=1}^{r} c_s t'_s + l_{10}\frac{m}{w} \pmod{m}.$$

Assuming that c_s are not all zero for $s > k$ and that σ is the least index $> k$ such that $c_\sigma \neq 0$ we take $m = 2w\, e_k |c_\sigma|$,

$$t'_s = \begin{cases} -\dfrac{b_j}{e_j}\dfrac{m}{w} & \text{for} \quad s \leq k, \\ 1 & \text{for} \quad s = \sigma, \\ 0 & \text{for} \quad s > k,\ s \neq \sigma \end{cases}$$

and get from (31)

$$c_\sigma \equiv 0 \bmod 2|c_\sigma|,$$

a contradiction. Therefore $c_s = 0$ for all $s > k$ and taking $m = 2we_k$, $t'_j = -\dfrac{b_j}{e_j}\dfrac{m}{w}$ for $j \leq k$ we get from (31)

$$l_{10}\frac{m}{w} - \sum_{j=1}^{k} \frac{b_j c_j}{e_j}\frac{m}{w} \equiv 0 (\bmod m),$$

hence

$$(32) \qquad l_{10} \equiv \sum_{j=1}^{k} \frac{b_j c_j}{e_j} (\bmod w^+).$$

Finally taking $m = we_k$ and for a fixed $j \leq k$

$$t'_s = \begin{cases} -\dfrac{m}{w}\dfrac{b_s}{e_s} + \dfrac{e_k}{e_j} & \text{if} \quad s = j, \\ -\dfrac{m}{w}\dfrac{b_s}{e_s} & \text{if} \quad s \neq j,\ s \leq k, \\ 0 & \text{if} \quad s > k, \end{cases}$$

we get from (31) and (32)

$$y_j e_k \equiv c_j e_k / e_j \ (\bmod e_k),$$

$$c_j / e_j \in Z.$$

Integers ξ_j defined by

$$[\xi_1,\ldots,\xi_k] = [c_1/e_1,\ldots,c_k/e_k]B^{-1}$$

satisfy (27) and (28) for i = 1 in virtue of (25), (29), (30) and (32). Take now $i \geqslant 1$ and consider the system of two congruences:

$$\sum_{j=1}^{k} x_j(L_{ij}(t_1,\ldots,t_r)+l_{ij}\frac{m}{w}) \equiv L_{io}(t_1,\ldots,t_r)+l_{iow}\frac{m}{w} -$$

$$-\sum_{j=1}^{k} \xi_j(L_{ij}(t_1,\ldots,t_r)+l_{ij}\frac{m}{w}) \pmod m$$

and

$$\sum_{j=1}^{k} x_j(L_{1j}(t_1,\ldots,t_r)+l_{1j}\frac{m}{w}) \equiv 0 \pmod m.$$

If $[x_1^o,\ldots,x_m^o]$ is a solution of the system (26), the above system has the solution $[x_1^o-\xi_1,\ldots,x_m^o-\xi_m]$, hence it is soluble for all moduli m and all integer vectors $[t_1,\ldots,t_r]$. Since L_{1j} are linearly independent we have in virtue of Lemma 4

$$L_{io} - \sum_{j=1}^{k}\xi_j L_{ij} = 0 \quad\text{and}\quad l_{io} - \sum_{j=1}^{k}\xi_j l_{ij} \equiv 0 \pmod w,$$

thus (27) and (28) hold for all $i \leqslant h$.

Lemma 7. In any algebraic number field K there exists a multiplicative basis, i.e. such a sequence $\pi_1,\pi_2,\ldots$ that any non-zero element of K is represented uniquely as $\zeta\prod_{s=1}^{r}\pi_s^{x_s}$, where x_s are rational integers and ζ is a root of unity.

Proof: see [3].

Lemma 8. Let K be an algebraic number field, w the number of roots of unity contained in K, $w \equiv 0 \bmod 4$, n a positive integer,

$$\sigma = \left(w, n, \operatorname*{l.c.m.}_{q \mid n, q \text{ prime}} [K(\zeta_q):K]\right).$$

If

(33) , $$n \equiv 0 \bmod (w,n) \operatorname*{l.c.m.}_{q \mid n, q \text{ prime}} [K(\zeta_q):K]$$

and $\alpha_1, \ldots, \alpha_r \in K$ have the property that

(34) $$\zeta_w^{x_0} \prod_{s=1}^{r} \alpha_s^{x_s} = \gamma^{n/\sigma}, \quad \gamma \in K \text{ implies } x_1 \equiv x_2 \equiv \ldots \equiv x_r \equiv 0 (\operatorname{mod} n/\sigma)$$

then for any integers $c_1, \ldots, c_r \equiv 0 \bmod \sigma$ and any c_0 there exists a set of prime ideals $\mathfrak{q}$ of $K(\zeta_n)$ of a positive Dirichlet density such that

(35) $$\left(\frac{\zeta_w}{\mathfrak{q}}\right)_n = \zeta_{(w,n)}^{c_0}, \quad \left(\frac{\alpha_s}{\mathfrak{q}}\right)_n = \zeta_n^{c_s} \quad (1 \leq s \leq r).$$

P r o o f . This is a special case ($\zeta_4 \in K$) of Theorem 4 of [2]. In this theorem only the existence of infinitely many prime ideals $\mathfrak{q}$ with property (35) is asserted, but the existence of a set of a positive Dirichlet density is immediately clear from the proof based on the Čebotarev density theorem.

P r o o f of Theorem 1. Without loss of generality we may assume that $\zeta_4 \in K$ and that α_{1j} $(j = 1,2,\ldots,k)$ are multiplicatively independent. Let us set

(36) $$\alpha_{ij} = \zeta_w^{a_{ij0}} \prod_{s=1}^{r} \pi_s^{a_{ijs}}, \quad \beta_i = \zeta_w^{b_{i0}} \prod_{s=1}^{r} \pi_s^{b_{is}},$$

where w is the number of roots of unity contained in K and π_s are elements of the multiplicative basis described in Lemma 7. Take an arbitrary modules $m \equiv 0 (\operatorname{mod} w)$ and set in Lemma 8,

$$n = m\, m_1, \text{ where } m_1 = \operatorname*{l.c.m.}_{p \leq P,\ p \text{ prime}} (p-1)$$

and P is the greatest prime factor of m. Since every prime factor q of n satisfies $q \leq P$ the number n satisfies (33). The condition (34) is clearly satisfied by $\alpha_s = \pi_s$ $(1 \leq s \leq r)$. Hence for any integers $c_1, \ldots, c_r \equiv 0 \bmod w$ there exists a set S of prime ideals $\mathfrak{q}$ of $K(\zeta_n)$ of positive Dirichlet density such that

$$(37) \qquad \left(\frac{\zeta_w}{\mathfrak{q}}\right)_n = \zeta_w, \quad \left(\frac{\pi_s}{\mathfrak{q}}\right)_n = \zeta_n^{c_s} \quad (1 \leq s \leq r).$$

The ideals $\mathfrak{p}$ of K divisible by at least one $\mathfrak{q} \in S$ form a set of positive Dirichlet density, hence by the assumption there exist integers x_j satisfying

$$\prod_{j=1}^{k} \alpha_{ij}^{x_j} \equiv \beta_i \pmod{\mathfrak{q}} \quad (i=1,2,\ldots,h)$$

for at least one $\mathfrak{q} \in S$. It follows from (36) and (37) that

$$\sum_{j=1}^{k} x_j \left(\sum_{s=1}^{r} a_{ijs} c_s + a_{ij0} \frac{n}{w} \right) \equiv$$

$$\equiv \sum_{s=1}^{r} b_{is} c_s + b_{i0} \frac{n}{w} \pmod{n} \quad (1 \leq i \leq h).$$

Now take $c_s = w m_1 t_s$ $(1 \leq s \leq r)$,

$$(38) \qquad \begin{cases} L_{ij} = w \sum_{s=1}^{r} a_{ijs} t_s & (1 \leq i \leq h,\ 1 \leq j \leq k), \\ L_{i0} = w \sum_{s=1}^{r} b_{is} t_s & (1 \leq i \leq h). \end{cases}$$

It follows that for all moduli $m \equiv 0 \bmod w$ and all integer vectors $[t_1, \ldots, t_r]$ the system of congruences

$$\sum_{j=1}^{k} x_j\, L_{ij}(t_1,\dots,t_r)+a_{ijo}\frac{m}{w} \equiv L_{io}(t_1,\dots,t_r)+b_{io}\frac{m}{w} \pmod m$$

is soluble in integers x_j. Since the numbers α_{1j} are multiplicatively independent the linear forms L_{1j} are linearly independent $(1\leq j\leq k)$. Hence by Lemma 6 there exist integers $\xi_1,\dots,\xi_k$ such that

$$\sum_{j=1}^{k}\xi_j L_{ij} = L_{io} \quad\text{and}\quad \sum_{j=1}^{k}\xi_j a_{ijo} \equiv b_{io} \pmod w \quad (1\leq i\leq h).$$

It follows from (36) and (38) that $\xi_1,\dots,\xi_k$ satisfy the system (2).

P r o o f of Corollary. In view of Theorem 1 it remains to consider the case when for each $i\leq h$ the number α_i is a root of unity. But then either there exists a positive integer $x\leq w$ such that

$$\alpha_i^{x} = \beta_i \quad (1\leq i\leq h)$$

or the system of congruences

$$\alpha_i^{x}\equiv \beta_i \pmod{\mathfrak{p}} \quad (1\leq i\leq h)$$

is soluble only for prime ideals $\mathfrak{p}$ dividing

$$\prod_{x=1}^{w} \underset{1\leq i\leq h}{\text{g.c.d.}} (\alpha_i^{x} - \beta_i).$$

P r o o f of Theorem 2. Since here $K = Q$ we write p instead of $\mathfrak{p}$ and denote by p_j the jth prime. We take

$$\alpha_{11} = -1,\ \alpha_{1j} = p_{j-1} \quad (2\leq j\leq k),\ \beta_1 = -1,$$

$$\alpha_{21} = 2,\ \alpha_{2j} = 1 \quad (2\leq j\leq k),\ \beta_2 = 1.$$

For $p = 2$ (1) has the solution $x_j = 0$ $(1 \leq j \leq k)$. For $p > 2$ we consider the index of 2, ind 2 with respect to a fixed primitive root of p. If $\frac{p-1}{(\mathrm{ind}\ 2, p-1)}$ is odd, (1) has a solution determined by

$$x_1 \equiv \begin{cases} 1 \pmod 2 \\ 0 \bmod \frac{p-1}{(\mathrm{ind}\ 2, p-1)} \end{cases}, \quad x_j = 0 \quad (2 \leq j \leq k).$$

If $\frac{p-1}{(\mathrm{ind}\ 2, p-1)}$ is even, (1) has a solution determined by

$$x_1 = 0, \quad x_2 \,\mathrm{ind}\, 2 \equiv \frac{p-1}{2} \pmod{p-1}, \quad x_j = 0 \ (3 \leq j \leq k).$$

On the other hand (2) is clearly unsoluble.

REFERENCES

[1] A. Schinzel: On power residues and exponential congruences, Acta Arith. 27 (1975) 397-420.

[2] A. Schinzel: Abelian binomials, power residues and exponential congruences, Acta Arith. 32 (1977) 245-274; Addendum ibid. 36 (1980) 101-104.

[3] Th. Skolem: On the existence of a multiplicative basis for an arbitrary algebraic field, Norske Vid. Selsk. Forh. (Trondheim) 20 (1947) no 2.

[4] L. Somer: Linear recurrences having almost all primes as maximal divisors (to appear).

[5] B.L. van der Waerden: Algebra II Teil. Berlin, Heidelberg, New York 1969.

INSTITUTE OF MATHEMATICS, POLISH ACADEMY OF SCIENCES,
00-950 WARSZAWA
Received December 17, 1984.