Collect. Math. **42**, 2 (1991), 125–136

Regular solutions of a congruence system

C. Calderón and M.J. de Velasco *

Departamento de Matemáticas, Facultad de Ciencias

Universidad del País Vasco, E-48080 Bilbao, Spain

Received March 2, 1990. Revised July 4, 1991

Abstract

In this paper we give bounds and recurrence formulae for the number of solutions of the system $\sum_{t=1}^{k} x_t^\nu \equiv \lambda_\nu (\mathrm{mod}\, q_\nu)$, $1 \leq \nu \leq n$, $\lambda_\nu, q_\nu \epsilon \mathbb{N}$, which satisfy the conditions $\gamma_i x_i \equiv \beta_i (\mathrm{mod}\, q), \mathrm{g.c.d.}(\gamma_i, q) = d_i | \beta_i$ and $q = \mathrm{l.c.m.}(q_1, \ldots, q_n)$, where γ_i, β_i and q are given integers.

1. Introduction and notations

Let $k \geq n \geq 2$, λ_ν, q_ν, $1 \leq \nu \leq n$ be natural numbers and $q = \mathrm{l.c.m.}(q_1, \ldots, q_n)$. $x_1, \ldots, x_k$ will denote unknows taken over a complete set of residues modulo q. The letter p will always stand for a prime number. Suppose that any prime number p dividing q is greater than n. Then a k-tuple $(x_1, \ldots, x_k)$ is called regular mod q if for any prime divisor p of q, there are at least n components which belong to different classes of residues mod p. A regular solution is denoted by $(x_1, \ldots, x_k)_n (\mathrm{mod}\, q)$. We shall study the number of regular solutions of the system

$$(1.1) \qquad x_1^\nu + \ldots + x_k^\nu \equiv \lambda_\nu (\mathrm{mod}\, q_\nu), \quad 1 \leq \nu \leq n; \quad x_1, \ldots, x_k \epsilon \mathbb{Z}/q\mathbb{Z}$$

where $x_{j+1}, \ldots, x_k$ satisfy the following conditions : $\gamma_i x_i \equiv \beta_i (\mathrm{mod}\, q)$, $\gamma_i, \beta_i \epsilon \mathbb{Z}$. From the symmetry of the system, we can suppose, without loss of generality that

* Supported in part by the University of the Basque Country

$1 < d_i = \text{g.c.d.}(\gamma_i, q)|\beta_i$, $i = j+1, \ldots, m$ and $d_i = 1$ for $i = m+1, \ldots, k$. We denote $S(q)$ the following set

$$S(q) = \Big\{ (x_1, \ldots, x_k)_n (\operatorname{mod} q) \mid 1 \le x_1, \ldots, x_j \le q; \gamma_i x_i \equiv \beta_i (\operatorname{mod} q)$$

$$1 < d_i = \text{g.c.d.}(\gamma_i, q)|\beta_i \ \ \forall i = j+1, \ldots, m; \text{g.c.d.}(\gamma_i, q) = 1, \forall i = m+1, \ldots, k \Big\}.$$

If $d_i = 1, \forall i = j+1, \ldots, k$ or $1 < d_i|\beta_i \ \ \forall i = j+1, \ldots, k$ this set is denoted by $S_1(q)$ or $S_2(q)$ respectively. For each n-tuple $(\lambda_1, \ldots, \lambda_n)$ of integers λ_ν, let $J_k(\lambda_1, \ldots, \lambda_n; q)$ be the number of regular solutions of the system

$$x_1^\nu + \ldots + x_k^\nu \equiv \lambda_\nu (\operatorname{mod} q); \quad 1 \le \nu \le n \qquad (x_1, \ldots, x_k) \epsilon S(q) \tag{1.2}$$

First we shall study this system when $q = p^\alpha$, $\alpha \ge 1$ and $p > n$. The symbol $\sum_{(x_1, \ldots, x_k)_n}^q$ means that the sum is restricted to the regular k-tuples $(x_1, \ldots, x_k)_n (\operatorname{mod} q) \epsilon S(q)$. We prove the following theorems

Theorem 1

1) If the system of congruences

$$x_1^\nu + \ldots + x_k^\nu \equiv \lambda_\nu (mod\, p); 1 \le \nu \le n, \quad (x_1, \ldots, x_k) \epsilon S_1(p),$$

is solvable, then the number of solutions verifies the following bound

$$J_k(\lambda_1, \ldots, \lambda_n; p) \le \begin{cases} j!, & \text{if } j \le n; \\ n! p^{j-n}, & \text{if } n < j \le k \end{cases} \tag{1.3}$$

2) If the above system has solutions in the set $S_2(p)$, then we have $J_k(\lambda_1, \ldots, \lambda_n; p) \le n! p^{k-n}$

In particular,

$$J_n(\lambda_1, \ldots, \lambda_n; p) \le \begin{cases} j!, & \text{if} (x_1, \ldots, x_n) \epsilon S_1(p); \\ n!, & \text{if } (x_1, \ldots, x_n) \epsilon S_2(p) \end{cases}$$

Theorem 2

Suppose that the number of unknowns $x_{j+1}, \ldots, x_k$ that belong to differents classes of residues mod p is s. If the system of congruences

$$x_1^\nu + \ldots + x_k^\nu \equiv \lambda_\nu (mod\, p^\alpha); 1 \le \nu \le n, \quad (x_1, \ldots, x_k) \epsilon S_1(p^\alpha) \quad \alpha \ge 2, \tag{1.4}$$

is solvable, then

(1.5)

$$J_k(\lambda_1, \ldots, \lambda_n; p^\alpha) \le p^{(\alpha-1)j - (\alpha-2)\frac{j}{n} - s}(p^s - 1)(n-1)^j + p^{j-n} J_k(\lambda_1, \ldots, \lambda_n; p^{\alpha-1})$$

By repeating the argument used in Theorem 2 we obtain the following corollary.

Corollary 1

The number of solutions of the system (1.4) verifies the following bound

$$J_k(\lambda_1,\ldots,\lambda_n;p^\alpha) \le (n-1)^j(p^s-1)p^{(\alpha-2)(1-1/n)j+j-s}\sum_{\delta=0}^{\alpha-2}p^{\delta(j/n-n)} + p^{(\alpha-1)(j-n)}J_k(\lambda_1,\ldots,\lambda_n;p) \tag{1.6}$$

where $J_k(\lambda_1,\ldots,\lambda_n;p)$ *is given in Theorem 1.*

Corollary 2

Suppose that $(x_1,\ldots,x_n)\epsilon S_2(p^\alpha)$ $\quad j\le n=k$*, then*

$$J_n(\lambda_1,\ldots,\lambda_n;p^\alpha)\le p^{(\alpha-1)(j-n)}J_n(\lambda_1,\ldots,\lambda_n;p)$$

where $J_n(\lambda_1,\ldots,\lambda_n;p)$ *is given in Theorem 1.*

Theorem 3

Suppose that system of congruences

$$x_1^\nu+\ldots+x_k^\nu\equiv\lambda_\nu(\mathrm{mod}\,p^\alpha);1\le\nu\le n,\quad (x_1,\ldots,x_k)\epsilon S_2(p^\alpha),\quad \alpha\ge 2$$

is solvable, and let $R=\min\{r_i|p^{r_i}=\text{g.c.d.}(\gamma_i,p^\alpha), i=j+1,\ldots,k\}$*. Then*

$$J_k(\lambda_1,\ldots,\lambda_n;p^\alpha)=p^{R(k-n)}J_k(\lambda_1,\ldots,\lambda_n;p^{\alpha-R}) \tag{1.7}$$

where $J_k(\lambda_1,\ldots,\lambda_n;p^{\alpha-R})$ *is the number of solutions of the system (1.2) mod* $q=p^\alpha$.

Theorem 4

For any $j+1\le i\le n$, $\hat{x}_i$ *denote the unique solution of the linear congruence*

$$(\alpha_i/d_i)x_i\equiv(\beta_i/d_i)(\mathrm{mod}\,p^\alpha/d_i), 1<d_i=p^{r_i}<p^\alpha \tag{1.8}$$

and let $\hat{\hat{x}}_i$ *be the solution of the same congruence when* $d_i=1$, $i=m+1,\ldots,k$*. We suppose that* ℓ,s *is the number of* $\hat{x}_i,\hat{\hat{x}}_i$ *respectively which are noncongruent mod* p*. If the system of congruences (1.2) with* $q=p^\alpha$ *is solvable, then*

$$J_k(\lambda_1,\ldots,\lambda_n;p^\alpha)=p^{m-n}J_k(\lambda_1,\ldots,\lambda_n;p^{\alpha-1});\qquad \text{when}\quad \ell\ge n \tag{1.9}$$

$$J_k(\lambda_1,\ldots,\lambda_n;p^\alpha)\le(n-1)^jp^{m-n+L_1-\ell+j(\alpha-2)(1-1/n)}(p^{n-L_1}-1)\times\prod_{\nu=j+1}^{m}p^{(r_\nu-1)(1-1/n)}+p^{m-n}J_k(\lambda_1,\ldots,\lambda_n;p^{\alpha-1});\quad \text{when}\quad \ell<n \tag{1.10}$$

being $L_1=\max\{\ell,n-L\}$, $L\le\ell+s$ *and* L *is the number of* $\hat{x}_{j+1},\ldots,\hat{\hat{x}}_k$ *which are noncongruent mod* p.

Theorem 5

Let $q = p_1^{\delta_1} \dots p_v^{\delta_v}$. *Then the following formula for the number of solutions of the system of congruences (1.2) holds*

$$J_k(\lambda_1, \dots, \lambda_n; q) = \prod_{t=1}^{v} J_k(\lambda_1, \dots, \lambda_n; p_t^{\delta_t}) \tag{1.11}$$

If $J_k(\lambda_1, \dots, \lambda_n; p_t^{\delta_t})$ *is the number of solutions* $(x_1, \dots, x_k) \epsilon S_2(p_t^{\delta_t})$ *of the system, then*

$$J_k(\lambda_1, \dots, \lambda_n; q) = \prod_{t=1}^{v} p_t^{R_t(k-n)} J_k(\lambda_1, \dots, \lambda_n; p_t^{\delta_t - R_t}) \tag{1.12}$$

If $d_i = \text{g.c.d.}(\gamma_i, p_t^{\delta_t}) = 1, \forall i = j+1, \dots, n, \quad \forall t = 1, \dots, v$, then from (1.11) and Corollary 2 we have

$$J_n(\lambda_1, \dots, \lambda_n; q) \leq \prod_{t=1}^{v} p_t^{(\delta_t - 1)(j-n)} J_n(\lambda_1, \dots, \lambda_n; p), \quad j \leq n = k$$

For any arbitrary modulus q_ν and any $k \geq n$ we obtain formulae for the number of solutions of the system (1.1) by means of the number solutions of the incomplete system

$$\left.\begin{array}{c} x_1^{n_1} + \dots + x_k^{n_1} \equiv \mu_{n_1} \\ \dots\dots\dots\dots\dots \\ x_1^{n_t} + \dots + x_k^{n_t} \equiv \mu_{n_t} \end{array}\right\} (\text{mod}\, p^\delta) \tag{1.13}$$

where $p|q$, and $1 \leq n_1 < \dots < n_t \leq n$.

Theorem 6

Let J_k *be the number of regular solutions of the system*

$$x_1^\nu + \dots + x_k^\nu \equiv \lambda_\nu (\text{mod}\, q_\nu); \quad 1 \leq \nu \leq n, \quad (x_1, \dots, x_k) \epsilon S(q)$$

where $q = \text{l.c.m.}(q_1, \dots, q_n) = p_1^{\delta_1} \dots p_v^{\delta_v}$. *Let* $1 \leq n_1 < \dots < n_{t_\ell} \leq n$ *by natural numbers such that* $q_{n_1}, \dots, q_{n_{t_\ell}} \subset \{q_1, q_2, \dots, q_n\}$.

1) If $p_\ell^{\delta_\ell} | q_{n_i} \quad \forall i = 1, \dots t_\ell$ *and* $\text{g.c.d.}(p_\ell^{\delta_\ell}, q_{m_i}) = 1, \forall m_i \epsilon \{1, 2, \dots, n\}, m_i \neq n_i$, *then,*

$$J_k = \frac{1}{q_1 \cdots q_n} \prod_{\ell=1}^{v} p_\ell^{\delta_\ell t_\ell} J_k(\lambda_{n_1}, \dots, \lambda_{n_{t_\ell}}; p_\ell^{\delta_\ell}) \tag{1.14}$$

2) If $p_\ell | q_{n_i}$ $\forall i = 1, \ldots t_\ell$ *and* g.c.d.$(p_\ell, q_{m_i}) = 1, \forall m_i \epsilon \{1, 2, \ldots, n\}, m_i \neq n_i$, *then*

$$(1.15) \qquad J_k = \frac{1}{q_1 \cdots q_n} \prod_{\ell=1}^{v} p_\ell^{\delta_\ell(t_\ell - s_\ell)} \sum_{z_{\ell 1}, \ldots z_{\ell s_\ell}=1}^{p_\ell^{\delta_\ell}} J_k(\mu_{n_1}, \ldots, \mu_{n_{t_\ell}}; p_\ell^{\delta_\ell})$$

where $s_\ell = \#\{q_{n_i}, i = 1, \ldots t_\ell; \ \ p_\ell^{\delta_\ell} | q_{n_i}\}$, $0 \leq s_\ell \leq t_\ell - 1$ *and* $\mu_{n_i} = \lambda_{n_i} + q_{n_i} z_{n_i, \ell}$, *if* $p_\ell^{\delta_\ell} \not| q_{n_i}$; $\mu_{n_i} = \lambda_{n_i}$, if $p_\ell^{\delta_\ell} | q_{n_i}$. *Moreover* $J_k(\mu_{n_1}, \ldots, \mu_{n_{t_\ell}}, p_\ell^{\delta_\ell})$ *is the number of regular solutions of the system (1.13).*

2. Previous lemmas

Following the notations of Korobov [1], let

$$(2.1) \qquad \delta_q(m) = \frac{1}{q} \sum_{x=1}^{q} e\left(\frac{mx}{q}\right) = \begin{cases} 1, & \text{if } m \equiv 0 (\operatorname{mod} q) \\ 0, & \text{otherwise.} \end{cases} \qquad e(t) = e^{2\pi i t}$$

then

$$J_k(\lambda_1, \ldots, \lambda_n; q) = \sum_{(x_1, \ldots, x_k)_n}^{q} \prod_{\nu=1}^{n} \delta_q(x_1^\nu + \ldots + x_k^\nu - \lambda_\nu)$$

hence by (2.1)

(2.2)

$$J_k(\lambda_1, \ldots, \lambda_n; q) = \frac{1}{q^n} \sum_{\substack{(x_1, \ldots, x_k)_n \\ a_1, \ldots, a_n = 1}}^{q} e\left(\frac{f(x_1) + \ldots + f(x_k) - (a_1 \lambda_1 + \ldots + a_n \lambda_n)}{q}\right)$$

where $f(x)$ is the polynomial of integer coefficients, $f(x) = a_1 x + \ldots + a_n x^n$. We denote

$$A_\alpha^r[f(x)] = \sum_{y=1}^{p^r} e\left(\frac{f(x + p^{\alpha - r} y)}{p^\alpha}\right)$$

Lemma 1

Let $R = \min\{r_\nu | \nu = N+1, \ldots, M\}$ $\quad M - N \geq n$ *and let* $a_\nu = p^R b_\nu, \nu = 1, \ldots, n$ *such that* $f(x) = p^R f_R(x_\nu)$. *Then the following formula holds for the values* $x_{N+1}, \ldots, x_M$ *of the systems* $(x_{N+1}, \ldots, x_M)_n (\operatorname{mod} p)$

$$(2.3) \qquad \prod_{\nu=N+1}^{M} A_\alpha^{r_\nu}[f(x_\nu)] = \begin{cases} p^{R(M-N)} \prod_{\nu=N+1}^{M} A_{\alpha-R}^{r_\nu - R}[f_R(x_\nu)], & \text{if } p^R | d; \\ 0, & \text{if } p^R \top d, \end{cases}$$

where $d = \text{g.c.d.}(a_1, \ldots, a_n)$ *and*

$$(2.4) \qquad A^r_\alpha[f(x)] = p\delta_p[f'(x)] \sum_{y=1}^{p^{r-1}} e\left(\frac{f(x+p^{\alpha-r}y)}{p^\alpha}\right); 1 \le r < \alpha$$

Proof. In $A^r_\alpha[f(x)]$ each y modulo p^r, can be written uniquely in the form $zp^{r-1}+y$, $1 \le y \le p^{r-1}$, $1 \le z \le p$. Hence, (2.4) follows from Taylor's Theorem. Moreover since at least n values among $x_{N+1}, \ldots, x_M$ are different mod p we have

$$(2.5) \qquad \prod_{\nu=N+1}^{M} \delta_p[f'(x_\nu)] = \begin{cases} 1, & \text{if } p|d; \\ 0, & \text{otherwise} \end{cases}$$

and if $f(x) = pf_1(x)$ we deduce

$$\prod_{\nu=N+1}^{M} A^{r_\nu}_\alpha[f(x_\nu)] = \begin{cases} p^{(M-N)} \prod_{\nu=N+1}^{M} A^{r_\nu-1}_{\alpha-1}[f_1(x_\nu)], & \text{if } p|d; \\ 0, & \text{if } p\top d, \end{cases}$$

Repeating this argument, we obtain (2.3). If $r = \alpha - 1$, then $A^{\alpha-1}_\alpha[f(x)] = A_\alpha[f(x)]$ and for $(x_1, \ldots, x_N)_n(\text{mod}\, p)$ we have (see Lemma 2 [1])

$$(2.6) \qquad \prod_{\nu=1}^{N} A_\alpha[f(x_\nu)] = \begin{cases} p^{(\alpha-1)N} \prod_{\nu=1}^{N} e\left(\frac{f(x_\nu)}{p^\alpha}\right), & \text{if } p^{\alpha-1}|d; \\ 0, & \text{if } p^{\alpha-1}\top d. \ \square \end{cases}$$

Lemma 2

Let $\alpha \ge 2$, $k \ge n \ge 2$. *Then if the system of congruences*

$$(2.7) \qquad x_1^\nu + \ldots + x_k^\nu \equiv \lambda_\nu (\text{mod}\, p^\alpha); 1 \le \nu \le n, \quad (x_1, \ldots, x_k)\epsilon S(p^\alpha),$$

is soluble, the number of regular solutions verifies the following formula
(2.8)

$$J_k(\lambda_1, \ldots, \lambda_n; p^\alpha) = p^{-\alpha n} \sum_{a_1,\ldots,a_n=1}^{p^\alpha} e\left(-\frac{a_1\lambda_1 + \ldots + a_n\lambda_n}{p^\alpha}\right)$$
$$\times \sum_{x_1,\ldots,x_j=1}^{p} \prod_{\nu=1}^{j} A_\alpha[f(x_\nu)] \prod_{\nu=j+1}^{m} A^{r_\nu}_\alpha[f(\hat{x}_\nu)] \prod_{\nu=m+1}^{k} e\left(\frac{f(\hat{x}_\nu)}{p^\alpha}\right)$$

where $A_\alpha[f(x_\nu)]$, $A^r_\alpha[f(x_\nu)]$ *are given in Lemma 1.*

Proof. Let $(x_1,\dots,x_k)\epsilon S(p^\alpha)$, then $x_1,\dots,x_j$ are taken over a complete set of residues modulo p^α and the solutions of the congruences

$$\gamma_i x_i \equiv \beta_i (\mathrm{mod}\, p^\alpha);\ \text{g.c.d.}(\gamma_i,p^\alpha)=p^{r_i},\ r_i<\alpha,\ \forall i=j+1,\dots,m$$

are $\hat{x}_i+p^{\alpha-r_i},\dots,\hat{x}_i+p^{r_i}p^{\alpha-r_i}$. Moreover each $x_1,\dots,x_j(\mathrm{mod}\, p^\alpha)$, can be written uniquely in the from py_i+x_i, with $1\le x_i\le p$, $1\le y_i\le p^{\alpha-1}$. Hence from (2.2) with $q=p^\alpha$ we have (2.8). □

3. Proof of theorems

Proof of Theorem 1. 1) By the symmetry of the system we can suppose that $x_1,\dots,x_n$ are different mod p and we write the system in the form

$$x_1^\nu+\dots+x_n^\nu\equiv\lambda_\nu-(x_{n+1}^\nu+\dots+x_k^\nu)(\mathrm{mod}\, p),\quad \nu=1,\dots,n\quad ,(x_1,\dots,x_k)\epsilon S_1(p)$$

For $j\le n$, the terms of the right side take the unique value $\delta_1,\dots,\delta_n$. Thus, we have a system of congruences of Linnik type (see [2,p-44] or [3,p-83]) and therefore

$$J_k(\lambda_1,\dots,\lambda_n;p)=J_n(\delta_1,\dots,\delta_n;p)\le j!\quad\text{if}\quad j\le n$$

For $j>n$, obviously, $J_k(\lambda_1,\dots,\lambda_n;p)=p^{j-n}J_n(\delta_1,\dots,\delta_n;p)\le n!p^{j-n}$. and so, (1.3) follows. If k=n, we have $J_k(\lambda_1,\dots,\lambda_n;p)=j!$ for $j\le n$.
2) This case is deduced in a similar manner to above when $n<j=k$. If g.c.d.$(\gamma_i,p)=1$, $\forall i=1,\dots,k$ being the system solvable then $J_k(\lambda_1,\dots,\lambda_n;p)=1$. □

Proof of Theorem 2. Since $q=p^\alpha$, by (2.2), we have

$$J_k(\lambda_1,\dots,\lambda_n;p^\alpha)=p^{j-\alpha n}\sum_{a_1,\dots,a_n=1}^{p^\alpha} e\left(-\frac{a_1\lambda_1+\dots+a_n\lambda_n}{p^\alpha}\right)$$
$$\times\sum_{(x_1,\dots,x_j)_{(n-s)}}^{p}\prod_{\nu=1}^{j}\delta_p[f'(x_\nu)]\sum_{y_\nu=1}^{p^{\alpha-2}} e\left(\frac{f(x_\nu+py_\nu)}{p^\alpha}\right)\prod_{\nu=j+1}^{k} e\left(\frac{f(\hat{x}_\nu)}{p^\alpha}\right)$$

For the sake of brevity we shall write, $J_k(\lambda_1,\dots,\lambda_n;p^\alpha)=p^{j-\alpha n}\{\sum_1+\sum_2\}$ where $\sum_1$ is the sum over the n-tuples $(a_1,\dots,a_n)$ such that g.c.d.$(a_i,p)=1$ for some $i=1,\dots,n$, and $\sum_2$ is the sum over the n-tuples $(a_1,\dots,a_n)$ such that $p|a_i$ for each $i = 1, \ldots, n$. As $n - s \leq j$, it follows that $f(x)$ is a polynomial of degree at least (n-s+1). Hence,

$$|\sum_1| \leq (n-1)^j p^{\alpha(n-s)}(p^{\alpha s} - p^{(\alpha-1)s})p^{(\alpha-2)(1-1/n)j} \tag{1}$$

and

$$\sum_2 = p^{(\alpha-1)n} J_k(\lambda_1, \ldots, \lambda_n; p^{\alpha-1}) \tag{2}$$

From (1), (2) we deduce (1.5). □

Proof of Theorem 3. Now, we observe that $f'(x)$ is a polynomial of degree at most (n-1). Moreover, if $p \not| d$ = g.c.d.$(a_1, \ldots, a_n)$ there are no regular solutions. Therefore

$$J_k(\lambda_1, \ldots, \lambda_n; p^\alpha) = p^{Rk-\alpha n} \sum_{a_1,\ldots,a_n=1}^{p^{\alpha-R}} e\left(-\frac{a_1\lambda_1 + \ldots + a_n\lambda_n}{p^{\alpha-R}}\right)$$
$$\times \sum_{(x_1,\ldots,x_j)}^{p} \prod_{\nu=1}^{j} \sum_{y_\nu=1}^{p^{\alpha-R-1}} e\left(\frac{f(x_\nu + py_\nu)}{p^{\alpha-R}}\right) \prod_{\nu=j+1}^{k} \sum_{y_\nu=1}^{p^{r_\nu-R}} e\left(\frac{f(\hat{x}_\nu + p^{\alpha-r_\nu}y_\nu)}{p^{\alpha-R}}\right)$$

when $p^R|d$ and $J_k(\lambda_1, \ldots, \lambda_n; p^\alpha) = 0$ otherwise. From this and (2.8) we deduce (1.7). □

Proof of Theorem 4. 1) If $\ell \geq n$, from (2.8) and (2.4) we have

$$J_k(\lambda_1, \ldots, \lambda_n; p^\alpha) = p^{-\alpha n} \sum_{a_1,\ldots,a_n=1}^{p^\alpha} e\left(\frac{-a_1\lambda_1 - \ldots - a_n\lambda_n}{p^{\alpha-1}}\right)$$
$$\times \sum_{x_1,\ldots,x_j=1}^{p} \prod_{\nu=1}^{j} A_\alpha[f(x_\nu)] \prod_{\nu=j+1}^{m} p\delta_p[f'(\hat{x}_\nu)]$$
$$\times \sum_{y_\nu=1}^{p^{r_\nu-1}} e\left(\frac{f(\hat{x}_\nu + p^{\alpha-r_\nu}y_\nu)}{p^\alpha}\right) \prod_{\nu=m+1}^{k} e\left(\frac{f(\hat{x}_\nu)}{p^\alpha}\right)$$

and from (2.3), (2.6) we deduce

$$J_k(\lambda_1, \ldots, \lambda_n; p^\alpha) = p^{-\alpha n} \sum_{a_1,\ldots,a_n=1}^{p^{\alpha-1}} e\left(-\frac{a_1\lambda_1 + \ldots + a_n\lambda_n}{p^{\alpha-1}}\right)$$
$$\times \sum_{x_1,\ldots,x_j=1}^{p} \prod_{\nu=1}^{j} pA_{\alpha-1}[f_1(x_\nu)] \prod_{\nu=j+1}^{m} pA_{\alpha-1}^{r_\nu-1}[f_1(\hat{x}_\nu)] \prod_{\nu=m+1}^{k} e\left(\frac{f_1(\hat{x}_\nu)}{p^{\alpha-1}}\right) \tag{3.1}$$

Using Lemma 2 we deduce the required conclusion.

2) Now, let $\ell < n$. Since $\hat{x}_{j+1}, \ldots, \hat{x}_m$ are roots of $f'(x)$, the coefficients of $f'(x)$ must satisfy the following system of ℓ linear congruences

$$\sum_{k=1}^{\ell} k a_k \hat{x}_{i_j}^{k-1} \equiv - \sum_{k=\ell+1}^{n} k a_k \hat{x}_{i_j}^{k-1} (\operatorname{mod} p); \forall j = 1, \ldots, \ell \tag{3.2}$$

where $\{i_1, \ldots, i_\ell\} \subset \{j+1, \ldots, m\}$ $\hat{x}_{i_1}, \ldots, \hat{x}_{i_\ell}$ are noncongruent mod p, and its determinant V is

$$V = \ell! \prod_{i_r < i_s} (x_{i_r} - x_{i_s}) \not\equiv 0 (\operatorname{mod} p)$$

It follows that the system (3.2) has a unique solution for each fixed value of $a_{\ell+1}, \ldots, a_n$. Suppose then, that $a_i = \hat{a}_i(a_{\ell+1}, \ldots, a_n) + p b_i$, $b_i \epsilon \mathbb{Z}/p^{\alpha-1}\mathbb{Z}, i = 1, \ldots, \ell$. Now, making a partition in the sum over $a_{\ell+1}, \ldots, a_n$, we have

$$J_k(\lambda_1, \ldots, \lambda_n; p^\alpha) = p^{m-\alpha n}\{\sum_1 + \sum_2\}$$

where

$$\sum_1 = \sum_{b_1, \ldots, b_\ell = 1}^{p^{\alpha-1}} \sum_{\substack{a_{\ell+1}, \ldots, a_n = 1 \\ \exists i, \text{g.c.d.}(\alpha_i, p) = 1}}^{p^\alpha} e\left(-\frac{a_1 \lambda_1 + \ldots + a_n \lambda_n}{p^\alpha}\right)$$
$$\times \sum_{(x_1, \ldots, x_j)_{n-L}}^{p} \prod_{\nu=1}^{j} \delta_p[f'(x_\nu)] \sum_{y_\nu=1}^{p^{\alpha-2}} e\left(\frac{f(x_\nu + p y_\nu)}{p^\alpha}\right)$$
$$\times \prod_{\substack{\nu=j+1 \\ (\hat{x}_{j+1}, \ldots, \hat{x}_k)_L (\operatorname{mod} p)}}^{m} \sum_{y_\nu=1}^{p^{r_\nu-1}} e\left(\frac{f(\hat{x}_\nu + p^{\alpha-r_\nu} y_\nu)}{p^\alpha}\right) \prod_{\nu=m+1}^{k} e\left(\frac{f(\hat{x}_\nu)}{p^\alpha}\right)$$

and by a similar argument to the one used in the proof of (1.5), we have

$$\sum_2 = p^{(\alpha-1)n} J_k(\lambda_1, \ldots, \lambda_n; p^{\alpha-1}) \tag{3.3}$$

We suppose that $L \leq \ell + s$ is the number of $\hat{x}_\nu$, $\nu = j+1, \ldots, k$, which are noncongruent mod p. Then at least $n - L$ x_ν, $\nu = 1, \ldots, j$ must be noncongruent mod p, that is $(x_1, \ldots, x_j; \hat{x}_{j+1}, \ldots, \hat{x}_k)_{(n-L,L)} (\operatorname{mod} p)$. Since $f'(x)$ is a polynomial of degree at least (n-L), $f(x)$ is of degree at least (n-L+1). Hence

$$|\sum_1| \leq (n-1)^j p^{(\alpha-1)\ell+\alpha(L_1-\ell)}(p^{\alpha(n-L_1)} - p^{(\alpha-1)(n-L_1)})p^{(\alpha-1)(1-1/n)j} \times \prod_{\nu=j+1}^{m} p^{(r_\nu-1)(1-1/n)}$$

where $L_1 = \max\{\ell, n-L\}$, and $r_{j+1}, \ldots, r_m \leq \alpha - 1$ The formula (1.10) is deduced from this. □

If $\ell \geq n$ or $\ell < n$ we can apply (1.9) or (1.10) in an iterative way, as long as the subsequent systems still satisfy this condition. Thus, successive applications of this argument reduce the modulo to p.

Proof of Theorem 5. (1.11) and (1.12) follow directly from Theorem 3 bearing in mind the multiplicative property of the number of solutions of a congruence system. □

Proof of Theorem 6. We considerer the system of congruences

$$x_1^\nu + \ldots + x_k^\nu \equiv \lambda_\nu + q_\nu z_\nu (\operatorname{mod} q), \quad 1 \leq \nu \leq n \quad (x_1, \ldots, x_k) \epsilon S(q)$$

where $z_1, \ldots, z_n$ are taken over a complete set of residues modulo q. Then by (1.11) we can write

$$J_k = \frac{1}{q_1 \cdots q_n} \sum_{z_1, \ldots, z_n = 1}^{q} \prod_{\ell=1}^{v} J_k(\lambda_1 + q_1 z_1, \ldots, \lambda_n + q_n z_n; p_\ell^{\delta_\ell}) \tag{3.4}$$

Let $z_i \equiv p_1'^{\delta_1} z_{i1} + \ldots + p_v'^{\delta_v} z_{iv} (\operatorname{mod} q)$, where $p_\ell'^{\delta_\ell} = (p_1^{\delta_1} \ldots p_v^{\delta_v})/p_\ell^{\delta_\ell}$ and the $z_{i\ell}$ are taken over a complete set of residues modulo $p_\ell^{\delta_\ell}$. Hence $z_i \equiv p_\ell'^{\delta_\ell} z_{i\ell} (\operatorname{mod} p_\ell^{\delta_\ell})$ and $p_1'^{\delta_1} z_{i1} + \ldots + p_v'^{\delta_v} z_{iv}$ are taken over a complete set of residues modulo q when $z_{i1}, \ldots, z_{iv}$ are taken over a complete set of residues modulo $p_1^{\delta_1}, \ldots, p_v^{\delta_v}$ respectively. Then

$$J_k = \frac{1}{q_1 \cdots q_n} \prod_{\ell=1}^{v} \sum_{z_{1\ell}, \ldots z_{n\ell}=1}^{p_\ell^{\delta_\ell}} J_k(\lambda_1 + q_1 p_\ell'^{\delta_\ell} z_{1\ell}, \ldots, \lambda_n + q_n p_\ell'^{\delta_\ell} z_{n\ell}; p_\ell^{\delta_\ell})$$

1) If $p_\ell^{\delta_\ell}|q_{n_i};\forall i=1,\dots,t_\ell$, $1\le n_1<\dots<n_{t_\ell}\le n$, $\{n_1,\dots,n_{t_\ell}\}\subset\{1,2,\dots,n\}$ and g.c.d.$(p_\ell^{\delta_\ell},q_{m_i})=1,\forall m_i\epsilon\{1,2,\dots,n\},m_i\neq n_i$, then,

$$J_k=\frac{1}{q_1\dots q_n}\prod_{\ell=1}^{v}p_\ell^{\delta_\ell t_\ell}J_k(\lambda_{n_1},\dots,\lambda_{n_{t_\ell}};p_\ell^{\delta_\ell})\le\frac{1}{q_1\dots q_n}\prod_{\ell=1}^{v}p_\ell^{\delta_\ell t_\ell}J_k(p_\ell^{\delta_\ell})$$

2) Let $p_\ell|q_{n_i};\forall i=1,\dots,t_\ell$, $1\le n_1<\dots<n_{t_\ell}\le n$, $\{n_1,\dots,n_{t_\ell}\}\subset\{1,2,\dots,n\}$ and g.c.d.$(p_\ell,q_{m_i})=1,\forall m_i\epsilon\{1,2,\dots,n\},m_i\neq n_i$ and set $s_\ell=\#\{q_{n_i},i=1,\dots t_\ell;\ \ p_\ell^{\delta_\ell}|q_{n_i}\}$, $0\le s_\ell\le t_\ell-1$. Then

$$J_k=\frac{1}{q_1\dots q_n}\prod_{\ell=1}^{v}p_\ell^{\delta_\ell(t_\ell-s_\ell)}\sum_{z_{\ell 1},\dots z_{\ell s_\ell}=1}^{p_\ell^{\delta_\ell}}J_k(\mu_{n_1},\dots,\mu_{n_{t_\ell}};p_\ell^{\delta_\ell})$$

where $\mu_{n_i}=\lambda_{n_i}+q_{n_i}z_{n_i,\ell}$, if $p_\ell^{\delta_\ell}\not|q_{n_i}$ *and* $\mu_{n_i}=\lambda_{n_i}$, if $p_\ell^{\delta_\ell}|q_{n_i}$. □

EXAMPLES :

1.-In the particular case $q_1=p_1^{\delta_1}$, $q_2=p_1^{\delta_1}p_2^{\delta_2}$, $\dots,q_n=p_1^{\delta_1}p_2^{\delta_2}\dots p_n^{\delta_n}=q$ and $(x_1,\dots,x_n)\epsilon S(q)$ then $p_\ell^{\delta_\ell}|q_\ell,\dots,q_n$ and $t_\ell=n-\ell+1,s_\ell=0$ so we have

$$J_k=\prod_{\ell=1}^{n}J_k(\lambda_\ell,\dots,\lambda_n;p_\ell^{\delta_\ell})$$

2.- Let $k=n$ $q_\nu=p^\nu,\forall\nu=1,\dots,n$, and let $(x_1,\dots,x_n)\epsilon S_2(p^\alpha)$ $j\le n=k$, then $q=p^n,v=1,\delta_v=t_v=n,s_v=1$, by (1.15) and corollary 2 so we have

$$J_n=p^{n(n-3)/2}\sum_{z=1}^{p^n}J_n(\lambda_1+pz,\dots,\lambda_{n-1}+p^{n-1}z,\lambda_n;p^n)\le p^{n(n-3)/2}p^np^{(n-1)(j-n)}n!$$

$$J_n\le n!p^{(n-1)(j-n/2)}$$

3.- Let $k=n$, $q_\nu=p^\nu$ $\forall\nu=1,\dots,r$, $q_\nu=p^r,r<n,\forall\nu=r+1,\dots,n$ and let $(x_1,\dots,x_n)\epsilon S_2(p^\alpha)$ such that $x_1,\dots,x_n$ hold the corollary 2 then $q=p^r,v=1$, $\delta_v=r,t_\ell=n,s_\ell=n-r+1$ and by (1.15) and corollary 2 we obtain

$$J_n=\frac{p^{r(r-1)}}{p^{r(n-r)+r(r+1)/2}}\sum_{z_1,\dots,z_{n-r+1}=1}^{p^r}J_n(\lambda_1+pz_1,\dots,\lambda_{r-1}+p^{r-1}z_{r-1},\lambda_r,\dots\lambda_r;p^r)$$

$$J_n\le n!p^{r(r-1)/2-(r-1)(n-j)}=n!p^{(r-1)(r/2-n-j)}$$

References

1. N.M. Korobov, Sobre unos sistemas completos de congruencias (Russian), *Acta Aritmética* **XXI** (1972), 357–366.
2. N.M. Korobov, *Las sumas trigonométricas y sus aplicaciones (Russian)*, Edit. Nauk, Moscú, 1988.
3. A.A. Karatzuba, *Fundamentos de la teoría analítica de los números*, Edit. Mir, Moscú, 1979.