ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 15, Number 2, Spring 1985

ON MULTIDIMENSIONAL COVERING SYSTEMS OF CONGRUENCES

J. FABRYKOWSKI

Dedicated in memory of E. G. Straus

Let us consider a homogeneous system of congruences:

$$\sum_{j=1}^{k} a_{ij}x_j \equiv 0 \bmod m_i,\ 1 \leqq i \leqq n \tag{1}$$

where $m_i \geqq 2$ and

$$(a_{i1}, a_{i2}, \ldots, a_{ik}, m_i) = 1. \tag{2}$$

In [2] we have proved that if $n \geqq 2$ and a homogneneous system of the form (1) covers a k-dimensional cube $C_k \subset Z_k$ with the side length 2^{n-1} and such that $0 = [0, 0, \ldots, 0] \in C_k$ then it is a covering system, i.e., it covers every k-dimensional integer vector. We conjectured that the length $2^{n-2} + 2$ of the side of our cube is sufficient for the assertion and gave an example showing that the length $2^{n-2} + 1$ is not enough for the purpose.

In this paper we show that for a fixed number of variables and congruences we can check the conjecture by performing a finite number of operations.

In fact we shall prove the following:

THEOREM. *If there exists a homogeneous system of congruences of* $k \geqq 2$ *variables that covers a k-dimensional cube* C_k *with the side length* $2^{n-2} + 2$ *and such that* $0 \in C_k$ *which is not covering, then there exists a system (not necessary homogeneous) having the same properties which has all moduli less than* $2\max(k, 2^{n-2} + 2)(2^{n-2} + 2)^{k-1}$.

PROOF. Suppose that (1) covers the cube C_k, $0 \in C_k$ and is not covering. Certainly we can assume that no proper subset of our system has the same properties. We split indices $i \leqq n$ into three disjoint classes A, B, C as follows:

$i \in A$ if the i-th congruence is satisfied by $k + 1$ integer points from C_k which form a linearly independent set.

Received by the editors April 11, 1984.

$i \in B$ if $i \notin A$ and the i-th congruence is satisfied by k linearly independent points from C_k.

$i \in C$ if $i \notin A \cup B$ and the i-th congruence is satisfied by $r(1 \leqq r \leqq k-1)$ lenearly independent points from C_k.

Suppose first that $i \in A$ and let $p_1, p_2, \ldots, p_{k+1}$, where $p_s = (p_{s1}, p_{s2}, \ldots, p_{sk})$, $1 \leqq s \leqq k+1$ be $k+1$ linearly independent points satisfying the i-th congruence of (1).

For every r, $1 \leqq r \leqq k+1$ we have the system of k congruences:

$$\sum_{j=1}^{k} a_{ij} p_{sj} \equiv 0 \bmod m_i,\ s \in J_r$$

where $J_r = \{1, 2, \ldots, r-1, r+1, \ldots, k+1\}$. Therefore for some integers L_s

$$\sum_{j=1}^{k} a_{ij} p_{sj} = m_i L_s,\ s \in J_r. \tag{3}$$

Applying Cramer's Rule to (3) we find

$$a_{ij} = m_i W_{rj} / V_r \tag{4}$$

where $V_r = \det[p_{sj}]_{1 \leqq j \leqq k,\, s \in J_r}$ and W_{rj} are determinants as desired. Since $a_{ij} \in Z$ then from (4) it follows that

$$m_i | V_r a_{ij},\ 1 \leqq r \leqq k+1,\ 1 \leqq j \leqq k,\ i \in A \tag{5}$$

and using (2) we obtain

$$m_i | V_r \text{ for every } 1 \leqq r \leqq k+1. \tag{6}$$

By virtue of the following identity

$$D = \det \begin{vmatrix} 1 & p_{11} & p_{12} & \cdots & p_{1k} \\ 1 & p_{21} & p_{22} & \cdots & p_{2k} \\ \cdots & \cdots & \cdots & \cdots & \cdots \\ 1 & p_{k+11} & p_{k+12} & \cdots & p_{k+1k} \end{vmatrix} = \sum_{r=1}^{k+1} (-1)^{r-1} V_r$$

and (6) it follows that $m_i | D$.

On the other hand it is known that $|D| = k! \Delta(p_1, \ldots p_{k+1})$, where $\Delta(p_1, \ldots, p_{k+1})$ denotes the k-dimensional measure of the simplex determined by the points $p_1, \ldots, p_{k+1}$. (See, e.g., [1]) Since $p_1, p_2, \ldots, p_{k+1} \in C_k$ then $|D| \leqq (2^{n-2}+2)^k$ so $m_i \leqq (2^{n-2}+2)^k$.

Let M be the least common multiple of all moduli m_i, $i \in A$. All prime divisors of M are less then $(2^{n-2}+2)^k$. Now we show that for every n and $k \geqq 2$ there are at least n prime numbers between Γ and 2Γ, where

$$\Gamma = \max(k, 2^{n-2}+2)(2^{n-2}+2)^{k-1}.$$

Suppose first that $k \geqq 2^{n-2} + 2$, so that

$$\Gamma = k(2^{n-2} + 2)^{k-1}.$$

We use the following inequality of P. Finsler [3]:

$$\pi(2y) - \pi(y) > y/(3 \log 2y).$$

Take $y = \Gamma$ and let us consider the expression

$$\frac{\Gamma}{3 \log 2\Gamma} = \frac{k(2^{n-2} + 2)^{k-1}}{3 \log 2k(2^{n-2} + 2)^{k-1}}.$$

If $A > 1$ then the function $f(x) = xA^{x-1}/(3 \log 2xA^{x-1})$ is increasing. Therefore it is enough to show that $f(2^{n-2} + 2) > n$ with $A = 2^{n-2} + 2$. It is easy to check the inequality for $n = 1, 2, 3$, and for $n \geqq 4$ we have $f(2^{n-1} + 2) \geqq 2f(2^{n-2} + 2)$ therefore the inequality follows by mathematical induction. Suppose now that $k < 2^{n-2} + 2$, so that $\Gamma = (2^{n-2} + 2)^k$. Let us consider the function

$$g(k, n) = \frac{(2^{n-2} + 2)^k}{3 \log 2(2^{n-2} + 2)^k}$$

which is decreasing with k, so taking $k = 2$ it is enough to show that $g(2, n) > n$ for every $n \geqq 1$. On the other hand the function

$$h(n) = \frac{g(2, n)}{n} = \frac{(2^{n-2} + 2)^2}{n\, 3 \log 2(2^{n-2} + 2)^2}$$

is increasing with n if $n \geqq 5$.

Moreover $h(5) \geqq 1$. If $n = 1, 2, 3$ or 4 by direct computation it is easy to verify that between Γ and 2Γ there are at least n primes.

Let us denote the primes in the interval $(\Gamma, 2\Gamma)$ by $q_1, q_2, q_3, \ldots$.

Let now $i \in B$ and denote our points by $p_1, p_2, \ldots, p_k$. They determine a $k - 1$ dimensional hyperplane having an equation $B_{i1}x_1 + B_{i2}x_2 + \cdots + B_{ik}x_k = B_{i0}$. Let us consider the congruences:

$$MB_{i1}x_1 + MB_{i2}x_2 + \cdots + MB_{ik}x_k \equiv B_{i0} \bmod q_i, \; i \in B. \tag{7}$$

Since $q_i \nmid M$ and as we shall prove, $q_i \nmid (B_{i1}, B_{i2}, \ldots, B_{ik})$ the system (7) has a solution $(x_1^0, x_2^0, \ldots, x_k^0)$. A $k - 1$ dimensional hyperplane determined by the points $p_1, \ldots, p_k$, where $p_s = (p_{s1}, p_{s2}, \ldots, p_{sk})$, $1 \leqq s \leqq k$, has an equation of the form:

$$\operatorname{Det} \begin{vmatrix} 1 & x_1 & x_2 & \cdots & x_k \\ 1 & p_{11} & p_{12} & \cdots & p_{1k} \\ \vdots & \vdots & \vdots & \cdots & \vdots \\ 1 & p_{k1} & p_{k2} & \cdots & p_{kk} \end{vmatrix} = 0.$$

Therefore for every $1 \leqq j \leqq k$, $i \in B$

$$B_{ij} = \det \begin{vmatrix} 1 & p_{11} & p_{12} & \cdots & p_{1j-1} & p_{1j+1} & \cdots & p_{1k} \\ \vdots & \vdots & \vdots & & \vdots & \vdots & & \vdots \\ 1 & p_{k1} & p_{k2} & \cdots & p_{kj-1} & p_{kj+1} & \cdots & p_{kk} \end{vmatrix}.$$

Similarly, as previously $|B_{ij}| = (k-1)!\Delta^{(j)}(p_1, p_2, \ldots, p_k)$ where $\Delta^{(j)}(p_1, \ldots, p_k)$ is the $k-1$ dimensional measure of the simplex determined by vertices $p_1^{(j)}, p_2^{(j)}, \ldots, p_k^{(j)}$, where $p_s^{(j)} = (p_{s1}, p_{s2}, \ldots, p_{sj-1}, p_{sj+1}, \ldots, p_k)$.

All points $p_s^{(j)} (1 \leqq s \leqq k)$ are in the $k-1$ dimensional cube $C_{k-1,j}$ with side length $2^{n-2}+2$. So $|B_{ij}| \leqq (2^{n-2}+2)^{k-1}$ and

$$0 < \sum_{i=1}^{k} |B_{ij}| \leqq k(2^{n-2}+2)^{k-1} \leqq \Gamma$$

which proves that $q_i \nmid (B_{i1}, B_{i2}, \ldots, B_{ik})$.

Now let $i \in C$. For every hyperplane $H_{r-1} (1 \leqq r \leqq k-1)$ in k-dimensional space we can find a $k-1$ dimensional hyperplane containing H_{r-1} and the point $P = [x_1^0 M, x_2^0 M, \ldots, x_k^0 M]$. It can be done by enlarging the set of points $p_1, p_2 \ldots p_r, P$ if $P \notin \{p_1, \ldots, p_r\}$ or $p_1, p_2, \ldots, p_r$ if $P \in \{p_1, \ldots, p_r\}$ by the points $p_{r+2}, \ldots, p_k$ or $p_{r+1}, p_{r+2}, \ldots, p_k$, respectively, and such that the enlarged set is linearly independent.

Let us consider for $i \in C$ equations $C_{i1}x_1 + C_{i2}x_2 + \ldots + C_{ik}x_k = C_{i0}$ such that

$$C_{i1}x_1^0 M + C_{12}x_2^0 M + \cdots + C_{ik}x_k^0 M = C_{i0}.$$

The system of congruences:

$$\sum_{j=1}^{k} a_{ij}x_j \equiv 0 \bmod m_i \quad i \in A \tag{8}$$

$$\sum_{j=1}^{k} B_{ij}x_j \equiv B_{i0} \bmod q_i \quad i \in B \tag{9}$$

$$\sum_{j=1}^{k} C_{ij}x_j \equiv C_{i0} \bmod q_i \quad i \in C \tag{10}$$

covers the same k-dimensional cube C_k as the system (1), the vector $[x_1^0 M, x_2^0 M, \ldots, x_k^0 M]$ is a common solution and the system is not covering. If it were a covering one then using Theorem 2 **[2]** we would infer that congruences (9) and (10) are not essential and so could be omitted and this would contradict the assumption that the system (1) is not covering.

REFERENCES

1. K. Borsuk, *Multidimensional Analytic Geometry*, PWM-Polish Scientific Publishers, Warsaw 1969.

2. J. Fabrykowski *Multidimensional covering systems of congruences*, Acta Arithmetica, to appear.

3. P. Finsler *Uber die Primzaheln zwischen n und* **2***n* Festschrift zum 60. Geburstag von Prof. Dr. Andreas Speiser, Zurich 1945, 118–122. see also E. Trost "Primzahlen" Satz **32**, Basel-Stuttgart 1953.