ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 27, Number 1, Winter 1997

ON HOMOGENEOUS COVERING CONGRUENCES

A. SCHINZEL

Dedicated to Professor E. Hlawka on the occasion of his eightieth birthday

ABSTRACT. Two problems on covering congruences proposed by T. Cochrane and G. Myerson are either solved or reduced to a classical problem of Erdős.

T. Cochrane and G. Myerson [**2**] called a cover for the additive group $\mathbf{Z}^n$ any system of congruences

$$\sum_{j=1}^{n} a_{ij}x_j \equiv a_{i0} \pmod{m_i}, \qquad 1 \le i \le r, \tag{1}$$

where

$$(a_{i0}, a_{i1}, \dots, a_{in}, m_i) = 1, \qquad 1 \le i \le r, \tag{2}$$

such that every vector $\langle x_1, \dots, x_n \rangle \in \mathbf{Z}^n$ satisfies at least one of them and

$$1 < m_1 < \cdots < m_r. \tag{3}$$

If $a_{i0} = 0$, $1 \le i \le r$, (1) is called a homogeneous cover.

We prefer to use the terms cover and homogeneous cover in a wider sense, without the condition (3), and we shall formulate the relevant results and problems in that way. The best known problem about covering congruences, due to Erdős [**3**], concerns the truth of the following statement.

E. *For every $c \in \mathbf{N}$ there exists a cover for $\mathbf{Z}$ with distinct moduli greater than c.*

Cochrane and Myerson proved the following lemma. Let $x \equiv a_i \pmod{m_i}$, $1 \le i \le r$, be a cover for $\mathbf{Z}$ in which moduli are distinct

Received by the editors on February 21, 1996.
1991 *Mathematics Subject Classification.* 11A07, 11B27.
Key words and phrases. Covering congruences.

and composite (hereafter a *composite cover*). Let $p_1, \dots, p_t$ be all the primes dividing $\Pi_1^r m_i$. Then the congruences

$$y \equiv 0 \pmod{p_j}, \qquad x - a_i y \equiv \pmod{m_i}, \quad 1 \le i \le r, \quad 1 \le j \le t \tag{4}$$

form a homogeneous cover with distinct moduli greater than 1.

They asked whether there are any homogeneous covers with distinct moduli greater than 1 that do not come from composite covers.

In order to answer the question, we make it precise by means of the following definitions.

A homogeneous cover for $\mathbf{Z}^p$

$$\sum_{k=1}^{p} b_{ik} x_k \equiv 0 \pmod{m_i}, \qquad 1 \le i \le r \tag{5}$$

comes from (1) with $a_{i0} = 0$ by a *simple transformation* if there exist integers c_{jk}, $1 \le j \le n$, $1 \le k \le p$, and d_i, $1 \le i \le r$, such that for all $i \le r$ we have

$$\sum_{k=1}^{p} b_{ik} x_k \equiv d_i \sum_{j=1}^{n} a_{ij} \left(\sum_{k=1}^{p} c_{jk} x_k \right) \pmod{m_i}.$$

A homogeneous cover $\sum_{k=1}^{p} c_{ik} x_k \equiv 0 \pmod{n_i}$ for $\mathbf{Z}^p$ comes from (5) by a *trivial extension* if

$$\left\{ \left\langle \sum_{k=1}^{p} c_{ik} x_k, n_i \right\rangle : 1 \le i \le s \right\} \supset \left\{ \left\langle \sum_{k=1}^{p} b_{ik} x_k, m_i \right\rangle : 1 \le i \le r \right\}.$$

We shall answer Cochrane and Myerson's question by proving

Theorem 1. *There exists a homogeneous cover for* $\mathbf{Z}^2$ *with distinct moduli greater than* 1 *that does not come from any cover* (4) *by a simple transformation followed by a trivial extension.*

An essential component of the proof is a lemma due to J.L. Selfridge, who has kindly agreed to its use in this paper.

Cochrane and Myerson further asked the following question which we rephrase in our terminology.

Question. Are there homogeneous covers for $\mathbf{Z}^n$, $n > 2$, with distinct moduli greater than 1 that do not come from similar covers for $\mathbf{Z}^2$ by a simple transformation followed by a trivial extension?

We shall answer partially this question by proving the following theorem.

Theorem 2. *E implies the affirmative answer to the Question.*

A cover for $\mathbf{Z}^n$ is called *irredundant* if it ceases to cover $\mathbf{Z}^n$ when one of the congruences is removed. Clearly every cover contains an irredundant cover.

The proof of Theorem 1 is based on the following lemmas.

Lemma 1 [J.L. Selfridge]. *There exists an irredundant cover* $x \equiv b_i \bmod n_i$ *for* $\mathbf{Z}$ *with distinct composite moduli* n_i, $1 \leq i \leq 21$, *satisfying*

$$\max_{1\leq i\leq 21} n_i = 96 \quad \text{and} \quad \text{l.c.m.}_{1\leq i\leq 21} n_i = 1440. \tag{6}$$

Proof. Such is the system $x \equiv b_i \pmod{n_i}$, where $\langle b_i, n_i\rangle = \langle 3,4\rangle$, $\langle 5,8\rangle$, $\langle 9,24\rangle$, $\langle 9,16\rangle$, $\langle 1,48\rangle$, $\langle 17,32\rangle$, $\langle 65,96\rangle$, $\langle 3,9\rangle$, $\langle 2,6\rangle$, $\langle 6,18\rangle$, $\langle 10,12\rangle$, $\langle 18,36\rangle$, $\langle 0,72\rangle$, $\langle 0,10\rangle$, $\langle 16,20\rangle$, $\langle 12,40\rangle$, $\langle 52,60\rangle$, $\langle 13,15\rangle$, $\langle 9,45\rangle$, $\langle 4,30\rangle$, $\langle 18,90\rangle$ for $i = 1,2,\ldots,21$, respectively.

The congruences $x \equiv b_i \pmod{n_i}$, $1 \leq i \leq 7$, cover all $x \equiv 1 \pmod 2$. The congruences $x \equiv b_i \pmod{n_i}$, $8 \leq i \leq 12$, cover all $x \equiv 2, 6, 8$ or $10 \pmod{12}$. The congruences $x \equiv b_i \pmod{n_i}$, $i = 14, 15, 17, 18, 20$, cover all $x \equiv 4 \pmod{12}$. The congruences $x \equiv b_i \pmod{n_i}$, $i = 8$, 10, 13, 14, 15, 16, 19, 21, cover all $x \equiv 0 \pmod{12}$. □

The system is irredundant since on removing the congruence $x \equiv a_i$

(mod n_i) the following integer remains uncovered

$$7, 5, 33, 25, 1, 17, 65, 48, 2, 6, 22, 126, \quad (7)$$
$$72, 40, 16, 172, 112, 28, 324, 4, 108$$

for $i = 1, 2, \dots, 21$, respectively.

Lemma 2. *There exists a cover* $x \equiv c_j \pmod{q_j}$ *for* $\mathbf{Z}$ *with distinct moduli* q_j, $1 \le j \le r$, *satisfying*

$$q_j > 19. \quad (8)$$

Proof. This is a result of Choi [**1**]. □

Proof of Theorem 1. Here is a system with the required property.

$$y \equiv 0 \pmod{p}, \quad p \text{ prime}, p|6Q, p \ne 5, \qquad Q = \operatorname*{l.c.m.}_{1\le j\le r} q_j, \quad (10)$$

$$y \equiv 0 \pmod{25}, \quad (11)$$

$$x - b_i y \equiv 0 \pmod{n_i}, \qquad 1 \le i \le 21, \quad (12)$$

$$5x - c_j y \equiv 0 \pmod{5q_j}, \quad \text{if } 1 \le j \le r,\ 5 \nmid c_j, \quad (13)$$

$$5x - (c_j + q_j)y \equiv 0 \pmod{5q_j}, \quad \text{if } 1 \le j \le s,\ 5 \mid c_j, 5 \nmid q_j, \quad (14)$$

where b_i, n_i and c_j, q_j have the meaning of Lemmas 1 and 2, respectively.

Clearly, the system (10)–(14) satisfies the condition (2) and all the moduli are distinctly greater than 1. We shall show that it covers $\mathbf{Z}^2$. Since the system is homogeneous it suffices to show that every pair $\langle x, y\rangle \in \mathbf{Z}^2$ with $(x, y) = 1$ satisfies at least one of the congruences (10)–(14).

If $(y, 30) = 1$ we choose $\bar{y} \in \mathbf{Z}$ such that $y\bar{y} \equiv 1 \pmod{1440}$. By Lemma 1 there exists an $i \le 21$ such that

$$x\bar{y} \equiv b_i \pmod{n_i}$$

and then (12) holds. If $(y, 30) > 1$, then either $(y, 6) > 1$ and then (10) holds for a $p \in \{2, 3\}$ or $y \equiv 0 \bmod 5$.

Now if $(y/5, Q) = 1$ we choose $\bar{\bar{y}} \in \mathbf{Z}$ such that $(y/5)\bar{\bar{y}} \equiv 1 \pmod{Q}$. By Lemma 2 there exists a $j \leq r$ such that

$$x\bar{\bar{y}} \equiv c_j \pmod{q_j}.$$

If we had $(c_j, q_j) \equiv 0 \pmod 5$, it would follow $x \equiv 0 \pmod 5$, contrary to $(x, y) = 1$. Therefore, $c_j \not\equiv 0 \pmod 5$ or $c_j + q_j \not\equiv 0 \pmod 5$. In the former case (13) holds, in the latter (14).

Finally, if $y \equiv 0 \pmod 5$, $(y/5, Q) > 1$ we have either (10) for a $p \mid Q$, $p \neq 5$ or (11).

Now we shall show that the system (10)–(14) does not come from any system (4) by a simple transformation followed by a trivial extension. First we observe that the congruences (12) are irredundant. Indeed, by Lemma 1 for each $h \leq 21$ there exists an integer x_h such that $x_h \not\equiv a_i \pmod{n_i}$ for all $i \neq h$. Now the pair $\langle x_h, 1\rangle$ does not satisfy any congruence except $x - b_h y \equiv 0 \pmod{n_h}$. It follows that a system (4) from which the system (10)–(14) were obtained would satisfy

$$\{n_1, \ldots, n_{21}\} \subset \{m_1, \ldots, m_s\}$$

and since, by (6), $\text{l.c.m.}_{1 \leq i \leq 21} n_i \equiv 0 \pmod 5$, 5 would occur among the moduli of the system (10)–(14), which is not the case. □

Remark. It is not an accident that to prove the existence of a homogeneous cover for $\mathbf{Z}^2$ with distinct moduli greater than 1 not coming from a composite cover for $\mathbf{Z}$ we have used the composite cover given in Lemma 1. Namely, as G. Myerson has informed me in a letter of December 6, 1995, he together with B. Jin and B. Reznick proved that from every homogeneous covering system for $\mathbf{Z}^2$ with distinct moduli greater than 1 one can obtain by some simple operations a composite cover for $\mathbf{Z}$.

Proof of Theorem 2. It follows from E that there exist 5 covers for $\mathbf{Z}$ with distinct moduli greater than 1 taken from 5 disjoint sets. Without loss of generality we may assume that these covers are irredundant. Let them be

$$x \equiv e_{ij} \pmod{n_{ij}}, \qquad i \leq 5,\ j \leq s_i,$$

and let N be the least common multiple of all the moduli. Here is a system with the property required in the theorem

$$z \equiv 0 \pmod{p} \quad \text{for all primes } p \text{ dividing } 3N, \tag{15}$$

$$x - 3e_{1j}z \equiv 0 \pmod{3n_{1_j}}, \qquad 1 \le j \le s_1, \tag{16}$$

$$y - 3e_{2j}z \equiv 0 \pmod{3n_{2j}}, \qquad 1 \le j \le s_2, \tag{17}$$

$$x - (3e_{3j}+1)z \equiv 0 \pmod{3n_{3j}}, \qquad 1 \le j \le s_3, \tag{18}$$

$$y - (3e_{4j}+1)z \equiv 0 \pmod{3n_{4j}}, \qquad 1 \le j \le s_4, \tag{19}$$

$$x - y - 3e_{5j}z \equiv 0 \pmod{3n_{5j}}, \qquad 1 \le j \le s_5. \tag{20}$$

It is clear that the system satisfies the condition (2). We shall show that it covers $\mathbf{Z}^3$. Take $\langle x, y, z\rangle \in \mathbf{Z}^3$. If $(z, 3N) = 1$ we choose $\bar{z} \in \mathbf{Z}$ such that $z\bar{z} \equiv 1 \bmod N$. Clearly we have one of five possibilities:

$$x \equiv 0 \pmod{3}, \tag{21}$$

$$y \equiv 0 \pmod{3}, \tag{22}$$

$$x \equiv z \pmod{3}, \tag{23}$$

$$y \equiv z \pmod{3}, \tag{24}$$

$$x - y \equiv 0 \pmod{3}. \tag{25}$$

In the case (21) we have for $j \le s_1$,

$$\frac{x}{3}\bar{z} \equiv e_{1j} \pmod{n_{1j}}$$

and then (16) holds.

In the case (22) we have for $j \le s_2$,

$$\frac{y}{3}\bar{z} \equiv e_{2j} \pmod{n_{2j}}$$

and then (17) holds.

In the case (23) we have for $j \le s_3$,

$$\frac{x-z}{3}\bar{z} \equiv e_{3j} \pmod{n_{3j}}$$

and then (18) holds.

In the case (24) we have for $j \le s_4$,

$$\frac{y-z}{3}\bar{z} \equiv e_{4j} \pmod{n_{4j}}$$

and then (19) holds.

In the case (25) we have for $j \le s_5$,

$$\frac{x-y}{3}\bar{z} \equiv e_{5j} \pmod{n_{5j}}$$

and then (20) holds.

Now we shall show that the congruence $z \equiv 0 \pmod 3$ of the system (15) and the first congruence of each of the systems (16), (17) is irredundant. Indeed, the triple $\langle 1,2,3\rangle$ does not satisfy any congruence of (15) except $z \equiv 0 \pmod 3$ and any of congruences (16)–(20). Further, since the systems $x \equiv e_{ij} \pmod{n_{ij}}$, $1 \le j \le s_i$, for $i = 1,2$, are irredundant there exist integers x_1 and x_2 such that

$$x_i \not\equiv e_{ij} \pmod{n_{ij}} \quad \text{for } i = 1,2 \quad \text{and} \quad 1 < j \le s_i.$$

Thus $\langle 3x_1, 2, 1\rangle$ satisfies only the congruence $x - 3e_{11}z \equiv 0 \pmod{3n_{11}}$ and $\langle 2, 3x_2, 1\rangle$ satisfies only the congruence $y - 3e_{21}z \equiv 0 \pmod{3n_{21}}$.

If the cover (15)–(20) would come from a cover $\sum_{j=1}^{2} a_{ij}x_j \equiv 0 \pmod{m_i}$, $1 \le i \le r$, for $\mathbf{Z}^2$ by a simple transformation followed by a trivial extension we should have for some integers c_{jk}, d_k

$$x - 3e_{11}z \equiv d_1 \sum_{j=1}^{2} a_{1j}(c_{j1}x + c_{j2}y + c_{j3}z) \pmod{3n_{11}},$$

$$y - 3e_{21}z \equiv d_2 \sum_{j=1}^{2} a_{2j}(c_{j1}x + c_{j2}y + c_{j3}z) \pmod{3n_{21}},$$

$$z \equiv d_3 \sum_{j=1}^{2} a_{3j}(c_{j1}x + c_{j2}y + c_{j3}z) \pmod 3.$$

This implies

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix} \equiv \begin{pmatrix} d_1a_{11} & d_1a_{12} \\ d_2a_{21} & d_2a_{22} \\ d_3a_{31} & d_3a_{32} \end{pmatrix} \begin{pmatrix} c_{11} & c_{12} & c_{13} \\ c_{21} & c_{22} & c_{23} \end{pmatrix} \pmod 3$$

which is impossible since the rank over $\mathbf{F}_3$ of the matrix on the lefthand side is 3, of that on the righthand side is at most 2.

REFERENCES

1. S.L.G. Choi, *Covering the set of integers by congruence classes of distinct moduli*, Math. Comput. **25** (1971), 885–895.

2. T. Cochrane and G. Myerson, *Covering congruences in higher dimensions*, Rocky Mountain J. Math. **26** (1996), 77–81.

3. P. Erdős, *On integers of the form* $2^k + p$ *and some related problems*, Summa Brasil. Math. **2** (1950), 192–210.

Mathematical Institute of the Polish Academy of Sciences, skr. poczt. 137, 00-950 Warszawa, Poland