ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 26, Number 1, Winter 1996

COVERING CONGRUENCES IN HIGHER DIMENSIONS

TODD COCHRANE AND GERRY MYERSON

ABSTRACT. We construct a set of covering congruences for the set of all ordered pairs of integers.

Erdős popularized the notion of a *set of covering congruences* (hereinafter, a *cover*). This is a finite set $(a_1, m_1), \dots , (a_r, m_r)$ of ordered pairs of integers with $1 < m_1 < \cdots < m_r$ such that every integer x satisfies at least one of the congruences $x \equiv a_j \pmod{m_j}$. The simplest example is $(0, 2), (0, 3), (1, 4), (1, 6), (11, 12)$.

It is obvious that there does not exist a *homogeneous* cover, that is, one in which $a_j = 0$ for all j (what homogeneous congruence is satisfied by 1?). Our purpose is to show that there is a homogeneous cover for the group of all ordered pairs of integers, that is,

Theorem. *There is a finite set of ordered triples $(a_1, b_1, m_1), \dots ,$ (a_r, b_r, m_r) with $1 < m_1 < \cdots < m_r$ and with $GCD(a_j, b_j, m_j) = 1$ for all j such that every pair of integers (x, y) satisfies at least one of the congruences $a_j x - b_j y \equiv 0 \pmod{m_j}$.*

The GCD condition is needed to weed out covers such as (1,0,2), (2,2,4), (0,3,6), in which repeated moduli are disguised by common factors. The theorem may not be too surprising, in view of the obvious correspondence between the one-variable congruence $x \equiv a \pmod{m}$ and the two-variable homogeneous congruence $x - ay \equiv 0 \pmod{m}$. But this correspondence, applied directly to a cover of the integers, does not produce a homogeneous cover of ordered pairs (at any rate, we don't see how it does), so a further idea is necessary. Such an idea is contained in Lemma 1, below.

Covering congruences in higher dimensions are discussed by Schinzel [**6**] and Fabrykowski [**2**]. Porubský [**5**] published a thorough survey of

Received by the editors on April 8, 1994, and in revised form on September 5, 1994.
1991 *Mathematics Subject Classification.* 11A07, 11B25.
Key words and phrases. Covering congruences.

covering problems. The results in these earlier papers do not seem to be applicable to the problems we discuss here.

We note in passing that any homogeneous cover for $\mathbf{Z} \oplus \mathbf{Z}$ extends trivially to a homogeneous cover for $\mathbf{Z}^n$ for any $n > 2$, where we might define such a cover as a finite set of homogeneous linear congruences in n variables, with distinct moduli and appropriate GCD conditions on the coefficients, such that every ordered n-tuple of integers satisfies at least one of the congruences. It suffices to view each congruence $a_j x - b_j y \equiv 0 \pmod{m_j}$ as a congruence in the n variables, with all but two of the coefficients equal to 0.

The homogeneous cover problem arose in the study of uniform distribution of sequences in higher dimensions [**4**]. Let S be a set of $m \times m$ integer matrices. We call S an m-cover if for every integer row m-vector $\mathbf{h}$ there is an integer row m-vector $\mathbf{k}$ and a matrix A in S such that $\mathbf{h} = \mathbf{k}A$.

A set of integers is a 1-cover if and only if it contains 1 or -1. For every $m > 1$, there are m-covers, even finite ones, containing no matrices of determinant ±1. For example, for $m = 2$, we can take

$$S = \left\{ \begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 0 & 2 \end{pmatrix}, \begin{pmatrix} 1 & 1 \\ -1 & 1 \end{pmatrix} \right\}.$$

The question arises as to whether there is a finite 2-cover containing no element of determinant ±1, and no two elements whose determinants are equal in absolute value; equivalently, whether $\mathbf{Z} \oplus \mathbf{Z}$ can be written as a finite union of proper subgroups, no two of the same index. As the set of solutions to $a_j x - b_j y \equiv 0 \pmod{m_j}$ forms a subgroup of index m_j (under the GCD condition), our theorem settles these questions in the affirmative.

Lemma 1. *Let $(a_1, m_1), \ldots, (a_r, m_r)$ be a cover of $\mathbf{Z}$ in which all the moduli are composite (hereinafter, a "composite cover"). Let $p_1, \ldots, p_t$ be all the primes dividing $M = \Pi_1^r m_j$. Then the triples $(0, 1, p_1), \ldots, (0, 1, p_t), (1, a_1, m_1), \ldots, (1, a_r, m_r)$ form a homogeneous cover for the group of ordered pairs of integers.*

Proof. Let (x, y) be an ordered pair of integers. If y and M are not relatively prime, then (x, y) satisfies at least one of the congruences

$y \equiv 0 \pmod{p_j}$. If y and M are relatively prime, let z be an integer such that $yz \equiv 1 \pmod{M}$. Now $xz \equiv a_j \pmod{m_j}$ for some j; multiplying through by y we see $x \equiv a_j y \pmod{m_j}$. □

To prove our theorem, then, we need only establish the existence of a composite cover. We present a particularly small example, shown to one of us by John Selfridge, as Lemma 2; first, we briefly describe two other constructions.

Dewar [**1**] constructed a cover in which all the moduli are divisible by 4. The construction is complicated, and the moduli are many and large (compared to those of Lemma 2).

A second construction uses the set $S = \{(1,4),(1,6),(3,8),(3,12),(23,24)\}$ obtained from the cover in the introductory paragraph by replacing each pair (a,m) with $(2a+1,2m)$. Every *odd* integer x satisfies at least one of the congruences $x \equiv a \pmod{m}$ with (a,m) in S, and all the moduli are composite. Now let $(a_1,m_1),\dots,(a_r,m_r)$ be a cover in which all the moduli are greater than 12 (such things exist; see section F13 of [**3**]). Then $T = \{(2a_1,2m_1),\dots,(2a_r,2m_r)\}$ covers the *even* integers, and every modulus is composite and greater than 24. The union of S and T is thus a composite cover. This cover, too, has many large moduli.

Lemma 2. *A composite cover is given by the set of pairs,* $(3,4)$, $(4,6)$, $(5,8)$, $(0,9)$, $(0,10)$, $(2,12)$, $(8,15)$, $(9,16)$, $(12,18)$, $(4,20)$, $(1,24)$, $(2,30)$, $(6,36)$, $(33,45)$, $(17,48)$, $(56,60)$, $(57,72)$, $(42,90)$, $(33,144)$, $(96,180)$.

Proof. The pairs $(3,4)$, $(5,8)$, and $(9,16)$ cover all the odd numbers except those congruent to $1 \pmod{16}$. Such odd numbers, if congruent to $1 \pmod{3}$, are covered by the pair $(1,24)$; if $2 \pmod{3}$, by $(17,48)$; this leaves the odd numbers that are $0 \pmod{3}$. Such numbers, depending on whether they are 0, 3 or $6 \pmod{9}$, are covered by $(0,9)$, $(57,72)$ or $(33,144)$, respectively.

Turning to the even numbers, $(4,6)$ and $(2,12)$ cover all but those congruent $0 \pmod{6}$ or $8 \pmod{12}$. Any number that is $8 \pmod{12}$ is 8, 20, 32, 44, or $56 \pmod{60}$; these are covered by $(8,15)$, $(0,10)$, $(2,30)$, $(4,20)$, and $(56,60)$, respectively. So we are left with the numbers divisible by 6.

The pairs $(12, 18)$ and $(6, 36)$ cover all the multiples of 6 except for the multiples of 18 and the numbers congruent to $24 \pmod{36}$. The former are covered by $(0, 9)$. The latter are 24, 60, 96, 132 or 168 $(\operatorname{mod} 180)$; these are covered by $(4, 20)$, $(0, 10)$, $(96, 180)$, $(42, 90)$ and $(33, 45)$, respectively, and now all the integers have been accounted for. □

Combining the two lemmas yields a homogeneous cover of $\mathbf{Z} \oplus \mathbf{Z}$, and proves the theorem.

We mention some open questions.

Are there homogeneous covers for $\mathbf{Z}^n$, $n > 2$, that are not trivial extensions or simple transformations of homogeneous covers for $\mathbf{Z}^2$? Are there any particularly simple or elegant ones?

Let us say that a subgroup H of $\mathbf{Z}^n$ is of Type 1 if it comes from a single linear congruence (equivalently, if $\mathbf{Z}^n/H$ is cyclic); otherwise, of Type 2. Is it possible, for $n \geq 2$, to write $\mathbf{Z}^n$ as a finite union of subgroups, no two of the same index, some or all of the subgroups being of Type 2? It is understood that we are not interested in examples where an expression as a union of Type 1 subgroups has been augmented by redundant subgroups of Type 2.

Are there any homogeneous covers that do not come from composite covers of $\mathbf{Z}$?

We close by mentioning some more composite covers John Selfridge has shown us. The one in Lemma 2 has 20 moduli, all dividing 720, none exceeding 180, divisible by no primes other than 2, 3 and 5. John has found a composite cover with no modulus exceeding 96. There are 21 moduli, all dividing 1440. He has found another composite cover with moduli divisible by no primes other than 2 and 3; there are 25 moduli, all dividing 3456, none exceeding 576.

REFERENCES

1. James Dewar, *On finite and infinite covering sets*, Proc. Washington State University Conference on Number Theory (James H. Jordan and William A. Webb, eds.), Washington State University, 1971.

2. J. Fabrykowski, *Multidimensional covering systems of congruences*, Acta Arith. **43** (1984), 191–208.

3. Richard K. Guy, *Unsolved problems in number theory*, Springer, New York, 1981.

4. G. Myerson, *A sample of recent developments in the distribution of sequences*, in *Number theory with an emphasis on the Markoff spectrum* (W. Moran and A. Pollington, eds.), Dekker, 1993.

5. Štefan Porubský, *Results and problems on covering systems of residue classes*, Mitteilungen Mathem. Seminar Giessen **150** (1981).

6. A. Schinzel, *Abelian binomials, power residues and exponential congruences*, Acta Arith. **32** (1977), 245–274.

Kansas State University and Center for Number Theory Research,
Manhattan, KS 66506, U.S.A.
E-mail address: cochrane@ksuvm.bitnet

Macquarie University, NSW 2109 Australia
E-mail address: gerry@mpce.mq.edu.au