ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volume 28, Number 3, Fall 1998

COVERING SYSTEMS OF HOMOGENEOUS CONGRUENCES

R.J. SIMPSON

A system of congruences $a_i \pmod{m_i}$, $i = 1, \ldots, t$, is called a *covering system* if every integer x satisfies $x \equiv a_i \pmod{m_i}$ for at least one value of i. If the moduli $m_i, \ldots, m_t$ are distinct, then it is an *incongruent* covering system. An example of an incongruent system is $\{0 \pmod 2, 0 \pmod 3, 1 \pmod 4, 1 \pmod 6, 11 \pmod{12}\}$. Such systems have a wide literature (see, for instance, the surveys by Guy [**2**, Sections F13, F14] and Porubsky [**5**]), and are the subject of two celebrated open questions. Are there incongruent covering systems with all moduli odd? Are there incongruent covering systems in which the smallest modulus is arbitrarily large? Erdös and Selfridge have offered money prizes for the answers to these questions [**2**].

Recently, Cochrane and Myerson [**1**] introduced the idea of a homogeneous covering system of $\mathbf{Z}^2$. This is a set of ordered triples $\{(a_i, b_i, m_i) : i = 1, \ldots, t\}$ with a_i, b_i, m_i having the greatest common divisor 1 such that every ordered pair of integers (x, y) satisfies

$$a_i x + b_i y \equiv 0 \pmod{m_i}$$

for at least one value of i. If the moduli m_i are distinct, the homogeneous system is *incongruent*. Cochrane and Myerson showed how to construct such systems by using an incongruent covering system (of $\mathbf{Z}$) in which each modulus is composite, such systems having been previously constructed by Selfridge. They asked if there exist homogeneous covers which do not come from composite systems. Gerry Myerson has informed me that he and Boping Jin have now shown that all homogeneous covers are, in a sense, equivalent to covers which can be obtained from composite systems. In this note we show how to construct a homogeneous cover without using a composite system and obtain some properties of such covers.

Received by the editors on April 3, 1996.

We begin with some notation. Let

$$s(a,m) = \{x \in \mathbf{Z} : x \equiv a \pmod{m}\}$$
$$h(a,b,m) = \{(x,y) \in \mathbf{Z}^2 : ax + by \equiv 0 \pmod{m}\}.$$

Notice that if n is a positive integer, then $h(a,b,m) = h(an,bn,mn)$. To avoid this redundancy we will follow Cochrane and Myerson and only allow such triples in which a, b and m have a greatest common divisor of 1. Note also that if $(m,n) = 1$, then $h(a,b,m) = h(an,bn,m)$. This means that, for any triple a, b, m there exists a triple a_1, b_1, m for which

$$h(a,b,m) = h(a_1,b_1,m)$$

with $\gcd(a_1,m) = a_1$. We say that $h(a_1,b_1,m)$ is the *standard form* of the two-dimensional congruence.

To introduce our method for constructing homogeneous systems, we will first describe a method for constructing one-dimensional covering systems. This depends on the following lemmas, the proofs of which are omitted since they are easy consequences of the Chinese remainder theorem.

Lemma 1. *If a, m, p and α are integers with $m \geq 1$, p prime and $\alpha \geq 0$, then*

$$s(a, mp^\alpha) = \bigcup_{i=0}^{p-1} s(a + ip^\alpha m, p^{\alpha+1}m).$$

Lemma 2. *If a, m and n are integers with m and n positive, then*

$$s(a,mn) \subseteq s(a,m).$$

Lemma 1 allows us to replace a congruence $s(a,m)$ with p congruences having modulus pm. We call this process *splitting* $s(a,m)$. Lemma 2 allows us to replace a congruence with another having smaller modulus. We call this process *consolidation*. We now illustrate how these two processes can be used to produce an incongruent one-dimensional covering system.

We start with $= s(0,1)$. We split this to give $s(0,1) = s(0,2) \cup s(1,2)$, split $s(1,2)$ to give $s(1,4) \cup s(3,4)$, and split $s(3,4)$ to give $s(3,12) \cup s(7,12) \cup s(11,12)$. This has produced the covering system

$$\{s(0,2), s(1,4), s(3,12), s(7,12), s(11,12)\}.$$

This is not incongruent. To make it so, we apply consolidation. We replace $s(3,12)$ with $s(3,3) = s(0,3)$ and $s(7,12)$ with $s(7,6) = s(1,6)$. By the lemmas, the resulting set

$$\{s(0,2), s(1,4), s(0,3), s(1,6), s(11,12)\}$$

is an incongruent covering system. Similar techniques have been used to construct incongruent covering systems with all moduli large, though the technical details then become spectacularly complicated [**3, 4**].

We now present results analogous to Lemmas 1 and 2 but applied to homogeneous congruences.

Lemma 3. *For any positive integers m and n, and any integers a and b,*

$$h(a,b,mn) \subseteq h(a,b,m).$$

Proof. If (x,y) satisfies

$$ax + by \equiv 0 \pmod{mn},$$

then (x,y) satisfies

$$ax + by \equiv 0 \pmod{m}. \qquad \square$$

Lemma 4. *If m_1 and m_2 are relatively prime, then*

$$h(a_1,b_1,m_1) \cap h(a_2,b_2,m_2) = h(\alpha,\beta,m_1m_2)$$

where $\alpha \equiv a_1 \pmod{m_1}$, $\alpha \equiv a_2 \pmod{m_2}$, $\beta \equiv b_1 \pmod{m_1}$, $\beta \equiv b_2 \pmod{m_2}$.

Proof. It is easy to check that (x, y) belongs to the homogeneous congruence on the right if and only if it belongs to both those on the left. □

Theorem 1. (a) *The collection of homogeneous congruences*

$$S = \{h(1, b, p^{\alpha+1}), h(0, 1, p^{\alpha+1}), \{h(1, b + jp^k, p^{\alpha+1}) : \\ 1 \le j < p, \qquad 0 \le k \le \alpha\}\}$$

covers $h(1, b, p^\alpha)$, *where* p *is a prime,* α *is a nonnegative integer and* b *is any integer.*

(b) *The collection* S *contains* $(\alpha + 1)(p - 1) + 2$ *homogeneous congruences. This is the least number of homogeneous congruences each having modulus* $p^{\alpha+1}$ *that will cover* $h(1, b, p^\alpha)$.

Proof. (a) Let $(x, y) \in h(1, b, p^\alpha)$. We will show that (x, y) belongs to a congruence in the collection S. We have

$$x + by = mp^\alpha$$

for some integer m. If $p \mid m$, then (x, y) belongs to $h(1, b, p^{\alpha+1})$ and we are done, so we suppose this does not occur. Write

$$y = p^\delta Y$$

where $p \nmid Y$, and choose $j \in \{1, \dots, p - 1\}$ such that

$$m + jY \equiv 0 \pmod{p}.$$

Then if $\delta > \alpha$ we have $(x, y) \in h(0, 1, p^{\alpha+1})$. Otherwise

$$\begin{aligned} x + (b + jp^{\alpha-\delta})y &= mp^\alpha + jp^{\alpha-\delta}p^\delta Y \\ &= p^\alpha(m + jY), \end{aligned}$$

which is divisible by $p^{\alpha+1}$. Thus, $(x, y) \in h(1, b + jp^{\alpha-\delta}, p^{\alpha+1})$ which is in S.

(b) Consider the set of ordered pairs

$$\{(p^\alpha, 0), (-b, 1), \{(-bp^i + mp^\alpha, p^i) : i = 0, \dots, \alpha, m = 1, \dots, p - 1\}\}.$$

Each of these belongs to $h(1, b, p^\alpha)$. We show that no two of them belong to the same homogeneous congruence with modulus $p^{\alpha+1}$. We prove this by contradiction. Suppose first that $(-bp^{i_1} + m_1 p^\alpha, p^{i_1})$ and $(-bp^{i_2} + m_2 p^\alpha, p^{i_2})$ are two members of the set above and that both belong to $h(\mu, \nu, p^{\alpha+1})$, and without loss of generality that $i_2 \geq i_1$. Then

$$\mu(-bp^{i_1} + m_1 p^\alpha) + \nu p^{i_1} \equiv 0 \pmod{p^{\alpha+1}}$$
$$\mu(-bp^{i_2} + m_2 p^\alpha) + \nu p^{i_2} \equiv 0 \pmod{p^{\alpha+1}}.$$

Note that p does not divide μ since this would require $p \mid \nu$, and we know μ, ν and $p^{\alpha+1}$ have no common factor.

After rearranging and multiplying the first congruence by $p^{i_2 - i_1}$ we get

$$(\nu - \mu b)p^{i_2} + \mu m_1 p^{\alpha + i_2 - i_1} \equiv 0 \pmod{p^{\alpha+1}}$$
$$(\nu - \mu b)p^{i_2} + \mu m_2 p^\alpha \equiv 0 \pmod{p^{\alpha+1}}.$$

Subtracting and dividing through by p^α gives $\mu(m_1 p^{i_2 - i_1} - m_2) \equiv 0 \pmod{p}$. Since p does not divide m_2 or μ, this implies $i_1 = i_2$ and $m_1 = m_2$.

Now suppose $(-bp^i + mp^\alpha, p^i)$ and $(p^\alpha, 0)$ both belong to $h(\mu, \nu, p^{\alpha+1})$. This requires that $p | \mu$ which is impossible unless $p | \nu$, but then μ, ν and $p^{\alpha+1}$ have p as a common factor which is not allowed.

Next suppose $(-bp^i + mp^\alpha, p^i)$ and $(-b, 1)$ both belong to $h(\mu, \nu, p^{\alpha+1})$. This leads to

$$p^i(\nu - \mu b) + \mu m p^\alpha \equiv 0 \pmod{p^{\alpha+1}}$$
$$\nu - \mu b \equiv 0 \pmod{p^{\alpha+1}},$$

which is impossible since $p \nmid m$.

Finally, suppose $(p^\alpha, 0)$ and $(-b, 1)$ both belong to $h(\mu, \nu, p^{\alpha+1})$. This would require both μ and ν being divisible by p which is not allowed.

Thus, each of the $(\alpha + 1)(p - 1) + 2$ ordered pairs belongs to a different homogeneous congruence, so we need this many homogeneous congruences to cover $h(1, b, p^\alpha)$. □

Corollary. *The homogeneous congruences $h(0, 1, p)$, $h(1, 0, p)$, $h(1, 1, p), \ldots, h(1, p - 1, p)$ cover $\mathbf{Z}^2$, and no smaller collection of homogeneous congruences with modulus p will do so.*

Proof. We note that $h(1,0,1) = \mathbf{Z}^2$ and apply the theorem using $\alpha = 0$. □

In Lemma 1 we saw that splitting an inhomogeneous congruence using the prime p introduced p new congruences, whereas in Theorem 1 we produce far more new congruences. This suggests that forming an incongruent system of homogeneous congruences will be more difficult than producing one with inhomogeneous congruences. However, the next theorem shows that the situation is not as bad as it seems.

Theorem 2. *If $\alpha \geq 1$, then the set of homogeneous congruences $\{h(1, b + jp^\alpha, p^{\alpha+1}), j = 0, \ldots, p-1\}$, together with any homogeneous congruence with modulus p covers $h(1, b, p^\alpha)$.*

Proof. Suppose $(x, y) \in h(1, b, p^\alpha)$ and that $(x, y) \notin h(1, b+jp^\alpha, p^{\alpha+1})$ for any $j, 0 \leq j < p$. That is,

$$x + by \equiv 0 \pmod{p^\alpha},$$

but

$$x + by + jp^\alpha y \not\equiv \pmod{p^{\alpha+1}}.$$

This is only possible if $p \mid y$ and hence $p \mid x$. In this case $(x, y) \in h(\mu, \nu, p)$ for any integers μ and ν, and the result follows. □

Remark. Equivalent results to Theorems 1 and 2 may be obtained for covering $h(b, 1, p^\alpha)$ with homogeneous congruences having modulus $p^{\alpha+1}$.

We now use these theorems to construct an incongruent covering system of homogeneous congruences. We use the operations of splitting and consolidation in the same way that they were used to produce covering systems of inhomogeneous congruences. Splitting replaces a homogeneous congruence with modulus m with a set of homogeneous congruences with modulus pm where p is a prime. If $m = 1$, we use the corollary and have $p + 1$ moduli. If $m > 1$ and $p \nmid m$, we use the

corollary with Lemma 4. If $p \mid m$, we use Theorem 2, combined with Lemma 4 if m is not a power of p. Consolidation uses Lemma 3 to replace a homogeneous congruence with modulus pm with one having modulus m.

We begin our system by splitting $\mathbf{Z}^2 = h(1,1,1)$ into $h(0,1,2), h(1,0,2)$ and $h(1,1,2)$. Then $h(0,1,2)$ is split into $h(0,1,4)$ and $h(2,1,4)$; then $h(0,1,4)$ is split into $h(0,1,8)$ and $h(4,1,8)$ and so on until we get $h(0,1,32)$ and $h(16,1,32)$. The first of these is then split into six congruences each having modulus 160, and these are consolidated to give congruences with moduli 5, 10, 20, 40, 80 and 160. Thus we cover $h(0,1,2)$ with homogeneous congruences having distinct moduli.

The homogeneous congruence $h(1,0,2)$ is then split into four congruences with modulus 6. These are successively split using the primes 2, 3 and 5 and finally consolidated to give homogeneous congruences with distinct moduli. The final system is shown in the table, from which the reader can trace the details of splitting and consolidation of the congruences covering $h(1,0,2)$.

TABLE 1. Homogeneous covering system.

$h(1,1,2)$	$=$	$h(1,1,2)$
$h(2,1,4)$	$=$	$h(2,1,4)$
$h(4,1,8)$	$=$	$h(4,1,8)$
$h(8,1,16)$	$=$	$h(8,1,16)$
$h(16,1,32)$	$=$	$h(16,1,32)$
$h(0,1,5)$	$=$	$h(0,1,5)$
$h(1,0,5) \cap h(0,1,2)$	$=$	$h(6,5,10)$
$h(1,1,5) \cap (0,1,4)$	$=$	$h(16,1,20)$
$h(1,2,5) \cap h(0,1,8)$	$=$	$h(16,17,40)$
$h(1,3,5) \cap h(0,1,16)$	$=$	$h(16,33,80)$
$h(1,4,5) \cap h(0,1,32)$	$=$	$h(96,129,160)$
$h(0,1,3)$	$=$	$h(0,1,3)$
$h(1,0,3) \cap h(1,0,2)$	$=$	$h(1,0,6)$

TABLE 1. Continued.

$h(1,1,3) \cap h(1,2,4)$	=	$h(1,10,12)$
$h(1,1,3) \cap h(1,4,8)$	=	$h(1,4,24)$
$h(1,1,3) \cap h(1,8,16)$	=	$h(1,40,48)$
$h(1,1,3) \cap h(1,0,5)$	=	$h(1,10,15)$
$h(1,1,3) \cap h(1,0,2) \cap h(1,1,5)$	=	$h(1,16,30)$
$h(1,1,3) \cap h(1,0,4) \cap h(1,2,5)$	=	$h(1,52,60)$
$h(1,1,3) \cap h(1,0,8) \cap h(1,3,5)$	=	$(1,88,120)$
$h(1,1,3) \cap h(1,0,16) \cap h(1,4,5)$	=	$h(1,64,240)$
$h(1,2,9)$	=	$h(1,2,9)$
$h(1,5,9) \cap h(1,0,2)$	=	$h(1,14,18)$
$h(1,8,9) \cap h(1,2,4)$	=	$h(1,26,36)$
$h(1,8,9) \cap h(1,4,8)$	=	$h(1,44,72)$
$h(1,8,9) \cap h(1,8,16)$	=	$h(1,8,144)$
$h(1,8,9) \cap h(1,0,5)$	=	$h(1,35,45)$
$h(1,8,9) \cap h(1,0,2) \cap (1,1,5)$	=	$h(1,26,90)$
$h(1,8,9) \cap h(1,0,4) \cap h(1,2,5)$	=	$h(1,152,180)$
$h(1,8,9) \cap h(1,0,8) \cap h(1,3,5)$	=	$h(1,8,360)$
$h(1,8,9) \cap h(1,0,16) \cap h(1,4,5)$	=	$h(1,224,720)$

Open questions. This system contains 31 homogeneous congruences. Cochrane and Myerson constructed a system containing 23. It would be interesting to know the least number of congruences that such a system need contain. I offer a price of \$100 for an incongruent system with 20 or fewer homogeneous congruences. We can also ask questions analogous to those asked by Erdös and Selfridge about inhomogeneous systems. Is there an incongruent homogeneous system with all moduli odd? It is likely to be extremely difficult to produce one, since nobody has been able to produce such an inhomogeneous system. It may be feasible to prove that none exists. I offer \$100 for either the construction of such a system or the proof of the impossibility of such a system. Finally we can ask for homogeneous systems with all moduli greater than some bound. The record for inhomogeneous systems in

Morikawa's [**4**] in which the smallest modulus is 24. I offer \$100 for a homogeneous system whose smallest modulus is at least 20.

Acknowledgment. Thanks to Gerry Myerson for his useful comments and corrections.

REFERENCES

1. Todd Cochrane and Gerry Myerson, *Covering congruences in higher dimensions*, Rocky Mountain J. Math. **26** (1996), 77–81.

2. Richard K. Guy, *Unsolved problems in number theory*, Second edition, Springer-Verlag, New York, 1994.

3. Ryozo Morikawa, *On a method to construct covering sets*, Bull. Fac. Liberal Arts Nagasaki Univ. **22** (1981), 1–12.

4. ———, *Some examples of covering sets*, Bull. Fac. Liberal Arts Nagasaki Univ. **21** (1981), 1–4.

5. Stefan Porubský, *Results and problems on covering systems of residue classes*, Mitt. Math. Sem. Giessen **150** 1981.

School of Mathematics and Statistics, Curtin University of Technology, PERTH, Western Australia
E-mail address: simpson@cs.curtin.edu.au