ON EXACT COVERINGS OF THE INTEGERS

BY

JOHN FRIEDLANDER

ABSTRACT

By an exact covering of modulus m, we mean a finite set of liner congruences $x \equiv a_i \pmod{m_i}$, $(i = 1,2,\dots,r)$ with the properties: (I) $m_i | m$, $(i = 1,2,\dots,r)$; (II) Each integer satisfies precisely one of the congruences. Let $\alpha \geqslant 0$, $\beta \geqslant 0$, be integers and let p and q be primes. Let $\mu(m)$ senote the Möbius function. Let $m = p^{\alpha} q^{\beta}$ and let $T(m)$ be the number of exact coverings of modulus m. Then, $T(m)$ is given recursively by

$$\sum_{d|m} \mu(d) \left(T\left(\frac{m}{d}\right)\right)^d = 1 .$$

1. Introduction

Several authors have considered different problems concerned with the covering of the integers by collections of congruences. In particular, we refer the reader to [1] and [2]. Many interesting questions have been raised and several are still unanswered. In this paper, a new problem is considered and various special cases are discussed.

Let m be a positive integer. We call a system of congruences

$$S: \begin{cases} x \equiv a_1(m_1) \\ x \equiv a_2(m_2) \\ \vdots \\ x \equiv a_r(m_r) \end{cases}$$

"a solution for m" if

Received March 22, 1972

I) $m_i \mid m$ $(i = 1, 2, \cdots r)$,

II) $0 \leqq a_i \leqq m_i - 1$ $(i = 1, 2, \cdots r)$,

III) Each integer n satisfies precisely one of the congruences.

We shall investigate the arithmetic function $T(m)$, the number of solutions for m. The main result obtained is

THEOREM A. *Let m be divisible by at most two distinct primes, say $m = p^{\alpha} q^{\beta}$ $(\alpha \geqq 0, \beta \geqq 0)$. Then*

$$\sum_{d \mid m} \mu(d) \left(T\left(\frac{m}{d} \right) \right)^{d} = 1$$

where μ denotes the Möbius function.

2. Some preliminaries

The first thing to notice is that the congruence $x \equiv 0\,(1)$ yields a solution for each m, which we shall call the trivial solution. Furthermore, it is clear that this is the only solution for $m = 1$. Hence, $T(1) = 1$.

The set of congruences

$$\begin{aligned} x &\equiv 0(m) \\ x &\equiv 1(m) \\ &\vdots \\ x &\equiv m-1(m) \end{aligned}$$

gives a solution for each m, which coincides with the trivial solution if and only if $m = 1$.

We shall call a set of congruences *redundant*, if it represents some integer more than once, and *incomplete*, if it fails to represent some integer.

Clearly the trivial solution is the only one for which there is an $m_i = 1$ because any congruence in addition to $x \equiv 0\,(1)$ would make the system redundant.

If m is a prime p, then it is clear that the two solutions mentioned above are the only ones. Hence, for any prime p, $T(p) = 2$.

Since $m_i \mid m$, then whenever $a \equiv b(m)$, a and b are covered by the same congruence in any solution S. Hence, it is sufficient to cover once each of the residue classes $\bmod m$.

Let $\mathscr{S}$ be the set of solutions for m. For $S \in \mathscr{S}$, we define $\mathscr{S}kS$, "the *skeleton* of S", to be the set of congruences of S for which m_i is a proper divisor of m.

If, for example, $m = 4$ and S is the solution

$$x \equiv 0(2)$$
$$x \equiv 1(4)$$
$$x \equiv 3(4)$$

then $\mathcal{S}kS$ is the congruence $x \equiv 0(2)$.

Given any irredundant set S' of congruences, for which the m_i are proper divisors of m, then there is clearly a unique solution S for m, such that $\mathcal{S}kS = S'$. Hence, the problem of evaluating $T(m)$ is just that of evaluating the number of irredundant sets for which $m_i \mid m$ properly, for all i.

3. Two simple examples

A) $m = p^2$

Apart from the trivial solution, the only possible values for m_i are p and p^2. Any subset of the residue classes mod p may be covered by their defining congruences, which then form the skeleton of a solution. Furthermore, all non-trivial solutions are found in this way.

Hence, $T(p^2) = 1 + 2^p$.

B) $m = p_1p_2$ $(p_1 \neq p_2)$

We first note that there can be no solution with $m_i = p_1$ and $m_j = p_2$. Such a set of congruences would be redundant by the Chinese Remainder Theorem. Hence, for any non-trivial solution S, either $m_i = p_1$ for all congruences in $\mathcal{S}kS$, or $m_i = p_2$ for all congruences in $\mathcal{S}kS$. There are 2^{p_2} of the first kind and 2^{p_1} of the second kind. Since the trivial solution has not been counted, and the solution $\mathcal{S}kS = \phi$ has been counted twice, hence

$$T(p_1p_2) = 2^{p_1} + 2^{p_2}.$$

4. A preliminary lemma

In this section we prove a lemma which will lead to Theorem A.

LEMMA. *Let $d \mid m$. The number of solutions for m, having all their moduli divisible by d, is $(T(m/d))^d$.*

PROOF. The cases $d = 1$ and $d = m$ are trivial and henceforth excluded.

Let $\mathcal{S}_d$ be the set of solutions for m such that $d \mid m_i$ for each i. Let $\mathcal{T}$ be the set of all solutions for m/d, and let $\mathcal{T}^d$ denote the Cartesian product of $\mathcal{T}$ with itself d times.

It suffices to find a bijection $\alpha: \mathcal{S}_d \to \mathcal{T}^d$. Let $S \in \mathcal{S}_d$. Since d divides each m_i, then whenever a and b are represented by the same congruence in S, we have $a \equiv b \pmod{d}$. Hence S may be split up into sets of congruences $S_i (i = 0, 1, \cdots, d-1)$ such that S_i represents precisely those integers $\equiv i \pmod{d}$, exactly once. Let S_i consist of the congruences

$$\begin{aligned} x &\equiv a_1(m_1) \\ &\vdots \\ x &\equiv a_r(m_r). \end{aligned}$$

Define T_i to be the set of congruences

$$\begin{aligned} x &\equiv b_1\left(\frac{m_1}{d}\right) \\ &\vdots \\ x &\equiv b_r\left(\frac{m_r}{d}\right) \end{aligned}$$

where $b_j = \dfrac{a_j - i}{d}$ $(j = 1, 2, \cdots, r)$.

Then $b_j \in Z$ since $a_j \equiv i(d)$ and $d \mid m_i$. Define α by,

$$\alpha(S) = (T_0, T_1, \cdots, T_{d-1}).$$

We shall show that α is indeed the required mapping.

A) $T_i \in \mathcal{T}$

PROOF. First we note that $m_j/d \mid m/d$ so that the congruences have allowable moduli. Suppose $x_0 \in Z$ is represented by two congruences in T_i, say

$$\begin{aligned} x_0 &\equiv b_1\left(\frac{m_1}{d}\right) \\ x_0 &\equiv b_2\left(\frac{m_2}{d}\right). \end{aligned}$$

Then

$$\frac{m_1}{d} \,\Big|\, x_0 - \frac{a_1 - i}{d}$$

so $m_1 \mid x_0 d - (a_1 - i)$ and similarly $m_2 \mid x_0 d - (a_2 - i)$. Hence

$$dx_0 + i \equiv \begin{cases} a_1(m_1) \\ a_2(m_2) \\ i(d) \end{cases}$$

which contradicts the irredundancy of S_i. Hence, T_i is irredundant. Let $x_0 \in Z$. Since S_i is complete for numbers $\equiv i(d)$, then $dx_0 + i$ is represented in S_i, say by.

$$dx_0 + i \equiv a_1(m_1).$$

Therefore $m_1 \mid dx_0 - (a_1 - i)$

$$\frac{m_1}{d} \Big| x_0 - \left(\frac{a_1 - i}{d}\right) .$$

Hence $x_0 \equiv b_1(m_1/d)$, so T_i is complete and $T_i \in \mathscr{T}$ $(i = 0, 1, \cdots, d-1)$.

B) α is injective

It is clearly sufficient to show that the map $\sigma: a_j \to b_j$ is injective for then so is the map: $S_i \to T_i$. Suppose

$$\frac{a_j - i}{d} \equiv \frac{a'_j - i}{d} \left(\operatorname{mod} \frac{m_j}{d}\right).$$

Then

$$a_j - i \equiv a'_j - i\ (m_j)$$

$$a_j \equiv a'_j(m_j)$$

and σ is injective.

C) α is surjective

First we note that distinct congruences in S_i are mapped onto distinct congruences in T_i. To see this, consider the two distinct congruences

$$x \equiv a_1(m_1)$$

$$x \equiv a_2(m_2).$$

If $m_1 \neq m_2$, then $m_1/d \neq m_2/d$. If $m_1 = m_2$ and we suppose $b_1 \equiv b_2(m_1/d)$, then

$$\frac{a_1 - i}{d} \equiv \frac{a_2 - i}{d} \left(\frac{m_1}{d}\right)$$

$$a_1 - i \equiv a_2 - i(m_1)$$

$$a_1 \equiv a_2(m_1)$$

and hence the result.

Now, let $(T_0, T_1, \cdots, T_{d-1}) \in \mathscr{T}^d$. Define S_i as a function of T_i by

$$a_j = i + db_j.$$

Since $d \mid m_j$ for all j, S_i can only represent integers $\equiv i(d)$. It is easy to show that if x_0 is represented by two congruences in S_i, then the corresponding two congruences in T_i would both represent $(x_0 - i)/d$. Furthermore, if $x_0 \equiv i(d)$, then x_0 is easily shown to be represented in S_i by the congruence corresponding to the one in T_i which represents $(x_0 - i)/d$. Thus α is surjective, and is our required bijection. This completes the proof of the lemma.

5. Some consequences of the lemma

COROLLARY 1. *Let m be a prime power, $m = p^n$ $(n \geqq 1)$. Then*

$$T(p^n) = 1 + (T(p^{n-1}))^p$$

PROOF. This follows immediately from the lemma by the observation that the trivial solution is the only one for which not all the m_i are divisible by p.

Example:

$$T(p) = 2$$

$$T(p^2) = 1 + 2^p$$

$$T(p^3) = 1 + (1 + 2^p)^p, \text{ etc.}$$

This corollary allows us to determine $T(p^n)$ inductively with much less work than the straightforward method.

COROLLARY 2. *Let $m = p^\alpha q^\beta$ $(\alpha \geqq 1, \beta \geqq 1)$. Then*

$$T(m) = \left(T\left(\frac{m}{p}\right)\right)^p + \left(T\left(\frac{m}{q}\right)\right)^q - \left(T\left(\frac{m}{pq}\right)\right)^{pq} + 1.$$

PROOF. In view of the Chinese Remainder Theorem, for any nontrivial solution. either $p \mid m_i$ for all i or $q \mid m_i$ for all i. By the lemma, there are $(T(m/p))^p$ of the first kind, and $(T(m/q))^q$ of the second kind. We have not yet counted the trivial solution, but we have counted twice those solutions for which all moduli are divisible by pq. Hence the result.

EXAMPLE. $m = p^2 q$

$$T(p^2 q) = (T(pq))^p + (T(p^2))^q - (T(p))^{pq} + 1$$

and these are in forms which we have already calculated.

Combining the two corollaries, we get Theorem A, a recursion formula which allows us to calculate $T(m)$, for all m divisible by no more than two distinct primes.

6. The general case

The general case seems to be considerably more complicated. In the case where m is divisible by at most two distinct primes, the Chinese Remainder Theorem ensured that any non-trivial solution had all its moduli divisible by a given prime p. This allowed us to utilize the lemma to determine a recursion formula for $T(m)$.

In the general case the above argument breaks down. Suppose that p_1, p_2, p_3 are distinct primes dividing m. Then, there is no reason why there should not be a solution containing $m_1 = p_2p_3$, $m_2 = p_3p_1$, $m_3 = p_1p_2$.

For example, take $m = 30$ and let $\mathscr{S}kS$ consist of the congruences

$$x \equiv 0(6)$$

$$x \equiv 3(10)$$

$$x \equiv 1(15).$$

Then $\mathscr{S}kS$ determines a solution S which is not adaptable to a reduction of the above type.

References

1. P. Erdös, *On a problem concerning congruences systems*, Mat. Lapok. 3 (1952), 122–128.
2. J. H. Jordan, *Convering classes of residues*, Canad. J. Math. 3 (19), (1967), 514–519.

The Pennsylvania State University
University Park, Pa. 16802