Constructions of Coverings of the Integers: Exploring an Erdős Problem

2008 Summer Math I
Cornell University

Juan Ortiz
jortiz@clunet.edu

Kristen Püschel
klp40@pitt.edu

Kelly Bickel
kelly.bickel@centre.edu

Michael Firrisa
mmfirrisa@smcm.edu

Introduction

A **covering of the integers** is a system of t linear congruences of the form $x \equiv b_i \pmod{m_i}$, such that $\forall\, i \leq t$, b_i and m_i are integral, $m_i > 1$, and for every integer $x \in \mathbb{Z}$, there is some $k \leq t$ such that $x \equiv b_k \,(mod\, m_k)$ For example, we have the following two sets of congruences:

$$\begin{aligned} x &\equiv 0 \pmod 2 \\ x &\equiv 1 \pmod 3 \\ x &\equiv 3 \pmod 4 \\ x &\equiv 5 \pmod 6 \\ x &\equiv 9 \pmod{12} \end{aligned} \qquad \begin{aligned} y &\equiv 1 \pmod 2 \\ y &\equiv 2 \pmod 4 \\ y &\equiv 4 \pmod 6 \\ y &\equiv 0 \pmod 8 \\ y &\equiv 0 \pmod{12} \\ y &\equiv 20 \pmod{24} \end{aligned}$$

Coverings with the Fewest Congruences

Lemma 1 *Let a set S of t congruences of the form $x \equiv b_i \,(mod\, m_i)$ be a minimal covering. If a prime p divides M, where $M = LCM(m_1, m_2, ..., m_t)$, then $t > p$.*

Lemma 2 *Let a set S of t congruences of the form $x \equiv b_i \,(mod\, m_i)$ be a minimal covering. If a prime p divides some modulus m_i, p is a divisor of at least p moduli.*

Theorem 3 *There are no coverings that contain only two, three, or four distinct moduli. Moreover, $\{2, 3, 4, 6, 12\}$ is the only set of moduli that can be used to form a covering with exactly five congruences.*

Candidates for LCMs

Consider the **LCM** (Least Common Multiple) of the moduli, and let $LCM(m_1...m_t) = M$. Then, a set S is a covering if and only if every $r \in \mathbb{z}_M$ is satisfied by one of the congruences.

Lemma 4 *If a set S is a covering and $LCM(m_1...m_t) = M$, then M is not a product of two or three distinct primes.*

By Lemmas **1, 2, 4,** the only candidates less than 50 for the LCMs of a covering are 12, 24, 36, and 48.

Lemma 5 *If a set S is a system of t congruences and $LCM(m_1...m_t) = M$, then S is not a covering if the sum of the reciprocals $\frac{1}{m_i}$ is less than 1, where $i \leq t$.*

"What is the largest natural number N such that there exists a covering system of the integers with distinct moduli all greater than or equal to N ?"

An Erdős Question: Mathematician Paul Erdős posed the above question. He conjectured that N could be arbitrarily large but could not prove it. He offered $500 for a proof or disproof of his hypothesis. This question has motivated our research.

Methods

Covering a Single Congruence

Theorem 6 *If there is a covering of the integers:*

$$\begin{aligned} x_1 &\equiv b_1 \pmod{m_1} \\ x_2 &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x_t &\equiv b_t \pmod{m_t} \end{aligned}$$

then the congruence $x \equiv B \pmod{\hat{M}}$ can be covered by the following system of congruences:

$$\begin{aligned} x_1 &\equiv B + b_1 \cdot \hat{M} \pmod{m_1 \cdot \hat{M}} \\ x_2 &\equiv B + b_2 \cdot \hat{M} \pmod{m_2 \cdot \hat{M}} \\ &\vdots \\ x_t &\equiv B + b_t \cdot \hat{M} \pmod{m_t \cdot \hat{M}} \end{aligned}$$

A particularly convenient covering of the integers only has moduli of the form $2^k \cdot p \cdot \hat{M}$, where p is a prime. Thus we can doubly use congruences whose moduli are divisible by the highest power of 2 in the system, as there are equivalent distinct coverings of these single congruences.

Finding Coverings with Large Least Moduli

We start by trying to find a covering with distinct moduli all greater than or equal to N, by hand. The process becomes difficult for $N \geq 5$. As a result, we write a greedy algorithm program (KN-program) that finds coverings. The KN-program tries to find a covering that use only the divisors of M, where M is the lcm of the moduli. The KN-program finds these linear congruences by looking at each modulus, m_n, one by one and choosing the residue, r_n, where $0 \leq r_n \leq m_n - 1$ that covers the most remaining integers 1 through k.

Results

Using the KN-program we found a system of linear congruences where the least modulus used was 11.

Least Modulus	LCM	Congruences	Prime Decomposition	$\sum \frac{1}{m_i}$
2	12	5	$2^2 \cdot 3$	1.3333
3	120	14	$2^3 \cdot 3 \cdot 5$	1.5000
3**	360	21	$2^3 3^2 \cdot 5$	1.7389
4	720	24	$2^4 3^2 \cdot 5$	1.5167
4**	10,800	55	$2^4 3^3 5^2$	1.7184
5*	720	29	$2^4 3^2 \cdot 5$	1.3778
5	4,320	43	$2^5 3^3 \cdot 5$	1.4164
5**	15,120	58	$2^4 3^3 \cdot 5 \cdot 7$	1.8289
6*	1,260	42	$2^2 3^2 \cdot 5 \cdot 7$	1.4286
7*	5,040	63	$2^4 3^2 \cdot 5 \cdot 7$	1.5111
7	30,240	81	$2^5 3^3 \cdot 5 \cdot 7$	1.5485
8*	45,360	83	$2^4 3^4 \cdot 5 \cdot 7$	1.4956
9*	226,800	163	$2^4 3^4 5^2 \cdot 7$	1.5159
10*	997,920	236	$2^5 3^4 \cdot 5 \cdot 7 \cdot 11$	1.6404
11*	21,621,600	275	$2^5 3^3 5^2 \cdot 7 \cdot 11 \cdot 13$	1.9791

* moduli with largest powers of 2, doubly used, ** linear congruences found by hand

References

[1] Guy, Richard K.,*On Unsolved Problems in Number Theory* (2nd Ed.), Springer-Verlag, New York, 1994.

[2] Jones, G. and J. Jones, *Elementary Number Theory*, Springer Verlag, London, 2003.

This was a learning by discovery project. Due to the discovery aspect, we only consulted the literature after we concluded our explorations. In some instances, our results have appeared in print, or are awaiting publication.

Acknowledgements

With thanks to the Summer Math Institute, Cornell University Math Department, the Center for Applied Math, the National Science Foundation, and Drs. Mark Kozek and Ravi Ramakrishna.