Constructions of Coverings of the Integers:
Exploring an Erdős Problem

2008 Summer Math I
Cornell University

Juan Ortiz
jortiz@clunet.edu

Kristen Püscher
klp40@pitt.edu

Kelly Bickel
kelly.bickel@centre.edu

Michael Firrissa
mmfirrissa@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 \( \forall 1 \leq i \leq t \), and \( m_i \) are integral, \( m_i > 1 \), and for every integer \( x \in \mathbb{Z} \), there is some \( k \leq t \) such that \( x \equiv b_k \pmod{m_k} \). For example, we have the following two sets of congruences:

\[
\begin{align*}
x & \equiv 0 \pmod{2} \\
x & \equiv 1 \pmod{2} \\
x & \equiv 1 \pmod{3} \\
x & \equiv 2 \pmod{4} \\
x & \equiv 3 \pmod{4} \\
x & \equiv 4 \pmod{6} \\
x & \equiv 5 \pmod{6} \\
x & \equiv 9 \pmod{12} \\
x & \equiv 18 \pmod{24}
\end{align*}
\]

Coverings with the Fewest Congruences

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

**Lemma 2** Let a set \( S \) of \( t \) congruences of the form \( x \equiv b_i \pmod{m_i} \) 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 \( \text{LCM}(m_1 \cdots m_t) = M \). Then, a set \( S \) is a covering if and only if every \( r \in \mathbb{Z} \) satisfies one of the congruences.

**Lemma 4** If a set \( S \) is a covering and \( \text{LCM}(m_1 \cdots m_t) = M \), 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 \( \text{LCM}(m_1 \cdots m_t) = M \), 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:

\[
\begin{align*}
x_i & \equiv b_i \pmod{m_i} \\
x_j & \equiv b_j \pmod{m_j} \\
& \quad \vdots \\
x_k & \equiv b_k \pmod{m_k}
\end{align*}
\]

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

\[
\begin{align*}
x_i & \equiv B + b_i \cdot M \pmod{m_i \cdot M} \\
x_j & \equiv B + b_j \cdot M \pmod{m_j \cdot M} \\
& \quad \vdots \\
x_k & \equiv B + b_k \cdot M \pmod{m_k \cdot M}
\end{align*}
\]

A particularly convenient covering of the integers only has moduli of the form \( 2^k \cdot p \cdot M \), 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 \( N > 5 \). As a result, we write a greedy algorithm program (KN-program) that finds coverings. The KN-program tries to find a covering that uses 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, \( m_i \), one by one and choosing the residue, \( r_m \), where \( 0 \leq r_m \leq m_i - 1 \) 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.

<table>
<thead>
<tr>
<th>Least Modulus</th>
<th>LCM</th>
<th>Coverings</th>
<th>Prime Decomposition</th>
<th>( \sum )</th>
</tr>
</thead>
<tbody>
<tr>
<td>2</td>
<td>12</td>
<td>4</td>
<td>2 \cdot 3 \cdot 7</td>
<td>1.375</td>
</tr>
<tr>
<td>3</td>
<td>12</td>
<td>4</td>
<td>2 \cdot 3 \cdot 7</td>
<td>1.200</td>
</tr>
<tr>
<td>4*</td>
<td>20</td>
<td>5</td>
<td>2 \cdot 5^2 \cdot 3</td>
<td>1.789</td>
</tr>
<tr>
<td>5</td>
<td>20</td>
<td>5</td>
<td>2 \cdot 5^2 \cdot 3</td>
<td>1.557</td>
</tr>
<tr>
<td>6</td>
<td>30</td>
<td>6</td>
<td>2 \cdot 3 \cdot 5 \cdot 7</td>
<td>1.195</td>
</tr>
<tr>
<td>7</td>
<td>42</td>
<td>6</td>
<td>2 \cdot 3 \cdot 5 \cdot 7</td>
<td>1.8289</td>
</tr>
<tr>
<td>8</td>
<td>56</td>
<td>6</td>
<td>2 \cdot 3 \cdot 5 \cdot 7</td>
<td>1.4296</td>
</tr>
<tr>
<td>9</td>
<td>63</td>
<td>6</td>
<td>2 \cdot 3 \cdot 5 \cdot 7</td>
<td>1.511</td>
</tr>
<tr>
<td>10*</td>
<td>90</td>
<td>6</td>
<td>2 \cdot 3 \cdot 5 \cdot 7</td>
<td>1.5405</td>
</tr>
<tr>
<td>11*</td>
<td>111</td>
<td>6</td>
<td>2 \cdot 3 \cdot 5 \cdot 7</td>
<td>1.6944</td>
</tr>
<tr>
<td>12</td>
<td>120</td>
<td>6</td>
<td>2 \cdot 3 \cdot 5 \cdot 7</td>
<td>1.9791</td>
</tr>
</tbody>
</table>

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

References

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 Kozeck and Ravi Ramakrishna.