Constructions of Coverings of the Integers

Exploring an Erdős Problem

K. Bickel, M. Firrisa, J.P. Ortiz, and K. Püschel

Cornell University
Summer Math Institute 2007

August 1, 2008

Acknowledgements

With Thanks to:

- The Summer Math Institute
- Cornell University Math Department
- The Center for Applied Math
- The National Science Foundation
- Dr. Mark Kozek (Whittier College)
- Dr. Ravi Ramakrishna (Cornell University)
- Alexandre Roch (Cornell University)

The Motivating Question

"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?"

Conjecture (Erdős)

For all $n \in \mathbb{N}$ there exists a covering with distinct moduli all greater than or equal to n.

The Motivating Question

"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?"

Conjecture (Erdős)

For all $n \in \mathbb{N}$ there exists a covering with distinct moduli all greater than or equal to n.

Defining a Covering

We start with a few terms:

- Given $m \in \mathbb{N}$, we say two integers a and b are **congruent mod** m if $a - b$ is divisible by m and write:

$$a \equiv b \pmod{m} \tag{1}$$

- We also use the variable form of (1), called a **linear congruence**, which is written:

$$x \equiv b \pmod{m},$$

where x is an unknown integer.

- A **covering of the integers** is a system of n linear congruences of the form $b_i \pmod{m_i}$, such that for every $x \in \mathbb{Z}$, there is some $k \leq n$ such that

$$x \equiv b_k \pmod{m_k}.$$

Defining a Covering

We start with a few terms:

- Given $m \in \mathbb{N}$, we say two integers a and b are **congruent mod** m if $a - b$ is divisible by m and write:

$$a \equiv b \pmod{m} \tag{1}$$

- We also use the variable form of (1), called a **linear congruence**, which is written:

$$x \equiv b \pmod{m},$$

where x is an unknown integer.

- A **covering of the integers** is a system of n linear congruences of the form $b_i \pmod{m_i}$, such that for every $x \in \mathbb{Z}$, there is some $k \leq n$ such that

$$x \equiv b_k \pmod{m_k}.$$

Defining a Covering

We start with a few terms:

- Given $m \in \mathbb{N}$, we say two integers a and b are **congruent mod** m if $a - b$ is divisible by m and write:

$$a \equiv b \pmod{m} \tag{1}$$

- We also use the variable form of (1), called a **linear congruence**, which is written:

$$x \equiv b \pmod{m},$$

  where x is an unknown integer.
- A **covering of the integers** is a system of n linear congruences of the form $b_i \pmod{m_i}$, such that for every $x \in \mathbb{Z}$, there is some $k \leq n$ such that

$$x \equiv b_k \pmod{m_k}.$$

Covering Example 1

- Recall: A **covering of the integers** is a system of linear congruences $b_i \pmod{m_i}$ such that for every integer x, $x \equiv b_k \pmod{m_k}$ for some $k \leq n$.
- An example is:

$$x \equiv 0 \pmod{2} \tag{2}$$
$$x \equiv 1 \pmod{2} \tag{3}$$

- All even integers satisfy congruence (2) and all odd integers satisfy congruence (3).

Covering Example 1

- Recall: A **covering of the integers** is a system of linear congruences $b_i \pmod{m_i}$ such that for every integer x, $x \equiv b_k \pmod{m_k}$ for some $k \leq n$.
- An example is:

$$x \equiv 0 \pmod{2} \tag{2}$$
$$x \equiv 1 \pmod{2} \tag{3}$$

- All even integers satisfy congruence (2) and all odd integers satisfy congruence (3).

Verifying a Covering

- We need some finite set E such that if every element $e \in E$ is satisfied by some congruence in S, then we know S covers the integers
- It is sufficient to consider the set $\mathbb{Z}_M$, where $M = \text{lcm}(m_1, m_2, ..., m_n)$.
- To check if S is a covering, we can just check that given $r \in \mathbb{Z}_M$, there is some $i \leq n$ such that:

$$r \equiv b_i \pmod{m_i}.$$

Verifying a Covering

- We need some finite set E such that if every element $e \in E$ is satisfied by some congruence in S, then we know S covers the integers
- It is sufficient to consider the set $\mathbb{Z}_M$, where $M = \text{lcm}(m_1, m_2, ..., m_n)$.
- To check if S is a covering, we can just check that given $r \in \mathbb{Z}_M$, there is some $i \leq n$ such that:

$$r \equiv b_i \pmod{m_i}.$$

Verifying a Covering

- We need some finite set E such that if every element $e \in E$ is satisfied by some congruence in S, then we know S covers the integers
- It is sufficient to consider the set $\mathbb{Z}_M$, where $M = \text{lcm}(m_1, m_2, ..., m_n)$.
- To check if S is a covering, we can just check that given $r \in \mathbb{Z}_M$, there is some $i \leq n$ such that:

$$r \equiv b_i \pmod{m_i}.$$

Covering Example 2

Let's consider the following set of congruences with moduli $\{2, 3, 4, 6, 12\}$:

$$x \equiv 0 \pmod 2$$
$$x \equiv 1 \pmod 3$$
$$x \equiv 3 \pmod 4$$
$$x \equiv 5 \pmod 6$$
$$x \equiv 9 \pmod{12}$$

Because $\text{lcm}\{2, 3, 4, 6, 12\} = 12$, to determine if this set covers the integers, we check whether our congruences cover the set Z_{12}.

Checking the Covering

We have $\mathbb{Z}_{12} = \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11\}$. By below, each $r \in \mathbb{Z}_{12}$ is satisfied by one of the congruences.

$$\begin{aligned} x &\equiv 0 \pmod 2 && \{0, 2, 4, 6, 8, 10\} \\ x &\equiv 1 \pmod 3 && \{1, 4, 7, 10\} \\ x &\equiv 3 \pmod 4 && \{3, 7, 11\} \\ x &\equiv 5 \pmod 6 && \{5, 11\} \\ x &\equiv 9 \pmod{12} && \{9\} \end{aligned}$$

Therefore, this set of congruences is a covering.

Remarks about Coverings

Remark 1

Let S be a system of n linear congruences of the form $b_i \pmod{m_i}$, and let $M = \text{lcm}(m_1, m_2, ..., m_n)$. Then, the maximum number of $r \in \mathbb{Z}_M$ that can be covered by S is given by

$$\sum_{i=1}^{n} \frac{M}{m_i}.$$

S is not a covering if

$$\sum_{i=1}^{n} \frac{M}{m_i} < M \quad \text{or, equivalently, if} \quad \sum_{i=1}^{n} \frac{1}{m_i} < 1.$$

Remarks about Coverings (cont.)

Remark 2

Let S be a system of n linear congruences of the form $b_i \pmod{m_i}$, and let $M = \text{lcm}(m_1, m_2, ..., m_n)$. The maximum distinct number of elements of $\mathbb{Z}_M$ that can be covered by two relatively prime moduli m_1, m_2 is given by:

$$Max = \frac{M}{m_1} + \frac{M}{m_2} - \frac{M}{m_1 \cdot m_2}.$$

This follows from the Chinese Remainder Theorem, which tells us that $\frac{M}{m_1 \cdot m_2}$ elements of $\mathbb{Z}_M$ will simultaneously satisfy each $b_1 \pmod{m_1}$ and $b_2 \pmod{m_2}$, for any integers b_1 and b_2.

Applications of Coverings

- Erdős disproved de Polignac's Conjecture that: For every sufficiently large odd number $k \in \mathbb{Z}$, there exists an $n \in \mathbb{N}$ and a prime p such that
$$k = 2^n + p.$$
- Sierpinski proved that there are an infinite number of odd numbers j such that:
$$j \cdot 2^n + 1 \text{ is composite for all } n \in \mathbb{N}.$$
- Schinzel equated two questions:

"Is there some $f(x) \in \mathbb{Z}[x]$ such that $f(x) \cdot x^n + 1$ is reducible for all $n \in \mathbb{N}$?" and

"Is there a finite covering of the integers that uses only distinct odd moduli?"

Applications of Coverings

- Erdős disproved de Polignac's Conjecture that: For every sufficiently large odd number $k \in \mathbb{Z}$, there exists an $n \in \mathbb{N}$ and a prime p such that
$$k = 2^n + p.$$
- Sierpinski proved that there are an infinite number of odd numbers j such that:
$$j \cdot 2^n + 1 \text{ is composite for all } n \in \mathbb{N}.$$
- Schinzel equated two questions:

"Is there some $f(x) \in \mathbb{Z}[x]$ such that $f(x) \cdot x^n + 1$ is reducible for all $n \in \mathbb{N}$?" and

"Is there a finite covering of the integers that uses only distinct odd moduli?"

Applications of Coverings

- Erdős disproved de Polignac's Conjecture that: For every sufficiently large odd number $k \in \mathbb{Z}$, there exists an $n \in \mathbb{N}$ and a prime p such that
$$k = 2^n + p.$$
- Sierpinski proved that there are an infinite number of odd numbers j such that:
$$j \cdot 2^n + 1 \text{ is composite for all } n \in \mathbb{N}.$$
- Schinzel equated two questions:

  "Is there some $f(x) \in \mathbb{Z}[x]$ such that $f(x) \cdot x^n + 1$ is reducible for all $n \in \mathbb{N}$?" and

  "Is there a finite covering of the integers that uses only distinct odd moduli?"

Questions We will Consider

Preliminary Questions:

1. What is the form of the lcm of a covering's moduli?
2. What is fewest number of congruences that a covering can have?

Primary Discussion:

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?

Questions We will Consider

Preliminary Questions:

1. What is the form of the lcm of a covering's moduli?
2. What is fewest number of congruences that a covering can have?

Primary Discussion:

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?

Which numbers qualify to be the lcm of the moduli of a covering?

The Form of the lcm of a Covering's Moduli

Theorem *: The lcm of distinct moduli for a covering of the integers is never of the form $k = p^n$ where k is the lcm, p is a prime and n is a natural number

Proof.

- The distinct moduli are $p, p^2, \ldots, p^n$. The most integers that any modulus can cover is $\frac{1}{p^i}$ where i is an element of $1, 2, ..., n$.
- The congruence covers at most $\frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + ... + \frac{1}{p^n}$
- However, $\frac{1}{p} + \frac{1}{p^2} + \frac{1}{p^3} + ... + \frac{1}{p^n} < 1$.
- Thus moduli with an lcm of p^n do not cover all the integers. □

The Form of the lcm of a Covering's Moduli

Theorem *: The lcm of distinct moduli for a covering of the integers is never of the form $k = pq$ where k is the lcm, p, q are distinct primes.

Proof.

- W.L.O.G., let $2 \leq p < q$, with distinct moduli being at most p, q, and pq.
- Since p and q are distinct primes

$$n \equiv x_p \mod p, n \equiv x_q \mod q$$

  has a unique solution, x_0, modulo pq.
- Hence $x_0 \equiv \ mod\ pq$ gets covered twice.
- U.B for residues covered is $\frac{1}{p} + \frac{1}{q} + \frac{1}{pq} - \frac{1}{pq} = \frac{1}{p} + \frac{1}{q} < \frac{2}{p} \leq 1$. Therefore pq is not the lcm of a covering

The Form of the lcm of a Covering's Moduli

Theorem *: The lcm of distinct moduli for a covering of the integers is never of the form $k = p_1 p_2 p_3$ where k is the lcm, p_1, p_2, p_3 are distinct primes.

- We used similar techiques to prove this theorem, but we had to break it up into a general case and a special case.
- $2, 3, 5$ actually give an upper bound of 1, which is inconclusive.
- We managed to prove at least one other overlap by showing how the residues $\pmod 2$, $\pmod 6$, $\pmod{10}$ behaved in relation to each other.

The Form of the lcm of a Covering's Moduli

- We made a conjecture that M cannot be the product of n distinct primes. However, we were quickly proven wrong when we found a covering using 210 as our lcm, 210 being the product of $2 \cdot 3 \cdot 5 \cdot 7$
- We made the observation that for k product of four distinct primes, our argument that k cannot be the lcm of a covering still worked as long as we removed 2 from our list of primes.
- Revised Conjecture: The lcm of distinct moduli for a covering of the integers is never of the form $k = p_1 p_2 p_3 ... p_n$ where k is the lcm, $p_1, p_2, p_3, ..., p_n$ are distinct primes and none of them can be 2.
- If we find a counterexample to this conjecture, we will have solved Erdos' problem of all odd moduli.

The Form of the lcm of a Covering's Moduli

- We made a conjecture that M cannot be the product of n distinct primes. However, we were quickly proven wrong when we found a covering using 210 as our lcm, 210 being the product of $2 \cdot 3 \cdot 5 \cdot 7$
- We made the observation that for k product of four distinct primes, our argument that k cannot be the lcm of a covering still worked as long as we removed 2 from our list of primes.
- Revised Conjecture: The lcm of distinct moduli for a covering of the integers is never of the form $k = p_1 p_2 p_3 ... p_n$ where k is the lcm, $p_1, p_2, p_3, ..., p_n$ are distinct primes and none of them can be 2.
- If we find a counterexample to this conjecture, we will have solved Erdos' problem of all odd moduli.

The Form of the lcm of a Covering's Moduli

- We made a conjecture that M cannot be the product of n distinct primes. However, we were quickly proven wrong when we found a covering using 210 as our lcm, 210 being the product of $2 \cdot 3 \cdot 5 \cdot 7$
- We made the observation that for k product of four distinct primes, our argument that k cannot be the lcm of a covering still worked as long as we removed 2 from our list of primes.
- Revised Conjecture: The lcm of distinct moduli for a covering of the integers is never of the form $k = p_1 p_2 p_3 ... p_n$ where k is the lcm, $p_1, p_2, p_3, ..., p_n$ are distinct primes and none of them can be 2.
- If we find a counterexample to this conjecture, we will have solved Erdos' problem of all odd moduli.

What is the fewest number of congruences a covering can have?

- What is the fewest number of congruences in a covering?
- Lemma 1. Let S be a system of n congruences such that S is a minimal covering. If a prime p divides M, where M is the lcm of the moduli, then $p < n$.
- Lemma 2. Let S be a system of n congruences such that S is a minimal covering. If a prime p divides m_i, where m_i is a modulus in S. Then there are at least p moduli which are divisible by p

What is the fewest number of congruences a covering can have?

- What is the fewest number of congruences in a covering?
- Lemma 1. Let S be a system of n congruences such that S is a minimal covering. If a prime p divides M, where M is the lcm of the moduli, then $p < n$.
- Lemma 2. Let S be a system of n congruences such that S is a minimal covering. If a prime p divides m_i, where m_i is a modulus in S. Then there are at least p moduli which are divisible by p

What is the fewest number of congruences a covering can have?

- What is the fewest number of congruences in a covering?
- Lemma 1. Let S be a system of n congruences such that S is a minimal covering. If a prime p divides M, where M is the lcm of the moduli, then $p < n$.
- Lemma 2. Let S be a system of n congruences such that S is a minimal covering. If a prime p divides m_i, where m_i is a modulus in S. Then there are at least p moduli which are divisible by p

What is the fewest number of congruences a covering can have?

- Theorem *: There is no covering of the integers using only two congruences.
- Theorem *: There is no covering of the integers using only three congruences.

What is the fewest number of congruences a covering can have?

Theorem **: There is no covering of the integers using only four congruences.

Observations:

- Moduli can't all be powers of two, or three. The sum of reciprocals will be less than 1.
- We need four numbers such that at least three are divisible by 3 and at least two are divisible by 2.
- 2 must be one of our moduli, otherwise $(3, 4, 6, 9)$ is the smallest yet inadequate option.
- The smallest set of moduli containing 2 and 3 are $(2, 3, 6, 9)$ which despite noble attempt, fails.
- The amalgamation of these facts leads to the proof for Theorem **.

What is the fewest number of congruences a covering can have?

Theorem: There is a unique covering of the integers using only five congruences.

Observations:

- We first show that 2 must be a modulus by testing $(3, 4, 6, 8, 9)$, which fails.
- One of $(3, 4)$ must also be a modulus by a similar argument used for 2.
- By assuming 3 is one of our moduli and 4 is not, we show 6 must be a modulus. We then show this leads to 4 having to be a modulus. If we had assumed 4 instead, we get 3 having to be a modulus, thus both 3 and 4 have to be moduli.
- Eventually we show that $6, 12$ are the only possibilities left for the last two moduli.

What is the fewest number of congruences a covering can have?

$$x \equiv b_1 \pmod 2$$
$$x \equiv b_2 \pmod 3$$
$$x \equiv b_3 \pmod 4$$
$$x \equiv b_4 \pmod 6$$
$$x \equiv b_5 \pmod{12},$$

A note of caution, you have to choose each b_i responsibly. Depending on your residues, this might not be a covering.

"Almost Covering": What We Mean

When trying to construct a covering, if we run out of distinct factors of the lcm with which to write congruences, we call the system we have an "almost covering," if most residues are covered.

Example 1: A Simple "Almost Covering"

We wish to find a covering of the integers with lcm of 8.

There are 3 available moduli:$\{2, 4, 8\}$.

Residue System, $\mathbb{Z}$ (mod 8):

$$\begin{array}{cccc} 0 & 1 & 2 & 3 \\ 4 & 5 & 6 & 7 \end{array}$$

Example 1: A Simple "Almost Covering"

Consider the system of congruences with lcm 8:

$$x \equiv 1 \pmod 2$$

Residue System: $\mathbb{Z} \pmod 8$

0	x	2	x
4	x	6	x

Example 1: A Simple "Almost Covering"

Consider the system of congruences with lcm 8:

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 4$$

Residue System: $\mathbb{Z} \pmod 8$

0	x	x	x
4	x	x	x

Example 1: A Simple "Almost Covering"

Consider the system of congruences with lcm M = 8:

$$x \equiv 1 \pmod 2$$
$$x \equiv 2 \pmod 4$$
$$x \equiv 4 \pmod 8$$

Residue System: $\mathbb{Z} \pmod 8$

0	x	x	x
x	x	x	x

Example 2: "Almost Covering" Through Less-than-Optimal Covering Efficiency

This 27-member system covers all but one element of $\mathbb{Z}$ (mod 720).

1 (mod 4)	1 (mod 5)	2 (mod 6)	3 (mod 8)
1 (mod 9)	2 (mod 10)	6 (mod 12)	4 (mod 15)
7 (mod 16)	4 (mod 18)	8 (mod 20)	12 (mod 24)
10 (mod 30)	3 (mod 36)	7 (mod 40)	43 (mod 45)
47 (mod 48)	24 (mod 60)	15 (mod 72)	15 (mod 80)
30 (mod 90)	39 (mod 120)	24 (mod 144)	60 (mod 180)
63 (mod 240)	103 (mod 360)	360 (mod 720)	0 (mod 720)

Computationally, "almost coverings" also arise when congruences are not used most efficiently. This set of moduli, with a reassignment of residues, CAN cover the integers.

Beginning Problem...

Problem:Can we find a system of congruences

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_n} \end{aligned}$$

such that (i) every integer satisfying $x \equiv 0 \pmod{720}$ also satisfies at least one of the congruences in our system, and (ii) all moduli are greater than 720?

Statement of the Problem

Problem: When considering a linear congruence, $x \equiv \mathcal{B} \pmod{\mathcal{M}}$, can we find a system of congruences

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ x &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x &\equiv b_n \pmod{m_n} \end{aligned}$$

such that every integer satisfying $x \equiv \mathcal{B} \pmod{\mathcal{M}}$ also satisfies at least one of the congruences in our system?

Coverings of $\mathbb{Z}$ Converted to Coverings of $\mathcal{B} \pmod{\mathcal{M}}$

Theorem

If the following system covers $\mathbb{Z}$:

$$\begin{aligned} x_1 &\equiv b_1 \pmod{m_1} \\ x_2 &\equiv b_2 \pmod{m_2} \\ &\vdots \\ x_n &\equiv b_n \pmod{m_n} \end{aligned}$$

then arbitrary congruence $x \equiv \mathcal{B} \pmod{\mathcal{M}}$ is covered by:

$$\begin{aligned} x_1 &\equiv \mathcal{B} + b_1 \cdot \mathcal{M} \pmod{m_1 \cdot \mathcal{M}} \\ x_2 &\equiv \mathcal{B} + b_2 \cdot \mathcal{M} \pmod{m_2 \cdot \mathcal{M}} \\ &\vdots \\ x_n &\equiv \mathcal{B} + b_n \cdot \mathcal{M} \pmod{m_n \cdot \mathcal{M}} \end{aligned}$$

Proof

Covering $x \equiv \mathcal{B} \pmod{\mathcal{M}} \Rightarrow \ \forall\ y \in \mathbb{Z},\ \mathcal{B} + \mathcal{M}y$ satisfies one of the congruences in our system.

We take $y \in \mathbb{Z}$ arbitrary. Does $\exists\ i = 1, 2, ..., n$, such that $\mathcal{B} + \mathcal{M}y$ satisfies one of the congruences?

$$\mathcal{B} + \mathcal{M}y \equiv \quad \mathcal{B} + b_i \cdot \mathcal{M} \quad \pmod{m_i \cdot \mathcal{M}}$$

Proof

Covering $x \equiv \mathcal{B} \pmod{\mathcal{M}} \Rightarrow \forall\ y \in \mathbb{Z},\ \mathcal{B} + \mathcal{M}y$ satisfies one of the congruences in our system.

We take $y \in \mathbb{Z}$ arbitrary. Does $\exists\ i = 1, 2, ..., n$, such that $\mathcal{B} + \mathcal{M}y$ satisfies one of the congruences?

$$\begin{aligned} \mathcal{B} + \mathcal{M}y &\equiv \mathcal{B} + b_i \cdot \mathcal{M} \pmod{m_i \cdot \mathcal{M}} \\ \mathcal{M}y &\equiv b_i \cdot \mathcal{M} \pmod{m_i \cdot \mathcal{M}} \end{aligned}$$

Proof

Covering $x \equiv \mathcal{B} \pmod{\mathcal{M}} \Rightarrow \ \forall\ y \in \mathbb{Z},\ \mathcal{B} + \mathcal{M}y$ satisfies one of the congruences in our system.

We take $y \in \mathbb{Z}$ arbitrary. Does $\exists\ i = 1, 2, ..., n$, such that $\mathcal{B} + \mathcal{M}y$ satisfies one of the congruences?

$$\begin{aligned} \mathcal{B} + \mathcal{M}y &\equiv \mathcal{B} + b_i \cdot \mathcal{M} \pmod{m_i \cdot \mathcal{M}} \\ \mathcal{M}y &\equiv b_i \cdot \mathcal{M} \pmod{m_i \cdot \mathcal{M}} \\ y &\equiv b_i \pmod{m_i} \end{aligned}$$

Proof

Covering $x \equiv \mathcal{B} \pmod{\mathcal{M}} \Rightarrow \ \forall\ y \in \mathbb{Z},\ \mathcal{B} + \mathcal{M}y$ satisfies one of the congruences in our system.

We take $y \in \mathbb{Z}$ arbitrary. Does $\exists\ i = 1, 2, ..., n$, such that $\mathcal{B} + \mathcal{M}y$ satisfies one of the congruences?

$$\begin{aligned} \mathcal{B} + \mathcal{M}y &\equiv \mathcal{B} + b_i \cdot \mathcal{M} && \pmod{m_i \cdot \mathcal{M}} \\ \mathcal{M}y &\equiv b_i \cdot \mathcal{M} && \pmod{m_i \cdot \mathcal{M}} \\ y &\equiv b_i && \pmod{m_i} \end{aligned}$$

The system $b_i \pmod{m_i},\ i = 1, 2, ..., n$ is a covering, by hypothesis, so what we want is indeed always true!

Observations

Recall the example:

$$x_1 \equiv 1 \pmod 2$$
$$x_2 \equiv 2 \pmod 4$$
$$x_3 \equiv 4 \pmod 8$$

covers all residues except for $x \equiv 0 \pmod{8 = 2^3}$.
This holds for all systems of the form $x \equiv 2^{i-1} \pmod{2^i}$, for $i = 1, 2, ..., n$. We always leave $0 \pmod{2^n}$ uncovered.

Patching the 2^n "Almost Covering"

We have proven that the residue 0 (mod 2^n) can be covered with a system of congruences with moduli divisible by a prime p we choose (such that $p < n + 1$). We have the freedom to make n arbitrarily large, because the system behaves identically for all n.

The 2-Trick Covering

The cover we've found is:

$$
\begin{aligned}
x_1 &\equiv 1 \pmod 2 & \qquad x_{n+1} &\equiv 0 \cdot 2^n \pmod{p2^{p1}} \\
x_2 &\equiv 2 \pmod 4 & \qquad x_{n+2} &\equiv 1 \cdot 2^n \pmod{p2^{p-2}} \\
x_3 &\equiv 4 \pmod 8 & \qquad x_{n+3} &\equiv 2 \cdot 2^n \pmod{p2^{p-3}} \\
&\vdots & &\vdots \\
x_n &\equiv 2^{n-1} \pmod{2^n} & \qquad x_{n+p-1} &\equiv (p-1) \cdot 2^n \pmod{p2^0}
\end{aligned}
$$

Characteristics of our Congruence Covering System

Consider an "almost covering" with lcm $= M = 2^t \cdot u$.

For each congruence we wish to cover, we can choose a different prime so the moduli of the second part of the covering will be distinct.

So long as we only try to doubly use moduli which are divisible by 2^t, our secondary systems will have distinct moduli for all of their component moduli.

The 2-Trick Cover

- We've applied this technique to our construction of coverings. It greatly reduces our least common multiple, because in place of large numbers of congruences with large moduli, we put one congruence with a relatively small modulus.

- This method helps to keep lcm's low, and saves computation time, if it can patch "almost coverings" into real coverings.

The 2-Trick Cover

- We've applied this technique to our construction of coverings. It greatly reduces our least common multiple, because in place of large numbers of congruences with large moduli, we put one congruence with a relatively small modulus.

- This method helps to keep lcm's low, and saves computation time, if it can patch "almost coverings" into real coverings.

Problem

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?

Conjecture (Erdős)

For all $n \in \mathbb{N}$ there exist a covering with distinct moduli all greater than or equal to n.

Problem

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?

Conjecture (Erdős)

For all $n \in \mathbb{N}$ there exist a covering with distinct moduli all greater than or equal to n.

Calculations done by hand

1. When we use moduli at least 3 or greater:
   - 21 linear congruences and has a lcm of 360 for the moduli.
2. When we use moduli at least 4 or greater:
   - 55 linear congruences and has a lcm of $10,800$ for the moduli.
3. When we use moduli at least 5 or greater:
   - 58 linear congruences and has a lcm of $15,120$ for the moduli.
4. When we restrict ourselves to use moduli at least 6 or greater, the process becomes very tedious and difficult.

Calculations done by hand

1. When we use moduli at least 3 or greater:
   - 21 linear congruences and has a lcm of 360 for the moduli.
2. When we use moduli at least 4 or greater:
   - 55 linear congruences and has a lcm of $10,800$ for the moduli.
3. When we use moduli at least 5 or greater:
   - 58 linear congruences and has a lcm of $15,120$ for the moduli.
4. When we restrict ourselves to use moduli at least 6 or greater, the process becomes very tedious and difficult.

Calculations done by hand

1. When we use moduli at least 3 or greater:
   - 21 linear congruences and has a lcm of 360 for the moduli.
2. When we use moduli at least 4 or greater:
   - 55 linear congruences and has a lcm of $10,800$ for the moduli.
3. When we use moduli at least 5 or greater:
   - 58 linear congruences and has a lcm of $15,120$ for the moduli.
4. When we restrict ourselves to use moduli at least 6 or greater, the process becomes very tedious and difficult.

Calculations done by hand

1. When we use moduli at least 3 or greater:
   - 21 linear congruences and has a lcm of 360 for the moduli.
2. When we use moduli at least 4 or greater:
   - 55 linear congruences and has a lcm of $10,800$ for the moduli.
3. When we use moduli at least 5 or greater:
   - 58 linear congruences and has a lcm of $15,120$ for the moduli.
4. When we restrict ourselves to use moduli at least 6 or greater, the process becomes very tedious and difficult.

A new approach

- As a result, we develop a greedy algorithm that finds systems of linear congruences that cover the integers.
- *Greedy algorithms* work in phases. In each phase, a decision is made that appears to be good, without regard for future consequences. In general, this means that some local optimum is chosen.
- Simple greedy algorithms are sometimes used to generate approximate answers, rather than using the more complicated algorithms generally required to generate an exact answer.

A new approach

- As a result, we develop a greedy algorithm that finds systems of linear congruences that cover the integers.
- *Greedy algorithms* work in phases. In each phase, a decision is made that appears to be good, without regard for future consequences. In general, this means that some local optimum is chosen.
- Simple greedy algorithms are sometimes used to generate approximate answers, rather than using the more complicated algorithms generally required to generate an exact answer.

A new approach

- As a result, we develop a greedy algorithm that finds systems of linear congruences that cover the integers.
- *Greedy algorithms* work in phases. In each phase, a decision is made that appears to be good, without regard for future consequences. In general, this means that some local optimum is chosen.
- Simple greedy algorithms are sometimes used to generate approximate answers, rather than using the more complicated algorithms generally required to generate an exact answer.

KN-program

- 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.

KN-program

- 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.

Example of KN-program

Example

- Find a covering where the all the moduli are greater than or equal to 3.
- Input a lcm= $M = 120$.
- We make a list all the possible moduli of this covering, and call it div[120]. In particular, div[120]= $\{3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$.
- Our goal is to find a covering that only uses distinct moduli from the list div[120] to cover the integers 1 through 120.
- Let lcmcover[120]= $\{1, 2, 3, ..., 120\}$.

Example of KN-program

Example

- Find a covering where the all the moduli are greater than or equal to 3.
- Input a lcm$=M=120$.
- We make a list all the possible moduli of this covering, and call it div[120]. In particular, div[120]$=\{3,4,5,6,8,10,12,15,20,24,30,40,60,120\}$.
- Our goal is to find a covering that only uses distinct moduli from the list div[120] to cover the integers 1 through 120.
- Let lcmcover[120]$=\{1,2,3,...,120\}$.

Example of KN-program

Example

- Find a covering where the all the moduli are greater than or equal to 3.
- Input a lcm$=M=120$.
- We make a list all the possible moduli of this covering, and call it div[120]. In particular, div[120]$=\{3,4,5,6,8,10,12,15,20,24,30,40,60,120\}$.
- Our goal is to find a covering that only uses distinct moduli from the list div[120] to cover the integers 1 through 120.
- Let lcmcover[120]$=\{1,2,3,...,120\}$.

Example of KN-program

Example

- Find a covering where the all the moduli are greater than or equal to 3.
- Input a lcm$=M=120$.
- We make a list all the possible moduli of this covering, and call it div[120]. In particular, div[120]$=\{3,4,5,6,8,10,12,15,20,24,30,40,60,120\}$.
- Our goal is to find a covering that only uses distinct moduli from the list div[120] to cover the integers 1 through 120.
- Let lcmcover[120]$=\{1,2,3,...,120\}$.

Example of KN-program

Example

- Find a covering where the all the moduli are greater than or equal to 3.
- Input a lcm$=M=120$.
- We make a list all the possible moduli of this covering, and call it div[120]. In particular, div[120]$=\{3,4,5,6,8,10,12,15,20,24,30,40,60,120\}$.
- Our goal is to find a covering that only uses distinct moduli from the list div[120] to cover the integers 1 through 120.
- Let lcmcover[120]$=\{1,2,3,...,120\}$.

Solution

The KN-programs calculates how many integers, r, satisfy each particular congruence

For $n \equiv 0 \pmod 3$, $r_0 = 40$,

For $n \equiv 1 \pmod 3$, $r_1 = 40$,

For $n \equiv 2 \pmod 3$, $r_2 = 40$,

from the lcmcover[120] array.
Now we remove all the integers from the lcmcover[120] array that satisfy the green congruence. We also insert 0 into the array called res[120].

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
...					

Solution

The KN-programs calculates how many integers, r, satisfy each particular congruence

$$\text{For } n \equiv 0 \pmod 3, r_0 = 40,$$
$$\text{For } n \equiv 1 \pmod 3, r_1 = 40,$$
$$\text{For } n \equiv 2 \pmod 3, r_2 = 40,$$

from the lcmcover[120] array.
Now we remove all the integers from the lcmcover[120] array that satisfy the green congruence. We also insert 0 into the array called res[120].

1	2	3	4	5	6
7	8	9	10	11	12
13	14	15	16	17	18
19	20	21	22	23	24
25	26	27	28	29	30
31	32	33	34	35	36
37	38	39	40	41	42
43	44	45	46	47	48
49	50	51	52	53	54
55	56	57	58	59	60
...					

Solution

The KN-programs calculates how many integers, r, satisfy each particular congruence

$$\text{For } n \equiv 0 \pmod 3, r_0 = 40,$$
$$\text{For } n \equiv 1 \pmod 3, r_1 = 40,$$
$$\text{For } n \equiv 2 \pmod 3, r_2 = 40,$$

from the lcmcover[120] array.
Now we remove all the integers from the lcmcover[120] array that satisfy the green congruence. We also insert 0 into the array called res[120].

1	2	4	5
7	8	10	11
13	14	16	17
19	20	22	23
25	26	28	29
31	32	34	35
37	38	40	41
43	44	46	47
49	50	52	53
55	56	58	59
...			

Solution

So, for modulus 4 we get that

For $n \equiv 0 \pmod 4$, $r_0 = 20$,
For $n \equiv 1 \pmod 4$, $r_1 = 20$,
For $n \equiv 2 \pmod 4$, $r_2 = 20$,
For $n \equiv 3 \pmod 4$, $r_3 = 20$,

from the lcmcover[120] array.
Now we remove all the integers from the lcmcover[120] array that satisfy the red congruence. We also insert 0 into the array called res[120].

1	2	4	5
7	8	10	11
13	14	16	17
19	20	22	23
25	26	28	29
31	32	34	35
37	38	40	41
43	44	46	47
49	50	52	53
55	56	58	59
...			

Solution

So, for modulus 4 we get that

$$\text{For } n \equiv 0 \pmod 4, r_0 = 20,$$
$$\text{For } n \equiv 1 \pmod 4, r_1 = 20,$$
$$\text{For } n \equiv 2 \pmod 4, r_2 = 20,$$
$$\text{For } n \equiv 3 \pmod 4, r_3 = 20,$$

from the lcmcover[120] array.
Now we remove all the integers from the lcmcover[120] array that satisfy the red congruence. We also insert 0 into the array called res[120].

1	2	4	5
7	8	10	11
13	14	16	17
19	20	22	23
25	26	28	29
31	32	34	35
37	38	40	41
43	44	46	47
49	50	52	53
55	56	58	59
...			

Solution

So, for modulus 4 we get that

For $n \equiv 0 \pmod 4$, $r_0 = 20$,
For $n \equiv 1 \pmod 4$, $r_1 = 20$,
For $n \equiv 2 \pmod 4$, $r_2 = 20$,
For $n \equiv 3 \pmod 4$, $r_3 = 20$,

from the lcmcover[120] array.
Now we remove all the integers from the lcmcover[120] array that satisfy the red congruence. We also insert 0 into the array called res[120].

1	2		5
7		10	11
13	14		17
19		22	23
25	26		29
31		34	35
37	38		41
43		46	47
49	50		53
55		58	59
...			

Solution

So, for modulus 6 we get that

For $n \equiv 0 \pmod 6$, $r_0 = 0$,
For $n \equiv 1 \pmod 6$, $r_1 = 16$,
For $n \equiv 2 \pmod 6$, $r_2 = 8$,
For $n \equiv 3 \pmod 6$, $r_3 = 0$,
For $n \equiv 4 \pmod 6$, $r_4 = 8$,
For $n \equiv 5 \pmod 6$, $r_5 = 16$,

1	2		
7			11
13	14		17
19		22	23
	26		29
31		34	
37	38		41
43		46	47
49			53
		58	59
...			

from the lcmcover[120] array.
Now we remove all the integers from the lcmcover[120] array that satisfy the blue congruence. We also insert 1 into the array called res[120].

Solution

So, for modulus 6 we get that

For $n \equiv 0 \pmod 6$, $r_0 = 0$,
For $n \equiv 1 \pmod 6$, $r_1 = 16$,
For $n \equiv 2 \pmod 6$, $r_2 = 8$,
For $n \equiv 3 \pmod 6$, $r_3 = 0$,
For $n \equiv 4 \pmod 6$, $r_4 = 8$,
For $n \equiv 5 \pmod 6$, $r_5 = 16$,

1	2		
7			11
13	14		17
19		22	23
	26		29
31		34	
37	38		41
43		46	47
49			53
		58	59
...			

from the lcmcover[120] array.
Now we remove all the integers from the lcmcover[120] array that satisfy the blue congruence. We also insert 1 into the array called res[120].

Solution

So, for modulus 6 we get that

For $n \equiv 0 \pmod 6$, $r_0 = 0$,
For $n \equiv 1 \pmod 6$, $r_1 = 16$,
For $n \equiv 2 \pmod 6$, $r_2 = 8$,
For $n \equiv 3 \pmod 6$, $r_3 = 0$,
For $n \equiv 4 \pmod 6$, $r_4 = 8$,
For $n \equiv 5 \pmod 6$, $r_5 = 16$,

from the lcmcover[120] array.
Now we remove all the integers from the lcmcover[120] array that satisfy the blue congruence. We also insert 1 into the array called res[120].

			11
2			17
		22	23
14			29
		34	
26			41
		46	47
38			53
		58	59
...			

Solution

- *We continue this process until lcmcover[120] array is empty or if we run out of moduli to use from the div[120] array.*
- *For this case, when the KN-program finishes we get the following arrays:*
  div[120]$= \{3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$
  res[120]$= \{0, 0, 0, 1, 2, 1, 5, 2, 3, 22, 29, 6, 14, 38\}$

Solution

- *We continue this process until lcmcover[120] array is empty or if we run out of moduli to use from the div[120] array.*
- *For this case, when the KN-program finishes we get the following arrays:*

$$div[120] = \{3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$$
$$res[120] = \{0, 0, 0, 1, 2, 1, 5, 2, 3, 22, 29, 6, 14, 38\}$$

Solution

- *We continue this process until lcmcover[120] array is empty or if we run out of moduli to use from the div[120] array.*
- *For this case, when the KN-program finishes we get the following arrays:*
  div[120]$= \{3, 4, 5, 6, 8, 10, 12, 15, 20, 24, 30, 40, 60, 120\}$
  res[120]$= \{0, 0, 0, 1, 2, 1, 5, 2, 3, 22, 29, 6, 14, 38\}$

The 2 trick

- We can modify the KN-program by inserting duplicate moduli into the div[M] array.
  - In particular, the moduli that we can insert into the div[M] are of the form $2^t \cdot u$, where 2^t is highest multiple of 2 of M and u is an odd factor of M. The moduli that we insert do not change change the size of the lcmcover[M] array.
- New div[120]= $\{3, 4, 5, 6, 8, 8, 10, 12, 15, 20, 24, 24, 30, 40, 40, 60, 120, 120\}$
- The div[M] array of modified KN-program is the only difference from the original KN-program.
- The modified KN-program finds systems of linear congruences that cover the integers using the same method as the original KN-program found them.

The 2 trick

- We can modify the KN-program by inserting duplicate moduli into the div[M] array.
  - In particular, the moduli that we can insert into the div[M] are of the form $2^t \cdot u$, where 2^t is highest multiple of 2 of M and u is an odd factor of M. The moduli that we insert do not change change the size of the lcmcover[M] array.
- New div[120]=
  $\{3, 4, 5, 6, 8, 8, 10, 12, 15, 20, 24, 24, 30, 40, 40, 60, 120, 120\}$
- The div[M] array of modified KN-program is the only difference from the original KN-program.
- The modified KN-program finds systems of linear congruences that cover the integers using the same method as the original KN-program found them.

The 2 trick

- We can modify the KN-program by inserting duplicate moduli into the div[M] array.
  - In particular, the moduli that we can insert into the div[M] are of the form $2^t \cdot u$, where 2^t is highest multiple of 2 of M and u is an odd factor of M. The moduli that we insert do not change change the size of the lcmcover[M] array.
- New div[120]=
  $\{3, 4, 5, 6, 8, 8, 10, 12, 15, 20, 24, 24, 30, 40, 40, 60, 120, 120\}$
- The div[M] array of modified KN-program is the only difference from the original KN-program.
- The modified KN-program finds systems of linear congruences that cover the integers using the same method as the original KN-program found them.

The 2 trick

- We can modify the KN-program by inserting duplicate moduli into the div[M] array.
  - In particular, the moduli that we can insert into the div[M] are of the form $2^t \cdot u$, where 2^t is highest multiple of 2 of M and u is an odd factor of M. The moduli that we insert do not change change the size of the lcmcover[M] array.
- New div[120]=
  $\{3, 4, 5, 6, 8, 8, 10, 12, 15, 20, 24, 24, 30, 40, 40, 60, 120, 120\}$
- The div[M] array of modified KN-program is the only difference from the original KN-program.
- The modified KN-program finds systems of linear congruences that cover the integers using the same method as the original KN-program found them.

Summary of results

Least modulus	lcm(m_i)= M	# of cong.	Prime Decomp. M	$\sum \frac{1}{m_i}$
2	12	5	$2^2 \cdot 3$	1.3333333
3	120	14	$2^3 \cdot 3 \cdot 5$	1.5
3	360	17	$2^3 \cdot 3^2 \cdot 5$	1.70833333
3	360	21	$2^3 \cdot 3^2 \cdot 5$	1.7388888
3	720	20	$2^4 \cdot 3^2 \cdot 5$	1.8055555
4	720	24	$2^4 \cdot 3^2 \cdot 5$	1.5166666
4	10,800	55	$2^4 \cdot 3^3 \cdot 5^2$	1.7184259
5	720	29	$2^4 \cdot 3^2 \cdot 5$	1.3777777
5	4,320	43	$2^5 \cdot 3^3 \cdot 5$	1.4164351
5	15,120	58	$2^4 \cdot 3^3 \cdot 5 \cdot 7$	1.8289021

linear congruences that use the 2 trick

linear congruences found by hand

Summary of results

Least modulus	lcm(m_i)= M	# of cong.	Prime Decomp. M	$\sum \frac{1}{m_i}$
6	1,260	42	$2^2 \cdot 3^2 \cdot 5 \cdot 7$	1.4285714
7	5,040	63	$2^4 \cdot 3^2 \cdot 5 \cdot 7$	1.5111111
7	30,240	81	$2^5 \cdot 3^3 \cdot 5 \cdot 7$	1.5485119
8	45,360	83	$2^4 \cdot 3^4 \cdot 5 \cdot 7$	1.4956128
9	226,800	163	$2^4 \cdot 3^4 \cdot 5^2 \cdot 7$	1.5159435
10	997,920	236	$2^5 \cdot 3^4 \cdot 5 \cdot 7 \cdot 11$	1.6403619
11	21,621,600	275	$2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	1.9791378

linear congruences that use the 2 trick

Note

Before closing, we note that the results we obtained arose through a learning by discovery project. Because of the discovery aspect of this process, we did not consult the literature until after we concluded our explorations. Thus, in some instances, we derived results that have appeared in print or are awaiting publications.

References

- Erdos, Paul. "On integers of the form $2^k + p$ and some related problems." *Summa Brasil.Math*, 2, 113-123.
- Gibson, D.J (2006).*Covering Systems.* Doctoral Dissertation at U Illinios at Urbana-Champaign, 2006.
- Guy, Richard K.,*On Unsolved Problems in Number Theory* (2nd Ed.), Springer-Verlag, New York, 1994.
- Filaseta, Michael."On coverings of the integers associated with an irreducibility theorem of A. Schinzel." *Number Theory for the Millennium* (2000), 1-24.
- Jones, G. and J. Jones, *Elementary Number Theory*, Springer Verlag, London, 2003.
- Sierpinski, Waclaw. "Sur un probléme concernment les nombres k Â· 2n +1." *Elem. Math.*, 15 (1960) 63-74.

Acknowledgements

With Thanks to:

- The Summer Math Institute
- Cornell University Math Department
- The Center for Applied Math
- The National Science Foundation
- Dr. Mark Kozek (Whittier College)
- Dr. Ravi Ramakrishna (Cornell University)
- Alexandre Roch (Cornell University)