Extreme Covering Systems

CTNT 2022 Conference

Jack R Dalton

University of South Carolina

June 9, 2022

Outline

- Introduction

Outline

- Introduction
- Motivation

Outline

- Introduction
- Motivation
- The Minimum Modulus Problem

Outline

- Introduction
- Motivation
- The Minimum Modulus Problem
- Related Problem

Outline

- Introduction
- Motivation
- The Minimum Modulus Problem
- Related Problem
- Main Results and Helpful Lemmas

Outline

- Introduction
- Motivation
- The Minimum Modulus Problem
- Related Problem
- Main Results and Helpful Lemmas
- Notation and a Pretty Picture

Outline

- Introduction
- Motivation
- The Minimum Modulus Problem
- Related Problem
- Main Results and Helpful Lemmas
- Notation and a Pretty Picture
- Tools Used in Main Results

Outline

- Introduction
- Motivation
- The Minimum Modulus Problem
- Related Problem
- Main Results and Helpful Lemmas
- Notation and a Pretty Picture
- Tools Used in Main Results
- Open Problems and Further Work

Outline

- Introduction
- Motivation
- The Minimum Modulus Problem
- Related Problem
- Main Results and Helpful Lemmas
- Notation and a Pretty Picture
- Tools Used in Main Results
- Open Problems and Further Work
- A Cute Photo of My Cat

Introduction

Definition

A covering system is a set of conguences in which every integer satisfies at least one of the congruences.

Introduction

Definition

A *covering system* *is a set of conguences in which every integer satisfies at least one of the congruences.*

Examples:

$$x \equiv 0 \pmod{2}, \qquad x \equiv 1 \pmod{2}$$

Introduction

Definition

A *covering system* *is a set of conguences in which every integer satisfies at least one of the congruences.*

Examples:

$$x \equiv 0 \pmod 2, \qquad x \equiv 1 \pmod 2$$

$$\begin{cases} x & \equiv 0 \pmod 2, \quad x \equiv 0 \pmod 3, \quad x \equiv 1 \pmod 4 \\ x & \equiv 3 \pmod 8, \quad x \equiv 7 \pmod{12}, \quad x \equiv 23 \pmod{24} \end{cases}$$

Introduction

Definition

A *covering system* *is a set of conguences in which every integer satisfies at least one of the congruences.*

Examples:

$$x \equiv 0 \pmod 2, \quad x \equiv 1 \pmod 2$$

$$\begin{cases} x & \equiv 0 \pmod 2, \quad x \equiv 0 \pmod 3, \quad x \equiv 1 \pmod 4 \\ x & \equiv 3 \pmod 8, \quad x \equiv 7 \pmod{12}, \quad x \equiv 23 \pmod{24} \end{cases}$$

Definition

A covering system is called distinct if no two of the moduli are equal.

Motivation

Conjecture (de Polignac, 1849)

All odd integers ≥ 3 *can be written as* $2^k + p$ *for* $k \in \mathbb{N}$ *and* p *is either a prime or* 1

Motivation

Conjecture (de Polignac, 1849)

All odd integers ≥ 3 *can be written as* $2^k + p$ *for* $k \in \mathbb{N}$ *and* p *is either a prime or* 1

Theorem (Erdős, 1950)

There exists an arithmetic progression consisting only of odd numbers, no term of which is of the form $2^k + p$*.*

Motivation

Conjecture (de Polignac, 1849)

All odd integers ≥ 3 *can be written as* $2^k + p$ *for* $k \in \mathbb{N}$ *and* p *is either a prime or* 1

Theorem (Erdős, 1950)

There exists an arithmetic progression consisting only of odd numbers, no term of which is of the form $2^k + p$*.*

The proof of the above is where Erdős invented covering systems.

Motivation 2

Erdős used the covering system from example 2 to construct the arithmetic progression which disproved de Polignac's conjecture.

Motivation 2

Erdős used the covering system from example 2 to construct the arithmetic progression which disproved de Polignac's conjecture.

Erdős also constructed a distinct covering system with least modulus 3 and largest modulus 120. Erdős wrote

Quote

"It seems likely that for every c there exists such a system all the moduli of which are $> c$."

Motivation 2

Erdős used the covering system from example 2 to construct the arithmetic progression which disproved de Polignac's conjecture.

Erdős also constructed a distinct covering system with least modulus 3 and largest modulus 120. Erdős wrote

Quote

"It seems likely that for every c there exists such a system all the moduli of which are $> c$."

Proving or disproving this statement became *the minimum modulus problem*. For decades many mathematicians believed that indeed, it is possible to construct covering systems with arbitrarily large least modulus.

The Minimum Modulus Problem

Conjecture

For any positive integer c, there exists a distinct covering system with minimum modulus greater than c.

Swift (1954) smallest modulus 4, later improved to 6

The Minimum Modulus Problem

Conjecture

For any positive integer c, there exists a distinct covering system with minimum modulus greater than c.

Swift (1954) smallest modulus 4, later improved to 6

Churchhouse (1968) with 9

The Minimum Modulus Problem

Conjecture

For any positive integer c, there exists a distinct covering system with minimum modulus greater than c.

Swift (1954) smallest modulus 4, later improved to 6

Churchhouse (1968) with 9

Krukenberg (1971) with 18

The Minimum Modulus Problem

Conjecture

For any positive integer c, there exists a distinct covering system with minimum modulus greater than c.

- Swift (1954) smallest modulus 4, later improved to 6
- Churchhouse (1968) with 9
- Krukenberg (1971) with 18
- Choi (1971) with 20

The Minimum Modulus Problem

Conjecture

For any positive integer c, there exists a distinct covering system with minimum modulus greater than c.

- Swift (1954) smallest modulus 4, later improved to 6
- Churchhouse (1968) with 9
- Krukenberg (1971) with 18
- Choi (1971) with 20
- Morikawa (1981) with 24

The Minimum Modulus Problem

Conjecture

For any positive integer c, there exists a distinct covering system with minimum modulus greater than c.

Swift (1954) smallest modulus 4, later improved to 6

Churchhouse (1968) with 9

Krukenberg (1971) with 18

Choi (1971) with 20

Morikawa (1981) with 24

Gibson (1996) with 25

The Minimum Modulus Problem

Conjecture

For any positive integer c, there exists a distinct covering system with minimum modulus greater than c.

- Swift (1954) smallest modulus 4, later improved to 6
- Churchhouse (1968) with 9
- Krukenberg (1971) with 18
- Choi (1971) with 20
- Morikawa (1981) with 24
- Gibson (1996) with 25
- Nielsen (2009) with 40 using a recursion

The Minimum Modulus Problem

Conjecture

For any positive integer c, there exists a distinct covering system with minimum modulus greater than c.

Swift (1954) smallest modulus 4, later improved to 6

Churchhouse (1968) with 9

Krukenberg (1971) with 18

Choi (1971) with 20

Morikawa (1981) with 24

Gibson (1996) with 25

Nielsen (2009) with 40 using a recursion

Owens (2014) with 42 (using over 10^{50} congruences)

Breakthrough

Turns out Erdős was wrong (gasp).

Theorem (Hough, 2015)

The minimum modulus in any distinct covering system does not exceed 10^{16}.

Breakthrough

Turns out Erdős was wrong (gasp).

Theorem (Hough, 2015)

The minimum modulus in any distinct covering system does not exceed 10^{16}.

Theorem (Balister, Bollobás, Morris, Sahasrabudhe, and Tiba, 2018)

The minimum modulus in any distinct covering system does not exceed 606000.

Breakthrough

Turns out Erdős was wrong (gasp).

Theorem (Hough, 2015)

The minimum modulus in any distinct covering system does not exceed 10^{16}.

Theorem (Balister, Bollobás, Morris, Sahasrabudhe, and Tiba, 2018)

The minimum modulus in any distinct covering system does not exceed 606000.

(This number makes my work possible)

Related Problem

Question

If the minimum modulus of a distinct covering system is m, then what is the smallest that the largest modulus can be?

Related Problem

Question

If the minimum modulus of a distinct covering system is m, then what is the smallest that the largest modulus can be?

Theorem (Krukenberg, 1971)

If the minimum modulus of a distinct covering system is 2, then the largest modulus is at least 12.

Related Problem

Question

If the minimum modulus of a distinct covering system is m, then what is the smallest that the largest modulus can be?

Theorem (Krukenberg, 1971)

If the minimum modulus of a distinct covering system is 2, then the largest modulus is at least 12.

Theorem (Krukenberg, 1971)

If the minimum modulus of a distinct covering system is 3, then the largest modulus is at least 36.

Main Results

Krukenberg said he proved the following but no proof has ever shown up in the literature:

Theorem

If the minimum modulus of a distinct covering system is 4, *then the largest modulus is at least* 60.

Main Results

Krukenberg said he proved the following but no proof has ever shown up in the literature:

Theorem

If the minimum modulus of a distinct covering system is 4*, then the largest modulus is at least* 60*.*

In the paper with Dr. Trifonov, we supply a proof.

Main Results

Krukenberg said he proved the following but no proof has ever shown up in the literature:

Theorem

If the minimum modulus of a distinct covering system is 4*, then the largest modulus is at least* 60*.*

In the paper with Dr. Trifonov, we supply a proof.

Also, we proved the following:

Theorem (D. and Trifonov, 2022)

For each integer $m \geq 3$*, there is no distinct covering system with all moduli in the interval* $[m, 8m]$

Helpful Lemma

One of the tools we used:

Lemma

If $\mathcal{C}$ is the list of congruences in a covering system, then

$$\sum_{n \in \mathcal{C}} \frac{1}{n} \geq 1.$$

Helpful Lemma

One of the tools we used:

Lemma

If $\mathcal{C}$ is the list of congruences in a covering system, then

$$\sum_{n \in \mathcal{C}} \frac{1}{n} \geq 1.$$

The probability that a random integer is in a particular congruence class modulo n is exactly $\frac{1}{n}$, so if all of the probablilities do not add up to at least 1, then the list of congruences is not a covering.

Weirdo Notation

To begin talking more about the details going into the results, we first need to introduce some tricky notation, called **coordinate representation** of a congruence.

Weirdo Notation

To begin talking more about the details going into the results, we first need to introduce some tricky notation, called **coordinate representation** of a congruence.

Consider the particular congruence $x \equiv r \pmod{n}$, where $n > 1$ has prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$ where p_k is the kth prime. For the moment, we suppose all $a_l \geq 1$.

Weirdo Notation

To begin talking more about the details going into the results, we first need to introduce some tricky notation, called **coordinate representation** of a congruence.

Consider the particular congruence $x \equiv r \pmod{n}$, where $n > 1$ has prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$where p_k is the kth prime. For the moment, we suppose all $a_l \geq 1$.

We find the remainders $r_1, r_2, \ldots, r_k$ when r is divided by $p_1^{a_1}, \ldots, p_k^{a_k}$ respectively.

Weirdo Notation

To begin talking more about the details going into the results, we first need to introduce some tricky notation, called **coordinate representation** of a congruence.

Consider the particular congruence $x \equiv r \pmod{n}$, where $n > 1$ has prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$ where p_k is the kth prime. For the moment, we suppose all $a_l \geq 1$.

We find the remainders $r_1, r_2, \ldots, r_k$ when r is divided by $p_1^{a_1}, \ldots, p_k^{a_k}$ respectively.

Let d_1 be the base p_1 - representation of r_1 with its base p_1 digits written in **reverse** order. Define similarly, $d_2, \ldots, d_k$.

Weirdo Notation

To begin talking more about the details going into the results, we first need to introduce some tricky notation, called **coordinate representation** of a congruence.

Consider the particular congruence $x \equiv r \pmod{n}$, where $n > 1$ has prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$where p_k is the kth prime. For the moment, we suppose all $a_l \geq 1$.

We find the remainders $r_1, r_2, \ldots, r_k$ when r is divided by $p_1^{a_1}, \ldots, p_k^{a_k}$ respectively.

Let d_1 be the base p_1 - representation of r_1 with its base p_1 digits written in **reverse** order. Define similarly, $d_2, \ldots, d_k$.

Then, $x \equiv r \pmod{n}$ is written $(d_1|\ d_2|\ \ldots|\ d_k)$ in our notation.

Example of Notation

For example, consider the congruence $x \equiv 6 \pmod{120}$.

Example of Notation

For example, consider the congruence $x \equiv 6 \pmod{120}$.
It is equivalent to the system of congruences

$$\begin{cases} x \equiv 6 \pmod{2^3}, \\ x \equiv 0 \pmod{3}, \text{ and} \\ x \equiv 1 \pmod{5}. \end{cases}$$

Example of Notation

For example, consider the congruence $x \equiv 6 \pmod{120}$.
It is equivalent to the system of congruences

$$\begin{cases} x \equiv 6 \pmod{2^3}, \\ x \equiv 0 \pmod{3}, \text{ and} \\ x \equiv 1 \pmod{5}. \end{cases}$$

Thus, for $x \equiv 6 \pmod{120}$ we have $r = 6$ and $n = 2^3 \cdot 3 \cdot 5$, and so

$$\begin{aligned} r &\equiv 6 \pmod{2^3} && \Rightarrow r_1 = 6 && \Rightarrow d_1 = 011_2, \\ r &\equiv 0 \pmod{3} && \Rightarrow r_2 = 0 && \Rightarrow d_2 = 0_3, \\ r &\equiv 1 \pmod{5} && \Rightarrow r_3 = 1 && \Rightarrow d_3 = 1_5. \end{aligned}$$

Example of Notation

For example, consider the congruence $x \equiv 6 \pmod{120}$.
It is equivalent to the system of congruences

$$\begin{cases} x \equiv 6 \pmod{2^3}, \\ x \equiv 0 \pmod{3}, \text{ and} \\ x \equiv 1 \pmod{5}. \end{cases}$$

Thus, for $x \equiv 6 \pmod{120}$ we have $r = 6$ and $n = 2^3 \cdot 3 \cdot 5$, and so

$$\begin{aligned} r &\equiv 6 \pmod{2^3} & &\Rightarrow r_1 = 6 & &\Rightarrow d_1 = 011_2, \\ r &\equiv 0 \pmod{3} & &\Rightarrow r_2 = 0 & &\Rightarrow d_2 = 0_3, \\ r &\equiv 1 \pmod{5} & &\Rightarrow r_3 = 1 & &\Rightarrow d_3 = 1_5. \end{aligned}$$

So $x \equiv 6 \pmod{120}$ is written $(011|\ 0|\ 1)$.

What?

So why would we use such crazy-looking notation?

What?

So why would we use such crazy-looking notation?

Because it makes both splitting a congruence modulo a prime nice and reducing a congruence modulo a prime nice, as well as it helps visualize coverings. More on this in the coming slides.

What?

So why would we use such crazy-looking notation?

Because it makes both splitting a congruence modulo a prime nice and reducing a congruence modulo a prime nice, as well as it helps visualize coverings. More on this in the coming slides.

One more little note about the notation: if one or more of the exponents a_l in the factorizatizion $n = p_1^{a_1} \cdots p_k^{a_k}$ is zero, then we put $*$ in the lth position of the notation for the congruence.

What?

So why would we use such crazy-looking notation?

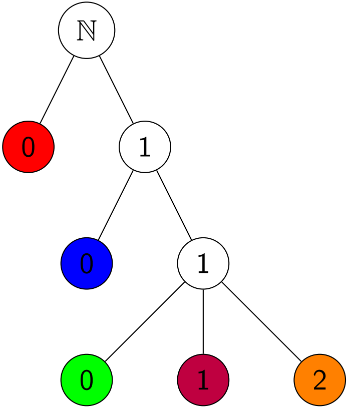
Because it makes both splitting a congruence modulo a prime nice and reducing a congruence modulo a prime nice, as well as it helps visualize coverings. More on this in the coming slides.

One more little note about the notation: if one or more of the exponents a_l in the factorizatizion $n = p_1^{a_1} \cdots p_k^{a_k}$ is zero, then we put $*$ in the lth position of the notation for the congruence.

For example,

$$x \equiv 1 \pmod{10} \text{ is written } (1| \ * \mid 1).$$

Building a Distinct Covering Using a Tree



Normal notation → our notation

0 (mod 2) → (0)

1 (mod 4) → (10)

0 (mod 3) → $(*|\ 0)$

5 (mod 6) → $(1|\ 2)$

7 (mod 12) → $(11|\ 1)$

Splitting a Congruence Modulo a Prime

Assume that p is prime, a is a nonnegative integer, n is a positive integer, and $p^a || n$.

Splitting a Congruence Modulo a Prime

Assume that p is prime, a is a nonegative integer, n is a positive integer, and $p^a || n$.

Splitting the residue class $r \pmod{n}$ modulo p means that we replace it by p residue classes modulo np by consecutively appending the base-p digits $0, 1, \ldots, p-1$ in the position corresponding to p^{a+1} in the coordinate representation of the residue class.

Splitting a Congruence Modulo a Prime

Assume that p is prime, a is a nonegative integer, n is a positive integer, and $p^a || n$.

Splitting the residue class $r \pmod{n}$ modulo p means that we replace it by p residue classes modulo np by consecutively appending the base-p digits $0, 1, \ldots, p-1$ in the position corresponding to p^{a+1} in the coordinate representation of the residue class.

For example, if we split $(1|\ 1|\ 4)$ modulo 3, we obtain the 'fibers' $(1|\ 10, 11, 12|\ 4)$.

Reducing a Congruence Modulo a Prime

Similarly, assume that p is prime, a and n are positive integers, and $p^a || n$.

Reducing a Congruence Modulo a Prime

Similarly, assume that p is prime, a and n are positive integers, and $p^a || n$.

Reducing the residue class $r \pmod{n}$ modulo p means that we delete the base-p digit in the position corresponding to p^a in the coordinate representation of the residue class.

Reducing a Congruence Modulo a Prime

Similarly, assume that p is prime, a and n are positive integers, and $p^a || n$.

Reducing the residue class $r \pmod{n}$ modulo p means that we delete the base-p digit in the position corresponding to p^a in the coordinate representation of the residue class.

For example, if we reduce $(0|\ 21|\ 34)$ modulo 5 we get $(0|\ 21|\ 3)$.

Reducing a Congruence Modulo a Prime

Similarly, assume that p is prime, a and n are positive integers, and $p^a || n$.

Reducing the residue class $r \pmod{n}$ modulo p means that we delete the base-p digit in the position corresponding to p^a in the coordinate representation of the residue class.

For example, if we reduce $(0|\ 21|\ 34)$ modulo 5 we get $(0|\ 21|\ 3)$.

Note, if you reduce a covering system modulo a prime, the resulting list of congruences will still be a covering (possibly not a disinct one).

Reducing a Congruence Modulo a Prime

Similarly, assume that p is prime, a and n are positive integers, and $p^a || n$.

Reducing the residue class $r \pmod{n}$ modulo p means that we delete the base-p digit in the position corresponding to p^a in the coordinate representation of the residue class.

For example, if we reduce $(0|\ 21|\ 34)$ modulo 5 we get $(0|\ 21|\ 3)$.

Note, if you reduce a covering system modulo a prime, the resulting list of congruences will still be a covering (possibly not a disinct one).

So if you reduce a set of congruences that you think could be a covering modulo a prime, and end up with some integers left uncovered, then the original set of congruences cannot be a covering.

A Fun Example

Lemma

Let $\mathcal{C}$ be a covering system such that $p^a | L$, where L is the lcm of moduli, for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a, and will still have a covering.

A Fun Example

Lemma

Let $\mathcal{C}$ be a covering system such that $p^a | L$, where L is the lcm of moduli, for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a, and will still have a covering.

This can be used relatively easily to show that there is no distinct covering system with all of the moduli in the interval $[2, 11]$.

A Fun Example

Lemma

Let $\mathcal{C}$ be a covering system such that $p^a | L$, where L is the lcm of moduli, for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a, and will still have a covering.

This can be used relatively easily to show that there is no distinct covering system with all of the moduli in the interval $[2, 11]$.

Suppose there is a distinct covering system with all of the moduli in the interval $[2, 11]$. Thus the set of moduli must be a subset of

$$\{2, 3, 2^2, 5, 2 \cdot 3, 7, 2^3, 3^2, 2 \cdot 5, 11\}$$

A Fun Example

Lemma

Let $\mathcal{C}$ be a covering such that $p^a | L$ for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a, and will still have a covering.

This can be used relatively easily to show that there is no distinct covering with all of the moduli in the interval $[2, 11]$.

Suppose there is a distinct covering with all of the moduli in the interval $[2, 11]$. Thus the set of moduli must be a subset of

$$\{2, 3, 2^2, 5, 2 \cdot 3, 7, 2^3, 3^2, 2 \cdot 5, \cancel{11}\}$$

A Fun Example

Lemma

Let $\mathcal{C}$ be a covering such that $p^a | L$ for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a, and will still have a covering.

This can be used relatively easily to show that there is no distinct covering with all of the moduli in the interval $[2, 11]$.

Suppose there is a distinct covering with all of the moduli in the interval $[2, 11]$. Thus the set of moduli must be a subset of

$$\{2, 3, 2^2, 5, 2 \cdot 3, \cancel{7}, 2^3, 3^2, 2 \cdot 5, \cancel{11}\}$$

A Fun Example

Lemma

Let $\mathcal{C}$ be a covering such that $p^a | L$ for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a, and will still have a covering.

This can be used relatively easily to show that there is no distinct covering with all of the moduli in the interval $[2, 11]$.

Suppose there is a distinct covering with all of the moduli in the interval $[2, 11]$. Thus the set of moduli must be a subset of

$$\{2, 3, 2^2, 5, 2 \cdot 3, \cancel{7}, 2^3, \cancel{3^2}, 2 \cdot 5, \cancel{11}\}$$

A Fun Example

Lemma

Let $\mathcal{C}$ be a covering such that $p^a | L$ for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a, and will still have a covering.

This can be used relatively easily to show that there is no distinct covering with all of the moduli in the interval $[2, 11]$.

Suppose there is a distinct covering with all of the moduli in the interval $[2, 11]$. Thus the set of moduli must be a subset of

$$\{2, 3, 2^2, 5, 2 \cdot 3, \cancel{7}, \cancel{2^3}, \cancel{3^2}, 2 \cdot 5, \cancel{11}\}$$

A Fun Example

Lemma

Let $\mathcal{C}$ be a covering such that $p^a | L$ for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a, and will still have a covering.

This can be used relatively easily to show that there is no distinct covering with all of the moduli in the interval $[2, 11]$.

Suppose there is a distinct covering with all of the moduli in the interval $[2, 11]$. Thus the set of moduli must be a subset of

$$\{2, 3, 2^2, \not{5}, 2 \cdot 3, \not{7}, \cancel{2^3}, \cancel{3^2}, \cancel{2 \cdot 5}, \cancel{11}\}$$

A Fun Example

Lemma

Let $\mathcal{C}$ be a covering such that $p^a | L$ for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a, and will still have a covering.

This can be used relatively easily to show that there is no distinct covering with all of the moduli in the interval $[2, 11]$.

Suppose there is a distinct covering with all of the moduli in the interval $[2, 11]$. Thus the set of moduli must be a subset of

$$\{2, \cancel{3}, 2^2, \cancel{5}, \cancel{2 \cdot 3}, \cancel{7}, \cancel{2^3}, \cancel{3^2}, \cancel{2 \cdot 5}, \cancel{11}\}$$

A Fun Example

Lemma

Let $\mathcal{C}$ be a covering such that $p^a | L$ for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a, and will still have a covering.

This can be used relatively easily to show that there is no distinct covering with all of the moduli in the interval $[2, 11]$.

Suppose there is a distinct covering with all of the moduli in the interval $[2, 11]$. Thus the set of moduli must be a subset of

$$\{2, \cancel{3}, \cancel{2^2}, \cancel{5}, \cancel{2 \cdot 3}, \cancel{7}, \cancel{2^3}, \cancel{3^2}, \cancel{2 \cdot 5}, \cancel{11}\}$$

A Fun Example

Lemma

Let $\mathcal{C}$ be a covering such that $p^a | L$ for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a, and will still have a covering.

This can be used relatively easily to show that there is no distinct covering with all of the moduli in the interval $[2, 11]$.

Suppose there is a distinct covering with all of the moduli in the interval $[2, 11]$. Thus the set of moduli must be a subset of

$$\{\cancel{2}, \cancel{3}, \cancel{2^2}, \cancel{5}, \cancel{2 \cdot 3}, \cancel{7}, \cancel{2^3}, \cancel{3^2}, \cancel{2 \cdot 5}, \cancel{11}\}$$

Does this always work?

Sadly, this previous lemma is not strong enough for showing that the interval $[3, 36]$ is also minimal, but we have a fancier lemma that helps:

Does this always work?

Sadly, this previous lemma is not strong enough for showing that the interval $[3, 36]$ is also minimal, but we have a fancier lemma that helps:

Lemma

Let $\mathcal{C}$ be a distinct covering system with all moduli in the interval $[c, d]$. If p is a prime and a is a positive integer such that $p^a(p+1) > d$, then we can discard all congruences whose moduli are multiples of p^a and still have a covering.

Does this always work?

Sadly, this previous lemma is not strong enough for showing that the interval $[3, 36]$ is also minimal, but we have a fancier lemma that helps:

Lemma

Let $\mathcal{C}$ be a distinct covering system with all moduli in the interval $[c, d]$. If p is a prime and a is a positive integer such that $p^a(p+1) > d$, then we can discard all congruences whose moduli are multiples of p^a and still have a covering.

Using the lemma from the previous slide, we get that if there exists a distinct covering system with all of the moduli in the interval $[3, 35]$, then the set of moduli must be a subset of

$$\{3, 2^2, 5, 2 \cdot 3, 2^3, 2 \cdot 5, 2^2 \cdot 3, 3 \cdot 5, 2^2 \cdot 5, 2^3 \cdot 3, 2 \cdot 3 \cdot 5\}$$

Does this always work?

Sadly, this previous lemma is not strong enough for showing that the interval $[3, 36]$ is also minimal, but we have a fancier lemma that helps:

Lemma

Let $\mathcal{C}$ be a distinct covering system with all moduli in the interval $[c, d]$. If p is a prime and a is a positive integer such that $p^a(p+1) > d$, then we can discard all congruences whose moduli are multiples of p^a and still have a covering.

Using the lemma from the previous slide, we get that if there exists a distinct covering system with all of the moduli in the interval $[3, 35]$, then the set of moduli must be a subset of

$$\{3, 2^2, 5, 2 \cdot 3, 2^3, 2 \cdot 5, 2^2 \cdot 3, 3 \cdot 5, 2^2 \cdot 5, 2^3 \cdot 3, 2 \cdot 3 \cdot 5\}$$

From there you have to break it down into cases, which seems a bit tedious for this talk, so we'll move on.

It Gets Worse

Showing the interval $[4, 60]$ is minimal for the congruences in a distinct covering system takes about 4 pages of cases and subcases, so let's just skip that too!

It Gets Worse

Showing the interval $[4, 60]$ is minimal for the congruences in a distinct covering system takes about 4 pages of cases and subcases, so let's just skip that too!
However, this last Lemma is one of the main ingredients for proving our theorem about the nonexistence of distinct covering systems with all of the moduli in the interval $[m, 8m]$ for $m \geq 3$.

It Gets Worse

Showing the interval $[4, 60]$ is minimal for the congruences in a distinct covering system takes about 4 pages of cases and subcases, so let's just skip that too!

However, this last Lemma is one of the main ingredients for proving our theorem about the nonexistence of distinct covering systems with all of the moduli in the interval $[m, 8m]$ for $m \geq 3$.

Let's look at some of those details now, by combining the previous lemma with our old friend

Lemma

If $\mathcal{C}$ is the list of congruences in a covering system, then

$$\sum_{n \in \mathcal{C}} \frac{1}{n} \geq 1.$$

Assume that for some integer $m \geq 3$ there is a distinct covering $\mathcal{C}$ with all moduli in the interval $[m, 8m]$.

Assume that for some integer $m \geq 3$ there is a distinct covering $\mathcal{C}$ with all moduli in the interval $[m, 8m]$.

Let $\mathcal{C}_m$ be a minimal covering (in the sense that if you remove any congruences, it is no longer a covering) which is a subset of $\mathcal{C}$.

Assume that for some integer $m \geq 3$ there is a distinct covering $\mathcal{C}$ with all moduli in the interval $[m, 8m]$.

Let $\mathcal{C}_m$ be a minimal covering (in the sense that if you remove any congruences, it is no longer a covering) which is a subset of $\mathcal{C}$.

Let L be the least common multiple of the moduli of the congruences in $\mathcal{C}_m$. By one of the lemmas, if $p^a | L$ for some prime p and a positive integer a, then the interval $[m, 8m]$ contains at least p multiples of p^a that are not multiple of p^{a+1}.

Assume that for some integer $m \geq 3$ there is a distinct covering $\mathcal{C}$ with all moduli in the interval $[m, 8m]$.

Let $\mathcal{C}_m$ be a minimal covering (in the sense that if you remove any congruences, it is no longer a covering) which is a subset of $\mathcal{C}$.

Let L be the least common multiple of the moduli of the congruences in $\mathcal{C}_m$. By one of the lemmas, if $p^a | L$ for some prime p and a positive integer a, then the interval $[m, 8m]$ contains at least p multiples of p^a that are not multiple of p^{a+1}.

Since one of every p consecutive multiples of p^a are divisible by p^{a+1}, we get that the interval $[m, 8m]$ must contain at least $p + 1$ multiples of p^a.

Denote by $\mathcal{M} \subseteq [m, 8m]$ the set of moduli from the congruences in $\mathcal{C}_m$.

Denote by $\mathcal{M} \subseteq [m, 8m]$ the set of moduli from the congruences in $\mathcal{C}_m$.

Let p be a prime. The number of multiples of p in the interval $[m, 8m]$ is

Denote by $\mathcal{M} \subseteq [m, 8m]$ the set of moduli from the congruences in $\mathcal{C}_m$.

Let p be a prime. The number of multiples of p in the interval $[m, 8m]$ is

$$n_p := \left\lfloor \frac{8m}{p} \right\rfloor - \left\lfloor \frac{m-1}{p} \right\rfloor = \frac{7m+1}{p} - \left\{ \frac{8m}{p} \right\} + \left\{ \frac{m-1}{p} \right\},$$

where $\{x\}$ denotes the fractional part of x.

Denote by $\mathcal{M} \subseteq [m, 8m]$ the set of moduli from the congruences in $\mathcal{C}_m$.

Let p be a prime. The number of multiples of p in the interval $[m, 8m]$ is

$$n_p := \left\lfloor \frac{8m}{p} \right\rfloor - \left\lfloor \frac{m-1}{p} \right\rfloor = \frac{7m+1}{p} - \left\{ \frac{8m}{p} \right\} + \left\{ \frac{m-1}{p} \right\},$$

where $\{x\}$ denotes the fractional part of x.

Since $0 \leq \{x\} < 1$, if we assume $p \geq \sqrt{7m+1}$, we get

$$n_p < \frac{7m+1}{p} + 1 \leq \sqrt{7m+1} + 1 \leq p + 1.$$

Thus, for each $p \geq \sqrt{7m+1}$ there are less than $p+1$ multiples of p in the interval $[m, 8m]$.

Thus, for each $p \geq \sqrt{7m+1}$ there are less than $p+1$ multiples of p in the interval $[m, 8m]$.

Therefore, if n is a modulus of one of the congruences in $\mathcal{C}_m$ (that is $n \in \mathcal{M}$), then all the prime divisors of n are less than $\sqrt{7m+1}$.

Thus, for each $p \geq \sqrt{7m+1}$ there are less than $p+1$ multiples of p in the interval $[m, 8m]$.

Therefore, if n is a modulus of one of the congruences in $\mathcal{C}_m$ (that is $n \in \mathcal{M}$), then all the prime divisors of n are less than $\sqrt{7m+1}$.

Since, the density of integers covered by a congruence modulo n is $1/n$, and $\mathcal{C}_m$ is a covering, we get

$$\sum_{\substack{m \leq n \leq 8m, \\ P(n) < \sqrt{7m+1}}} \frac{1}{n} \geq \sum_{n \in \mathcal{M}} \frac{1}{n} \geq 1,$$

where $P(n)$ denotes the largest prime divisor of n.

Let

$$S_m = \sum_{n \in \mathcal{M}} \frac{1}{n} \quad \text{and} \quad T_m = \sum_{\substack{m \le n \le 8m, \\ P(n) < \sqrt{7m+1}}} \frac{1}{n}.$$

Let

$$S_m = \sum_{n \in \mathcal{M}} \frac{1}{n} \quad \text{and} \quad T_m = \sum_{\substack{m \le n \le 8m, \\ P(n) < \sqrt{7m+1}}} \frac{1}{n}.$$

We checked by direct computation (using python), and a shortcut, that $T_m < 1$ for all $m \in [26, 606000]$.

Let

$$S_m = \sum_{n \in \mathcal{M}} \frac{1}{n} \quad \text{and} \quad T_m = \sum_{\substack{m \le n \le 8m, \\ P(n) < \sqrt{7m+1}}} \frac{1}{n}.$$

We checked by direct computation (using python), and a shortcut, that $T_m < 1$ for all $m \in [26, 606000]$.

We didn't need to check the sum for all values of m because we could make jumps by defining:

$$a_n = \begin{cases} \frac{1}{n}, & \text{if } P(n) < \sqrt{7n+1} \\ 0 & \text{otherwise.} \end{cases},$$

then using the inequality $T_{m-1} \le T_m + a_{m-1}$

Let

$$S_m = \sum_{n \in \mathcal{M}} \frac{1}{n} \quad \text{and} \quad T_m = \sum_{\substack{m \le n \le 8m, \\ P(n) < \sqrt{7m+1}}} \frac{1}{n}.$$

We checked by direct computation (using python), and a shortcut, that $T_m < 1$ for all $m \in [26, 606000]$.

We didn't need to check the sum for all values of m because we could make jumps by defining:

$$a_n = \begin{cases} \frac{1}{n}, & \text{if } P(n) < \sqrt{7n+1} \\ 0 & \text{otherwise.} \end{cases} ,$$

then using the inequality $T_{m-1} \le T_m + a_{m-1}$

Using this shortcut, the next value of T_m that we needed to calculate after T_{606000} was T_{286067}.

Let

$$S_m = \sum_{n \in \mathcal{M}} \frac{1}{n} \quad \text{and} \quad T_m = \sum_{\substack{m \le n \le 8m, \\ P(n) < \sqrt{7m+1}}} \frac{1}{n}.$$

We checked by direct computation (using python), and a shortcut, that $T_m < 1$ for all $m \in [26, 606000]$.

We didn't need to check the sum for all values of m because we could make jumps by defining:

$$a_n = \begin{cases} \frac{1}{n}, & \text{if } P(n) < \sqrt{7n+1} \\ 0 & \text{otherwise.} \end{cases},$$

then using the inequality $T_{m-1} \le T_m + a_{m-1}$

Using this shortcut, the next value of T_m that we needed to calculate after T_{606000} was T_{286067}.

There were a few counterexamples for $m \in [3, 25]$, where $T_m > 1$, but these were fixed by considering the squares of some of the primes.

Open Problems and Further Work

Conjecture

If the least modulus of a distinct covering system is 5*, then its largest modulus is at least* 108*.*

Open Problems and Further Work

Conjecture

If the least modulus of a distinct covering system is 5*, then its largest modulus is at least* 108*.*

We can show that if the least modulus of a distinct covering system is 5, then its largest modulus is at least 84. However, the result is too weak, and the proof too long, to be included in our paper.

Open Problems and Further Work

Conjecture

If the least modulus of a distinct covering system is 5, *then its largest modulus is at least* 108.

We can show that if the least modulus of a distinct covering system is 5, then its largest modulus is at least 84. However, the result is too weak, and the proof too long, to be included in our paper.

I was able to use this weaker result to show the nonexistence of distinct covering systems with all of the moduli in the interval $[m, 9m]$ for $m \geq 3$ except for the numbers $m = 24$ and $m = 48$.

Thank you for coming to my talk!

Thank you for coming to my talk!