Open Problems in Covering Systems PANTS XXXIV UNC Charlotte

Jack R Dalton

University of South Carolina

September 25, 2022

University of South Carolina

< 口 > < 同 >

Definition

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

Jack R Dalton Open Problems in Covering Systems

Definition

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

Examples:

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

University of South Carolina

Definition

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

Examples:

Jack R Dalton

$$x \equiv 0 \pmod{2}, \quad x \equiv 1 \pmod{2}$$
$$\begin{cases} x \equiv 1 \pmod{2}, & x \equiv 0 \pmod{3}, \\ x \equiv 2 \pmod{4}, & x \equiv 4 \pmod{6}, & x \equiv 8 \pmod{12} \end{cases}$$

Open Problems in Covering Systems

Definition

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

Examples:

$$x \equiv 0 \pmod{2}, \quad x \equiv 1 \pmod{2}$$
$$\begin{cases} x \equiv 1 \pmod{2}, & x \equiv 0 \pmod{3}, \\ x \equiv 2 \pmod{4}, & x \equiv 4 \pmod{6}, & x \equiv 8 \pmod{12} \end{cases}$$

Definition

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

University of South Carolina

Open Problems in Covering Systems

Motivation

In the 1950's, Erdős constructed a distinct covering system with least modulus 3 and largest modulus 120. Erdős wrote

Quote

Jack R Dalton

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

Motivation

In the 1950's, Erdős 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.

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

University of South Carolina

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

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 10-18

University of South Carolina

Conjecture

Jack R Dalton

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 10-18 Choi (1971) with 20

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 10-18 Choi (1971) with 20 Morikawa (1981) with 24

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 10-18 Choi (1971) with 20 Morikawa (1981) with 24 Gibson (1996) with 25

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 10-18 Choi (1971) with 20 Morikawa (1981) with 24 Gibson (1996) with 25 Nielsen (2009) with 40

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 10-18 Choi (1971) with 20 Morikawa (1981) with 24 Gibson (1996) with 25 Nielsen (2009) with 40 Owens (2014) with 42 To get the one with smallest modulus 18, Krukenberg takes a covering system with smallest modulus 5 and lcm of the moduli 2^73^25 that has 43 congruences, and repeatedly replaces the smallest modulus with sets of larger ones, adding new prime factors to the lcm.



To get the one with smallest modulus 18, Krukenberg takes a covering system with smallest modulus 5 and lcm of the moduli $2^{7}3^{2}5$ that has 43 congruences, and repeatedly replaces the smallest modulus with sets of larger ones, adding new prime factors to the lcm.

The resulting covering system has over 1700 congruences, but runs into an obstruction when trying to replace the congruence with modulus 18 with anything higher.

To get the one with smallest modulus 18, Krukenberg takes a covering system with smallest modulus 5 and lcm of the moduli $2^{7}3^{2}5$ that has 43 congruences, and repeatedly replaces the smallest modulus with sets of larger ones, adding new prime factors to the lcm.

The resulting covering system has over 1700 congruences, but runs into an obstruction when trying to replace the congruence with modulus 18 with anything higher.

It seems as though this game could be played more carefully to obtain arbitrarily larger smallest modulus, but...

Turns out there is an upper bound on the smallest modulus:

Theorem (Hough, 2015)

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

▲ロト▲団ト▲臣ト▲臣ト 臣 のへで

Jack R Dalton Open Problems in Covering Systems

Turns out there is an upper bound on the smallest modulus:

Theorem (Hough, 2015)

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

This was then improved to get:

(ロ・・御・・言・・言・・ 同・ うへの

University of South Carolina

Turns out there is an upper bound on the smallest modulus:

Theorem (Hough, 2015)

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

This was then improved to get:

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

The minimum modulus in any distinct covering system does not exceed 616000.

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?



Question

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

One way to consider this problem is the following:

Theorem (D. and Trifonov, 2022)

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

University of South Carolina

We can be more specific with a few smaller cases:

Theorem (Krukenberg, 1971)

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



University of South Carolina

We can be more specific with a few smaller cases:

Theorem (Krukenberg, 1971)

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

To show this, we need a lemma.

メロトメタトメミトメミト ヨーのへ(

University of South Carolina

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



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

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

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

University of South Carolina

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

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

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

Open Problems in Covering Systems

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

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

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

Open Problems in Covering Systems

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

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

$$\{2, 3, 2^2, 5, 2 \cdot 3, \cancel{1}, 2^3, \cancel{2}, 2 \cdot 5, \cancel{1}\}$$

Open Problems in Covering Systems

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

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

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

University of South Carolina

Open Problems in Covering Systems

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

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

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

Open Problems in Covering Systems

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

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

Open Problems in Covering Systems

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

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

Open Problems in Covering Systems

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

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

Open Problems in Covering Systems

Theorem (Krukenberg, 1971)

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



University of South Carolina
Theorem (Krukenberg, 1971)

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

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

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

Open Problems in Covering Systems

Theorem (Krukenberg, 1971)

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

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

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

University of South Carolina

At this point, we need a couple more lemmas.

Lemma (Krukenberg)

Let C be a covering such that $p^a||L$ for some prime p and integer $a \ge 1$. Let C_1 be the subset of C consisting of congruences whose moduli are divisible by p^a . Suppose $|C_1| = p$ and the moduli of the congruences in C_1 are $p^a m_1, \ldots, p^a m_p$. Then, one can replace the congruences in C_1 by a single congruence with modulus

$$p^{a-1}$$
lcm (m_1,\ldots,m_p)

and the resulting set will still be a covering.

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

Notice there are 5 moduli in this set divisible by 5, so we can apply the previous lemma and get that 5, 10, 15, 20, and 30 can be replaced by a single congruence modulo $lcm\{1, 2, 3, 4, 6\} = 12$.

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

Notice there are 5 moduli in this set divisible by 5, so we can apply the previous lemma and get that 5, 10, 15, 20, and 30 can be replaced by a single congruence modulo $lcm\{1, 2, 3, 4, 6\} = 12$.

So, if a distinct covering system with moduli in [3, 35] exists, so does a covering using the following list:

[3, 4, 6, 8, 12, 12, 24]

University of South Carolina

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

Notice there are 5 moduli in this set divisible by 5, so we can apply the previous lemma and get that 5, 10, 15, 20, and 30 can be replaced by a single congruence modulo $lcm\{1, 2, 3, 4, 6\} = 12$.

So, if a distinct covering system with moduli in [3, 35] exists, so does a covering using the following list:

 $\left[3,4,6,8,12,12,24\right]$

< (17) > <

University of South Carolina

At this point we need another lemma.

Lemma

Let C be a covering system and let p be a prime. Let C_0 be the subset of C of congruences whose moduli are not divisible by p. Let \mathcal{M}_0 be the list of the moduli of the congruences in C_0 . Similarly, let C_1 be the subset of C of congruences whose moduli are divisible by p, and let \mathcal{M}_1 be the list of the moduli of the congruences in C_1 .

Lemma

Let C be a covering system and let p be a prime. Let C_0 be the subset of C of congruences whose moduli are not divisible by p. Let \mathcal{M}_0 be the list of the moduli of the congruences in C_0 . Similarly, let C_1 be the subset of C of congruences whose moduli are divisible by p, and let \mathcal{M}_1 be the list of the moduli of the congruences in C_1 . Reducing the covering C modulo p produces p coverings where each modulus in \mathcal{M}_0 is used in each of the p coverings but each modulus n in \mathcal{M}_1 is replaced by n/p and is used in just one of the

p coverings.

If there were a covering with the moduli

[3, 4, 6, 8, 12, 12, 24],

then we could reduce this covering modulo 3, and get 3 coverings where the moduli 4 and 8 can be used in each, but each of the moduli in the list [1, 2, 4, 4, 8] can be used in only one of them.

University of South Carolina

If there were a covering with the moduli

[3, 4, 6, 8, 12, 12, 24],

then we could reduce this covering modulo 3, and get 3 coverings where the moduli 4 and 8 can be used in each, but each of the moduli in the list [1, 2, 4, 4, 8] can be used in only one of them.

Placing the 1 in the first finishes that one off. Placing the 8 and the 2 in the second brings the sum of the reciprocals to exactly 1, a minimum requirement for the moduli in a covering system. All that is left is [4, 4, 4, 8], the reciprocals of which do not add to 1 and thus we have a contradiction.

Theorem

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



University of South Carolina

Open Problems in Covering Systems

Theorem

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

This one uses the same tools, but is more technical, and much longer, so take a peek at our paper if you are curious!

University of South Carolina

Krukenberg also constructed a distinct covering system with least modulus 5 and largest modulus 108. He conjectured that one cannot replace 108 by a smaller constant.



Krukenberg also constructed a distinct covering system with least modulus 5 and largest modulus 108. He conjectured that one cannot replace 108 by a smaller constant.

Question

Prove or disprove that if the least modulus of a distinct covering system is 5, then its largest modulus is at least 108.



Krukenberg also constructed a distinct covering system with least modulus 5 and largest modulus 108. He conjectured that one cannot replace 108 by a smaller constant.

Question

Prove or disprove that 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 is 5, then its largest is at least 84.

Krukenberg also constructed a distinct covering system with least modulus 5 and largest modulus 108. He conjectured that one cannot replace 108 by a smaller constant.

Question

Prove or disprove that 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 is 5, then its largest is at least 84.

The tools are the same as for showing [4, 60] minimal.



University of South Carolina

Question

Describe the distinct covering systems with least common multiple of the moduli of the form $2^a 3^b 5^c$ where a, b, and c are positive integers.

University of South Carolina

Question

Describe the distinct covering systems with least common multiple of the moduli of the form $2^a 3^b 5^c$ where a, b, and c are positive integers.

Krukenberg already provided such description in the case when $L = 2^a 3^b 5^c$ and one of the exponents *a*, *b*, and *c* is zero.

Question

Describe the distinct covering systems with least common multiple of the moduli of the form $2^a 3^b 5^c$ where a, b, and c are positive integers.

Krukenberg already provided such description in the case when $L = 2^a 3^b 5^c$ and one of the exponents *a*, *b*, and *c* is zero. Using Krukenberg's results and the results of our paper, one can find such a description when $a \ge b \ge c \ge 1$ and the minimum modulus m = 2, 3, 4 with one exception.

Question

Describe the distinct covering systems with least common multiple of the moduli of the form $2^a 3^b 5^c$ where a, b, and c are positive integers.

Krukenberg already provided such description in the case when $L = 2^a 3^b 5^c$ and one of the exponents *a*, *b*, and *c* is zero. Using Krukenberg's results and the results of our paper, one can find such a description when $a \ge b \ge c \ge 1$ and the minimum modulus m = 2, 3, 4 with one exception. Extra work is needed to show that there is no distinct covering system with m = 4 and $L = 900 = 2^2 3^2 5^2$.



University of South Carolina

Theorem (D. and Trifonov, 2022)

(i) If the minimum modulus in a distinct covering is 3, then the least common multiple of all the moduli is at least 120;
(ii) If the minimum modulus in a distinct covering is 4, then the least common multiple of all the moduli is at least 360.

Theorem (D. and Trifonov, 2022)

(i) If the minimum modulus in a distinct covering is 3, then the least common multiple of all the moduli is at least 120;
(ii) If the minimum modulus in a distinct covering is 4, then the least common multiple of all the moduli is at least 360.

Furthermore, Krukenberg constructed a distinct covering system with m = 5 and L = 1440.

Theorem (D. and Trifonov, 2022)

(i) If the minimum modulus in a distinct covering is 3, then the least common multiple of all the moduli is at least 120;
(ii) If the minimum modulus in a distinct covering is 4, then the least common multiple of all the moduli is at least 360.

Furthermore, Krukenberg constructed a distinct covering system with m = 5 and L = 1440.

Question

Prove or disprove that if the least modulus of a distinct covering system is 5, then the least common multiple of its moduli is at least 1440.



Question

Prove or disprove that the least modulus of any distinct covering system with squarefree moduli is 2.

University of South Carolina

Question

Prove or disprove that the least modulus of any distinct covering system with squarefree moduli is 2.

It has been shown that at least one even modulus is needed for a distinct covering system with square-free moduli.

Question

Prove or disprove that the least modulus of any distinct covering system with squarefree moduli is 2.

It has been shown that at least one even modulus is needed for a distinct covering system with square-free moduli.

Showing that the least modulus of any distinct covering system with squarefree moduli is 2 will lead to a complete solution of the *minimum modulus problem* in the squarefree case.



University of South Carolina

Combining this covering with one Krukenberg constructed with minimum modulus 13, we get a double covering of the integers.



University of South Carolina

Combining this covering with one Krukenberg constructed with minimum modulus 13, we get a double covering of the integers.

Question

Find the largest integer c such that there exists a finite set of congruences with distinct moduli with the property that every integer satisfies at least c of the congruences.

University of South Carolina

Combining this covering with one Krukenberg constructed with minimum modulus 13, we get a double covering of the integers.

Question

Find the largest integer c such that there exists a finite set of congruences with distinct moduli with the property that every integer satisfies at least c of the congruences.

In other words, what is the largest number of times we can cover the integers by a finite system of congruences with distinct positive moduli? This problem was considered by Joshua Harrington who constructed three distinct covering systems with non-intersecting sets of moduli. Thus we have that we can at least triple cover the integers. This problem was considered by Joshua Harrington who constructed three distinct covering systems with non-intersecting sets of moduli. Thus we have that we can at least triple cover the integers.

Recall that Balister et al. showed that the least modulus of any distinct covering system does not exceed 616000, so the most number of times we can cover the integers with a distinct covering is \leq 616000.

Thank you for coming to my talk!



Jack R Dalton Open Problems in Covering Systems