Constructions of Coverings of the Integers: Exploring an Erdős Problem

Kelly Bickel, Michael Firrisa, Juan Ortiz, and Kristen Pueschel *

August 20, 2008

Abstract

In this paper, we study necessary conditions for small sets of congruences with distinct moduli to cover the integers, and we construct larger covering systems that address a problem of Erdős: "What is the largest minimum modulus needed for a set of congruences with distinct moduli to cover the integers?" We show that the fewest number of distinct moduli necessary to cover the integers is 5, and that there is only one set of distinct moduli with which to construct a covering with only 5 congruences. We determine which natural numbers less than 50 can be the least common multiple of the moduli of a covering. We establish that the minimum modulus for a covering system of distinct moduli is at least 11.

1 Introduction

In this paper, we explore the technique of "covering the integers": representing the integers with finite systems of linear congruences. The power of these systems in number theory was most famously demonstrated by Hungarian Paul Erdős [1]. For example, he used coverings to disprove a conjecture of de Polignac's:

Conjecture 1. *For every sufficiently large odd number $k \in \mathbb{Z}$, there exists an $n \in \mathbb{N}$ and a prime p such that*

$$k = 2^n + p.$$

With coverings Erdős constructed an infinite family of odd numbers k that fail the conjecture.

Before considering the applications of and some questions about coverings, we will formalize our basic ideas about these systems of congruences. We begin with a description of the terminology we use throughout this paper, and we state a classic theorem that figures prominently in our arguments.

Given $m \in \mathbb{N}$, we say that two integers a and b are **congruent modulo** m if and only if there exists $k \in \mathbb{Z}$ such that

$$a - b = k \cdot m.$$

*Summer Math Institute, Cornell University

If so, then we write

$$a \equiv b \pmod{m}.$$

For the purposes of this paper, we assume $m > 1$.

We are interested in all integers $a \in \mathbb{Z}$ such that $a \equiv b \pmod{m}$. Therefore, we will typically use variable notation for our integer a and define an analog of equations in one variable. A congruence of the form

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

where x is an unknown integer, is a **linear congruence** in one variable.

A **covering of the integers**, or covering, is a system of n linear congruences of the form

$$x \equiv b_i \pmod{m_i}, \ \ i \in \{1, 2, ..., n\},$$

such that every integer satisfies at least one of these congruences. For example, the congruences

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

form a covering of the integers. To check that this system of congruences covers the integers, we observe that all even numbers satisfy congruence (1) and all odd numbers satisfy congruence (2). Hence, all integers satisfy at least one of these congruences, and so the above system covers the integers. Similarly, the congruence $x \equiv 0 \pmod{1}$ is trivially a covering, because all integers are divisible by 1.

For the rest of the paper, we will restrict ourselves to using only distinct moduli in our coverings. Thus, calling a system of congruences a covering implies that the moduli of the congruences are distinct. We also assume that all moduli are greater than one.

The **least common multiple (lcm)** of a set of n natural numbers $\{m_1, m_2, \ldots, m_n\}$ is the smallest natural number M such that for all $i \in \{1, 2, ..., n\}$, m_i is a divisor of M. To check that a given system of congruences is a covering, it is enough to show that every non-negative integer less than the least common multiple of the moduli of the system, M satisfies at least one congruence in the system. We now formalize and justify this claim.

Given $M \in \mathbb{N}$, and $r \in \mathbb{N}$ such that $r \in \{0, 1, ..., M-1\}$, the **residue class** $r \pmod{M}$ is the set $[r] := \{x \in \mathbb{Z} : x \equiv r \pmod{M}\}$. We call r a residue of M. The **residue system** of M is the set of all residues modulo M : $\{0, 1, 2, \ldots, M-1\}$, which we will denote $\mathbb{Z}_M$. Every integer $z \in \mathbb{Z}$ is congruent to exactly one $r \in \mathbb{Z}_M$.

Now, we consider a system of n linear congruences of the form $x \equiv b_i \pmod{m_i}$. Let $M = \operatorname{lcm}\{m_1, m_2, \ldots, m_n\}$ and consider the set $\mathbb{Z}_M$. Because each integer $z \in \mathbb{Z}$ is congruent to exactly one $r \in \mathbb{Z}_M$, if each residue r satisfies at least one of the congruences in our system, then so will every integer $z \in \mathbb{Z}$. As this holds for arbitrary z, our set of congruences covers the integers. Explicitly, if we have $z \equiv r \pmod{M}$ and $r \equiv b_i \pmod{m_i}$, then there exist $\hat{\gamma}$ and y such that:

$$z = r + M \cdot \hat{\gamma} = r + m_i \cdot \gamma \qquad \text{and} \qquad r = b_i + m_i \cdot y$$
$$z = (b_i + m_i \cdot y) + m_i \cdot \gamma$$
$$z = b_i + m_i \cdot (y + \gamma)$$

$$z \equiv \qquad b_i \pmod{m_i}$$

Thus, as claimed, every integer congruent to $r \pmod{M}$ is congruent to $b_i \pmod{m_i}$, so we have only to cover the elements of $\mathbb{Z}_M$ to cover the integers.

Let us consider the following set of congruences:

$$x_1 \equiv 0 \pmod{2} \tag{3}$$
$$x_2 \equiv 1 \pmod{3} \tag{4}$$
$$x_3 \equiv 3 \pmod{4} \tag{5}$$
$$x_4 \equiv 5 \pmod{6} \tag{6}$$
$$x_5 \equiv 9 \pmod{12} \tag{7}$$

To determine if this system covers the integers, we check whether our congruences cover the residue system Z_{12}, because $\operatorname{lcm}\{2, 3, 4, 6, 12\} = 12$. That is, we want each of the residues $r \in \{0, 1, ..., 11\}$ to satisfy at least one of the congruences in our system. We have:

a. $\{0, 2, 4, 6, 8, 10\}$ satisfy congruence (3).

b. $\{1, 4, 7, 10\}$ satisfy congruence (4).

c. $\{3, 7, 11\}$ satisfy congruence (5).

d. $\{5, 11\}$ satisfy congruence (6).

e. $\{9\}$ satisfies congruence (7).

Hence, every residue $r \in \mathbb{Z}_{12}$ satisfies at least one of the congruences in our system. Thus every integer satisfies at least one of the congruences in our system, and so this system is a covering of the integers.

We make use of the following in several of our constructions.

Remark 1. *Take $M \in \mathbb{N}$ and let m be a divisor of M and $b \in \mathbb{Z}$. The number of elements of $\mathbb{Z}_M$ congruent to $b \pmod{m}$ is $\frac{M}{m}$.*

Remark 2. *Take $M \in \mathbb{Z}$. If we consider a system of congruences that has as moduli all the divisors of M, then an upperbound $\mathscr{M}$, on the number of residues $r \in \mathbb{Z}_M$ that can be covered is given by*

$$\mathscr{M} = \sum_m \frac{M}{m},$$

where m divides M and $m > 1$. We cannot have a covering if

$$\mathscr{M} < M.$$

In the event that some of the congruences have moduli that are relatively prime, we make use of the Chinese Remainder Theorem. We do not include the proof.

Theorem 1. ***(Chinese Remainder Theorem** [5]) Let $m_1, m_2, \ldots m_t$ be positive integers greater than 1 such that the $\gcd(m_i, m_j) = 1$ for $i \neq j$. Then the system*

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

has a unique solution $\pmod{m_1 \cdot m_2 \cdot \ldots \cdot m_t}$.

Theorem 2. *Let $m_1,\ m_2$ be relatively prime divisors of M and consider a covering that uses congruences $\pmod{m_1}$ and $\pmod{m_2}$. The number μ of elements of $\mathbb{Z}_M$ that simultaneously satisfy each of these congruences is:*

$$\mu = \frac{M}{m_1 \cdot m_2}.$$

Proof. Let $b_1 \pmod{m_1}$ and $b_2 \pmod{m_2}$ be congruences in our covering. By Theorem 1, there is one unique solution $y \pmod{m_1 \cdot m_2}$. Hence, y is congruent to both $b_1 \pmod{m_1}$ and $b_2 \pmod{m_2}$. Because m_1, m_2 both divide M and are relatively prime, $m_1 \cdot m_2$ is a divisor of M, and so by Remark 1, there are precisely $\frac{M}{m_1 \cdot m_2}$ elements of $\mathbb{Z}_M$ congruent to y, all of which satisfy the congruences $b_1 \pmod{m_1}$ and $b_2 \pmod{m_2}$. □

Corollary 1. *The maximum number of distinct elements $\mathscr{M}$ of $\mathbb{Z}_M$ that can be covered by two congruences*

$$\begin{aligned} b_1 &\pmod{m_1} \\ b_2 &\pmod{m_2} \end{aligned}$$

is given by:

$$\mathscr{M} = \frac{M}{m_1} + \frac{M}{m_2} - \mu.$$

Proof. Let C_1 denote the set of elements of $\mathbb{Z}_M$ congruent to $b_1 \pmod{m_1}$, let C_2 denote the set of elements of $\mathbb{Z}_M$ congruent to $b_2 \pmod{m_2}$, let $C = C_1 \cup C_2$ denote the set of elements of $\mathbb{Z}_M$ congruent to either $b_1 \pmod{m_1}$ or $b_2 \pmod{m_2}$, and let $\hat{C} = C_1 \cap C_2$ denote the set of elements of $\mathbb{Z}_M$ congruent to both $b_1 \pmod{m_1}$ and $b_2 \pmod{m_2}$.

We denote the cardinality of a set C by $|C|$.

$$|C| = |C_1 \cup C_2| = |C_1| + |C_2| - |C_1 \cap C_2| = |C_1| + |C_2| - |\hat{C}|.$$

By Remarks 1 and 2, $|C_1| = \frac{M}{m_1}$ and $|C_2| = \frac{M}{m_2}$. By Remark 9, the cardinality of $|\hat{C}|$ is $\frac{M}{m_1 \cdot m_2} = \mu$. Therefore,

$$|C| = \frac{M}{m_1} + \frac{M}{m_2} - \mu.$$

□

Now that we have a better understanding of coverings, we can proceed to their applications and the questions that motivate this paper.

The motivating question behind this paper stems from one of Erdős' favorite covering questions. [4]

"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?"

Erdős conjectured that N could be arbitrarily large.

In this paper, first we study necessary conditions for small sets of congruences with distinct moduli to cover the integers. We show that the fewest number of distinct moduli necessary to cover the integers is 5, and that there is only one set of moduli with which to construct a covering which has only 5 congruences. We determine which natural numbers less than 50 can be the least common multiple of the moduli of a covering.

Then, we establish that the minimum modulus N for a covering system of the integers with distinct moduli is at least 11.

2 Coverings with few moduli

In this section we show that a system of congruences

$$x \equiv b_i \pmod{m_i}, \ \ i \in \{1, ..., n\}$$

can be a covering of the integers only when $n \geq 5$. Furthermore, we show that the only distinct moduli that can be used to make a covering with 5 congruences are {2, 3, 4, 6, 12}.

Let a system S of n linear congruences of the form $x \equiv b_i \pmod{m_i}$ be a covering of the integers. S is a **minimal covering** if for all integers $j \in \{1, ..., n\}$, the system $S \backslash \{x \equiv b_j \pmod{m_j}\}$ is not a covering. We note that if $\hat{S}$ is a covering that is not minimal, then we can write $\hat{S} = S \cup \{x \equiv b_{j_1} \pmod{m_{j_1}}, \ldots, x \equiv b_{j_m} \pmod{m_{j_m}}\}$ where S is a minimal covering. That is, for all non-minimal coverings $\hat{S}$, there exists a minimal covering S such that $S \subset \hat{S}$. Thus we consider minimal coverings because the non-existence of a minimal covering implies the non-existence of the general covering. If a covering is non-minimal, then there are congruences which are irrelevant. Thus, we only consider the relevant congruences, the minimal covering.

We begin with two lemmas.

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

Proof. Suppose (towards a contradiction) that $n \leq p$.

First, we suppose that p divides every m_i for all i. Then, the maximum number of elements covered by set of congruences is

$$\mathscr{M} = \frac{M}{m_1} + \frac{M}{m_2} + \cdots + \frac{M}{m_n} \leq \frac{M}{p} + \frac{M}{p} + \cdots + \frac{M}{p},$$

since each modulus is a multiple of p. Because we have $n \leq p$ congruences,

$$\frac{M}{p} + \frac{M}{p} + \cdots + \frac{M}{p} \leq \frac{pM}{p} = M.$$

However, equality only occurs when every modulus is equal to p, which violates our assumption that all the moduli are distinct. Hence, there must be at least one modulus of S which is not divisible by p.

Therefore, we assume that there is some number of moduli, s, divisible by p, where $1 \leq s < n < p$. Then we can write our covering as follows:

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ x &\equiv b_s \pmod{m_s} \\ &\vdots \\ x &\equiv b_n \pmod{m_n}, \end{aligned}$$

where the moduli $\{m_1, \ldots, m_s\}$ are divisible by p, and the moduli $\{m_{s+1}, \ldots, m_n\}$ are not divisible by p.

Consider $\mathbb{Z}_p$, which contains p elements. Because $s < p$ there must be some residue $r \in \mathbb{Z}_p$ such that $r \not\equiv b_i \pmod{p}$ for $i \leq s$.

Since we have a covering of the integers, all integers must satisfy at least one of the congruences. Let us consider integers of the form

$$y = r + zp, \quad z \in \mathbb{Z}.$$

We observe that these y cannot satisfy the first s congruences of our covering, because $b_i - r$ is not divisible by p for $i \in \{1, \ldots, s\}$, from above, whereas zp, m_i always are divisible by p. Thus, for all $z \in \mathbb{Z}$,

$$y = r + zp \equiv b_j \pmod{m_j}, \quad j \in \{s+1, \ldots, n\}.$$

Because we assumed p does not divide m_j, it follows that m_j and p are relatively prime. Then there exist integers $\hat{c}$ and $\hat{d}$ such that

$$(\hat{d} \cdot p) + (\hat{c} \cdot m_j) = 1.$$

Multiplying both sides by $(b_j - r)$ gives us

$$(b_j - r) \cdot (\hat{d} \cdot p) + (b_j - r) \cdot (\hat{c} \cdot m_j) = (b_j - r). \tag{8}$$

We have that for all $z \in \mathbb{Z}$

$$y = r + zp \equiv b_j \pmod{m_j}, \quad j \in \{s+1, \ldots, n\},$$

which combined with equation (8) implies

$$\begin{aligned} zp &\equiv (b_j - r) \pmod{m_j} \\ &\equiv (b_j - r) \cdot (\hat{d} \cdot p) + (b_j - r) \cdot (\hat{c} \cdot m_j) \pmod{m_j} \\ &\equiv (b_j - r) \cdot (\hat{d} \cdot p) \pmod{m_j} \end{aligned}$$

because $(\hat{c} \cdot m_j) \equiv 0 \pmod{m_j}$. Because p and m_j are relatively prime, we can divide both sides of our congruence to yield

$$z \equiv (b_j - r) \cdot \hat{d} \pmod{m_j}.$$

Since z was an arbitrary integer, every integer must be covered by some congruence $\pmod{m_j}$, where $j \in \{s+1, \ldots, n\}$. Since the term $(b_j - r) \cdot \hat{d}$ depends only on p and m_j, the term is independent of any z and so

$$(b_j - r) \cdot \hat{d} \pmod{m_j}$$

covers all integers z such that

$$r + zp \equiv b_j \pmod{m_j}.$$

Then, we have a covering with distinct moduli using only moduli m_j for $j \in \{s+1, \ldots, n\}$. This contradicts the minimality of our original covering. Therefore, there can be no minimal covering of n congruences, where the lcm of the moduli is a multiple of a prime p and $p > n$. Our result follows. □

Lemma 2. *Let a set S of n congruences of the form $x \equiv b_i \pmod{m_i}$ be a minimal covering. If a prime p divides some modulus m_i, then p is a divisor of at least p moduli.*

Proof. By Theorem 1, we have that $n > p$. Suppose (towards a contradiction) that there are fewer than p moduli divisible by p. Then we can write our covering in the following manner:

$$\begin{aligned} x &\equiv b_1 \pmod{m_1} \\ &\vdots \\ x &\equiv b_s \pmod{m_s} \\ &\vdots \\ x &\equiv b_n \pmod{m_n}, \end{aligned}$$

where the moduli $\{m_1, \ldots, m_s\}$ are divisible by p, the moduli $\{m_{s+1}, \ldots, m_n\}$ are not divisible by p, and $s < p$.

We continue in the same manner as our previous proof, and consider $\mathbb{Z}_p$, which contains p elements. Because $s < p$, there must be some $r \in \mathbb{Z}_p$ such that $r \not\equiv b_i \pmod{p}$ for all $i \leq s$.

Since we have a covering of the integers, all integers must satisfy at least one congruence. Let us consider integers of the form:

$$y = r + qp, \quad q \in \mathbb{Z}.$$

Observe that y cannot satisfy the first s congruences of our covering. Therefore, for all $q \in \mathbb{Z}$,

$$y = r + qp \equiv b_j \pmod{m_j}, \quad j \in \{s+1, \ldots, n\}$$

Because we assumed m_j does not divide p, it follows that m_j and p are relatively prime. Then there exist integers $\hat{d}$ and $\hat{c}$ such that

$$(\hat{d} \cdot p) + (\hat{c} \cdot m_j) = 1.$$

Multiplying both sides by $(b_j - r)$ gives us

$$(b_j - r) \cdot (\hat{d} \cdot p) + (b_j - r) \cdot (\hat{c} \cdot m_j) = (b_j - r). \tag{9}$$

For all $q \in \mathbb{Z}$, from above, we know that

$$y = r + qp \equiv b_j \pmod{m_j}, \quad j \in \{s+1, \ldots, n\}.$$

Combining this with Equation 9 yields

$$\begin{aligned} qp &\equiv (b_j - r) \pmod{m_j} \\ &\equiv (b_j - r) \cdot (\hat{d} \cdot p) + (b_j - r) \cdot (\hat{c} \cdot m_j) \pmod{m_j} \\ &\equiv (b_j - r) \cdot (\hat{d} \cdot p) \pmod{m_j}, \end{aligned}$$

because $(\hat{c} \cdot m_j) \equiv 0 \pmod{m_j}$. Because p and m_j are relatively prime, we can divide both sides of our congruence to yield:

$$q \equiv (b_j - r) \cdot \hat{d} \pmod{m_j}.$$

Since q was an arbitrary integer, every integer is covered by some congruence $\pmod{m_j}$, where $j \in \{s+1, \ldots, n\}$. Since the term $(b_j - r) \cdot \hat{d}$ depends only on p and m_j, that term is independent of any q and so

$$(b_j - r) \cdot \hat{d} \pmod{m_j}$$

covers all integers q such that

$$r + qp \equiv b_j \pmod{m_j}.$$

That is, we have a covering that uses only the moduli m_j for $j \in \{s+1, \ldots, n\}$. This is a contradiction of the minimality of our original covering. Therefore, given a set S of linear congruences, if a prime p divides at least one modulus but divides less than p of them, then S is not a minimal covering.

□

We now have the tools to discuss coverings with few congruences.

Theorem 3. *There is no covering of the integers that has only two congruences.*

Proof. Suppose for the contradiction that such a covering exists. Then we have some system:

$$\begin{aligned} b_1 \pmod{m_1} \\ b_2 \pmod{m_2} \end{aligned}$$

which is a covering of the integers. Because m_1 and m_2 are integers greater than 1, we can write each of m_1 and m_2 as a product of primes. By Lemma 1, we know that if a prime p divides m_1 or m_2, there must be at least $p+1$ congruences in our covering. However, there are no primes such that $p < 2$. Therefore, there are no primes that can be factors of m_1 or m_2, and we have a contradiction. Hence, we can have no covering using only two congruences. □

Theorem 4. *There is no covering of the integers that has only three congruences.*

Proof. Suppose (towards a contradiction) that such a covering exists. Then, we have some system of congruences S defined as:

$$\begin{aligned} b_1 \pmod{m_1} \\ b_2 \pmod{m_2} \\ b_3 \pmod{m_3} \end{aligned}$$

which is a covering of the integers. Because m_1, m_2 and m_3 are integers greater than 1, we can write each of m_1, m_2, and m_3 as a product of primes.

By Theorem 1, we know that if a prime p divides m_1, m_2, or m_3 there must be at least $p+1$ congruences in our covering. The only prime p such that $p < 3$ is 2. Therefore, all of m_1, m_2, and m_3 must be powers of 2.

Let $M = \operatorname{lcm}(m_1, m_2, m_3)$. Then, an upper bound $\mathscr{M}$ on the number of elements of $\mathbb{Z}_M$ that S can cover is given by

$$\begin{aligned}\mathscr{M} &= \frac{M}{m_1} + \frac{M}{m_2} + \frac{M}{m_3} \\ &\leq \frac{M}{2} + \frac{M}{4} + \frac{M}{8} \\ &= \frac{7M}{8} < M.\end{aligned}$$

Because we assumed S was a covering, this is contradiction and so there is no covering using only three congruences. □

Theorem 5. *There is no covering of the integers using only four congruences.*

Proof. Suppose (towards a contradiction) that such a covering exists. Then there is a system of linear congruences S defined as

$$\begin{aligned} b_1 \pmod{m_1} \\ b_2 \pmod{m_2} \\ b_3 \pmod{m_3} \\ b_4 \pmod{m_4}\end{aligned}$$

which is a covering of the integers. Because m_1, m_2, m_3, and m_4 are integers greater than 1, we can write each modulus as a product of primes. By Lemma 1, we know that if a prime p divides any of our moduli there must be at least $p+1$ congruences in our covering. The only primes p such that $p < 4$ are 2 and 3. Therefore, all of m_1, m_2, m_3, and m_4 must be multiples of only two or three.

First we show that these moduli cannot all be divisible only by 2. Let $M = \operatorname{lcm}(m_1, m_2, m_3, m_4)$. Then, an upper bound $\mathscr{M}$ on the number of elements of $\mathbb{Z}_M$ that S can cover is given by

$$\begin{aligned}\mathscr{M} &= \frac{M}{m_1} + \frac{M}{m_2} + \frac{M}{m_3} + \frac{M}{m_4} \\ &\leq \frac{M}{2} + \frac{M}{4} + \frac{M}{8} + \frac{M}{16} \\ &= \frac{15N}{16} < M\end{aligned}$$

Because we assumed S was a covering, this is a contradiction. By a similar argument, these moduli cannot all be divisible only by 3.

Thus both two and three are divisors of at least one modulus each. By Lemma 2, at least two moduli must be multiples of 2 and at least three moduli must be multiples of 3.

Next we show that 2 must be one of the moduli. If not, the set of smallest moduli satisfying Lemma 2 is $\{3, 4, 6, 9\}$. Then, an upper bound $\mathscr{M}$ on the number of elements of $\mathbb{Z}_M$ that S can cover is given by

$$\begin{aligned}\mathscr{M} &= \frac{M}{3} + \frac{M}{4} + \frac{M}{6} + \frac{M}{9} \\ &= \frac{31M}{36} < M\end{aligned}$$

So 2 must be one of the moduli. By a similar argument, 3 must also be one of the moduli.

Thus both 2 and 3 have to appear as moduli of our covering. The set of smallest moduli satisfying Lemma 2 that contains 2 and 3 is $\{2, 3, 6, 9\}$. Then, an upperbound $\mathscr{M}$ on the number of elements of $\mathbb{Z}_M$ that S can cover is given by

$$\begin{aligned}\mathscr{M} &= \frac{M}{2} + \frac{M}{3} + \frac{M}{6} + \frac{M}{9} - \frac{M}{6} \\ &= \frac{17M}{18} < M.\end{aligned}$$

Therefore, there can be no covering of the integers with only four congruences. □

Theorem 6. *There is a unique set of moduli with which it is possible to construct a five-congruence covering of the integers:*

$$\begin{aligned} x_1 &\equiv b_1 \pmod 2 \\ x_2 &\equiv b_2 \pmod 3 \\ x_3 &\equiv b_3 \pmod 4 \\ x_4 &\equiv b_4 \pmod 6 \\ x_5 &\equiv b_5 \pmod{12} \end{aligned}$$

Proof. We start with a few observations, similar to the arguments used in the proof of Theorem 5.

- By Lemma 1, the moduli can only have prime factorizations of powers of 2 and 3.
- One of the moduli must be 2. The most efficient covering system that does not include 2 as one of the moduli has moduli $\{3, 4, 6, 8, 9\}$ but

  $$\frac{M}{3} + \frac{M}{4} + \frac{M}{6} + \frac{M}{8} + \frac{M}{9} = \frac{7M}{8} + \frac{M}{9} < M,$$

  so this set of moduli cannot be used to construct a covering.
- One of {3,4} must be the modulus of one of the congruences. It follows by a similar argument to that of the previous observation.

Next we show that 4 must always be one of the moduli of our system. Suppose for the contradiction that it is not a modulus. By our observations, 3 is one of the elements, and 6 is also, because without 6 we could at best have $\{2, 3, 8, 9, 12\}$ but

$$\frac{M}{2} + \frac{M}{3} + \frac{M}{8} + \frac{M}{9} + \frac{M}{12} - \frac{M}{6} = \frac{7M}{8} + \frac{M}{9} < M$$

(We subtract $\frac{M}{6}$ because 2 and 3 are relatively prime, and therefore, by the Chinese Remainder Theorem, will overlap in one-sixth of the integers.) Thus if a covering exists, $\{2, 3, 6\}$ are moduli. Our system is

$$\begin{aligned} x &\equiv b_1 \pmod 2 \\ x &\equiv b_2 \pmod 3 \\ x &\equiv b_3 \pmod 6 \\ x &\equiv b_4 \pmod{m_4} \\ x &\equiv b_5 \pmod{m_5}, \end{aligned}$$

where $m_4, m_5 > 6$. Maximally, we can cover all but one residue modulo 6,

$$\frac{6}{2} + \frac{6}{3} + \frac{6}{6} - \frac{6}{6} = 3 + 2 + 1 - 1 = 5.$$

Let a be the residue $\pmod 6$ uncovered. That means that

$$\begin{aligned} 6z + a &\equiv b_4 \pmod{m_4} \\ 6z + a &\equiv b_5 \pmod{m_5} \end{aligned}$$

must be satisfied for all $z \in \mathbb{Z}$. If this is a covering and a consistent system, we will be able to re-write the congruences above as

$$\begin{aligned} z &\equiv \hat{b}_4 \pmod{\hat{m}_4} \\ z &\equiv \hat{b}_5 \pmod{\hat{m}_5} \end{aligned}$$

and every $z \in \mathbb{Z}$ must satisfy at least one of these congruences. Thus, $\hat{m}_4, \hat{m}_5 \leq 2$. First we observe that neither of $\hat{m}_4, \hat{m}_5 = 1$. For the contradiction, and without loss of generality, suppose $\hat{m}_4 = 1$. Then

$$z \equiv \frac{b_4 - a}{\gcd(6, m_4)} \pmod{\frac{m_4}{\gcd(6, m_4)}},$$

implies that $\hat{m}_4 = \frac{m_4}{\gcd(6, m_4)} = 1$, which is impossible if $m_4 > 6$. However, we note that if

$$\frac{m_4}{\gcd(6, m_4)} = 2,$$

then we must have one of the three following possibilities

$$\hat{m}_5 = \frac{m_5}{\gcd(6, m_5)} = 2 \quad \Rightarrow \quad \begin{aligned} \frac{m_5}{6} = 2 &\Rightarrow m_4 = m_5 = 12 \\ \frac{m_5}{3} = 2 &\Rightarrow m_5 = 6 \\ \frac{m_5}{2} = 2 &\Rightarrow m_5 = 4 \end{aligned}$$

As all of these are contradictions to our hypotheses, we cannot have a 5-congruence covering without a congruence of modulus 4.

Thus we have that $\{2,4\}$ must be moduli for two of the congruences of our covering. That is, our system of congruences must be:

$$\begin{aligned} x &\equiv b_1 \pmod 2 \\ x &\equiv b_2 \pmod 4 \\ x &\equiv b_3 \pmod{m_3} \\ x &\equiv b_4 \pmod{m_4} \\ x &\equiv b_5 \pmod{m_5} \end{aligned}$$

We note that $\pmod 4$ the first two congruences maximally cover all but one residue:

$$\frac{4}{2} + \frac{4}{4} = 2 + 1 = 3$$

Let a be the residue $\pmod 4$ uncovered by the first two congruences. Thus to have a covering we must have that for all $z \in \mathbb{Z}$,

$$a + 4 \cdot z \equiv b_j \pmod{m_j}$$

has to be satisfied for $j \in \{3,4,5\}$, and by lemma 2, $m_3,\ m_4,\ m_5$ must all be divisible by 3. If this is a covering and a consistent system, we will be able to re-write the congruences above as

$$\begin{aligned} z &\equiv \hat{b}_3 \pmod{\hat{m}_3} \\ z &\equiv \hat{b}_4 \pmod{\hat{m}_4} \\ z &\equiv \hat{b}_5 \pmod{\hat{m}_5} \end{aligned}$$

and every $z \in \mathbb{Z}$ must satisfy at least one of these congruences. We note that

$$z \equiv \frac{b_j - a}{\gcd(m_j, 4)} \pmod{\frac{m_j}{\gcd(m_j, 4)}}, \qquad j \in \{3,4,5\}$$

is the rewritten form of the congruences. The divisors of 4 are $\{1,2,4\}$ and so $\gcd(m_j, 4) \in \{1,2,4\}$. The first multiples of 3 satisfying these are $\{\{3,9,15\},\{6,18,30\},\{12,24,36\}\}$. We note that in these sets, the least $\hat{m}_j$ possible is 3. This is achieved by the least elements of each:

$$\begin{aligned} z \equiv\ & \tfrac{b_3-a}{\gcd(3,4)} \equiv b_3 - a && \pmod{\left(\frac{3}{\gcd(3,4)} = 3\right)} \\ z \equiv\ & \tfrac{b_4-a}{\gcd(6,4)} \equiv \tfrac{b_4-a}{2} && \pmod{\left(\frac{6}{\gcd(6,4)} = 3\right)} \\ z \equiv\ & \tfrac{b_5-a}{\gcd(12,4)} \equiv \tfrac{b_5-a}{4} && \pmod{\left(\frac{12}{\gcd(12,4)} = 3\right)} \end{aligned}$$

Clearly, in order to preserve the covering property, no other modulus is an acceptable substitute. Thus we have a unique set of moduli $\{2,3,4,6,12\}$ with which to construct a 5-congruence covering. Such a covering exists. In the introduction we showed that the system

$$x_1 \equiv 0 \pmod 2$$

$$\begin{aligned} x_2 &\equiv 1 \pmod 3 \\ x_3 &\equiv 3 \pmod 4 \\ x_4 &\equiv 5 \pmod 6 \\ x_5 &\equiv 9 \pmod{12} \end{aligned}$$

is a covering of the integers. □

3 Form of the Least Common Multiple of a Covering's Moduli

Theorem 7. *If S is a covering of the integers, with moduli $\{m_1, m_2, \ldots m_n\}$, and $M = \operatorname{lcm}(m_1, m_2, ..., m_n)$ then $M \neq p^{\,\xi}$, where p is a prime, $\xi \in \mathbb{N}$.*

Proof. For the contrapositive, consider a system of linear congruences, in which $M = p^{\,\xi}$ for p prime and $\xi \in \mathbb{N}$. Then the moduli of the congruences are elements of $\{p, p^2, ..., p^{\,\xi}\}$. An upperbound $\mathscr{M}$ on the number of elements of Z_M that can be covered is:

$$\mathscr{M} = \frac{M}{p^1} + \frac{M}{p^2} + \cdots + \frac{M}{p^{\,\xi}}$$

This is a truncation of a strictly positive geometric series that will always converge. We note that the sum of the geometric series is $\mathcal{Z} = \frac{M}{p-1}$, with $p \geq 2$. Clearly the infinite sum is greatest for $p = 2 : \ \mathcal{Z} = \frac{M}{2-1} = M$. Because the number of moduli in our system is always finite, $\mathscr{M} < \mathcal{Z} \leq M, \ \forall\, \xi \in \mathbb{N}, \ \forall\, p$ prime, so S is not a covering. Therefore a set of congruences with lcm of the moduli $M = p^{\,\xi}$ cannot be a covering, and so our result follows. □

Theorem 8. *If S is a covering of the integers, with moduli $\{m_1, m_2, \ldots m_n\}$, and $M = \operatorname{lcm}(m_1, m_2, ..., m_n)$ then $M \neq p_1 \cdot p_2$, where p_1 and p_2 are distinct primes.*

Proof. Suppose for the contrapositive that S is a system of linear congruences in which $M = p_1 \cdot p_2$, where p_1 and p_2 are distinct primes. Without loss of generality let $2 \leq p_1 < p_2$. The moduli of the congruences are elements of $\{p_1, p_2, \ p_1 \cdot p_2\}$. An upperbound $\mathscr{M}$ on the number of elements of Z_M that can be covered is:

$$\mathscr{M} = \frac{M}{p_1} + \frac{M}{p_2} + \frac{M}{p_1 \cdot p_2} - \frac{M}{p_1 \cdot p_2} = \frac{M}{p_1} + \frac{M}{p_2} < 2\left(\frac{M}{p_1}\right) \leq M.$$

(We subtract $\frac{M}{p_1 \cdot p_2}$ because p_1, p_2 are relatively prime, and so we apply the Chinese Remainder Theorem.) Therefore a set of congruences S with $M = p_1 \cdot p_2$, where p_1 and p_2 are distinct primes, cannot be a covering, and so our result follows. □

Remark 3. *The least number that is neither the product of two primes nor a power of a prime is 12. Thus 12 is the smallest candidate to be the lcm of the moduli of a covering system. ($2^1, 3^1, 2^2, 5^1, 3 \cdot 2, 7^1, 2^3, 3^2, 2 \cdot 5, 11^1$ all fail to be candidates, by the previous two theorems.)*

Theorem 9. *If S is a covering of the integers, with moduli $\{m_1, m_2, \ldots m_n\}$, and $M = \operatorname{lcm}(m_1, m_2, ..., m_n)$ then $M \neq p_1 \cdot p_2 \cdot p_3$ where p_1, p_2, p_3 are distinct primes.*

Proof. Suppose for the contrapositive that S is a system of linear congruences in which $M = p_1 \cdot p_2 \cdot p_3$, where p_1, p_2, p_3 are distinct primes. Without loss of generality let $2 \leq p_1 < p_2 < p_3$. The moduli of the congruences are elements of $\{p_1,\ p_2,\ p_3,\ p_1p_2,\ p_1p_3,\ p_2p_3,\ p_1p_2p_3\}$. There are 4 possible moduli divisible by p_1, and similarly 4 divisible by p_2 and p_3 respectively. By an application of Lemma 1 we see that even for the case where the primes are $\{2, 3, 5\}$, the three smallest distinct primes, S cannot be a covering, as there are too few multiples of 5, and so our result follows. □

Interestingly, there exists a covering S such that $M = \text{lcm}\,(m_1, m_2, ..., m_n) = p_1 \cdot p_2 \cdot p_3 \cdot p_4$, where $p_1,\ p_2,\ p_3,\ p_4$ are distinct primes. The lcm, $M = 210 = 2 \cdot 3 \cdot 5 \cdot 7$. If we do not allow 2 to be a modulus, then no covering exists. These results await extension to larger products of primes. We conjecture that if 2 is not an allowed modululs, then no coverings exist where $M = p_1 \cdot p_2, \ldots, p_m$ for m arbitrarily large, $p_1, \ldots, p_m$ distinct primes greater than two. We note that a counterexample to this conjecture would be a proof of another open Erdős conjecture: "There does not exist a covering of the integers in which all moduli are odd."

Corollary 2. *Elements of* $\{12, 24, 36, 48\}$ *are the only natural numbers less than (or equal to) 50 that are candidates to be the lcm of the moduli of a covering system.*

Proof. All powers of primes less than 50 are not candidates, by Theorem 7. This removes: $\{2, 3, 4, 5, 7, 8, 9, 11, 13, 16, 17, 19, 23, 25, 27, 29, 31, 32, 37, 41, 43, 47, 49\}$. All numbers of the form p_1p_2 and $p_1p_2p_3$ where p_1, p_2, p_3 are prime are not candidates, by Theorems 8, 9. This removes: $\{6, 10, 14, 15, 21, 22, 26, 33, 34, 35, 38, 39, 46\}$ and $\{30, 42\}$. By Theorem 6 the number of factors that are potential moduli must be greater than six, except for the integer 12. This removes: $\{18, 20, 28, 44, 45, 50\}$. Finally, we apply Lemma 1 and consider the factors of $40 : \{2, 4, 5, 8, 10, 20, 40\}$. Only 4 of these potential moduli are divisible by 5, and so any system of linear congruences constructed with 40 as the lcm would fail to be a covering. This leaves the candidates $\{12, 24, 36, 48\}$. □

4 Tools for Covering Construction

In pursuing the primary problem, we began with minimal machinery to advance and check our work. Increasing the least modulus requires both an increase in the lcm and generally, an increase in the number of congruences. Although, as will be shown in the next section, it is certainly possible to construct coverings by hand with least modulus greater than two, hand-checking a covering is tedious and error-prone. Thus it was in our best interests to develop both a program to check our coverings and some tools to keep our least common multiples relatively small.

4.1 A Program to Check Coverings

The program *cover* has an input of an n-tuplet of residues and a corresponding n-tuplet of moduli. It first calculates the lcm of the moduli. Then, in a nested for-loop, each residue of the lcm is tested for congruence with (at least) one element of our system. If the residue is covered, the success is recorded and the next residue is tested. Finally, the number of successes is compared to the number of residues, and any residues left uncovered appear in a matrix.

4.2 Covering Single Congruences

This work addresses the following problem:

Problem: Given a set of linear congruences $S \cup \{x \equiv \mathcal{B} \pmod{\mathcal{M}}\}$ that cover a residue system, where $\mathcal{M}$ is the only non-distinct modulus , find a secondary system R of distinct congruences that can cover (and thus replace) the unacceptable congruence.

If all of the moduli in R are distinct from those of S, and every integer satisfying $x \equiv \mathcal{B} \pmod{\mathcal{M}}$ also satisfies one of the congruences in R, then $S \cup R$ will be a covering of the integers. We hope to find criteria that guarantee the existence of a secondary system R for certain moduli or congruences, where R preserves the distinct-moduli property of our coverings. Such criteria would allow us to represent systems R by the congruence they cover: $\mathcal{B} \pmod{\mathcal{M}}$, and thus doubly use these moduli in our constructions. The repeat would really be representative of the secondary system R. Such results are attractive because it is generally easier to deal with a single congruence than with a system of congruences. Also, such repeats would provide "extra" moduli for a given lcm, with which to construct systems of congruences, thus improving chances of constructing a covering system.

We begin by covering the single congruence, without concern for the system of which it is a part.

Theorem 10. *If the system*

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

is a covering of the integers, then the linear congruence $x \equiv \mathcal{B} \pmod{\mathcal{M}}$ can be covered by the secondary system of linear congruences R :

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

If R is a covering of the congruence $x \equiv \mathcal{B} \pmod{\mathcal{M}}$, we'll be able to show that if x_o satisfies $\mathcal{B} \pmod{\mathcal{M}}$, then there exists $i \in \{1, 2, ..., n\}$ such that $x_o \equiv \mathcal{B} + b_i \cdot \mathcal{M} \pmod{m_i \cdot \mathcal{M}}$.

Proof. By hypothesis, we have a covering, so $\forall\ z \in \mathbb{Z},\ \exists\ i \in \{1, 2, ..., n\}$ such that $z \equiv b_i \pmod{m_i}$, so we can find $y \in \mathbb{Z}$ such that $z = b_i + m_i \cdot y$.
We consider x_o congruent to $\mathcal{B} \pmod{\mathcal{M}}$:

$$\begin{aligned} x_o \equiv \mathcal{B} \pmod{\mathcal{M}} \Rightarrow \quad x_o &= \mathcal{B} + \mathcal{M} \cdot z_o \\ &= \mathcal{B} + \mathcal{M} \cdot (b_i + m_i \cdot y_o) \end{aligned}$$

$$
\begin{aligned}
&= \mathcal{B} + \mathcal{M} \cdot b_i + \mathcal{M} \cdot m_i \cdot y_o \\
&= (\mathcal{B} + \mathcal{M} \cdot b_i) + (m_i \cdot \mathcal{M}) \cdot y_o \;\Rightarrow\; x_o \equiv \mathcal{B} + \mathcal{M} \cdot b_i \pmod{m_i \cdot \mathcal{M}}
\end{aligned}
$$

That is, for arbitrary integer x_o congruent to $\mathcal{B} \pmod{M}$, there is some congruence in the system R which x_o satisfies. As it is true for arbitrary integer, it is true for all integers, and so R is a covering of of the congruence $x \equiv \mathcal{B} \pmod{\mathcal{M}}$. □

The following secondary covering system uses only 5 congruences, and so has been considered to cover single congruences when constructing systems S that already have many congruences, even with a repeated modulus.

Corollary 3. ***(The Five Trick)*** *Given some $x \equiv \mathcal{B} \pmod{\mathcal{M}}$, we can cover all elements of $[\mathcal{B}] \pmod{\mathcal{M}}$ using the following set of five congruences:*

$$
\begin{aligned}
x_1 &\equiv \mathcal{B} + 0\mathcal{M} \pmod{2\mathcal{M}} \\
x_2 &\equiv \mathcal{B} + 1\mathcal{M} \pmod{3\mathcal{M}} \\
x_3 &\equiv \mathcal{B} + 3\mathcal{M} \pmod{4\mathcal{M}} \\
x_4 &\equiv \mathcal{B} + 5\mathcal{M} \pmod{6\mathcal{M}} \\
x_5 &\equiv \mathcal{B} + 9\mathcal{M} \pmod{12\mathcal{M}}
\end{aligned}
$$

Proof. In the introduction we proved that the following system is a covering of the integers.

$$
\begin{aligned}
x_1 &\equiv 0 \pmod{2} \\
x_2 &\equiv 1 \pmod{3} \\
x_3 &\equiv 3 \pmod{4} \\
x_4 &\equiv 5 \pmod{6} \\
x_5 &\equiv 9 \pmod{12}
\end{aligned}
$$

Our result follows from Theorem 10. □

Although this particular covering is convenient because it has only five congruences, we see that in the context of doubly-using moduli, it will not be very useful. The system $S \cup R$ is not a covering if one of the moduli used in R already appears in S; it is a hypothesis that coverings are systems of congruences in which all moduli are distinct.

We note that the moduli of R are always of the form $2^\alpha \cdot 3^\beta \cdot \mathcal{M}$, where $\alpha \in \{0, 1, 2\},\ \beta \in \{0, 1\},\ \alpha = \beta \neq 0$. The lcm of the moduli of our original system S can be written $M = 2^t \cdot 3^\tau \cdot u$ for u odd and not divisible by 3. Because presumably all available candidate moduli will be used in the construction of S, if $\mathcal{M} \neq 2^t \cdot 3^\tau \cdot u_i$, for u_i odd and not divisible by 3, then there is some modulus m_j that is a candidate modulus for S, where $m_j = 2^\alpha \cdot 3^\beta \cdot \mathcal{M}$ where $\alpha \in \{0, 1, 2\},\ \beta \in \{0, 1\},\ \alpha = \beta \neq 0$. That is, if we consider the secondary covering R, for $x \equiv \mathcal{B} \pmod{\mathcal{M}}$, we observe that $S \cup R$ will not be a covering because the moduli in $S \cup R$ are not distinct. The relative scarcity of satisfactory moduli, and their small covering-efficiency motivates the search for a more convenient family of coverings, in particular, one that is without moduli divisible by 3.

We first construct the more convenient covering; this construction consists of two parts.

Lemma 3. *For any system of congruences of the form*

$$\begin{aligned} x_1 &\equiv 2^0 \pmod{2^1} \\ x_2 &\equiv 2^1 \pmod{2^2} \\ &\vdots \\ x_\eta &\equiv 2^{\eta-1} \pmod{2^\eta} \end{aligned}$$

all residues of $\mathbb{Z}_{2^\eta}$ are covered, except for $x \equiv 0 \pmod{2^\eta}$.

Proof. We proceed by induction.
Base case: Consider $\eta = 1$. The system of congruences is:

$$x \equiv 2^{1-1} \equiv 1 \pmod{2^1}$$

This congruence covers all residues of $\{0, 1\}$ except for $0 \pmod 2$.
Inductive hypothesis: Suppose true for $\eta = k$. Then the system

$$\begin{aligned} x_1 &\equiv 2^0 \pmod{2^1} \\ x_2 &\equiv 2^1 \pmod{2^2} \\ &\vdots \\ x_k &\equiv 2^{k-1} \pmod{2^k} \end{aligned}$$

does not cover $0 \pmod{2^k}$, but all integers of other form are covered.

Consider the system in which $\eta = 2^{k+1}$:

$$\begin{aligned} x_1 &\equiv 2^0 \pmod{2^1} \\ x_2 &\equiv 2^1 \pmod{2^2} \\ &\vdots \\ x_k &\equiv 2^{k-1} \pmod{2^k} \\ x_{k+1} &\equiv 2^k \pmod{2^{k+1}} \end{aligned}$$

The first k congruences already cover all residues not congruent to $0 \pmod{2^k}$ by the induction hypothesis; that is the only integers uncovered are of the form

$$x \equiv 0 \pmod{2^{k+1}}, \;\; x \equiv 2^k \pmod{2^{k+1}}.$$

Clearly, integers of the latter form are covered by the system above. This leaves the integers $0 \pmod{2^{k+1}}$ uncovered, as desired. Thus by the principle of induction, our lemma is true. □

Lemma 4. *Let $x \equiv 0 \pmod{2^\eta}$ and let $p \leq \eta + 1$, where p is an odd prime. Then $[0] \pmod{2^\eta}$ is covered by the secondary system of congruences R:*

$$\begin{aligned} x_1 &\equiv 0 \cdot 2^\eta \pmod{p \cdot 2^{p-1}} \\ x_2 &\equiv 1 \cdot 2^\eta \pmod{p \cdot 2^{p-2}} \\ x_3 &\equiv 2 \cdot 2^\eta \pmod{p \cdot 2^{p-3}} \\ &\vdots \\ x_p &\equiv (p-1) \cdot 2^\eta \pmod{p \cdot 2^0} \end{aligned}$$

Proof. We will show that if $x \equiv 0 \pmod{2^\eta}$, then x satisfies one of the congruences of R. Observations:

- We can write every integer z in the form $z = r + y \cdot p$, where $r \in \mathbb{Z}_p$ and $y \in \mathbb{Z}$.
- $0 \leq r \leq p-1 \;\Rightarrow\; 0 \leq (p-1) - r \leq p-1 \leq \eta$.

$$\begin{aligned} x_o \equiv 0 \pmod{2^\eta} \;\Rightarrow\; x_o &= z_o \cdot 2^\eta \\ &= (r_o + y_o \cdot p) \cdot 2^\eta \\ &= r_o \cdot 2^\eta + (y_o \cdot p \cdot 2^\eta) \\ &= r_o \cdot 2^\eta + (y_o \cdot p \cdot 2^{\,\eta-(p-r_o-1)} \cdot 2^{\,p-r_o-1}) \\ &= r_o \cdot 2^\eta + (y_o \cdot 2^{\,\eta-(p-r_o-1)}) \cdot (p \cdot 2^{\,p-r_o-1}) \;\Rightarrow\; x_o \equiv r_o \cdot 2^\eta \pmod{p \cdot 2^{\,p-r_o-1}} \end{aligned}$$

That implies that x_o satisfies one of the congruences of R, as desired. Because x_o was arbitrary, our conclusion follows. □

Thus, we can cover the integers first by an application of Lemma 4 (with $\eta \geq p+1$), and then by an application of Lemma 4. We now arrive at a result similar to the five trick:

Corollary 4. ***(The 2 Trick)*** *Given some $\mathcal{B} \pmod{\mathcal{M}}$, we can cover all elements $x \equiv \mathcal{B} \pmod{\mathcal{M}}$ using the following system of $n = p + \eta$ congruences :*

$$\begin{aligned} x_1 &\equiv 2^0\mathcal{M} + \mathcal{B} \pmod{2^1\mathcal{M}} \\ x_2 &\equiv 2^1\mathcal{M} + \mathcal{B} \pmod{2^2\mathcal{M}} \\ &\vdots \\ x_\eta &\equiv 2^{\eta-1}\mathcal{M} + \mathcal{B} \pmod{2^\eta\mathcal{M}} \\ x_{\eta+1} &\equiv 0 \cdot 2^\eta\mathcal{M} + \mathcal{B} \pmod{p \cdot 2^{p-1}\mathcal{M}} \\ x_{\eta+2} &\equiv 1 \cdot 2^\eta\mathcal{M} + \mathcal{B} \pmod{p \cdot 2^{p-2}\mathcal{M}} \\ x_{\eta+3} &\equiv 2 \cdot 2^\eta\mathcal{M} + \mathcal{B} \pmod{p \cdot 2^{p-3}\mathcal{M}} \\ &\vdots \\ bx_n &\equiv (p-1) \cdot 2^\eta\mathcal{M} + \mathcal{B} \pmod{p \cdot 2^0\mathcal{M}} \end{aligned}$$

To doubly use a modulus, we must know that the secondary system of congruences R covering $x_k \equiv \mathcal{B} \pmod{\mathcal{M}}$ has moduli distinct from those of the main system of congruences (and secondary systems covering other congruences). The 2-Trick covering system is useful because it is versatile. The first part of the system always behaves in the same way, regardless of the η that's used, as the the result holds for the whole class of systems having that form. This gives us the freedom to choose the prime p for the second part of the system, because p is restricted only by η. When we consider the moduli in R, we note that they are of the form $2^\alpha \cdot p^\delta \cdot \mathcal{M}$, where $\alpha \in \{0, 1, ..., \eta\},\ \delta \in \{0, 1\},\ \alpha + \delta \neq 0$.

The lcm of the moduli of our original system S can be written $M = 2^t \cdot \hat{u}$ for $\hat{u}$ odd. Because all available candidate moduli will be used in the construction of S, if $\mathcal{M} \neq 2^t \cdot \hat{u}_i$ for $\hat{u}_i$ odd, then the modulus $m_j = 2\mathcal{M}$ is a candidate modulus for S. That is, if we consider the secondary covering R, for $x \equiv \mathcal{B} \pmod{\mathcal{M}}$, we observe that $S \cup R$ will not be a covering because the moduli

in $S \cup R$ are not distinct. If we choose p such that p and M are relatively prime, and consider only moduli of the form $\mathcal{M} = 2^t \cdot \hat{u}_i$ for $\hat{u}_i$ odd, then the moduli of R and those of S will be distinct. If there are two such moduli, then choosing $p_1,\ p_2$ such that $p_1 \neq p_2$, we have that the moduli of R_1 and R_2 are distinct, because $\mathcal{M}_1, \mathcal{M}_2$ are distinct factors of the first η_1 and η_2 moduli, respectively. Also $p_1,\ p_2$ are distinct factors of the remaining p_1 and p_2 moduli, and are also relatively prime to $\mathcal{M}_1, \mathcal{M}_2$, so that the first and second portions of systems R_1 and R_2 also preserve the distinct-moduli property that we imposed. Effectively, we can represent our R systems with single congruences.

We illustrate the power of these results with a simple example. By hand, a covering which has no congruences modulo 2, requires at least 18 congruences, and the lcm of the moduli can be no smaller than 360. If we use the arguments presented above, we can make a covering with effectively 6 congruences and an lcm of 12:

$$\begin{aligned} x_1 &\equiv 1 \pmod 3 \\ x_2 &\equiv 0 \pmod 4 \\ x_3 &\equiv 2 \pmod 4 \\ x_4 &\equiv 3 \pmod 6 \\ x_5 &\equiv 5 \pmod{12} \\ x_6 &\equiv 11 \pmod{12} \end{aligned}$$

5 Covering Construction

This section addresses the Erdős 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?" We construct coverings to show that $N \geq 2, 3, ..., 11$. The coverings appear in the appendix.

To show $N \geq 3$, we restrict ourselves to use distinct moduli greater than and equal to 3. By hand it is possible to find a covering which uses 21 linear congruences and has 360 as the lcm of the moduli (1).

To show $N \geq 4$, we restrict ourselves to use distinct moduli greater than and equal to 4. Because finding a covering system by hand is difficult, the program *cover* is used to check our work. There is a covering which uses 55 linear congruences and has $10,800$ as the lcm of the moduli (2).

To show $N \geq 5$, even with the aid of the program *cover*, the construction of a covering system is very tedious and difficult. In spite of this, it is possible to find by hand a covering which uses 58 linear congruences and has $15,120$ as the lcm of the moduli (3).

As our lowerbound on N increases, it is apparent that if coverings exist, the number of linear congruences and the lcm become very great. Consequently, more tools are required to make construction reasonable. As a result, we developed a greedy algorithm that finds systems of linear congruences that cover the integers.

Greedy algorithms work in phases by breaking up a difficult problem into a series of smaller, easier subproblems. In each phase, a decision is made that appears to be good, without regard to future consequences. In general, this means that some local optimum is chosen. This "take what you can get now" strategy is the source of the name for this class of algorithms. When the algorithm terminates, we hope that the local optimum solutions are equal to the global optimum

solution; otherwise, the algorithm produces a suboptimal solution. If the absolute best answer is not required, then simple greedy algorithms can be valuable for generating approximate answers. The algorithms required to generate exact answers are often more complicated and have longer running times than greedy algorithms [7].

We developed a greedy algorithm to find systems of linear congruences that cover the integers. This algorithm will be referred to as the KN-program for the remainder of the paper. The KN-program takes a number M and tries to find a covering system that uses only the divisors of M : $m_1, m_2, ..., m_n$ as moduli. Thus, M is the lcm of the moduli of the system of congruences. The KN-program finds linear congruences by looking at a fixed modulus, m_i, and choosing the residue, $r_i \in \mathbb{Z}_{m_i}$, such that $x \equiv r_i \pmod{m_i}$ is satisfied by the greatest number of uncovered elements of $\mathbb{Z}_M$.

5.1 Steps of the KN-program

This section explains the steps taken when the KN-program attempts to construct a covering.

We set M to be the lcm of the moduli for a system of linear congruences. The program finds all the divisors of M and inserts them into an array called div[M]. The moduli of our system are all elements of div[M]. The moduli are stored in this array in nondecreasing order. Next, the integers 1 through M are made into an array called lcmcover[M]. We note that lcmcover[M], with ordering removed and considered $\pmod{M}$ is equivalent to the residue system $\mathbb{Z}_M$. Thus to cover all the integers we only need to cover all the integers in the lcmcover[M] array. The KN-program takes the first modulus, m_1, in our div[M] array and finds the residue, $r_1 \in \mathbb{Z}_{m_1}$, which covers the most elements of the lcmcover[M] array. The algorithm then removes all integers of the form $m_1 \cdot z + r_1,\ z \in \mathbb{N}$ from the lcmcover[M] array. Finally, the KN-program inserts r_1 (and all following residues r_i) into an array called res[M]. Thus, between res[M] and div[M], the locally optimal linear congruence $x \equiv r_1 \pmod{m_1}$ is stored.

Again, the KN-program removes all integers of the form $m_2 \cdot z + r_2,\ z \in \mathbb{N}$, from the reduce lcmcover[M] array. Finally the KN-program inserts the residue, r_2, into the res[M] array. Furthermore, the KN-program continues this process until the lcmcover[M] array is empty, and we have a covering, or it uses all of the modulus from the div[M] array, and the system is not a covering. The i-th entry of res[M] (r_i) and the i-th entry of div[M] (m_i) represent the congruence $x \equiv r_i \pmod{m_i}$, and so in the case of success, the covering system is stored in these two arrays.

Using techniques developed in the previous section, we can modify the KN-program. The "2-Trick" allows us to doubly use some moduli, that is, to insert duplicate moduli into the div[M] array. In particular, these repeatable moduli are of the form $2^t \cdot u$ where 2^t is the highest power of 2 that's a factor of M and u is an odd factor of M. Recall that because the doubly used moduli do not change the lcm of the system of congruences, we do not change the size of the lcmcover[M] array. The size of the div[M] array increases without changing the size of the lcmcover[M] array. This augmentation of the div[M] array is the only change between the original KN-program and the modified version; the modified KN-program uses the same steps as the original to find systems of congruences that cover the integers.

Using the modified KN-program, we found a covering that shows $N \geq 11$, that is, all moduli are greater than or equal to 11.

Least Modulus	LCM of Moduli	Number of Congruences	Prime Decomposition	$\sum \frac{1}{m_i}$	Remarks
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	**
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	3,0240	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
** linear congruences done by hand

Appendix 1: Coverings

To conserve space the moduli and residues are left unassembled in the div[k] and res[k] arrays:

$N \geq 3$:

LCM $120 = 2^3 \cdot 3 \cdot 5$
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)

LCM$360 = 2^3 \cdot 3^2 \cdot 5$ no Trick
div[360]=(3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60)
res[360]=(0, 0, 0, 1, 2, 2, 1, 5, 2, 4, 3, 22, 29, 14, 6, 8, 14)

(1) LCM$360 = 2^3 \cdot 3^2 \cdot 5$ done by hand
div[360] = (3, 4, 5, 6, 8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 120, 180, 360)

LCM $720 = 2^4 \cdot 3^2 \cdot 5$ no Trick
div[720]=(3, 4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 30, 36, 40, 45, 48, 60, 72)
res[720]=(0, 0, 0, 1, 2, 2, 1, 5, 8, 6, 5, 14, 22, 8, 35, 6, 44, 14, 46, 71)

$N \geq 4$:

LCM $720 = 2^4 \cdot 3^2 \cdot 5$ no Trick

div[720]= (4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 30, 36, 40, 45, 48, 60, 72, 80, 90, 120, 144, 180)
res[720]=(0, 0, 1, 2, 0, 1, 5, 3, 6, 3, 7, 11, 9, 2, 6, 42, 46, 23, 14, 14, 29,119, 62, 102)

(2) LCM $10, 800$ done by hand
div[10,800] = (4, 5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 25, 27, 30, 36, 40, 45, 50, 48, 54, 60, 72, 75, 80, 90, 100, 108, 120, 144, 150, 180, 200, 216, 225, 240, 270, 300, 360, 400, 432, 450, 540, 600, 675, 720, 900, 1080, 1200, 1350, 1800, 2160, 2700, 3600, 5400)

$N \geq 5$:
LCM $4, 320 = 2^5 \cdot 3^3 \cdot 5$ with no trick
div[4,320]=(5, 6, 8, 9, 10, 12, 15, 16, 18, 20, 24, 27, 30, 32, 36, 40, 45, 48, 54, 60, 72, 80, 90, 96, 108, 120, 135, 144, 160, 180, 216, 240, 270, 288, 360, 432, 480, 540, 720, 864, 1080, 1440, 2160)
res[4,320]=(0, 0, 1, 1, 1, 2, 2, 3, 4, 3, 8, 7, 9, 5, 16, 13, 14, 20, 16, 27, 31, 77, 29, 44, 106, 109, 44, 139, 117, 7, 79, 188, 89, 92, 79, 43, 476, 539, 44, 53, 269, 619, 619)

LCM 720 with trick
div[720]=(5, 6, 8, 9, 10, 12, 15, 16, 16, 18, 20, 24, 30, 36, 40, 45, 48, 48, 60, 72, 80, 80, 90, 120, 144, 144, 180, 240, 240)
res[720]=(0, 0, 1, 1, 1, 2, 2, 3, 5, 4, 3, 8, 9, 16, 7, 34, 20, 44, 59, 34, 13,27, 49, 29, 70, 142, 57, 157, 237)

(3) LCM $15, 120$ done by hand
div[15120] = (5, 6, 7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 24, 27, 28, 30, 35, 36, 40, 42, 45, 48, 54, 56, 60, 63, 70, 72, 80, 84, 90, 105, 108, 112, 120, 126, 140, 168, 180, 189, 210, 216, 240, 252, 270, 280, 315, 336, 360, 378, 420, 432, 504, 540, 560, 630, 720)

$N \geq 6$:
LCM 1260 with trick
div[1260]=(6, 7, 9, 10, 12, 12, 14, 15, 18, 20, 20, 21, 28, 28, 30, 35, 36, 36, 42, 45, 60, 60, 63, 70, 84, 84, 90, 105, 126, 140, 140, 180, 180, 210, 252, 252, 315, 420, 420, 630, 1260, 1260)
res[1260]=(0, 0, 1, 1, 2, 8, 1, 4, 4, 3, 5, 2, 3, 5, 9, 27, 16, 34, 11, 7, 15, 33, 4, 13, 17, 47, 27, 104, 121, 55, 17, 87, 115, 177, 103, 25, 102, 73,327, 205, 1213, 1257)

$N \geq 7$:
LCM 5040 with trick
div[5040]=(7, 8, 9, 10, 12, 14, 15, 16, 16, 18, 20, 21, 24, 28, 30, 35, 36, 40, 42, 45, 48, 48, 56, 60, 63, 70, 72, 80, 80, 84, 90, 105, 112, 112, 120, 126, 140, 144, 144, 168, 180, 210, 240, 240, 252, 280, 315, 336, 336, 360, 420, 504, 560, 560, 630, 720, 720, 840, 1008, 1008, 1260, 1680, 1680)
res[5040]=(0, 0, 0, 1, 2, 1, 4, 4, 12, 3, 3, 4, 5, 2, 7, 5, 6, 33, 11, 24, 10, 22, 3, 47, 3, 55, 30, 13, 17, 10, 87, 100, 34, 50, 89, 23, 45, 138, 46, 143, 119, 65, 133, 137, 166, 255, 60, 190, 286, 179, 299, 354, 82, 306, 555, 213, 359, 839, 642, 1006, 419, 418, 1199)

LCM 30240 with no trick
div[30240]=(7, 8, 9, 10, 12, 14, 15, 16, 18, 20, 21, 24, 27, 28, 30, 32, 35, 36, 40, 42, 45, 48, 54, 56, 60, 63, 70, 72, 80, 84, 90, 96, 105, 108, 112, 120, 126, 135, 140, 144, 160, 168, 180, 189, 210, 216, 224, 240, 252, 270, 280, 288, 315, 336, 360, 378, 420, 432, 480, 504, 540, 560, 630,

672, 720, 756, 840, 864, 945, 1008, 1080, 1120, 1260, 1440, 1512, 1680, 1890, 2016, 2160, 2520, 3024)
res[30240]=(0, 0, 0, 1, 2, 1, 4, 4, 3, 3, 4, 5, 6, 2, 7, 12, 5, 30, 33, 10, 24, 44, 24, 3, 47, 13, 65, 17, 15, 22, 29, 28, 55, 42, 17, 13, 41, 42, 45, 12, 55, 82, 179, 132, 95, 213, 54, 137, 34, 59, 195, 46, 149, 334, 137, 118, 179, 204, 455, 370, 267, 535, 509, 166, 257, 69, 545, 69, 690, 118, 537, 62, 59, 213, 473, 1529, 375, 1630, 2013, 2489, 1959)

$N \geq 8$:

LCM 45360 with trick
div[45360]=(8, 9, 10, 12, 14, 15, 16, 16, 18, 20, 21, 24, 27, 28, 30, 35, 36, 40, 42, 45, 48, 48, 54, 56, 60, 63, 70, 72, 80, 80, 81, 84, 90, 105, 108, 112, 112, 120, 126, 135, 140, 144, 144, 162, 168, 180, 189, 210, 216, 240, 240, 252, 270, 280, 315, 324, 336, 336, 360, 378, 405, 420, 432, 432, 504, 540, 560, 560, 567, 630, 648, 720, 720, 756, 810, 840, 945, 1008, 1008, 1080, 1134, 1260, 1296)
res[45360]=(0, 0, 1, 2, 1, 4, 4, 12, 3, 3, 4, 5, 6, 2, 7, 0, 30, 33, 5, 10, 10, 22, 15, 3, 47, 6, 65, 6, 2, 18, 24, 11, 29, 40, 105, 62, 78, 13, 41, 44, 55, 42, 17, 51, 17, 59, 31, 115, 41, 226, 137, 178, 89, 265, 160, 159, 238, 334, 137, 94, 134, 395, 258, 402, 473, 539, 25, 50, 157, 265, 113, 130, 257, 10, 59, 329, 779, 766, 641, 809, 346, 149, 1102)

$N \geq 9$:

LCM 15120*3*5 with trick
div[15120*3*5]=(9, 10, 12, 14, 15, 16, 16, 18, 20, 21, 24, 25, 27, 28, 30, 35, 36, 40, 42, 45, 48, 48, 50, 54, 56, 60, 63, 70, 72, 75, 80, 80, 81, 84, 90, 100, 105, 108, 112, 112, 120, 126, 135, 140, 144, 144, 150, 162, 168, 175, 180, 189, 200, 210, 216, 225, 240, 240, 252, 270, 280, 300, 315, 324, 336, 336, 350, 360, 378, 400, 400, 405, 420, 432, 432, 450, 504, 525, 540, 560, 560, 567, 600, 630, 648, 675, 700, 720, 720, 756, 810, 840, 900, 945, 1008, 1008, 1050, 1080, 1134, 1200, 1200, 1260, 1296, 1296, 1350, 1400, 1512, 1575, 1620, 1680, 1680, 1800, 1890, 2025, 2100, 2160, 2160, 2268, 2520, 2700, 2800, 2800, 2835, 3024, 3024, 3150, 3240, 3600, 3600, 3780, 4050, 4200, 4536, 4725, 5040, 5040, 5400, 5670, 6300, 6480, 6480, 7560, 8100, 8400, 8400, 9072, 9072, 9450, 10800, 10800, 11340, 12600, 14175, 15120, 15120, 16200, 18900, 22680, 25200, 25200, 28350, 32400, 32400)
res[15120*3*5]=(0, 0, 1, 1, 2, 3, 7, 4, 4, 2, 5, 1, 3, 6, 8, 11, 33, 14, 10, 33, 31, 43, 6, 21, 26, 28, 3, 36, 17, 11, 34, 74, 12, 35, 42, 16, 7, 93, 27, 47, 52, 59, 48, 126, 15, 123, 146, 66, 41, 86, 118, 38, 96, 22, 137, 186, 112, 232, 142, 102, 166, 136, 37, 120, 299, 335, 296, 358, 101, 196, 396, 282, 382, 255, 363, 5, 257, 416, 65, 123, 319, 74, 89, 95, 209, 561, 366, 178, 538, 143, 768, 502, 113, 578, 329, 833, 179, 929, 263, 59, 299, 935, 425, 641, 96, 739, 647, 591, 173, 1103, 395, 473, 353, 38, 1019, 1055, 281, 395, 473, 546, 249, 809, 200, 1151, 1403, 3119, 713, 1409, 2849, 2999, 443, 515, 425, 4371, 3035, 1775, 281, 1253, 731, 2585, 6473, 6443, 641, 5771, 1841, 7553, 6473, 2441, 3521, 6671, 7733, 3419, 206, 3419, 12089, 3881, 1505, 4529, 12593, 16121, 8963, 7355, 31931)

$N \geq 10$:

LCM 997,920 with trick
div[997,920]=(10, 11, 12, 14, 15, 16, 18, 20, 21, 22, 24, 27, 28, 30, 32, 32, 33, 35, 36, 40, 42, 44, 45, 48, 54, 55, 56, 60, 63, 66, 70, 72, 77, 80, 81, 84, 88, 90, 96, 96, 99, 105, 108, 110, 112, 120,

126, 132, 135, 140, 144, 154, 160, 160, 162, 165, 168, 176, 180, 189, 198, 210, 216, 220, 224, 224, 231, 240, 252, 264, 270, 280, 288, 288, 297, 308, 315, 324, 330, 336, 352, 352, 360, 378, 385, 396, 405, 420, 432, 440, 462, 480, 480, 495, 504, 528, 540, 560, 567, 594, 616, 630, 648, 660, 672, 672, 693, 720, 756, 770, 792, 810, 840, 864, 864, 880, 891, 924, 945, 990, 1008, 1056, 1056, 1080, 1120, 1120, 1134, 1155, 1188, 1232, 1260, 1296, 1320, 1386, 1440, 1440, 1485, 1512, 1540, 1584, 1620, 1680, 1760, 1760, 1782, 1848, 1890, 1980, 2016, 2016, 2079, 2160, 2268, 2310, 2376, 2464, 2464, 2520, 2592, 2592, 2640, 2772, 2835, 2970, 3024, 3080, 3168, 3168, 3240, 3360, 3360, 3465, 3564, 3696, 3780, 3960, 4158, 4320, 4320, 4455, 4536, 4620, 4752, 5040, 5280, 5280, 5544, 5670, 5940, 6048, 6048, 6160, 6237, 6480, 6930, 7128, 7392, 7392, 7560, 7920, 8316, 8910, 9072, 9240, 9504, 9504, 10080, 10080, 10395, 11088, 11340, 11880, 12320, 12320, 12474, 12960, 12960, 13860, 14256, 15120, 15840, 15840, 16632, 17820, 18144, 18144, 18480, 20790, 22176, 22176, 22680, 23760, 24948, 27720, 28512, 28512)

res[997920]=(0, 0, 1, 1, 2, 3, 0, 4, 0, 2, 7, 3, 5, 8, 11, 27, 5, 6, 10, 14, 3, 6, 33, 23, 4, 1, 9, 28, 60, 4, 16, 63, 18, 34, 12, 17, 10, 52, 47, 95, 3, 56, 22, 86, 37, 52, 69, 17, 48, 36, 45, 40, 74, 154, 66, 26, 53, 30, 132, 102, 16, 206, 39, 76, 93, 205, 179, 112, 81, 41, 102, 209, 15, 87, 148, 13, 96, 120, 256, 77, 54, 74, 222, 237, 96, 106, 282, 125, 310, 116, 35, 232, 472, 133, 153, 65, 202, 69, 39, 52, 361, 276, 183, 58, 245, 581, 47, 402, 741, 536, 142, 768, 293, 159, 231, 336, 48, 893, 696, 988, 405, 329, 857, 418, 349, 909, 795, 971, 250, 81, 1086, 399, 353, 119, 762, 42, 448, 303, 106, 521, 606, 1169, 776, 1656, 40, 161, 1776, 676, 159, 1671, 448, 958, 2235, 806, 257, 553, 1785, 713, 1047, 2343, 2606, 581, 1020, 346, 807, 529, 1577, 3161, 2559, 1505, 3185, 766, 653, 1673, 1506, 316, 2824, 447, 2175, 2416, 3855, 4396, 1049, 4913, 1286, 113, 5201, 3496, 4936, 1311, 2561, 2626, 283, 1193, 3076, 6593, 470, 1145, 1553, 2296, 3220, 8896, 545, 1145, 2254, 7006, 2393, 7433, 5596, 4672, 6593, 4396, 11866, 4166, 4144, 2273, 2993, 2296, 8969, 4073, 1313, 2753, 15088, 2956, 8105, 11633, 9233, 11326, 19649, 4865, 21713, 16486, 8302, 6593, 7313, 22865)

$N \geq 11$:

LCM 21,621,600 with trick

div[21,621,600] = (11, 12, 13, 14, 15, 16, 18, 20, 21, 22, 24, 25, 26, 27, 28, 30, 32, 32, 33, 35, 36, 39, 40, 42, 44, 45, 48, 50, 52, 54, 55, 56, 60, 63, 65, 66, 70, 72, 75, 77, 78, 80, 84, 88, 90, 91, 96, 96, 99, 100, 104, 105, 108, 110, 112, 117, 120, 126, 130, 132, 135, 140, 143, 144, 150, 154, 156, 160, 160, 165, 168, 175, 176, 180, 182, 189, 195, 198, 200, 208, 210, 216, 220, 224, 224, 225, 231, 234, 240, 252, 260, 264, 270, 273, 275, 280, 286, 288, 288, 297, 300, 308, 312, 315, 325, 330, 336, 350, 351, 352, 352, 360, 364, 378, 385, 390, 396, 400, 416, 416, 420, 429, 432, 440, 450, 455, 462, 468, 480, 480, 495, 504, 520, 525, 528, 540, 546, 550, 560, 572, 585, 594, 600, 616, 624, 630, 650, 660, 672, 672, 675, 693, 700, 702, 715, 720, 728, 756, 770, 780, 792, 800, 800, 819, 825, 840, 858, 864, 864, 880, 900, 910, 924, 936, 945, 975, 990, 1001, 1008, 1040, 1050, 1056, 1056, 1080, 1092, 1100, 1120, 1120, 1144, 1155, 1170, 1188, 1200, 1232, 1248, 1248, 1260, 1287, 1300, 1320, 1350, 1365, 1386, 1400, 1404, 1430, 1440, 1440, 1456, 1485, 1512, 1540, 1560, 1575, 1584, 1638, 1650, 1680, 1716, 1755, 1760, 1760, 1800, 1820, 1848, 1872, 1890, 1925, 1950, 1980, 2002, 2016, 2016, 2079, 2080, 2080, 2100, 2145, 2160, 2184, 2200, 2275, 2288, 2310, 2340, 2376, 2400, 2400, 2457, 2464, 2464, 2475, 2520, 2574, 2600, 2640, 2700, 2730, 2772, 2800, 2808, 2860, 2912, 2912, 2925, 2970, 3003, 3024, 3080, 3120, 3150, 3168, 3168, 3276, 3300)

res[21,621,600] = (0, 0, 0, 1, 1, 2, 2, 3, 2, 1, 6, 0, 1, 5, 5, 4, 10, 26, 4, 7, 8, 4, 19, 3, 5, 7, 14, 5, 5, 14, 2, 13, 28, 17, 10, 3, 67, 22, 10, 18, 3, 39, 9, 9, 82, 7, 38, 86, 58, 15, 15, 56, 104, 19, 41, 19,

118, 101, 11, 15, 22, 27, 21, 47, 40, 39, 51, 79, 159, 85, 131, 70, 145, 112, 35, 122, 6, 91, 195, 129, 11, 77, 173, 97, 209, 70, 73, 69, 51, 161, 31, 229, 10, 231, 145, 47, 197, 27, 75, 94, 280, 109, 255, 37, 110, 13, 21, 235, 185, 57, 233, 71, 245, 185, 4, 111, 25, 295, 77, 285, 251, 406, 123, 189, 370, 448, 325, 147, 147, 387, 382, 245, 191, 335, 373, 247, 21, 85, 53, 249, 576, 337, 430, 53, 231, 577, 135, 589, 303, 639, 220, 179, 165, 95, 28, 411, 329, 581, 543, 231, 769, 95, 495, 210, 295, 551, 73, 171, 459, 13, 220, 539, 205, 497, 472, 960, 853, 301, 19, 233, 35, 109, 637, 67, 555, 345, 187, 747, 153, 921, 171, 193, 435, 25, 441, 1065, 807, 424, 735, 769, 115, 711, 641, 1335, 381, 413, 1371, 507, 1421, 1183, 1255, 81, 447, 415, 113, 749, 1465, 807, 601 , 801, 153, 593, 135, 49, 1509, 717, 1017, 1845, 1215, 1513, 1029, 1001, 2009, 1796, 673, 1713, 1035, 1063, 1049, 805, 1865, 1540, 1481, 2305, 711, 241, 2235, 1035, 1022, 2089, 1473, 1495, 793, 405, 665, 1033, 2365, 2121, 245, 2765, 2129, 285, 513, 737, 640, 43, 938, 2977, 2705, 1965, 1715, 853, 1381, 133, 2965)

Appendix 2: Code for *cover* and the KN-program

***cover* (MATLAB)**

function out = wahoo(A)
y = length(A)
for $i = 1 : y$;
x = lcm$(x, A(i))$;
end;
out = x

$A = [2, 3, 4, 6, 12]$;
$B = [1, 2, 2, 4, 0]$;
y = wahoo(A);
z = length(A);
flag1= zeros$(1, y)$;
for$j = 1 : y$
for$i = 1 : z$
if$(B(i) ==$ mod $(j, A(i)))$;
flag1(j) = 1;
end
end
if(sum(flag1)==length(flag1))
disp('Success!')

end
end
find(flag1==0)

A= [moduli]
B= [residues]
y takes the LCM of the set of moduli.

The KN-program (Mathematica):

$$
\begin{aligned}
&Clear[div, trick, best, res, lcmcover, covered, done, i, M, r, z]\\
&M = 15120 * 3 * 11 * 2;\\
&div[M] = Divisors[M];\\
&If[Mod[M, 2] == 0,\\
&For[q = 1, q < (Length[div[M]] + 1), q++,\\
&If[Mod[div[M][[q]], 2] == 1,\\
&div[M] = AppendTo[div[M], M/(div[M][[q]])], 0]\\
&];\\
&div[M] = Sort[div[M], \#1 < \#2\&], 0]\\
&r = 9;\\
&For[i = 1, i < r + 1, i++,\\
&div[M] = Delete[div[M], 1]\\
&]\\
&Clear[lcmcover, s]\\
&res[M] = Table[-1, \{i, Length[div[M]]\}];\\
&lcmcover[M] = Table[i, i, M];\\
&dcheck = 9;\\
&For[s = 3, s < (Length[div[M]] + 1 - dcheck), s++,\\
&y = 0;\\
&T = 0;\\
&For[w = 0, w < (div[M][[s]]), w++,\\
&x = 0;\\
&For[t = 1, t < (Length[lcmcover[M]] + 1), t++,\\
&If[Mod[lcmcover[M][[t]], div[M][[s]]] == w, x++, 0]\\
&If[x > y, T = w; y = x; res[M] = ReplacePart[res[M], T, s], 0];\\
&];\\
&];\\
&lcmcover[M] =
\end{aligned}
$$

$$DeleteCases[(lcmcover[M]-T)/div[M][[s]],\_Integer]div[M][[s]]+$$
$$T;$$
$$Print[T];Print[mod];$$
$$If[Length[lcmcover[M]]==0,s=(Length[div[M]]+1-dcheck);$$
$$Print[done],0];$$
$$]$$

References

[1] Erdős, Paul (1950): "On integers of the form $2^k + p$ and some related problems." *Summa Brasil.Math*, 2, 113-123.

[2] Filaseta, Michael (2000). "On coverings of the integers associated with an irreducibility theorem of A. Schinzel." *Number Theory for the Millennium* (2000), 1-24.

[3] Gibson, D.J (2006). *Covering Systems.* Doctoral Dissertation at U Illinios at Urbana-Champaign, 2006.

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

[5] Jones, F. and J. Jones, *Elementary Number Theory*, Springer-Verlag, London, 2003.

[6] Sierpinski, Waclaw. "Sur un probleme concernment les nombres k 2n +1." *Elem. Math.*, 15 (1960) 63-74.

[7] Weiss, Mark Allen, *Data Structures and Algorithm Analysis in Java™* Addison-Wesley, 1999.