MATHEMATICS OF COMPUTATION
Volume 78, Number 266, April 2009, Pages 1127–1146
S 0025-5718(08)02154-6
Article electronically published on September 10, 2008

A COVERING SYSTEM WITH LEAST MODULUS 25

DONALD JASON GIBSON

Abstract. A collection of congruences with distinct moduli, each greater than 1, such that each integer satisfies at least one of the congruences, is said to be a covering system. A famous conjecture of Erdös from 1950 states that the least modulus of a covering system can be arbitrarily large. This conjecture remains open and, in its full strength, appears at present to be unattackable. Most of the effort in this direction has been aimed at explicitly constructing covering systems with large least modulus. Improving upon previous results of Churchhouse, Krukenberg, Choi, and Morikawa, we construct a covering system with least modulus 25. The construction involves a large-scale computer search, in conjunction with two general results that considerably reduce the complexity of the search.

1. Introduction

A collection of congruences with distinct moduli, each greater than 1, such that each integer satisfies at least one of the congruences, is said to be a *covering system*. The requirement that the moduli be distinct and greater than 1 is what makes covering systems an interesting and nontrivial subject; indeed, it is not obvious that there exist any covering systems. The first occurrence of covering systems appears to be in a 1950 paper of Erdös [4], showing that the congruences $\{0 \bmod 2,\ 0 \bmod 3,\ 1 \bmod 4,\ 3 \bmod 8,\ 7 \bmod 12,\ 23 \bmod 24\}$ form a covering system. Erdös used this result to answer a question of Romanoff, showing that there exists an infinite arithmetic progression consisting only of odd numbers, no term of which can be written as a prime plus a power of 2.

Aside from its intrinsic interest, the study of covering systems is motivated by problems in seemingly unrelated areas. In addition to the Romanoff problem, covering systems arise in similar representation problems from additive number theory (e.g., Sierpiński [21]) and irreducibility questions for certain polynomials (e.g., Schinzel [19], Filaseta [7]). Covering systems have surprising connections to finite geometry (e.g., Berger, Felzenbaum, and Fraenkel [1], and Simpson and Zeilberger [22]), group theory (e.g., Korec and Znám [12]), and error-correcting codes (e.g., Schönheim [20]). For more on these applications, we refer the reader to the surveys of Znám [25] and Porubský and Schönheim [17].

Erdös remained interested in covering systems throughout his life, and he posed several problems and conjectures about such systems (see, for example, the section on Covering Congruences in [6]), the most famous of which is the following:

Received by the editor August 27, 2007 and, in revised form, February 23, 2008.
2000 *Mathematics Subject Classification.* Primary 11B25; Secondary 11A07, 11B75.

Least Modulus Conjecture. There exist covering systems with least modulus arbitrarily large.

Erdös [5] offered $1000 for a solution to the Least Modulus Conjecture. Indeed, he began the section in [5] pertaining to covering congruences by stating "I start with my favourite problem...". The Least Modulus Conjecture remains unsolved and seems to be an extremely hard problem.

The first systematic attack on the Least Modulus Conjecture is due to Churchhouse [3] in 1968. Using a computer, he found covering systems with least modulus $m_1 = 2, \ldots, 9$. The system with least modulus 9 uses the divisors of $604,800 = 2^7 \times 3^3 \times 5^2 \times 7$ as moduli.

Next, in 1971, Krukenberg [13] gave examples of covering systems with least modulus $m_1 = 2, \ldots, 18$. The system with $m_1 = 18$ uses the divisors of

$$2^7 \times 3^3 \times 5^2 \times 7^2 \times 11^2 \times 13^2 \times 17^2 \times 19 = 475,371,719,222,400$$

as moduli. Krukenberg remarked, "The structure at this stage is, to say the least, quite complicated and not easy to visualize."

At roughly the same time, Choi [2] used a theoretical result to find a covering system with least modulus 20. He wrote, "It is conceivable that a further elaboration of the method of the present paper is capable of producing a more favorable N than 20 but the amount of computations may then become prohibitive." Neither Krukenberg nor Choi appears to have used computers to aid in the search.

Using a different theoretical approach, in 1981, Morikawa [15] (also see [14]) exhibited a covering system with least modulus 24. The papers containing this claim appeared in an obscure Japanese publication and are somewhat difficult to follow.

A result of Stockmeyer and Meyer [23] relates covering systems to a famous problem from computational complexity. Specifically, they established that determining whether a given set of congruences forms a covering system is co-NP-complete.

On the theoretical side, Filaseta, Ford, Konyagin, Pomerance, and Yu [8] showed in recent work that, for a covering system to exist with least modulus m_1, the number of congruences in the system must be very large, in the sense that the sum of the reciprocals of the moduli tends to infinity if m_1 tends to infinity. (Easy density considerations show that the sum of the reciprocals is greater than or equal to 1.)

In this paper (also see the author's thesis [9]), we construct a covering system with least modulus 25. This improves both the acknowledged record of Choi and Morikawa's claim of 24. By a different method, Nielsen [16] exhibits a covering system with least modulus 36.

In Sections 2 and 3, we prove two results which show that, subject to certain conditions, a set of congruences that is an almost cover, in the sense that it covers $\mathbb{N}$ save for certain sparse arithmetic progressions, or that it covers $\mathbb{N}$ but allows some congruences to have the same moduli, can be transformed into a legitimate covering system with distinct moduli.

In Section 4, we describe the algorithm used to produce the covering system. Our basic approach is a greedy algorithm. Used by Churchhouse to exhibit covering systems with least modulus 9 and smaller, the method remains applicable and effective today. With today's computers, a least modulus of the order of the mid teens is attainable, but a pure greedy search seems incapable of reaching the values

18 and 20 of Krukenberg and Choi. To construct a covering system with least modulus 25, we therefore employ a combination of this method and the two results from Sections 2 and 3.

In Section 5, we describe the implementation of the algorithm.

In Section 6, we present our main result, which establishes a new record for the Least Modulus Conjecture by exhibiting a covering system with a least modulus of 25.

We believe the methods we use here are applicable to other problems on covering systems, and we plan on investigating some of these problems in future work. For this reason, we have stated and proved the results in Sections 2 and 3 in a slightly more general form than what we will need here.

2. Converting almost covers to covers: First method

In this section, we present a result, Proposition 1, based on ideas from Morikawa's paper [14], which, in turn, have their origins in Krukenberg's work (see Theorems 6.1 and 6.2 in [13]).

The main result of this section, Proposition 1, depends on Lemmas 1 and 2.

To simplify the statements of the results in this section, we define, for a set of congruences $\mathcal{C}$, $\mu(\mathcal{C})$ as the least modulus appearing in $\mathcal{C}$, i.e.,

$$\mu(\mathcal{C}) = m_1 \quad \text{if} \quad \mathcal{C} = \{a_i \bmod m_i : 1 \le i \le k\}, \quad m_1 \le m_2 \le \cdots \le m_k. \tag{2.1}$$

Trivially, a congruence $0 \bmod p$ in a set of congruences can be replaced by p^{r-1} congruences $\bmod p^r$ which replace the modulus p by a larger one (if $r > 1$) at the expense of using this larger modulus multiple times. Lemma 1 shows that under certain conditions, a set of congruences can be transformed in a similar manner, but without having this increase in multiplicity. Where the initial set of congruences $\mathcal{C}$ in some sense misses the progression $0 \bmod p^e$, the resulting set of congruences $\mathcal{C}'$ misses a much sparser progression, $0 \bmod p^{e+r}$.

Lemma 1. *Let $L = p^e Q$, where p is a prime, $e \in \mathbb{N}$, and $(p, Q) = 1$. Let $\mathcal{C}$ be a set of congruences whose moduli are distinct divisors of L.*

Let $r \in \mathbb{N}$, let $\mathcal{D}_p$ and $\mathcal{D}'_p$ be the sets of congruences defined by

$$\mathcal{D}_p = \{j \bmod p^e : 0 \le j \le p^{e-1} - 1\}, \tag{2.2}$$

$$\mathcal{D}'_p = \{j \bmod p^{e+r} : 0 \le j \le p^{e-1} - 1\}, \tag{2.3}$$

and let $\mathcal{K}$ be a set of congruences whose moduli are prime power divisors of Q.

If $\mathcal{C} \cup \mathcal{D}_p \cup \mathcal{K}$ covers $\mathbb{N}$, then there exists a set of congruences $\mathcal{C}'$ having the following properties:

(i) *The moduli of the congruences in $\mathcal{C}'$ are distinct divisors of $p^r L$.*
(ii) *$\mu(\mathcal{C}') = \mu(\mathcal{C})$.*
(iii) *$\mathcal{C}' \cup \mathcal{D}'_p \cup \mathcal{K}$ covers $\mathbb{N}$.*

Proof. We shall construct $\mathcal{C}'$ by augmenting the given set of congruences $\mathcal{C}$ by sets of r new congruences. Here each set of r new congruences will correspond to a congruence $a \bmod m$ from $\mathcal{C}$ with $p^e \| m$, where e is the positive integer specified in the hypotheses of the lemma.

Specifically, fix a congruence $a \bmod m$ from $\mathcal{C}$ with $p^e \| m$. Let x, y, and b be defined (via the division algorithm) by

$$a \equiv xp^{e-1} + b \bmod p^e, \quad 0 \le x \le p-1, \quad 0 \le b \le p^{e-1} - 1, \tag{2.4}$$

$$a \equiv y \bmod \frac{m}{p^e}, \quad 0 \le y \le \frac{m}{p^e} - 1. \tag{2.5}$$

We define a set $\mathcal{C}_m$ of r new congruences by

$$\mathcal{C}_m = \{b_t(m) \bmod p^t m : 1 \le t \le r\},$$

with $b_t = b_t(m)$ satisfying

$$b_t \equiv xp^{e+t-1} + b \bmod p^{e+t}, \tag{2.6}$$

$$b_t \equiv y \bmod \frac{m}{p^e}. \tag{2.7}$$

Since, by the hypothesis $p^e \| m$, we have $(p^{e+t}, m/p^e) = 1$, the Chinese Remainder Theorem guarantees that this system has a solution b_t and that the solution is unique modulo $p^t m$.

We now define $\mathcal{C}'$ by

$$\mathcal{C}' = \mathcal{C} \cup \bigcup_{\substack{a \bmod m \in \mathcal{C} \\ p^e \| m}} \mathcal{C}_m. \tag{2.8}$$

We need to show that this system satisfies properties (i)–(iii) of the lemma.

Observe that a modulus of $\mathcal{C}'$ is either a modulus of $\mathcal{C}$, or it is of the form $p^t m$, $1 \le t \le r$, where m ranges over those moduli of $\mathcal{C}$ with $p^e \| m$. Since, by assumption, the moduli of $\mathcal{C}$ are distinct, those of $\mathcal{C}'$ are also distinct. Moreover, since, by hypothesis, each modulus m is a divisor of L, the latter moduli are divisors of $p^r L$. Hence property (i) holds.

Property (ii), that $\mathcal{C}$ and $\mathcal{C}'$ have the same least modulus, holds trivially, since the new moduli are all larger than the smallest modulus m in $\mathcal{C}$, and each modulus in $\mathcal{C}$ is also a modulus in $\mathcal{C}'$.

It remains to show (iii), i.e., that $\mathcal{C}' \cup \mathcal{D}'_p \cup \mathcal{K}$ covers $\mathbb{N}$. To that end, fix $n \in \mathbb{N}$, and first suppose that for each j with $0 \le j \le p^{e-1} - 1$ we have $n \not\equiv j \bmod p^e$. Hence, n is not covered by $\mathcal{D}_p$. Since $\mathcal{C} \cup \mathcal{D}_p \cup \mathcal{K}$ covers $\mathbb{N}$, n must be covered by a congruence from $\mathcal{C} \cup \mathcal{K}$. By (2.8), this same congruence belongs to $\mathcal{C}' \cup \mathcal{K}$, and so n is covered by $\mathcal{C}' \cup \mathcal{D}'_p \cup \mathcal{K}$.

Now suppose that $n \equiv j \bmod p^e$ for some j such that $0 \le j \le p^{e-1} - 1$. Then $p^f \| (n-j)$ for some $f \ge e$. We consider two cases, namely $f \ge e+r$ and $e \le f < e+r$.

In the first case, we have $p^f \| (n-j)$ with $f \ge e + r$, so that

$$n \equiv j \bmod p^{e+r}.$$

Since $0 \le j \le p^{e-1} - 1$, n is covered by a congruence from $\mathcal{D}'_p$.

In the second case, we have $p^f \| (n-j)$ with $e \le f < e + r$. Let n' be a solution to the system

$$n' \equiv \frac{n-j}{p^f} p^{e-1} + j \bmod p^e, \tag{2.9}$$

$$n' \equiv n \bmod \frac{L}{p^e}. \tag{2.10}$$

Such a solution is guaranteed to exist by the Chinese Remainder Theorem, since, by assumption, $L = p^e Q$ with $(p, Q) = 1$, and so $(p^e, L/p^e) = 1$. Since $(n-j)/p^f \not\equiv 0 \bmod p$ and $0 \le j \le p^{e-1} - 1$, we have $n' \not\equiv 0, 1, \ldots, p^{e-1} - 1 \bmod p^e$, and so n' is not covered by $\mathcal{D}_p$. Since $\mathcal{C} \cup \mathcal{D}_p \cup \mathcal{K}$ covers $\mathbb{N}$, n' must be covered by a congruence in $\mathcal{C}$ or in $\mathcal{K}$. If n' is covered by a congruence in $\mathcal{K}$, (2.10) yields that n is covered by the same congruence, since the moduli in $\mathcal{K}$ are prime power divisors of $Q = L/p^e$. It remains therefore to consider the case when n' is covered by some congruence in $\mathcal{C}$, say $n' \equiv a \bmod m \in \mathcal{C}$. We will show that n is covered by some congruence from $\mathcal{C}'$.

To that end, we first show that we may assume that $p^e \| m$. If not, we can write $m = p^\alpha w$, with $(p, w) = 1$ and $0 \le \alpha < e$, since, by assumption, p^e is the largest power of p dividing any of the moduli in $\mathcal{C}$. By (2.9), we have

$$n' \equiv j \equiv n \bmod p^\alpha. \tag{2.11}$$

By (2.10), we have

$$n' \equiv n \bmod w. \tag{2.12}$$

Combining (2.11) and (2.12) gives

$$n' \equiv n \bmod p^\alpha w,$$

and so $n \equiv a \bmod m$. Since the congruence $a \bmod m$ belongs to $\mathcal{C}$, and hence to $\mathcal{C}'$, n is covered by $\mathcal{C}' \cup \mathcal{D}'_p \cup \mathcal{K}$.

Therefore, we may assume that $p^e \| m$. Setting $t = f - e + 1$, we claim that the congruence $b_t(m) \bmod p^t m \in \mathcal{C}'$ covers n. To see this, note that by (2.4) and (2.5), $n' \equiv a \bmod m$ is equivalent to

$$n' \equiv a \equiv xp^{e-1} + b \bmod p^e, \tag{2.13}$$

$$n' \equiv a \equiv y \bmod \frac{m}{p^e}. \tag{2.14}$$

Comparing (2.13) with (2.9) yields that $b = j$ and

$$x \equiv \frac{n-j}{p^f} \bmod p. \tag{2.15}$$

From (2.15), we get

$$xp^{e+t-1} \equiv n - j \bmod p^{e+t}, \tag{2.16}$$

or equivalently,

$$n \equiv xp^{e+t-1} + j \equiv b_t(m) \bmod p^{e+t}. \tag{2.17}$$

From (2.10), we get

$$n \equiv n' \bmod \frac{m}{p^e}. \tag{2.18}$$

Combining (2.18) with (2.14) and (2.7) yields

$$n \equiv n' \equiv y \equiv b_t(m) \bmod \frac{m}{p^e}. \tag{2.19}$$

By (2.17) and (2.19), we have

$$n \equiv b_t(m) \bmod p^t m,$$

and so n is covered by a congruence from $\mathcal{C}'$. This concludes the proof of the claim that $\mathcal{C}' \cup \mathcal{D}'_p \cup \mathcal{K}$ covers $\mathbb{N}$. □

Lemma 2. *Let $L = \prod_{i=1}^{s} p_i^{e_i}$, where $p_1 < \cdots < p_s$ are primes, and, for $1 \le i \le s$, we have $e_i \in \mathbb{N}$. Let $\mathcal{C}$ be a set of congruences whose moduli are distinct divisors of L.*

For $1 \le i \le s$, let $r_i \in \mathbb{N}$, and let $\mathcal{D}$ and $\mathcal{D}'$ be the sets of congruences defined by

$$\mathcal{D} = \bigcup_{i=1}^{s} F_i, \tag{2.20}$$

$$\mathcal{D}' = \bigcup_{i=1}^{s} G_i, \tag{2.21}$$

with each F_i and G_i defined by

$$F_i = \{j \bmod p_i^{e_i} : 0 \le j \le p_i^{e_i - 1} - 1\}, \tag{2.22}$$

$$G_i = \{j \bmod p_i^{e_i + r_i} : 0 \le j \le p_i^{e_i - 1} - 1\}. \tag{2.23}$$

If $\mathcal{C} \cup \mathcal{D}$ covers $\mathbb{N}$, then there exists a set of congruences $\mathcal{C}'$ having the following properties:

(i) *The moduli of the congruences in $\mathcal{C}'$ are distinct divisors of $\prod_{i=1}^{s} p_i^{e_i + r_i}$.*
(ii) *$\mu(\mathcal{C}') = \mu(\mathcal{C})$.*
(iii) *$\mathcal{C}' \cup \mathcal{D}'$ covers $\mathbb{N}$.*

Proof. We proceed by induction, applying Lemma 1 a total of s times. Specifically, we shall show that for each k with $1 \le k \le s$, there exists a set of congruences $\mathcal{C}^{(k)}$ whose moduli are distinct divisors of $L \prod_{i=1}^{k} p_i^{r_i}$, with $\mu(\mathcal{C}^{(k)}) = \mu(\mathcal{C})$, and such that

$$\mathcal{C}^{(k)} \cup G_k \cup \mathcal{K}^{(k)}$$

covers $\mathbb{N}$, where

$$\mathcal{K}^{(k)} = \bigcup_{i=1}^{k-1} G_i \cup \bigcup_{i=k+1}^{s} F_i, \tag{2.24}$$

(2.25)

with each G_i and F_i defined by (2.23) and (2.22), respectively.

The result of the lemma follows with the choice $\mathcal{C}' = \mathcal{C}^{(s)}$.

We begin by applying Lemma 1 with $p = p_1$, $e = e_1$, $Q = \prod_{i=2}^{s} p_i^{e_i}$, $r = r_1$, and with $\mathcal{D}_p$ and $\mathcal{D}'_p$ defined as in Lemma 1, i.e.,

$$\mathcal{D}_p = F_1, \tag{2.26}$$

$$\mathcal{D}'_p = G_1. \tag{2.27}$$

Define the set of congruences $\mathcal{K} = \mathcal{K}^{(1)}$ by

$$\mathcal{K} = \bigcup_{i=2}^{s} F_i.$$

Observe that we have

$$\mathcal{D}_p \cup \mathcal{K} = F_1 \cup \mathcal{K} = \mathcal{D},$$

where $\mathcal{D}$ is the set of congruences defined by (2.20). By hypothesis, $\mathcal{C} \cup \mathcal{D}_p \cup \mathcal{K} = \mathcal{C} \cup \mathcal{D}$ covers $\mathbb{N}$, so that by Lemma 1, there exists a set of congruences $\mathcal{C}'$ whose moduli are distinct divisors of $p^r L$, with $\mu(\mathcal{C}') = \mu(\mathcal{C})$, and such that $\mathcal{C}' \cup \mathcal{D}'_p \cup \mathcal{K}$ covers $\mathbb{N}$. We set $\mathcal{C}^{(1)} = \mathcal{C}'$, and note that $\mathcal{D}'_p = G_1$.

Suppose now that after k applications of Lemma 1, we have obtained a set of congruences $\mathcal{C}^{(k)}$ whose moduli are distinct divisors of $L\prod_{i=1}^{k} p^{r_i}$, with $\mu(\mathcal{C}^{(k)}) = \mu(\mathcal{C})$, and such that

$$\mathcal{C}^{(k)} \cup G_k \cup \mathcal{K}^{(k)}$$

covers $\mathbb{N}$, where G_k and $\mathcal{K}^{(k)}$ are defined by (2.23) and (2.24), respectively.

We apply Lemma 1 to the set of congruences $\mathcal{C}^{(k)}$, with $p = p_{k+1}$, $e = e_{k+1}$, $Q = \prod_{i=1}^{k} p_i^{e_i+r_i} \prod_{i=k+2}^{s} p_i^{e_i}$, $r = r_{k+1}$, and with $\mathcal{D}_p$ and $\mathcal{D}'_p$ defined as in Lemma 1, i.e.,

$$\mathcal{D}_p = F_{k+1}, \tag{2.28}$$

$$\mathcal{D}'_p = G_{k+1}. \tag{2.29}$$

Define the set of congruences $\mathcal{K} = \mathcal{K}^{(k+1)}$ by

$$\mathcal{K}^{(k+1)} = \bigcup_{i=1}^{k} G_i \cup \bigcup_{i=k+2}^{s} F_i.$$

Note that we have

$$\begin{aligned} G_k \cup \mathcal{K}^{(k)} &= G_k \cup \bigcup_{i=1}^{k-1} G_i \cup \bigcup_{i=k+1}^{s} F_i \\ &= \bigcup_{i=1}^{k} G_i \cup \bigcup_{i=k+1}^{s} F_i \\ &= F_{k+1} \cup \mathcal{K}^{(k+1)}. \end{aligned}$$

By the induction hypothesis,

$$\mathcal{C}^{(k)} \cup G_k \cup \mathcal{K}^{(k)} = \mathcal{C}^{(k)} \cup F_{k+1} \cup \mathcal{K}^{(k+1)}$$

covers $\mathbb{N}$, and so, by Lemma 1, there exists a set of congruences $\mathcal{C}'$ whose moduli are distinct divisors of $L\prod_{i=1}^{k+1} p^{r_i}$, with $\mu(\mathcal{C}') = \mu(\mathcal{C})$, and such that $\mathcal{C}' \cup \mathcal{D}'_p \cup \mathcal{K}$ covers $\mathbb{N}$. Defining $\mathcal{C}^{(k+1)} = \mathcal{C}'$ and noting that $\mathcal{D}'_p = G_{k+1}$, we then have that

$$\mathcal{C}^{(k+1)} \cup G_{k+1} \cup \mathcal{K}^{(k+1)}$$

covers $\mathbb{N}$. Property (i) of Lemma 1 guarantees that the moduli of $\mathcal{C}^{(k+1)}$ are distinct, and property (ii) of Lemma 1 gives $\mu(\mathcal{C}^{(k+1)}) = \mu(\mathcal{C}^{(k)})$, completing the induction. □

Proposition 1. *Let $L = \prod_{i=1}^{s} p_i^{e_i}$, where $p_1 < \cdots < p_s$ are primes, and, for $1 \le i \le s$, we have $e_i \in \mathbb{N}$. Let $\mathcal{C}$ be a set of congruences whose moduli are distinct divisors of L.*

Let $\mathcal{D}$ be the set of congruences defined by

$$\mathcal{D} = \bigcup_{i=1}^{s} \{j \bmod p_i^{e_i} : 0 \le j \le p_i^{e_i-1} - 1\}. \tag{2.30}$$

If $\mathcal{C} \cup \mathcal{D}$ covers $\mathbb{N}$, then for any $w > 1$ such that $(w, L) = 1$ there exist constants $J_i = J_i(\mathcal{C}, w)$, $1 \le i \le s$, and a set of congruences $\mathcal{C}''$ with the following properties:

(i) *The moduli of the congruences in* $\mathcal{C}''$ *are distinct, and are divisors either of* $\prod_{i=1}^{s} p_i^{J_i}$ *or of the form* $p_i^{j_i} w$, $j_i \le J_i$.
(ii) $\mu(\mathcal{C}'') = \mu(\mathcal{C})$.
(iii) $\mathcal{C}''$ *covers* $\mathbb{N}$.

Here $\mu(\cdot)$ *is defined, as in* (2.1)*, as the least modulus of a given set of congruences.*

Remarks. (i) The moduli from $\mathcal{C}$ are distinct, but the moduli from $\mathcal{D}$ need not be distinct. In particular, a modulus $p_i^{e_i}$ from $\mathcal{D}$ will appear with multiplicity $p_i^{e_i-1}$, which is larger than 1 when $e_i > 1$. Moreover, it is possible that a modulus $p_i^{e_i}$ appearing in a congruence from $\mathcal{D}$ also appears as a modulus in a congruence from $\mathcal{C}$. By the proposition, the congruences from $\mathcal{D}$ can be replaced by other congruences whose moduli are distinct amongst themselves and also avoid the moduli from $\mathcal{C}$.

(ii) With minor changes, the quantity L in both Lemma 2 and Proposition 1 can be replaced by $Q\prod_{i=1}^{s} p_i^{e_i}$, where, for $1 \le i \le s$, we have $(p_i, Q) = 1$. Such a modification might be useful when constraints other than size restrict the moduli under consideration.

(iii) Apart from the constraints $w > 1$ and $(w, L) = 1$, the choice of w is arbitrary. The flexibility in the choice of w allows Proposition 1 to be applicable in the search for a covering system when the moduli of the system are required to meet particular divisibility constraints, but this flexibility is not always needed. For the Least Modulus Conjecture, any w meeting these constraints is sufficient.

Proof. We shall apply Lemma 2 to the set of congruences $\mathcal{C}$ to obtain a set of congruences $\mathcal{C}'$, and we shall augment $\mathcal{C}'$ by additional congruences to form $\mathcal{C}''$ and ensure that $\mathcal{C}''$ covers $\mathbb{N}$, as described below.

Let $h_i \in \mathbb{N}$ be minimal such that $p_i^{h_i} w > \mu(\mathcal{C})$, let $J_i = h_i + p_i^{e_i-1} w$, and let $r_i = J_i - e_i$. We apply Lemma 2 with this choice of r_i to the set of congruences $\mathcal{C}$, obtaining a set of congruences $\mathcal{C}'$ satisfying properties (i)–(iii) of Lemma 2.

Fix i and k_i with $1 \le i \le s$ and $0 \le k_i \le p_i^{e_i-1} - 1$. We form the w additional congruences

$$a_{i,j,k_i} \bmod p_i^j w, \quad h_i + k_i w < j \le h_i + (k_i+1)w, \tag{2.31}$$

with

$$a_{i,j,k_i} \equiv k_i \bmod p_i^j,$$
$$a_{i,j,k_i} \equiv j \bmod w.$$

We define the set of congruences $\mathcal{C}''$ to be the set $\mathcal{C}'$ together with the totality of the congruences (2.31) with $1 \le i \le s$ and $0 \le k_i \le p_i^{e_i-1} - 1$. We need to show that $\mathcal{C}''$ satisfies properties (i)–(iii) of the proposition.

Property (i) follows from (2.31) and from property (i) of Lemma 2. Since, by our choice of h_i, $p_i^{h_i} w > \mu(\mathcal{C})$ for $1 \le i \le s$, property (ii) follows from property (ii) of Lemma 2.

It remains to show that property (iii) holds, i.e., that $\mathcal{C}''$ covers $\mathbb{N}$. Let $n \in \mathbb{N}$. If n is not covered by a congruence from $\mathcal{C}'$, then by property (iii) of Lemma 2, we have $n \equiv k_i \bmod p_i^{e_i+r_i}$ for some i with $1 \le i \le s$ and k_i with $0 \le k_i \le p_i^{e_i-1} - 1$. We shall show that n is covered by one of the congruences from (2.31). Indeed, note that, since $n \equiv j \bmod w$ for some j with $h_i + k_i w < j \le h_i + (k_i+1)w$, we have $n \equiv a_{i,j,k_i} \bmod p_i^j w$.This concludes the proof of property (iii) and the proposition. □

3. Converting almost covers to covers: Second method

Proposition 2. *Let $L = \prod_{i=1}^{s} p_i^{e_i}$ with $p_1 < p_2 < \cdots < p_s$ primes. Let $r \in \mathbb{N}$, let $p_s < q_1 < \cdots < q_r$ denote r primes exceeding p_s, and let $m_1, \ldots, m_r$ be r positive integers satisfying*

$$m_i | L, \qquad d(m_i) \geq q_i - i + 1, \tag{3.1}$$

where $d(m_i)$ is the number of divisors of m_i. Let $\mathcal{C}$ be a set of congruences with distinct moduli, with each modulus a divisor of L. If, for some choice of congruences $\{a_i \bmod m_i : 1 \leq i \leq r\}$,

$$\mathcal{C} \cup \bigcup_{i=1}^{r} \{a_i \bmod m_i\}$$

covers a set $A \subset \mathbb{N}$, then there exists a system of congruences $\mathcal{C}'$ with the following properties:

(i) *The moduli of the congruences in $\mathcal{C}'$ are distinct divisors of $L \prod_{j=1}^{r} q_j$.*
(ii) *$\mu(\mathcal{C}') \geq \min(\mu(\mathcal{C}), q_1)$.*
(iii) *$\mathcal{C}'$ covers A.*

Here $\mu(\cdot)$ is defined, as in (2.1)*, as the least modulus of a given set of congruences.*

Remarks. (i) In practice, the moduli of $\mathcal{C}$ will be most of the divisors m of L (e.g., all m exceeding a certain bound). Thus, each element of the sequence $\{m_i\}_{i=1}^{r}$ is typically a modulus that already appears in $\mathcal{C}$. The point of the proposition is that congruences to such repeated moduli can be replaced by congruences to unique moduli.

(ii) The sequence $\{m_i\}_{i=1}^{r}$ may contain repeated elements. (See the example below.)

(iii) A reasonable (efficient) choice for the primes q_i appearing in the proposition is the first r primes exceeding p_s. Similarly, in our application, we choose m_i to be minimal satisfying (3.1).

Proof. We shall use induction to establish, for each i with $1 \leq i \leq r$, the following statement:

(P_i) For every arithmetic progression $a \bmod m$ with $d(m) \geq q_i - i + 1$, there exists a set of congruences $\mathcal{K}_i(a, m)$ whose moduli are distinct divisors of $m \prod_{j=1}^{i} q_j$, with each modulus having largest prime divisor q_i, and such that $\mathcal{K}_i(a, m)$ covers the progression $a \bmod m$.

We first show that the result of the proposition follows from this statement. Assume (P_i) holds for each i, and set

$$\mathcal{C}' = \mathcal{C} \cup \bigcup_{i=1}^{r} \mathcal{K}_i(a_i, m_i).$$

Observe that, by (P_i), any congruence $a \bmod m$ from the set $\mathcal{K}_i(a_i, m_i)$ has $m | m_i \prod_{j=1}^{i} q_j$, and, furthermore, since $m_i | L$, we have $m | L \prod_{j=1}^{r} q_j$. This establishes the first part of (i).

To establish the second part of (i), i.e., the distinctness of the moduli, we need to consider three types of moduli pairs: the pairs from a single $\mathcal{K}_i$, those from $\mathcal{K}_i$ and $\mathcal{K}_j$ with i and j distinct, and pairs with one modulus from $\mathcal{C}$ and another from some $\mathcal{K}_i$. First, (P_i) ensures that the moduli from any single $\mathcal{K}_i(a_i, m_i)$ are

distinct. Next, if $a \bmod m$ is a congruence from $\mathcal{K}_i(a_i, m_i)$ and $a' \bmod m'$ is a congruence from $\mathcal{K}_j(a_j, m_j)$ with $i < j$, then the moduli m and m' are distinct, since by (P_i) and (P_j), m has largest prime divisor q_i, while m' has largest prime divisor q_j. Finally, if $a \bmod m$ is a congruence from $\mathcal{C}$ and $a' \bmod m'$ is a modulus from $\mathcal{K}_i(a_i, m_i)$, then m and m' are distinct, since $q_i | m'$ but $q_i \nmid m$. Thus, (i) holds.

To see that (ii) holds, i.e., that $\mu(\mathcal{C}') = \min(\mu(\mathcal{C}), q_1)$, notice that if $a \bmod m$ is a congruence from $\mathcal{K}_i(a_i, m_i)$, then by (P_i), we have $q_i | m$, and so $m \geq q_1$.

Finally, since, by hypothesis,

$$\mathcal{C} \cup \bigcup_{i=1}^{r} \{a_i \bmod m_i\}$$

covers A, and, by (P_i), $\mathcal{K}_i(a_i, m_i)$ covers $a_i \bmod m_i$ for each i, it follows that $\mathcal{C}'$ covers A, giving property (iii).

It remains to establish (P_i) for $1 \leq i \leq r$. We begin with $i = 1$, and fix an arithmetic progression $a \bmod m$, with m such that $d(m) \geq q_1$.

Let $d_1 < \cdots < d_\tau$, with $\tau = d(m)$, be the divisors of m. Note that we have $\tau = d(m) \geq q_1$, and so we can define $\mathcal{K}_1(a, m)$ as the set of congruences

$$\begin{gathered} b_{11} \bmod d_1 q_1 \\ \vdots \\ b_{1q_1} \bmod d_{q_1} q_1, \end{gathered} \tag{3.2}$$

where $b_{1j} = b_{1j}(a, m)$ is a solution to the congruence system

$$\begin{aligned} b_{1j} &\equiv a \bmod m, \\ b_{1j} &\equiv j \bmod q_1. \end{aligned}$$

Since $m | L$ and $(L, q_1) = 1$, we have $(m, q_1) = 1$, and so such a solution exists by the Chinese Remainder Theorem.

We must show that (P_1) holds. By construction, the moduli of $\mathcal{K}_1(a, m)$ are distinct divisors of mq_1, and each has largest prime divisor q_1. To see that $\mathcal{K}_1(a, m)$ covers $a \bmod m$, note that any n with $n \equiv a \bmod m$ satisfies $n \equiv j \bmod q_1$ for some $j = 1, \ldots, q_1$, and so $n \equiv b_{1j} \bmod mq_1$, thus establishing (P_1).

Note that if the sequence $\{m_i\}_{i=1}^r$ were only required to satisfy

$$m_i | L, \qquad d(m_i) \geq q_i$$

(instead of (3.1)), the result would follow by the same argument. In order to obtain the stated form, additional arguments are needed.

Now suppose that $2 \leq i \leq r$ and that $(P_1), \ldots, (P_{i-1})$ have been established. To establish (P_i), first fix an arithmetic progression $a \bmod m$, with m such that $d(m) \geq q_i - i + 1$. Let $d_1 < \cdots < d_\tau$, with $\tau = d(m)$, be the divisors of m. Note that we have $\tau = d(m) \geq q_i - i + 1$, and so we can define $\mathcal{K}_i'(a, m)$ as the set of $q_i - i + 1$ congruences

$$\begin{gathered} b_{ii} \bmod d_{i1} q_i \\ \vdots \\ b_{iq_i} \bmod d_{iq_i - i + 1} q_i, \end{gathered} \tag{3.3}$$

where $b_{ij} = b_{ij}(a,m)$ is a solution to the congruence system

$$\begin{aligned} b_{ij} &\equiv a \bmod m, \\ b_{ij} &\equiv j \bmod q_i. \end{aligned} \tag{3.4}$$

As before, the Chinese Remainder Theorem guarantees the existence of a solution.

Since the $i-1$ arithmetic progressions

$$b_{ij} \bmod mq_i, \quad 1 \le j \le i-1,$$

are not covered by $\mathcal{K}_i'(a,m)$, we need to augment $\mathcal{K}_i'(a,m)$ by additional congruences to cover these progressions. To do so, we begin by fixing j with $1 \le j \le i-1$. Since

$$d(m) \ge q_i - i + 1 \ge q_j - j + 1,$$

where the latter inequality holds because $q_1 < \cdots < q_r$, by (P_j), there exists a set of congruences $\mathcal{K}_j(a,m)$ whose moduli are distinct divisors of $m_i q_1 \dots q_j$ with each modulus having largest prime divisor q_j, and such that $\mathcal{K}_j(a,m)$ covers $a \bmod m$.

We shall now describe a set $\mathcal{K}_j''(a,m)$ that covers the arithmetic progression $b_{ij} \bmod mq_i$. For each $a' \bmod m' \in \mathcal{K}_j(a,m)$, form a corresponding congruence $a'' \bmod m''$, where $m'' = m'q_i$ and a'' is a solution to the congruence system

$$\begin{aligned} a'' &\equiv a' \bmod m', \\ a'' &\equiv j \bmod q_i, \end{aligned} \tag{3.5}$$

the existence of such a solution being guaranteed by the Chinese Remainder Theorem, and we let $\mathcal{K}_j''(a,m)$ be the set of all such congruences $a'' \bmod m''$. Since, by (P_j), $\mathcal{K}_j(a,m)$ covers $a \bmod m$, it is clear from (3.4) and (3.5) that $\mathcal{K}_j''(a,m)$ covers $b_{ij} \bmod mq_i$. Moreover, the moduli of $\mathcal{K}_j''(a,m)$ are distinct divisors of $m(q_1 \dots q_j)q_i$, with each modulus having largest prime divisor q_i and second largest prime divisor q_j.

Finally, we define $\mathcal{K}_i(a,m)$ by

$$\mathcal{K}_i(a,m) = \mathcal{K}_i'(a,m) \cup \bigcup_{j=1}^{i-1} \mathcal{K}_j''(a,m),$$

and we must show that the requirements of (P_i) have been met. By (3.3), (3.5), and the construction of the sets $\mathcal{K}_j''(a,m)$ with $1 \le j \le i-1$, we get that the moduli of $\mathcal{K}_i(a,m)$ are divisors of $m\prod_{j=1}^{i} q_j$, with each modulus having largest prime divisor q_i.

To see the distinctness of the moduli from $\mathcal{K}_i(a,m)$, first note that the moduli from any particular $\mathcal{K}_j''(a,m)$ with $1 \le j \le i-1$ are distinct as noted previously in the construction of the sets $\mathcal{K}_j''(a,m)$, and that the moduli from $\mathcal{K}_i'(a,m)$ are distinct by inspection of (3.3). That the moduli from $\mathcal{K}_i(a,m)$ are distinct now follows by observing that if m' is a modulus from $\mathcal{K}_j''(a,m)$ and m'' is a modulus from $\mathcal{K}_h''(a,m)$, then m' and m'' both have q_i as their largest prime divisor, but differ in their second largest prime divisor, as noted in the construction of the sets $\mathcal{K}_j''(a,m)$.

To conclude the proof, it remains to show that $\mathcal{K}_i(a,m)$ covers $a \bmod m$. As before, if $n \equiv a \bmod m$, then $n \equiv j \bmod q_i$ for some $j = 1, \dots, q_i$. If $i \le j \le q_i$, then n is covered by one of the congruences from (3.3), and if $1 \le j \le i-1$, then n is covered by $\mathcal{K}_j''(a,m)$.

This establishes (P_i), and the result follows by induction. □

Example 1. In this example, we shall examine the conditions of Proposition 2 when it is applied to $L = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$, the number that we shall later use as a starting point in the search for a covering system with least modulus 25. Since, in that search, the primes 19 and 23 will be needed for a different purpose than that of this theorem, we take q_i to be the i-th prime greater than 23, i.e., $q_1 = 29$, $q_2 = 31$, and so on. Note that (3.1) restricts q_i to $q_i - i + 1 \leq d(L)$. Since $d(L) = 1728$, a small calculation yields $r = 297$ and $q_{297} = 2017$ as the maximal values satisfying (3.1).

We seek to find moduli $\{m_i\}_{i=1}^{297}$ satisfying (3.1), and, for our application, we shall take m_i to be minimal, subject to this constraint.

We begin by finding m_1, i.e., the smallest modulus that Proposition 2 guarantees as available for use. With $q_1 = 29$, we have $q_1 - 1 + 1 = 29$, and (3.1) requires that $d(m_1) \geq 29$. A short calculation gives that the smallest divisor m of L with $d(m) \geq 29$ is 720, and so $m_1 = 720$. Indeed, since $d(720) = 30$ and $q_2 - 2 + 1 = 31 - 2 + 1 = 30$, we get $m_2 = 720$ as well.

For m_3, we seek the smallest m with $m|L$ such that $d(m) \geq q_3 - 3 + 1 = 37 - 3 + 1 = 35$. Another short calculation gives that the smallest divisor with this property is 1260, with $d(1260) = 36$. Similarly, one can compute that to have $d(m) \geq q_4 - 4 + 1 = 41 - 4 + 1 = 38$, we take $m = m_4 = 1680$, with $d(1680) = 40$.

We can proceed in this manner to compute the remaining moduli from this theorem, $m_5 \leq \cdots \leq m_{297}$. The divisor condition (3.1) is very restrictive, e.g., $q_{256} = 1697$, and (3.1) requires that $d(m) \geq 1697 - 256 + 1 = 1442$. The smallest modulus m with $m|L$ that has this property is L itself, and so we get that $m_{256} = m_{257} = \cdots = m_{297} = L$. Thus, Proposition 2 gives us modulus L with multiplicity $297 - 256 + 1 = 42$.

4. Algorithmic approach

In the search for a covering system using divisors of a candidate number L as moduli for the congruences, an exhaustive search fails because of the enormous size of the search space of possible sets of congruences. To reduce the size of the space considered, i.e., to consider only a small subset of the many possible lists of congruences, we employ a greedy algorithm. The results of Sections 2 and 3 significantly enhance the greedy search, and these results are easily incorporated into the algorithm.

In the context of covering systems, a greedy algorithm proceeds by selecting a "good" choice of residue class for a given modulus, dependent upon previously selected congruences, but independent of the possible choices for the remaining moduli, as we shall describe below.

We begin with a candidate L, and we let $1 < m_1 < \cdots < m_k$ be divisors of L that we wish to use as moduli. Note that any system of congruences to such moduli is equivalent to a union of congruences to modulus L, and so it suffices to work within the interval $I = [0, L - 1]$. Each of the m_i congruences with modulus m_i is considered in turn; the congruence $a_i \bmod m_i$ that eliminates the most of what remains from the interval I is selected, and the part of the interval I that $a_i \bmod m_i$ covers is removed from consideration.

We use two methods to resolve ties between equally good classes. The first method uses a pseudorandom function, which is equivalent to using a (possibly complicated) deterministic rule. Specifically, if a tie occurs between two classes,

then the currently examined class replaces the earlier one, or not, according to the outcome of the equivalent of a coin flip.

The second method uses an easily described deterministic rule to resolve ties. If several congruences of the form $a \bmod m$, $0 \le a \le m-1$, tie for efficiency, we select the class with the largest value of a.

The decision to use the largest of the classes rather than the smallest of the classes is arbitrary, as is the use of a deterministic procedure rather than a random one. Since, in practice, there seems to be little to indicate that any one of the tied classes works better than the others, what matters is that *some* choice is made. The use of randomized choices simply provides an easy way of making different choices during different runs of the program, thus creating some level of flexibility.

A key enhancement to this algorithm is the use of Propositions 1 and 2. Proposition 1 supplies additional congruences, given by (2.30), and the corresponding arithmetic progressions in I can be marked as covered before further calculations for any of the moduli $m_1, \ldots, m_k$.

Proposition 2 allows certain moduli to be used with multiplicity greater than 1. For such moduli, instead of selecting the single best class, we select the appropriate number of "best" classes, ordering the classes by how much each covers of what remains from the interval I.

Tables 1–4 illustrate the dramatic impact the use of Proposition 1 has on the complexity of the search. Although Churchhouse [3] used a greedy algorithm in his search, he did not use any further theoretical enhancements. He found covering systems with least modulus $m_1 = 2, \ldots, 9$, as indicated below. In Tables 1–4, m_1 is the least modulus, and the congruences of the associated covering system have moduli that are divisors of L.

TABLE 1. Churchhouse's Least Modulus Results

m_1	L	L
2	$2^2 \cdot 3$	12
3	$2^3 \cdot 3 \cdot 5$	120
4	$2^4 \cdot 3^2 \cdot 5$	720
5	$2^3 \cdot 3^2 \cdot 5 \cdot 7$	2,520
6	$2^5 \cdot 3^2 \cdot 5 \cdot 7$	10,080
7	$2^5 \cdot 3^3 \cdot 5 \cdot 7$	30,240
8	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7$	75,600
9	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7$	604,800

Using Proposition 1 and applying a similar greedy search, we can afford to use much smaller values of L. However, it should be noted that the covering system produced in this manner contains congruences whose moduli are divisors of a (possibly quite large) multiple of L. We do not claim that these values of L are optimal in any sense. Note that, in the last row of Table 2, $m_1 = 9$, but $9 \nmid L$. The congruence modulo 9 in the corresponding covering system is superfluous, but is included in the system for purposes of comparison to Table 1.

TABLE 2. Least Modulus Results via Proposition 1

m_1	L	L
2	2	2
3	$2 \cdot 3$	6
4	$2^2 \cdot 3$	12
5	$2 \cdot 3 \cdot 5$	30
6	$2^3 \cdot 3 \cdot 5$	120
7	$2^2 \cdot 3 \cdot 5 \cdot 7$	420
8	$2^3 \cdot 3 \cdot 5 \cdot 7$	840
9	$2^4 \cdot 3 \cdot 5 \cdot 7$	$1,680$

In contrast to Churchhouse, Krukenberg did not use a computer to search for covering systems. In [13], Krukenberg found covering systems with least modulus $m_1 = 2, \ldots, 18$. Table 3 summarizes the results with $m_1 = 10, \ldots, 18$. Note that many of the values of L are too large for easy computer implementation.

TABLE 3. Krukenberg's Least Modulus Results

m_1	L	L
10	$2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$	$1,663,200$
11	$2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	$21,621,600$
12	$2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 13$	$237,837,600$
13	$2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 13 \cdot 17$	$4,043,239,200$
14	$2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11^2 \cdot 13^2 \cdot 17$	$52,562,109,600$
15	$2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17$	$367,934,767,200$
16	$2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19$	$6,990,760,576,800$
17	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17 \cdot 19$	$27,963,042,307,200$
18	$2^7 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11^2 \cdot 13^2 \cdot 17^2 \cdot 19$	$475,371,719,222,400$

For these values of m_1, a greedy algorithm and Proposition 1 allow one to obtain covering systems with far smaller L. Again, note that the covering system produced contains congruences whose moduli are divisors of a large multiple of L. In many ways, e.g., total number of moduli used, Krukenberg's covering systems are superior to those obtained in this computational manner.

As before, in several rows of Table 4, we have $m_1 \nmid L$. The congruence modulo m_1 in the corresponding covering system is superfluous, but is included for purposes of comparison to the other table.

TABLE 4. Least Modulus Results via Proposition 1

m_1	L	L
10	$2^3 \cdot 3^2 \cdot 5^2 \cdot 7$	$12,600$
11	$2^4 \cdot 3^2 \cdot 5^2 \cdot 7$	$25,200$
12	$2^4 \cdot 3^2 \cdot 5^2 \cdot 7$	$25,200$
13	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$	$831,600$
14	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$	$831,600$
15	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11$	$831,600$
16	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	$10,810,800$
17	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	$10,810,800$
18	$2^4 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13$	$10,810,800$

5. Implementation

Although a greedy algorithm is easy to describe, the implementation of it in the context of the Least Modulus Problem requires some care. Using divisors of a large number L as moduli for a set of congruences and working within the interval $I = [0, L-1]$, since, as noted earlier, any system of congruences to such moduli is equivalent to a union of congruences to modulus L, the main problem is the size of L (in the sense of magnitude and number of divisors). To store such an interval I requires space proportional to L. Also, in examining each possible residue class for a given modulus, the entire interval I must be examined, which requires time proportional to L. While a program that works with moderate values of L, e.g., $L = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$, might require a significant portion of a computer's memory and have running time on the order of days, the same program cannot possibly work with the larger values $L' = L \cdot 19$ or $L'' = L \cdot 19 \cdot 23$.

An implementation of a greedy algorithm must overcome this size obstacle, and it must also be able to incorporate Propositions 1 and 2. To overcome the problem of large values of L, we note that if a moderate value of L in the program could produce a set of congruences that almost covers $\mathbb{N}$, in the sense of density, then it is more economical to keep track of those few members of I that are not covered than to keep track of the entirety of I. Thus, we use two programs: a primary program that, given L, produces a set of congruences (by means of a greedy algorithm) that covers a high density subset of $\mathbb{N}$, and a secondary program that, given L' with $L|L'$ along with the short list of elements of I not covered by the congruences from the primary program, produces (also by a greedy algorithm) a set of congruences that either covers what remains, or covers a large subset of what remains. This secondary program can be used multiple times, if needed.

To use Proposition 1, the programs must be able to keep track of the congruences $\mathcal{D}$ from the theorem. Since the moduli of the congruences in $\mathcal{D}$ are divisors of L, these congruences are equivalent to a union of congruences with modulus L, and thus can be represented as a subset of the interval I (that, by Proposition 1, need not be covered by the congruences produced by the greedy search). In the primary program, those integers in I that satisfy one of the congruences from $\mathcal{D}$ can be marked as covered, and a greedy algorithm can then proceed in its normal fashion,

producing a subset of I that is covered. With the above choice of parameters, this approach indeed succeeds in producing covering systems with least modulus 18, and possibly slightly beyond 18. However, if the moduli are restricted to be greater than or equal to 25 (in an attempt to obtain a cover with least modulus 25), then it appears unavoidable that a small subset of I is left uncovered. We therefore employ a secondary program that uses the parameter $L' = L \cdot 19$ in place of L and with the uncovered part of I as input. These uncovered classes modulo L that serve as input are equivalent to a larger set of uncovered classes modulo L', and these classes can be checked and removed from consideration if already covered by a congruence from $\mathcal{D}'$.

In addition to Proposition 1, we can also appeal to Proposition 2, which allows certain moduli to be used more than once in congruences. The programs must be able to provide for multiple selections of the residue class for such moduli. When required to determine congruences for a modulus with multiplicity larger than 1, instead of selecting the single best class, a program can select the appropriate number of "good" classes, either by a strict ordering of classes by efficiency, or by some randomized process.

As indicated above, the primary program keeps track of an interval $I = [0, L - 1]$, marking integers in I as covered as new congruences are selected. Since an integer in I is either covered or not covered, we use an array of bits for the internal representation of I.

The primary program selects congruences by means of a greedy algorithm. It examines the moduli in order of increasing size of modulus, and for each modulus m, it examines the efficiency of $a \bmod m$ for increasing a. Since m is potentially large, the program does not store the efficiency of each of these m congruences before making a selection. Instead, although it examines all of the congruences, the program keeps a running tally of only a small number (the multiplicity of the modulus) of potentially "good" classes. If a new class is more efficient than one of these, then it replaces the old one, with ties being resolved through a random algorithm. (Specifically, if a tie occurs, then the new class replaces the old one, or not, according to the outcome of the equivalent of a coin flip.) The primary program uses both Propositions 1 and 2.

The secondary program keeps track of a list of those integers not covered by any congruence from a given list (e.g., a list generated by the primary program), removing integers from the list as new congruences are selected. Intended for use after the primary program and primarily for the search for a covering system with least modulus 25, the advantage of this secondary program is that, instead of storing the full interval I in memory, it only stores the potentially much smaller number of integers in I that are yet to be covered. The secondary program uses Proposition 1, but not Proposition 2. (In practice, the latter theorem is not needed at this stage, and it would be far less effective here than in its first application in the primary program.)

The secondary program, like the primary program, selects congruences via a greedy algorithm. Specifically, it examines the available moduli in order of increasing size and selects the congruence that is the most efficient, i.e., the congruence that covers the most of the currently uncovered integers.

6. Results

In this section, we establish the existence of a covering system with least modulus 25. To do so, we shall require Propositions 1 and 2, in addition to substantial computer assistance. Roughly speaking, the idea is to use a greedy algorithm to direct a computer search, using the sets of congruences associated with the two propositions to make the search easier, as described in Section 4. Practical constraints, explained in Section 5, force this to be a multi-stage process.

Theorem 1. *There exists a covering system with least modulus* 25.

Proof. We shall establish the existence of a covering system $\mathcal{C}''$ with least modulus 25 by applying Proposition 1, with $Q = 1$, $L = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot \prod_{j=1}^{297} q_j$, where $q_1 = 29 < \cdots < q_{297} = 2017$ are the first 297 primes greater than 23, and with $\mathcal{C}$ to be described below. Note that in applying Proposition 1, we need to ensure that $\mathcal{C} \cup \mathcal{D}$ covers $\mathbb{N}$, where $\mathcal{D}$ is given by (2.30) and appears in Appendix B.

We shall describe $\mathcal{C}$ in three stages. The first part of the set of congruences $\mathcal{C}$ will be derived (via Proposition 2) from those congruences appearing in Appendix C[1], which were generated by the primary program. These congruences have moduli which are divisors (in fact, all divisors greater than or equal to 25) of $L_1 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$, but the moduli are not all distinct. By Proposition 2, some (see Example 1) of the moduli may be repeated. By applying Proposition 2 to the set of congruences in Appendix C, we obtain, but do not list, a set of congruences $\mathcal{C}'$ whose moduli are divisors (all greater than or equal to 25) of $L_1 \cdot \prod_{j=1}^{297} q_j$, distinct, and such that they cover the same arithmetic progressions listed in Appendix C. We shall return to $\mathcal{C}'$ later.

The congruences in Appendix C do not cover $\mathbb{N}$, but together with those congruences from $\mathcal{D}$ whose moduli divide L_1, they cover all but 278,477 classes modulo L_1. These classes are part of the input to the secondary program.

The second part of the set of congruences $\mathcal{C}$ appears in Appendix D, and was generated by the secondary program. These congruences have moduli which are divisors (all greater than 25) of $L_2 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 = L_1 \cdot 19$, divisible by 19, distinct, and distinct from those moduli appearing in Appendix C. The congruences from that appendix (together with those congruences from $\mathcal{D}$ whose moduli divide L_1) left 278,477 classes modulo L_1 not covered, and these 278,477 classes are equivalent to $278,477 \cdot 19 = 5,291,063$ classes modulo L_2 that are not covered. The congruences listed in Appendix D, along with the congruence 0 mod 19 from $\mathcal{D}$, cover all but 52,295 classes modulo L_2 of those 5,291,063 remaining classes. These 52,295 classes are part of the input to another instance of the secondary program.

The final part of the set of congruences $\mathcal{C}$ appears in Appendix E. These congruences have moduli (all greater than 25) which are divisors of $L_3 = L_1 \cdot 19 \cdot 23 = L_2 \cdot 23$, divisible by 23, distinct, and distinct from those moduli appearing in Appendix C and Appendix D. The congruences from those appendices (together with the moduli from $\mathcal{D}$ whose moduli divide L_2) left 52,295 classes modulo L_2 not covered, and these classes are equivalent to $52,295 \cdot 23 = 1,202,785$ classes modulo L_3 that are not covered. The congruences listed in Appendix E, along with the congruence 0 mod 23 from $\mathcal{D}$, cover these remaining classes.

[1]Appendices C, D, and E can be seen on the web in the on-line supplement to this paper.

In short, the congruences from Appendices B (the congruences $\mathcal{D}$ from Proposition 1), C, D, and E together cover all of $\mathbb{N}$. We take the set $\mathcal{C}$ to be the set of congruences $\mathcal{C}'$ together with the congruences in Appendices D and E. The set of congruences $\mathcal{C}'$ not only covers the same arithmetic progressions as the congruences in Appendix C, but also has distinct moduli, as guaranteed by Proposition 2. Also, these moduli are divisors of $L_1 \cdot \prod_{j=1}^{297} q_j$, and hence are distinct from those moduli appearing in Appendices D and E, since the moduli from $\mathcal{C}'$ are not divisible by 19 and 23, respectively.

Finally, since we have a set of congruences $\mathcal{C}$ whose moduli are distinct and divisors of L, and such that $\mathcal{C} \cup \mathcal{D}$ covers $\mathbb{N}$, where $\mathcal{D}$ is given by (2.30) (also see Appendix B), we may take $w = 2027$ (the least prime larger than any of those appearing as a factor of L), since $(w, L) = 1$, in Proposition 1 to obtain that there exists a covering system with least modulus 25. □

Appendix A. Explanation of the tables

These tables contain the lists of congruences used in Theorem 1. There are a total of four lists of congruences: the congruences $\mathcal{D}$ from Proposition 1, the congruences generated by the primary program, and two sets of congruences generated by the secondary program.

The first list, Table 5 in Appendix B, contains the congruences $\mathcal{D}$ from Proposition 1, which depend on the particular choice in Theorem 1 of $L = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot \prod_{j=1}^{297} q_j$, with q_j the first 297 primes greater than 23. These congruences are of the form $a \bmod p^e$, $0 \le a \le p^{e-1} - 1$, where $p^e \| L$. Note that these congruences occur in a hypothesis of Proposition 1 and do not actually belong to the covering system with least modulus 25.

The second list, Appendix C, contains congruences whose moduli are divisors (in fact, all divisors greater than or equal to 25) of $L_1 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17$, as described in Theorem 1. Notice that some of the moduli are repeated multiple times; e.g., modulus 720 occurs 3 times, while modulus L_1 occurs 43 times. These moduli are marked by an asterisk. This list is part of the output of the primary program.

The third list, Appendix D, contains congruences whose moduli are divisors (all greater than 25) of $L_2 = L_1 \cdot 19$, as described in Theorem 1. All of these moduli are distinct. This list is part of the output of the secondary program.

The fourth list, Appendix E, contains congruences whose moduli are divisors (all greater than 25) of $L_3 = L_1 \cdot 19 \cdot 23 = L_2 \cdot 23$, as described in Theorem 1. Like the moduli of the previous list, all of these moduli are distinct. This list is part of the output of the secondary program, a different instance of the program than the one that generated the congruences in Appendix D.

Appendix B. Congruences coming from Proposition 1

The proof of Proposition 2 contains an application of Proposition 1 with $L = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \cdot \prod_{j=1}^{297} q_j$, where $q_1, \ldots, q_{297}$ are the first 297 primes greater than 23. In Proposition 1, $\mathcal{D}$ is defined by

$$\mathcal{D} = \bigcup_{i=1}^{s} \{j \bmod p_i^{e_i} : 0 \le j \le p_i^{e_i - 1} - 1\},$$

where $p_i^{e_i} \| L$. Here $s = 9 + 297 = 306$, and $\mathcal{D}$ contains $16 + 9 + 5 + 7 + 5 + 297 = 339$ congruences.

TABLE 5. List of Congruences $\mathcal{D}$ from Proposition 1

$a \bmod 2^5$	$0 \le a \le 15$
$a \bmod 3^3$	$0 \le a \le 8$
$a \bmod 5^2$	$0 \le a \le 4$
$a \bmod 7^2$	$0 \le a \le 6$
$0 \bmod p$	$11 \le p \le 2017$

REFERENCES

1. Marc A. Berger, Alexander Felzenbaum, and Aviezri S. Fraenkel, *Necessary condition for the existence of an incongruent covering system with odd moduli. II*, Acta Arith. **48** (1987), no. 1, 73–79. MR893463 (88j:11002)
2. S. L. G. Choi, *Covering the set of integers by congruence classes of distinct moduli*, Math. Comp. **25** (1971), 885–895. MR0297692 (45:6744)
3. R. F. Churchhouse, *Covering sets and systems of congruences*, Computers in Mathematical Research, North-Holland, Amsterdam, 1968, pp. 20–36. MR0240045 (39:1399)
4. P. Erdös, *On integers of the form $2^k + p$ and some related problems*, Summa Brasil. Math. **2** (1950), 113–123. MR0044558 (13:437i)
5. ———, *On some of my problems in number theory I would most like to see solved*, Number theory (Ootacamund, 1984), Lecture Notes in Math., vol. 1122, Springer, Berlin, 1985, pp. 74–84. MR797781
6. P. Erdős and R. L. Graham, *Old and new problems and results in combinatorial number theory*, Monographies de L'Enseignement Mathématique [Monographs of L'Enseignement Mathématique], vol. 28, Université de Genève L'Enseignement Mathématique, Geneva, 1980. MR592420 (82j:10001)
7. Michael Filaseta, *Coverings of the integers associated with an irreducibility theorem of A. Schinzel*, Number theory for the millennium, II (Urbana, IL, 2000), A K Peters, Natick, MA, 2002, pp. 1–24. MR1956242 (2003k:11015)
8. Michael Filaseta, Kevin Ford, Sergei Konyagin, Carl Pomerance, and Gang Yu, *Sieving by large integers and covering systems of congruences*, J. Amer. Math. Soc. **20** (2007), no. 2, 495–517 (electronic). MR2276778
9. Donald Jason Gibson, *Covering systems*, Ph.D. thesis, University of Illinois, Urbana-Champaign, 2006.
10. Song Guo and Zhi-Wei Sun, *On odd covering systems with distinct moduli*, Adv. in Appl. Math. **35** (2005), no. 2, 182–187. MR2152886 (2006e:11018)
11. Richard K. Guy, *Unsolved problems in number theory*, Third Edition, Problem Books in Mathematics, Springer-Verlag, New York, 2004. MR2076335 (2005h:11003)
12. Ivan Korec and Štefan Znám, *On disjoint covering of groups by their cosets*, Math. Slovaca **27** (1977), no. 1, 3–7. MR0485421 (58:5260)
13. C. E. Krukenberg, *Covering sets of the integers*, Ph.D. thesis, University of Illinois, Urbana-Champaign, 1971.
14. Ryozo Morikawa, *On a method to construct covering sets*, Bull. Fac. Liberal Arts Nagasaki Univ. **22** (1981), no. 1, 1–11. MR639636 (84i:10057)
15. ———, *Some examples of covering sets*, Bull. Fac. Liberal Arts Nagasaki Univ. **21** (1981), no. 2, 1–4. MR639635 (84j:10064)
16. Pace Nielsen, *A covering system whose smallest modulus is large*, preprint.
17. Š. Porubský and J. Schönheim, *Covering systems of Paul Erdős. Past, present and future*, Paul Erdős and his mathematics, I (Budapest, 1999), Bolyai Soc. Math. Stud., vol. 11, János Bolyai Math. Soc., Budapest, 2002, pp. 581–627. MR1954716 (2004d:11006)
18. N. P. Romanoff, *Über einige Sätze der additiven Zahlentheorie*, Math. Ann. **109** (1934), 668–678. MR1512916
19. A. Schinzel, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. **13** (1967/1968), 91–101. MR0219515 (36:2596)

20. J. Schönheim, *Covering congruences related to modular arithmetic and error correcting codes*, Ars Combin. **16** (1983), no. B, 21–25. MR737106 (85d:11007)
21. W. Sierpiński, *Sur un problème concernant les nombres* $k \cdot 2^n + 1$, Elem. Math. **15** (1960), 73–74. MR0117201 (22:7983)
22. R. J. Simpson and Doron Zeilberger, *Necessary conditions for distinct covering systems with square-free moduli*, Acta Arith. **59** (1991), no. 1, 59–70. MR1133237 (92i:11014)
23. L. J. Stockmeyer and A. R. Meyer, *Word problems requiring exponential time: Preliminary report*, Fifth Annual ACM Symposium on Theory of Computing (Austin, Tex., 1973), Assoc. Comput. Mach., New York, 1973, pp. 1–9. MR0418518 (54:6557)
24. J. D. Swift, *Sets of covering congruences*, Bull. Amer. Math. Soc. **60** (1954), 390.
25. Štefan Znám, *A survey of covering systems of congruences*, Acta Math. Univ. Comenian. **40(41)** (1982), 59–79. MR686961 (84e:10004)

Eastern Kentucky University, 313 Wallace Building, 521 Lancaster Avenue, Richmond, Kentucky 40475-3102