Covering subsets of the integers by congruences

Michael Filaseta, Wilson Harvey

ACTA ARITHMETICA
Online First version

Covering subsets of the integers by congruences

by

Michael Filaseta (Columbia, SC) and Wilson Harvey (Monroe, LA)

1. Introduction. In 1950, P. Erdős [1] introduced the concept of covering systems (or coverings for short) of the integers to show that a positive proportion of the positive odd integers cannot be expressed as a prime plus a power of 2. His argument was based on the observation that

$$\begin{aligned} n &\equiv 0 \pmod 2 \;\Rightarrow\; 2^n \equiv 1 \pmod 3,\\ n &\equiv 0 \pmod 3 \;\Rightarrow\; 2^n \equiv 1 \pmod 7,\\ n &\equiv 1 \pmod 4 \;\Rightarrow\; 2^n \equiv 2 \pmod 5,\\ n &\equiv 3 \pmod 8 \;\Rightarrow\; 2^n \equiv 8 \pmod{17},\\ n &\equiv 7 \pmod{12} \;\Rightarrow\; 2^n \equiv 11 \pmod{13},\\ n &\equiv 23 \pmod{24} \;\Rightarrow\; 2^n \equiv 121 \pmod{241}, \end{aligned}$$

where the congruences on the left form a *covering* of the integers, that is, a finite set of congruences with distinct moduli > 1 having the property that every integer satisfies at least one congruence in the set. The rest of the Erdős argument is fairly simple. One takes a positive odd integer N satisfying the congruences on the right above, that is, the following:

$$\begin{aligned} &x \equiv 1 \pmod 3, \quad x \equiv 1 \pmod 7, \quad x \equiv 2 \pmod 5,\\ &x \equiv 8 \pmod{17}, \quad x \equiv 11 \pmod{13}, \quad x \equiv 121 \pmod{241}. \end{aligned} \tag{1.1}$$

If $N = 2^n + p$ where n is an integer ≥ 0 and p is a prime, then $p = N - 2^n$ and the implications above imply that $p \in S := \{3, 5, 7, 13, 17, 241\}$. What Erdős had in mind to handle the case that $p \in S$ is unclear. However, with a little effort it can be shown that if N satisfies the congruences in (1.1) and n is an integer ≥ 0, then $N - 2^n$ cannot equal a prime in the set S. More precisely, $N \equiv 1 \pmod 3$ implies $N - 2^n \equiv 0$ or $2 \pmod 3$, and the

2010 *Mathematics Subject Classification*: Primary 11A07; Secondary 11B25.
Key words and phrases: covering system, subsets of integers.
Received 14 December 2016; revised 23 July 2017.
Published online *.

condition $N \equiv 1 \pmod 7$ implies $N - 2^n \equiv 0$, 4 or 6 (mod 7). As no prime p in S satisfies both $p \equiv 0$ or 2 (mod 3) and $p \equiv 0$, 4 or 6 (mod 7), the result of Erdős follows.

Coverings of the integers have found a number of interesting applications; for example, see [2, 4, 5, 11, 15, 16, 17]. The literature on the subject is extensive (cf. [7]). There has in particular been a great deal of interest in two old problems on the subject. The first, recently resolved by Bob Hough [9], is whether the minimum modulus of a covering system of the integers consisting of congruences can be arbitrarily large. Bob Hough [9] has shown that this minimum modulus is $\leq 10^{16}$. In the other direction, Pace Nielsen [13] has shown that the minimum modulus can be as large as 40, and later his ideas were extended by Tyler Owens [14] who showed the minimum modulus can be as large as 42. The second problem is to determine whether or not there is a covering of the integers consisting only of odd moduli. This problem remains open, though recent work of Bob Hough and Pace Nielsen [10] shows that every covering of the integers has some modulus divisible by either 2 or 3. With this in mind, Ognian Trifonov (private communication) has raised the question as to what nice sets of integers can be covered by a finite collection of congruences where all moduli are distinct and arbitrarily large or where all moduli are distinct odd numbers > 1. To formalize this discussion better, we make the following definitions.

Definition 1.1. A *covering* of a set $S \subseteq \mathbb{Z}$ is a finite set $\{x \equiv a_j \pmod{m_j} : 1 \leq j \leq r\}$ of congruences such that the moduli m_j are distinct integers > 1 and each $s \in S$ satisfies at least one of them. An *odd covering* of a set $S \subseteq \mathbb{Z}$ is a covering C of S where each m_j is odd. An *exact covering* of a set $S \subseteq \mathbb{Z}$ is a covering C of S for which each $s \in S$ satisfies exactly one of the congruences in C. If $S = \mathbb{Z}$, we speak of a *covering of the integers*, an *odd covering of the integers*, and an *exact covering of the integers*, respectively.

We emphasize that, in this paper, as defined above, coverings will always refer to systems of congruences where the moduli are distinct and > 1. This will allow for our results, which include these conditions, to be stated more succinctly. We also freely use the terminology that a set $S \subseteq \mathbb{Z}$ *is covered* by a set of congruences (or a set of congruences *covers* S) to mean that the set of congruences form a covering of S as defined above. On the other hand, we will still have use of sets C of congruences with repeated moduli such that every element of some set S satisfies at least one congruence from C. To be consistent, we do not refer to such C as coverings of S (see, for example, Lemma 2.2 used in the proof of Proposition 2.10, and the statement of Theorem 2.5).

The idea of covering subsets of the integers is not really new. For example, the motivating paper by Erdős [1] demonstrates that (1.1) is not

only an odd covering of the powers of 2 but a covering of the powers of 2 where the moduli are primes. Hence, the idea that one can cover a subset of $\mathbb{Z}$ in some nice way is in fact part of the point of the original use of coverings given by Erdős [1]. Analogously to (1.1) providing a covering of the powers of 2, A. Granville [6] has pointed out that

$$\begin{aligned} &x \equiv 1 \pmod 2, \quad x \equiv 0 \pmod 3, \quad x \equiv 1 \pmod 7, \\ &x \equiv 0 \pmod{17}, \quad x \equiv 2 \pmod{19}, \quad x \equiv 15 \pmod{23} \end{aligned} \tag{1.2}$$

provides a covering of the Fibonacci numbers. As in (1.1), the moduli in (1.2) are primes. It is also of interest that the sum of the reciprocals of the moduli in (1.1) is $0.816\ldots < 1$ and the sum of the reciprocals of the moduli in (1.2) is $1.131\ldots > 1$. For coverings of the integers, it is well-known and not difficult to see that the sum of the reciprocals of the moduli is always > 1.

We have not addressed the literature on exact coverings of the integers. A classic argument (cf. [3]) using a complex variable shows that there is no exact covering of the integers; more precisely, if a finite system of congruences $x \equiv a_j \pmod{m_j}$, where $1 \le j \le r$ and $m_1 \le \cdots \le m_r$, is such that every integer satisfies exactly one congruence in the system, then $m_r = m_{r-1}$ so that the system is not a covering of the integers. On the other hand, there can be exact coverings for subsets of the integers.

The concept of covering subsets of $\mathbb{Z}$ sparks a great deal of questions, and our hope here is to raise some interest in the topic. Some explicit examples of coverings of subsets of $\mathbb{Z}$ that we obtain include:

- There is an odd covering of the set of primes.
- There is an odd covering of the numbers that are sums of two squares.
- There is an exact covering of the powers of 2 consisting of moduli only divisible by primes larger than any prescribed value and with the sum of the reciprocals of the moduli smaller than any prescribed $\varepsilon > 0$.
- There is a covering of the Fibonacci numbers consisting of moduli only divisible by primes larger than any prescribed value and with the sum of the reciprocals of the moduli smaller than any prescribed $\varepsilon > 0$.
- There is an exact odd covering of the Fibonacci numbers.

Our demonstration of the second example above involves a lengthy construction using 64731 congruences, though no real attempt has been made to minimize this number. In the third and fourth examples, the conditions stated imply that we can find such coverings where the moduli are odd and with the minimum modulus larger than any prescribed value. These two examples, in particular, might suggest that subsets $\mathcal{N} = \{n_1, n_2, \ldots\}$ of the integers for which n_j increases sufficiently fast are more easily covered using large moduli, but we show in the next section that this is not in general true. More precisely, we show that there are sets $\mathcal{N}$ for which the n_j increase as

fast as one wants but which cannot be covered by congruences with moduli all $> 10^{16}$. An analogous result is obtained for odd coverings of subsets of the integers provided no odd covering of the integers exists.

Among the questions we have not addressed are the following. Does there exist a covering of the set of primes or of the set of numbers which are sums of two squares that uses only moduli that are greater than an arbitrary fixed bound M? Does there exist an odd covering of the set of squarefree numbers? Does there exist an odd covering of the set of squarefree numbers using moduli that are all $> 10^{100}$? Although we were able to obtain some results for subsets of the form $S_f = \{f(n) : n \in \mathbb{Z}^+\}$, where $f(x) \in \mathbb{Z}[x]$, we are far from a general result in this direction. In particular, is it true that for every such S_f, there is an odd covering of S_f? Although it will be clear that part of our approach for Fibonacci numbers generalizes to other recursive sequences, we have not obtained a result for arbitrary recursive sequences in the integers.

2. Preliminary results. In this section, we discuss some basic results in the general spirit of understanding coverings of subsets of $\mathbb{Z}$, and then turn to some further results that follow from recent work from [8] and [9].

PROPOSITION 2.1. *If there is no odd covering of the integers, then there is no odd covering of the odd integers.*

Proof. Suppose there exists an odd covering C of the odd integers. Thus, $C = \{x \equiv a_i \pmod{m_i} : 1 \le i \le r\}$, where each m_i is odd and $1 < m_1 < \cdots < m_r$. To establish the proposition, it suffices to show that C covers all the integers.

Define $M = \prod_{j=1}^{r} m_j$, and note that M is odd. Let $n \in \mathbb{Z}$. Then either n is odd and covered by a congruence in C, or $n + M$ is odd and thus covered by a congruence in C. We deduce that $n + \varepsilon M \equiv a_k \pmod{m_k}$ for some $k \in \{1, \dots, r\}$ and $\varepsilon \in \{0, 1\}$. But $m_k \mid M$, so $n \equiv n + \varepsilon M \equiv a_k \pmod{m_k}$. Thus, n necessarily satisfies a congruence from C. ∎

LEMMA 2.2. *Let $t \in \mathbb{Z}$ and $S \subseteq \mathbb{Z}$. Given a set $C = \{x \equiv a_k \pmod{m_k} : 1 \le k \le r\}$ of congruences such that every element of S satisfies at least one congruence in C, the set $C_t = \{x \equiv a_k + t \pmod{m_k} : 1 \le k \le r\}$ has the property that every element of $S_t = \{s + t : s \in S\}$ satisfies at least one congruence in C_t.*

Proof. Fix $x_0 \in S_t$. We may write $x_0 = s_0 + t$ for some $s_0 \in S$. The conditions in the lemma imply there exists $k_0 \in \{1, \dots, r\}$ with $s_0 \equiv a_{k_0} \pmod{m_{k_0}}$. Further, $x_0 = s_0 + t \equiv a_{k_0} + t \pmod{m_{k_0}}$, so x_0 satisfies a congruence in C_t. ∎

The following is a simple consequence of the previous two results.

COROLLARY 2.3. *If there is no odd covering of the integers, then there is no odd covering of the even integers.*

Along the lines of basic results like Lemma 2.2, we note that if C is a set of congruences with the least common multiple of the moduli equal to L, then C is a covering of $\mathbb{Z}$ if and only if C is a covering of a set S containing L consecutive integers. In particular, C is a covering of $\mathbb{Z}$ if and only if C is a covering of $\mathbb{Z}^+$.

DEFINITION 2.4. Let $\mathcal{P}$ be a property that can be satisfied by some subsets of $\mathbb{Z}^+$. We say that *there exist arbitrarily thin sets S satisfying $\mathcal{P}$* if for all functions f with $f(x) \to \infty$ as $x \to \infty$, there exists a set S, depending on f, satisfying $\mathcal{P}$ and an $x_0 \in \mathbb{R}^+$ such that

$$|\{s \in S : s \le x\}| \le f(x) \quad \text{for all } x \ge x_0.$$

THEOREM 2.5. *Let $r \in \mathbb{Z}^+$. Let $\mathcal{N}$ be a possibly infinite set of congruences $x \equiv a \pmod m$, with $0 \le a < m$, such that for any finite set C of congruences from $\mathcal{N}$, with each modulus appearing in C at most r times, there exists some integer which fails to satisfy every congruence in C. Then there exist arbitrarily thin sets $S \subseteq \mathbb{Z}^+$ such that for any finite set C of congruences from $\mathcal{N}$, with each modulus appearing in C at most r times, there exists some element of S which fails to satisfy every congruence in C.*

Proof. Let $C(M)$ denote the set of all finite subsets

$$C = \{x \equiv a_k \pmod{m_k} : 1 \le k \le s\} \subseteq \mathcal{N} \quad \text{with } m_1 \cdots m_s \le M.$$

Given the definition of $\mathcal{N}$, we have $0 \le a_j < m_j$ for each j. Note that for any M, there are finitely many sets C in $C(M)$. As every finite subset C of $\mathcal{N}$ belongs to $C(M)$ for some positive integer M, we deduce that the finite subsets of $\mathcal{N}$ are countably many.

We take the finite subsets C of $\mathcal{N}$ where each modulus appears in C at most r times, and we order them $C_1, C_2, \ldots$. By the conditions in the theorem, for each C_j, there is some integer n_j which fails to satisfy every congruence in C_j. Then for every subset $C \subseteq \mathcal{N}$, with each modulus appearing in C at most r times, there exists some element of $S = \{n_1, n_2, \ldots\}$ which fails to satisfy every congruence in C.

Observe that if a number n fails to satisfy every congruence in C_k, then so does any number that is of the form n plus a multiple of the product of the moduli in C_k. Hence, the values n_k may grow at any desired rate, implying that the set S can be constructed to be arbitrarily thin. ∎

The case $r = 1$ is of particular importance to us. If we take $\mathcal{N}$ equal to the set of congruences $x \equiv a \pmod m$ where $m > 10^{16}$ and $a \in [0, m)$ or if $\mathcal{N}$ is the set of congruences $x \equiv a \pmod m$ where m is odd and > 1 and $a \in [0, m)$, then we obtain respectively the following two results.

Corollary 2.6. *There are arbitrarily thin sets $S \subseteq \mathbb{Z}$ for which no covering of S exists using only moduli greater than 10^{16}.*

Corollary 2.7. *If there is no odd covering of the integers, then there are arbitrarily thin sets $S \subseteq \mathbb{Z}$ for which no odd covering of S exists.*

There is an alternative approach to establishing Corollaries 2.6 and 2.7: they both follow from the following.

Theorem 2.8. *There exist arbitrarily thin sets $S \subseteq \mathbb{Z}^+$ such that if C is a set of congruences that covers S, then C is a covering of the integers.*

Proof. We give an explicit construction of S. Let $x \geq 3$. For simplicity, we describe a set $S \subseteq \mathbb{Z}^+$ which has $\ll (\log\log x)^2$ elements up to x with the property in the theorem, and then we briefly indicate how to modify it to obtain thinner sets S. Define

$$S = \{n + u^{u!} - 1 : n \in \mathbb{Z}^+,\, u \in \mathbb{Z}^+,\, u \geq n\}.$$

One easily checks that $u! \geq 2^{u-1}$ for all positive integers u. If $s = n + u^{u!} - 1 \in S$ and $s \leq x$, then $u^{2^{u-1}} \leq x$ so that $u \ll \log\log x$. On the other hand, $u \geq n$, so also $n \ll \log\log x$. It follows that there are $\ll (\log\log x)^2$ elements of S up to x.

Suppose C is a set of congruences that covers S. Let $n' \in \mathbb{Z}^+$. Then $n' + u^{u!} - 1 \in S$ where we can choose the integer $u \geq n'$ as we want. We choose a prime u that is larger than m for each modulus m appearing in a congruence in C. With $\phi(x)$ denoting the Euler ϕ-function, we deduce $u^{\phi(m)} \equiv 1 \pmod{m}$ for each such m. Also, $1 \leq \phi(m) \leq m \leq u$ implies $\phi(m)$ divides $u!$ for each modulus m appearing in a congruence in C. We deduce then that $u^{u!} \equiv 1 \pmod{m}$ for each such m. Since C covers S, there is a congruence $x \equiv a \pmod{m}$ in C for which

$$n' + u^{u!} - 1 \equiv a \pmod{m}.$$

Hence, $u^{u!} \equiv 1 \pmod{m}$ implies that n' satisfies the congruence $x \equiv a \pmod{m}$ in C. Recalling the remark after Corollary 2.3, we see that C is a covering of the integers. More generally, one can repeat this argument with $u^{u!}$ in the definition of S replaced by $u^{w(u)!}$ with $w(u)$ tending to infinity as quickly as one wants to obtain a set S as thin as one wants to complete the proof of the theorem. ∎

Corollary 2.6 makes use of the result by B. Hough [9] mentioned in the introduction. Our next result similarly relies on this work. To clarify a distinction in these two results, we note that Corollary 2.6 is a statement about the existence of thin sets S, whereas our next result is a statement about all sets S which are sufficiently dense in the set of integers.

PROPOSITION 2.9. *Let $S \subseteq \mathbb{Z}^+$ satisfy*

$$\limsup_{X\to\infty} \frac{|\{s \in S : s \le X\}|}{X} = 1. \tag{2.1}$$

Then S cannot be covered by a set of congruences with minimum modulus $> 10^{16}$.

Proof. Fix $S \subseteq \mathbb{Z}^+$, and suppose

$$C = \{x \equiv a_j \pmod{m_j} : 1 \le j \le r\}, \quad \text{where } 10^{16} < m_1 < \cdots < m_r,$$

is a covering of S. From [9], we know that C is not a covering of the integers, so there is an integer x_0 with $x_0 \not\equiv a_j \pmod{m_j}$ for each $1 \le j \le r$. Let L be the least common multiple of $m_1, \dots, m_r$ (note that the product of these moduli will also suffice here). Thus, $L \equiv 0 \pmod{m_j}$ for each j. Hence, for every integer k, the number $x_0(k) = x_0 + kL$ satisfies $x_0(k) \not\equiv a_j \pmod{m_j}$ for each $1 \le j \le r$. It follows that

$$\liminf_{X\to\infty} \frac{\left|\left\{x \in \mathbb{Z}^+ : x \le X,\, x \not\equiv a_j \pmod{m_j},\, \forall j \in \{1,\dots,r\}\right\}\right|}{X} \ge \frac{1}{L}.$$

Thus, asymptotically at least $1/L$ of the positive integers are not covered by C. Since C is a covering of S, we can deduce that the left-hand side of (2.1) is at most $1 - 1/L < 1$. The proposition follows. ∎

In connection with the above result, it should be noted that there are sets with density arbitrarily close to 1 which can be covered using moduli that are larger than any prescribed value. For example, if we want to use only moduli $> M$, then we can take $z \ge M$,

$$S = \{n \in \mathbb{Z}^+ : \exists p \in (z, e^z] \text{ such that } p \,|\, n\}$$

and $C = \{x \equiv 0 \pmod{p} : z < p \le e^z\}$. The asymptotic density of the set of positive integers not in S is

$$\lim_{X\to\infty} \frac{|\{s \notin S : s \in \mathbb{Z} \cap [1, X]\}|}{X} = \prod_{z<p\le e^z} \left(1 - \frac{1}{p}\right) \sim \frac{\log z}{z}$$

as z tends to infinity. Hence, by choosing z sufficiently large, the density of S can be made $> 1 - \varepsilon$ for any fixed $\varepsilon > 0$.

The following proposition, concerning an odd covering of the prime numbers, makes use of recent work of J. Harrington [8].

PROPOSITION 2.10. *There exists an odd covering of the prime numbers.*

Proof. In [8], J. Harrington established the existence of a system C of congruences where the moduli are all odd and > 1, the modulus 3 is used exactly twice, no other modulus is repeated, and every integer satisfies at least one of the congruences. By Lemma 2.2 with $S = \mathbb{Z}$ and an appropriate choice of t, we may suppose that $x \equiv 0 \pmod 3$ is one of the congruences

in C. The only prime $p \equiv 0 \pmod 3$ is $p = 3$. Thus, since every integer satisfies a congruence in C, every prime $p \neq 3$ must satisfy a congruence in C that is different from $x \equiv 0 \pmod 3$. We construct an odd covering C' of the primes as in the proposition by removing $x \equiv 0 \pmod 3$ from C and including in C' instead the congruence $x \equiv 3 \pmod m$ where m is any odd integer > 1 that does not appear as a modulus in C. Therefore, this last congruence is satisfied by the prime 3, and the other congruences in C' cover the remaining primes. ∎

3. Powers of 2 and the Fibonacci numbers. In this section, we obtain a theorem for coverings of the powers of 2 and a similar result for coverings of the Fibonacci numbers. The main distinction in the covering results obtained is that, for the powers of 2, we are able to construct an exact covering. At the end of this section, however, we demonstrate an example of an exact odd covering of the Fibonacci numbers.

THEOREM 3.1. *Let $P \geq 2$, $M \geq 2$, and $\varepsilon > 0$. There exists a finite set of congruences*

$$x \equiv a_j \pmod{m_j} \quad \text{for } 1 \leq j \leq r, \tag{3.1}$$

with distinct moduli $m_j > 1$, that satisfies each of the following:

(i) *For each $n \geq 0$, the number 2^n satisfies exactly one of the congruences in (3.1). (Thus, the congruences form an exact covering of the powers of 2.)*
(ii) *Each prime divisor of each m_j is $> P$. (In particular, the congruences form an odd covering of the powers of 2.)*
(iii) *Each m_j is $> M$. (Hence, the minimum modulus is arbitrarily large.)*
(iv) *The sum of the reciprocals of the moduli m_j is $< \varepsilon$. (Therefore, the sum of the reciprocals of the moduli is arbitrarily small.)*

COMMENT. The main reason for stating (iii) above is to emphasize that the minimum modulus can be arbitrarily large; this is a consequence of (ii) since each m_j is > 1.

Proof of Theorem 3.1. Define $A(n) = 2^{2^n} - 1$ and $B(n) = 2^{2^n} + 1$. By K. Zsigmondy's Theorem [18], for each $n \geq 1$, there is a prime p dividing $A(n)$ which fails to divide $A(k)$ for every integer $k \in [0, n)$. Alternatively, we can use that

$$\begin{aligned} &A(n) = B(n-1)A(n-1) = B(n-1)B(n-2)\cdots B(0), \\ &B(n-1) - A(n-1) = 2 \end{aligned} \tag{3.2}$$

to see that, for $n \geq 1$, the number $B(n-1) > 1$ is a divisor of $A(n)$ that is relatively prime to $A(k)$ for each $k \in [0, n)$. For $n \geq 1$, we let d_n be any

such divisor of $A(n)$, that is, a divisor > 1 that is relatively prime to each $A(k)$ with $0 \le k < n$. In particular, note that the values of d_n are pairwise relatively prime.

For n a positive integer, d_n has the property that the powers of 2 repeat modulo d_n with period 2^n. To clarify, first, if $r = 2^n$, then

$$2^{\ell+r} \equiv 2^\ell \pmod{d_n} \quad \text{for every integer } \ell \ge 0,$$

which follows since the same congruence with the modulus replaced by $A(n)$ is easily seen to hold and $d_n \mid A(n)$. Second, the minimum positive integer r for which $2^r \equiv 1 \pmod{d_n}$ must divide 2^n, which can be seen by observing that if two different values of r satisfy $2^r \equiv 1 \pmod{d_n}$, then so does their greatest common divisor. Thus, the minimum r satisfying $2^r \equiv 1 \pmod{d_n}$ is a power of 2 that is $\le 2^n$. Finally, $2^r \equiv 1 \pmod{d_n}$ cannot hold for r a power of 2 that is $< 2^n$ since d_n does not divide $A(k)$ with $0 \le k < n$. Thus, indeed the powers of 2 repeat modulo d_n with period 2^n.

In a moment, we will consider a product D of distinct d_j. Observe that if n is the largest subscript of d_j in the product D, then the period of the sequence of powers of 2 modulo D is 2^n. Furthermore, in this case, the numbers 2^i for $0 \le i < 2^n$ are distinct modulo D.

The coprimality of d_n and d_k for $0 \le k < n$ is enough to ensure that d_n tends to infinity with n and that in fact the minimum prime divisor of d_n tends to infinity with n. We now fix $k \in \mathbb{Z}^+$ such that every d_n with $n \ge k$ has all prime divisors $> P$ and $d_n > M$ for each $n \ge k$. In particular, from (3.2), the $n - k + 1$ numbers

$$d_k, d_{k+1}, \ldots, d_{n-1}, d_n \tag{3.3}$$

are pairwise relatively prime divisors > 1 of $A(n)$.

We consider the set S_n of 2^{n-k} integers formed by taking arbitrary products of distinct numbers from the first $n - k$ divisors of $A(n)$ listed in (3.3). Since these divisors are pairwise relatively prime, these 2^{n-k} integers are distinct. Thus, the size of S_n is 2^{n-k}. For each $D = d_n s$ where $s \in S_n$, we consider a congruence of the form $x \equiv 2^a \pmod{D}$. We take $a \in [0, 2^n)$ so that distinct $s \in S_n$ are assigned distinct a. Observe that the congruence $x \equiv 2^a \pmod{D}$ covers the integers 2^m satisfying $m \equiv a \pmod{2^n}$ and no other powers of 2. We use these 2^{n-k} congruences formed from the 2^{n-k} elements of S_n as described to cover 2^m for m from 2^{n-k} residue classes modulo 2^n.

Given the above, we begin with $n = k$. Thus, initially, we have one congruence formed from the unique element of S_k, and this congruence covers 2^m for m in this unique residue class modulo 2^k. This residue class corresponds to two residue classes modulo 2^{k+1}. We then take $n = k + 1$ and cover two more residue classes modulo 2^{k+1}. Thus, at this point four

different residue classes are covered modulo 2^{k+1}. A straightforward induction argument shows that if we continue in this manner, taking $n = k + j$ for increasing values of j, we cover $(j+1)2^j$ different residue classes modulo 2^{k+j}. We stop this process when $j = J = 2^k - 1$ since at that point we will be covering

$$(J+1)2^J = 2^k 2^{2^k-1} = 2^{2^k+k-1}$$

different residue classes modulo $2^{k+J} = 2^{2^k+k-1}$. In other words, after considering all $j \in \{0, 1, \dots, J\}$, we cover 2^m for m from every residue class modulo 2^{k+J}, and thus the congruences formed cover every power of 2. Furthermore, each power of 2 satisfies at most one of the congruences in this construction. Thus, we obtain a covering system of the powers of 2 satisfying (i)–(iii).

Finally, we address (iv). Recall that we can take $d_n = B(n-1) = 2^{2^{n-1}}+1$ for every positive integer n. Our set of congruences constructed from S_n above, with $n = k + j$ where $0 \le j \le 2^k - 1$, consist of $|S_n| = 2^j$ moduli divisible by d_n. If we take $d_n = B(n-1) = 2^{2^{n-1}} + 1$, the sum of the reciprocals of all moduli in our covering of the powers of 2 is

$$\le \sum_{j=0}^{2^k-1} \frac{2^j}{2^{2^{k+j-1}}+1} \le \sum_{j=k}^{\infty} \frac{2^j}{2^{2^{j-1}}+1}. \tag{3.4}$$

The series

$$\sum_{m=0}^{\infty} \frac{2^m}{2^{2^{m-1}}+1}$$

converges, for example, by the inequality

$$\frac{2^m}{2^{2^{m-1}}+1} \le \frac{1}{2^{2^{m-1}-m}} \le \frac{1}{2^{m-2}} \quad \text{for every integer } m \ge 0.$$

It follows that the last series in (3.4) tends to 0 as $k \to \infty$. Thus, by choosing k sufficiently large, we deduce that (iv) also holds. ∎

We turn next to a covering of the Fibonacci numbers F_n. Thus, $F_0 = 0$, $F_1 = 1$ and $F_{n+1} = F_n + F_{n-1}$ for $n \ge 1$. Our argument will make use of the Lucas numbers L_n defined by $L_0 = 2$, $L_1 = 1$, and $L_{n+1} = L_n + L_{n-1}$ for $n \ge 1$. Take $\alpha = (1+\sqrt{5})/2$ and $\beta = (1-\sqrt{5})/2$. Then we have the classical formulas

$$F_n = \frac{\alpha^n - \beta^n}{\alpha - \beta} \quad \text{and} \quad L_n = \frac{\alpha^n + \beta^n}{\alpha + \beta} = \alpha^n + \beta^n$$

for all $n \ge 0$. Our next lemma easily follows from these identities, and we omit the proof.

LEMMA 3.2. *Let u and v denote integers with $u \ge v \ge 0$. The Fibonacci and Lucas numbers satisfy the following properties:*

(a) $F_{u+v} = F_u L_v - (-1)^v F_{u-v}$.
(b) $L_{2u} = L_u^2 - 2(-1)^u$.

We will also make use of the following lemmas.

LEMMA 3.3. *Let j be a positive integer. The Fibonacci numbers modulo the Lucas number L_{2^j} are periodic with period dividing 2^{j+2}.*

Proof. Let n be a positive integer. Taking $u = n + 2^{j+1} + 2^j$ and $v = 2^j$ in Lemma 3.2(a), we have

$$F_{n+2^{j+2}} = F_{u+v} = F_u L_v - (-1)^v F_{u-v} = F_u L_v - (-1)^v F_{n+2^{j+1}}.$$

With $u' = n + 2^j$ and $v = 2^j$, we deduce from Lemma 3.2(a) that

$$F_{n+2^{j+1}} = F_{u'+v} = F_{u'} L_v - (-1)^v F_{u'-v} = F_{u'} L_v - (-1)^v F_n.$$

Thus,

$$F_{n+2^{j+2}} = F_u L_v - (-1)^v (F_{u'} L_v - (-1)^v F_n) = (F_u - (-1)^v F_{u'}) L_v + F_n,$$

so that $F_{n+2^{j+2}} - F_n$ is divisible by $L_v = L_{2^j}$. ∎

LEMMA 3.4. *For j and k non-negative integers with $j \neq k$, we have* $\gcd(L_{2^j}, L_{2^k}) = 1$.

Proof. Since $L_1 = 1$, it follows from Lemma 3.2(b) and induction that L_{2^j} and L_{2^k} are odd. We suppose as we may that $k > j \geq 1$. Let p be a prime divisor of L_{2^j}. In particular, $p > 2$. Lemma 3.2(b) with $u = 2^j$ implies $L_{2^{j+1}} \equiv -2 \pmod{p}$ and by induction $L_{2^{j+t}} \equiv 2 \pmod{p}$ for every integer $t \geq 2$. Hence, $L_{2^k} \equiv \pm 2 \pmod{p}$. Since $p > 2$, we deduce $p \nmid L_{2^k}$. ∎

The following are consequences of the previous two lemmas.

COROLLARY 3.5. *Let $P = L_{2^{a_1}} \cdots L_{2^{a_k}}$ for some integer $k > 0$ and some a_j satisfying $1 \leq a_1 < \cdots < a_k$. The Fibonacci numbers modulo P are periodic with period dividing 2^{a_k+2}.*

COROLLARY 3.6. *The minimum prime divisor of L_{2^j} goes to infinity with j.*

Our next lemma is an easy consequence of Lemma 3.2 (b) and induction, and we leave out further details of its proof.

LEMMA 3.7. *For every positive integer j, we have $L_{2^j} \geq 10^{2^{j-3}} + 1$.*

THEOREM 3.8. *Let $P \geq 2$, $M \geq 2$, and $\varepsilon > 0$. There exists a finite set of congruences*

$$x \equiv a_j \pmod{m_j} \quad \text{for } 1 \leq j \leq r, \tag{3.5}$$

with distinct moduli $m_j > 1$, that satisfies each of the following:

(i) *For each $n \geq 0$, the Fibonacci number F_n satisfies at least one of the congruences in* (3.5). (*Thus, the congruences form a covering of the Fibonacci numbers.*)
(ii) *Each prime divisor of each m_j is $> P$.* (*In particular, the congruences form an odd covering of the Fibonacci numbers.*)
(iii) *Each m_j is $> M$.* (*Hence, the minimum modulus is arbitrarily large.*)
(iv) *The sum of the reciprocals of the moduli m_j is $< \varepsilon$.* (*Therefore, the sum of the reciprocals of the moduli is arbitrarily small.*)

Proof. The argument is similar to the proof of Theorem 3.1. From Corollary 3.6, there is a $k \in \mathbb{Z}^+$ such that for every $j \geq k$, L_{2^j} has each of its prime divisors $> P$. Momentarily, we fix such a $k \geq 3$, and consider $n \geq k$. In the end, we will want to choose k large. Lemma 3.2(a) with $u = v$ implies

$$F_{2^{n+1}} = F_{2^n} L_{2^n} = F_{2^{n-1}} L_{2^{n-1}} L_{2^n} = \cdots = L_{2^1} \cdots L_{2^n}.$$

Combining the above with Lemma 3.4, we see that the Lucas numbers

$$L_{2^k}, L_{2^{k+1}}, \ldots, L_{2^n} \tag{3.6}$$

are relatively prime divisors of $F_{2^{n+1}}$. Note that $k \geq 3$ easily implies $L_{2^j} > 1$ for every $j \geq k$.

We consider the set S_n of the 2^{n-k} distinct integers formed by taking arbitrary products of distinct numbers from the first $n-k$ divisors of $F_{2^{n+1}}$ listed in (3.6). For each $D = D(s,n) = s \cdot L_{2^n}$ where $s \in S_n$, we consider a congruence of the form $x \equiv F_a \pmod{D}$ where $0 \leq a < 2^{n+2}$. We take a so that distinct $s \in S_n$ are assigned distinct $a \in [0, 2^{n+2})$. Let C_n denote the set of these 2^{n-k} congruences corresponding to the 2^{n-k} elements of S_n. By Corollary 3.5, the congruence $x \equiv F_a \pmod{D}$ covers the integers F_m satisfying $m \equiv a \pmod{2^{n+2}}$. Thus, C_n covers the set of F_m for m from at least 2^{n-k} residue classes modulo 2^{n+2}.

With the above set-up, we begin with $n = k$, so that the set C_k just described contains one congruence which covers the set of F_m for m from at least one residue class modulo 2^{k+2}. This one residue class modulo 2^{k+2} corresponds to two residue classes, say r_1 and r_2, modulo 2^{k+3}. We then select $a \in [0, 2^{k+3})$ in creating the two congruences $x \equiv F_a \pmod{D}$ for C_{k+1} so that each of these a's belongs to neither r_1 nor r_2. Thus, $C_k \cup C_{k+1}$ covers the integers belonging to a total of four residue classes modulo 2^{k+3}. Similarly, we create four congruences for C_{k+2} that cover F_m for m from at least four residue classes modulo 2^{k+4} so that the congruences in $C_k \cup C_{k+1} \cup C_{k+2}$ cover F_m for m from at least 12 residue classes modulo 2^{k+4}. Inductively, for $0 \leq j \leq J$ with $J = 2^{k+2} - 1$, we create 2^j congruences for C_{k+j} so that the congruences in $C_k \cup C_{k+1} \cup \cdots \cup C_{k+j}$ cover F_m for m from at least $(j+1)2^j$ residue classes modulo 2^{k+j+2}. Observe that when $j = J$, the congruences in $C_k \cup \cdots \cup C_{k+J}$ cover F_m for m from at least $2^{k+2^{k+2}+1}$

residue classes modulo $2^{k+2^{k+2}+1}$. Thus, we obtain a collection of distinct congruences from $C = C_k \cup \cdots \cup C_{k+J}$ that satisfy (i) and (ii).

If we take k sufficiently large, for example so that $L_{2^k} > M$, then (iii) is also satisfied. For (iv), observe that C_{k+i} consists of 2^i congruences with each modulus $\geq L_{2^{k+i}}$. For any integer k, we note that $2^{k-3} \geq k-3$. Since $k \geq 3$, we deduce from Lemma 3.7 that the sum of the reciprocals of the moduli in C is bounded above by

$$\sum_{i=0}^{J} \frac{2^i}{10^{2^{k+i-3}}+1} \leq \sum_{i=0}^{J} \frac{2^{k+i-3}}{10^{2^{k+i-3}}+1} < \sum_{t=k-3}^{\infty} \left(\frac{2}{10}\right)^t = \frac{5}{4} \cdot \left(\frac{1}{5}\right)^{k-3}.$$

Thus, taking k sufficiently large, we can also ensure that (iv) holds. ∎

Observe that Theorem 3.1 establishes the existence of an exact covering of the powers of 2, whereas Theorem 3.8 establishes a covering of the Fibonacci numbers which is not necessarily exact. In the general context of the other conditions in these results, we were not able to strengthen Theorem 3.8 to give an exact covering of the Fibonacci numbers. On the other hand, it is of some interest to note that an exact odd covering of the Fibonacci numbers does exist. In the first column of Table 1 below, we give such a covering and leave the details of the verification to the reader. The second column lists the Fibonacci numbers covered by each congruence in the first column.

Table 1. An exact odd covering of the Fibonacci numbers

Congruence	n for which F_n satisfies the congruence
$x \equiv 2 \pmod 3$	$n \equiv 3, 5, 6 \pmod 8$
$x \equiv 0 \pmod 7$	$n \equiv 0 \pmod 8$
$x \equiv 13 \pmod{21}$	$n \equiv 7, 9, 10 \pmod{16}$
$x \equiv 3 \pmod{141}$	$n \equiv 4, 12 \pmod{32}$
$x \equiv 1 \pmod{329}$	$n \equiv 1, 2, 31 \pmod{32}$
$x \equiv 843 \pmod{987}$	$n \equiv 20 \pmod{32}$
$x \equiv 610 \pmod{2207}$	$n \equiv 15, 49 \pmod{64}$
$x \equiv 1597 \pmod{103729}$	$n \equiv 17, 47 \pmod{64}$
$x \equiv 311184 \pmod{311187}$	$n \equiv 60 \pmod{64}$
$x \equiv 317811 \pmod{726103}$	$n \equiv 28 \pmod{64}$
$x \equiv 2584 \pmod{3261}$	$n \equiv 18 \pmod{128}$
$x \equiv 1464 \pmod{7609}$	$n \equiv 50 \pmod{128}$
$x \equiv 6112 \pmod{22827}$	$n \equiv 82 \pmod{128}$
$x \equiv 50712 \pmod{51089}$	$n \equiv 114 \pmod{128}$

4. Sums of two squares. In this section, we prove

THEOREM 4.1. *There is an odd covering of the set of integers which are sums of two squares.*

We will make use of the following classical result. We omit the proof. Recall that $p^e \,\|\, n$ means that $p^e \mid n$ and $p^{e+1} \nmid n$, where we allow for $e = 0$.

LEMMA 4.2. *An $n \in \mathbb{Z}^+$ is a sum of two squares if and only if each prime $p \equiv 3 \pmod 4$ satisfies $p^e \,\|\, n$ for some even non-negative integer e.*

For vectors $\vec{a} = \langle a_1, \dots, a_t\rangle$ and $\vec{m} = \langle m_1, \dots, m_t\rangle$, with $a_1, \dots, a_t$ arbitrary integers and with $m_1, \dots, m_t$ positive pairwise relatively prime integers, we denote by $[\![\vec{a}, \vec{m}]\!]$ the unique congruence $x \equiv A \pmod M$, given by the Chinese Remainder Theorem, where $M = m_1 \cdots m_t$ and where $A \in [0, M) \cap \mathbb{Z}$, corresponding to simultaneously satisfying the congruences

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \ \dots, \ x \equiv a_t \pmod{m_t}.$$

We stress that we are interested only in the case where the m_j are positive pairwise relatively prime integers. For convenience later, we do not require that $a_j \in [0, m_j)$.

Our next two lemmas are similar in nature. The basic idea behind these lemmas has been used by a number of authors and can be traced back to at least C. E. Krukenberg's 1971 dissertation [12].

LEMMA 4.3. *Let p be a prime. Let $S \subseteq \mathbb{Z}^+$ have the property that given any integers $m \geq 1$ and u with $p \nmid m$ and any $s_1 \in S$, there is an $s_2 \in S$ such that $s_2 \equiv s_1 \pmod m$ and $s_2 \equiv u \pmod p$. Let C_1, C_2 and $C = C_1 \cup C_2$ be sets of congruences given by*

$$C_1 = \{[\![\langle a_j\rangle, \langle m_j\rangle]\!] : 1 \leq j \leq r\} \quad \text{and} \quad C_2 = \{[\![\langle b_j, b_j\rangle, \langle p, m_j'\rangle]\!] : 1 \leq j \leq s\},$$

where p is a prime, each modulus m_j appearing in C_1 is at least 2 and relatively prime to p, and each modulus pm_j' appearing in C_2 is non-divisible by p^2 (and hence exactly divisible by p). Suppose that every integer in

$$\big\{s' \in S : s' \equiv a \pmod p \text{ for some } a \in \{0, 1, \dots, p-2\}\big\}$$

satisfies at least one congruence in C. Then every integer in S satisfies at least one of the $r + ts + q$ congruences given below:

(i) $[\![\langle a_j\rangle, \langle m_j\rangle]\!]$ *for* $1 \leq j \leq r$,
(ii) $[\![\langle p^{i-1} - 1 + b_j p^{i-1}, b_j\rangle, \langle p^i, m_j'\rangle]\!]$ *for* $1 \leq i \leq t$ *and* $1 \leq j \leq s$,
(iii) $[\![\langle j, -1\rangle, \langle q, p^{t-j}\rangle]\!]$ *for* $0 \leq j \leq q-1$,

where q is an arbitrary fixed prime such that $q \nmid (pm_1' \cdots m_s')$ and where $t \in \mathbb{Z}$ satisfies $t \geq q$.

We will turn to the proof shortly. We note first that $S = \mathbb{Z}^+$ has the property required of S in the second sentence of the lemma. Perhaps less

clear is that the set S of integers which are sums of two squares has this property, and this will be the S of interest to us (and we will only require $p = 5$). We explain next why the integers that are sums of two squares can be used for S in Lemma 4.3.

As a preliminary result, we let a and b be integers with $\gcd(a, 2b) = 1$. We show first that there are infinitely many $n \in \mathbb{Z}$ such that $an+b$ is a prime that is 1 modulo 4. Since a is odd, there is an $n_0 \in \mathbb{Z}$ such that $an_0 + b \equiv 1 \pmod 4$. Let $n = n_0 + 4k$ where k is an integer to be determined. Thus, $an + b = an_0 + b + 4ak$. Since $an_0 + b \equiv 1 \pmod 4$ and $\gcd(a, b) = 1$, we deduce $\gcd(an_0 + b, 4a) = 1$. Dirichlet's Theorem on primes in arithmetic progressions implies now that there are infinitely many integers k such that, with n chosen as above, $an + b$ is a prime congruent to 1 modulo 4.

To see that the integers that are sums of two squares can be used for S in Lemma 4.3 with p an arbitrary prime, let m and u be as stated and let s_1 be a sum of two squares. We suppose as we may that $u \in \{0, 1, \dots, p-1\}$. If $s_1 = 0$, then we define $v = 1$. If $s_1 \neq 0$, we define v as a positive integer such that if $q^e \mid s_1$ where q is a prime and e is a positive integer, then $e + 2 \leq 2v$. Set $d = \gcd(s_1, m^{2v})$, $s' = s_1/d$ and $m' = m^{2v}/d$. Note that $\gcd(s', m') = 1$. Also, the definition of v implies that if q is a prime and e is a positive integer satisfying $q^e \parallel d$, then $q^e \parallel s_1$. From Lemma 4.2, we see that since s_1 and m^{2v} are each a sum of two squares, so are d, s' and m'. Since $p \nmid m$, we have $p \nmid d$. Also, since $p \nmid m$, there is a $k_0 \in \mathbb{Z}$ such that $s_1 + k_0 m^{2v} \equiv u \pmod{p^2}$. Let $k = k_0 + p^2\ell$, where ℓ is an integer to be chosen. We take

$$s_2 = s_1 + km^{2v} = s_1 + k_0 m^{2v} + p^2 \ell m^{2v} = d(s' + k_0 m' + p^2 m'\ell).$$

Observe that $s_2 \equiv s_1 \pmod m$ and $s_2 \equiv s_1 + k_0 m^{2v} \equiv u \pmod p$. We are left with showing s_2 is a sum of two squares. We consider a couple cases.

If $u = 0$, then

$$s_2 = dp^2\left(\frac{s' + k_0 m'}{p^2} + m'\ell\right).$$

The expression $(s' + k_0 m')/p^2$ is an integer relatively prime to m'. If m' is odd, then our preliminary result above with $a = m'$ and $b = (s' + k_0 m')/p^2$ implies that we can take ℓ so that $a\ell + b$ is a prime congruent to 1 modulo 4. As s_2 is then a product of the 3 numbers d, p^2 and $a\ell + b$ each of which is a sum of two squares, so is s_2. If m' is even, then m is even and our definition of v implies $4 \mid m'$. Also, $p \nmid m$, so p is odd, and $p^2 \equiv 1 \pmod 4$. Since $\gcd(s', m') = 1$, s' is odd. Since s' is a sum of two squares, $s' \equiv 1 \pmod 4$. Thus, Dirichlet's Theorem implies there is an $\ell \in \mathbb{Z}$ such that $(s' + k_0 m')/p^2 + m'\ell$ is a prime that is 1 modulo 4. Again, we see that s_2 is a sum of two squares.

If $u \neq 0$, then $s' + k_0 m'$ is not divisible by p. Further, it is relatively prime to m'. If m' is even, then, as in the last case, $4 \mid m'$, $s' \equiv 1 \pmod 4$ and there is an ℓ such that $s' + k_0 m' + p^2 m'\ell$ is a prime that is 1 modulo 4.

Thus, s_2 is a sum of two squares. So suppose m' is odd. If p is odd, then we use our preliminary result above with $a = p^2m'$ and $b = s' + k_0m'$ to see that we can take ℓ with $a\ell + b$ a prime congruent to 1 modulo 4. Again, we deduce that s_2 is then a sum of two squares. Suppose now that $p = 2$. In this case, $u \in \{0, 1\}$ and $u \neq 0$, so $u = 1$. Hence, $s_1 + k_0m^{2v} \equiv u \pmod{p^2}$ implies $s_1 + k_0m^{2v} \equiv 1 \pmod 4$. Since $p \nmid m$, we see that m is odd. Thus, d is odd. Since d is a sum of two squares, $d \equiv 1 \pmod 4$. We deduce that

$$s' + k_0m' \equiv d(s' + k_0m') \equiv s_1 + k_0m^{2v} \equiv 1 \pmod 4.$$

Since $s' + k_0m'$ is relatively prime to $4m'$, we can choose ℓ in such a way that $s' + k_0m' + p^2m'\ell = s' + k_0m' + 4m'\ell$ is a prime congruent to 1 modulo 4. Again, s_2 is a sum of two squares.

Before proceeding to the proof of Lemma 4.3, we note that if $m_1, \dots, m_r$ are distinct and $m'_1, \dots, m'_s$ are distinct, then the various moduli appearing in (i)–(iii) are all distinct. The condition $q \nmid (pm'_1 \cdots m'_s)$ makes this easier to see; however, it is more than one needs. We note also that if one is interested in not introducing new prime divisors into the product of the moduli, this generally can be done by instead taking q to be an integer not divisible by p and different from each modulus m'_j.

Proof of Lemma 4.3. For each $u \in \{0, 1, \dots, p-1\}$, we define

$$C_2^{(u)} = \{[\![\langle b_j\rangle, \langle m'_j\rangle]\!] : 1 \le j \le s,\ b_j \equiv u \pmod p\}.$$

We begin by showing that for each $u \neq p-1$, each element of S satisfies a congruence in $C_1 \cup C_2^{(u)}$.

Fix $u \in \{0, 1, \dots, p-2\}$, and let T_u denote the set of $j \in \{1, \dots, s\}$ for which $b_j \equiv u \pmod p$. Let $n \in S$, and set

$$m = \Big(\prod_{j=1}^{r} m_j\Big)\Big(\prod_{j\in T_u} m'_j\Big).$$

By the condition on S in the lemma, there is an $n_0 \in S$ such that $n_0 \equiv u \pmod p$ and for some integer n' we have

$$n_0 = n + mn' = n + \Big(\prod_{j=1}^{r} m_j\Big)\Big(\prod_{j\in T_u} m'_j\Big)n'.$$

Since each integer in S that is u modulo p satisfies a congruence in C, either $n_0 \equiv a_j \pmod{m_j}$ for some $j \in \{1, \dots, r\}$ or $n_0 \equiv b_j \pmod{pm'_j}$ for some $j \in \{1, \dots, s\}$. In the former case, n, being congruent to n_0 modulo each m_j, satisfies a congruence in C_1. In the latter case, $n \equiv n_0 \equiv b_j \pmod{m'_j}$ for some $j \in \{1, \dots, s\}$. Also, $b_j \equiv n_0 \equiv u \pmod p$, so $j \in T_u$. Thus, in this case, n satisfies a congruence in $C_2^{(u)}$. Hence, each integer in S satisfies a congruence in $C_1 \cup C_2^{(u)}$.

Note that (ii) with $i = 1$ corresponds to the congruences in C_2. Thus, every integer congruent to $0, 1, \dots, p-3$, or $p-2$ modulo p satisfies a congruence from either (i) or (ii). We restrict ourselves now to integers $n \in S$ that are congruent to $p-1$ modulo p. Observe that either $n = -1$ or there is some $\ell \geq 1$ such that

$$n \equiv -1 \pmod{p^\ell} \quad \text{and} \quad n \not\equiv -1 \pmod{p^{\ell+1}}. \tag{4.1}$$

First, we consider $n \neq -1$ and the case in (4.1) where $\ell \leq t-1$. Then, with ℓ as above, $n \equiv p^\ell - 1 + p^\ell u \pmod{p^{\ell+1}}$ where $u \not\equiv p-1 \pmod{p}$. Suppose n does not satisfy a congruence in C_1. Then since each integer in S satisfies a congruence in $C_1 \cup C_2^{(u)}$, there is a $j \in T_u$ such that $n \equiv b_j \pmod{m'_j}$. Since $j \in T_u$, we have $b_j \equiv u \pmod{p}$, which implies $up^\ell \equiv b_j p^\ell \pmod{p^{\ell+1}}$. Hence, $n \equiv p^\ell - 1 + p^\ell b_j \pmod{p^{\ell+1}}$. Thus, n satisfies (ii) with $i = \ell + 1$.

So far, we know that n satisfies a congruence in (i) or (ii) provided $n \neq -1$ and the value of ℓ in (4.1) satisfies $\ell \leq t-1$. Now, suppose $n = -1$, or ℓ in (4.1) is $\geq t$. Either of these implies that $n \equiv -1 \pmod{p^i}$ for every integer $i \in [1, t]$. Also, $n \equiv k \pmod{q}$ for some $k \in \{0, 1, \dots, q-1\}$. Since $1 \leq t - k \leq t$, we obtain $n \equiv -1 \pmod{p^{t-k}}$, so n satisfies the congruence in (iii) corresponding to $j = k$. ∎

LEMMA 4.4. *Let ℓ, r and s be integers with $\ell \geq 1$, $0 \leq r \leq \ell$ and $0 \leq s \leq \ell$. Let $b_1, \dots, b_\ell$ and $m_1, \dots, m_\ell$ be integers, with each $m_j > 1$. Let $b'_1, \dots, b'_r$, $b''_1, \dots, b''_s$, $m'_1, \dots, m'_r$ and $m''_1, \dots, m''_s$ be such that $\{(b'_j, m'_j) : 1 \leq j \leq r\}$ and $\{(b''_j, m''_j) : 1 \leq j \leq s\}$ are both subsets of $\{(b_j, m_j) : 1 \leq j \leq \ell\}$. Let p be an odd prime such that $p \nmid (3m_1 \cdots m_\ell)$, and let a, w and t be integers with $w \geq 1$ and $t \geq p-1$. Suppose n is an integer which satisfies the congruence $[\![\langle a, b_1, \dots, b_\ell\rangle, \langle 3^w, m_1, \dots, m_\ell\rangle]\!]$. Then n satisfies at least one of the following congruences:*

(i) $[\![\langle a + 2(3^w + 3^{w+1} + \cdots + 3^{i-2}), b'_1, \dots, b'_r\rangle, \langle 3^i, m'_1, \dots, m'_r\rangle]\!]$ *for* $w+1 \leq i \leq t$,

(ii) $[\![\langle a + 2(3^w + 3^{w+1} + \cdots + 3^{i-2}) + 3^{i-1}, b''_1, \dots, b''_s\rangle, \langle 3^i, m''_1, \dots, m''_s\rangle]\!]$ *for* $w+1 \leq i \leq t$,

(iii) $[\![\langle a + 2(3^w + 3^{w+1} + \cdots + 3^{t-k-1}), k\rangle, \langle 3^{t-k}, p\rangle]\!]$ *for* $0 \leq k \leq p-1$,

where empty sums are interpreted as equal to 0.

Proof. Let n be an integer satisfying the congruence

$$[\![\langle a, b_1, \dots, b_\ell\rangle, \langle 3^w, m_1, \dots, m_\ell\rangle]\!].$$

If $n \equiv a \pmod{3^{w+1}}$, then n satisfies (i) with $i = w+1$. If $n \equiv a + 3^w \pmod{3^{w+1}}$, then n satisfies (ii) with $i = w+1$. Since $n \equiv a \pmod{3^w}$, we are left with the case $n \equiv a + 2 \cdot 3^w \pmod{3^{w+1}}$. Again, there are three possibilities. If $n \equiv a + 2 \cdot 3^w \pmod{3^{w+2}}$, then n satisfies (i) with $i = w+2$. If $n \equiv a + 2 \cdot 3^w + 3^{w+1} \pmod{3^{w+2}}$, then n satisfies (ii) with $i = w+2$.

We are left then with $n \equiv a + 2(3^w + 3^{w+1}) \pmod{3^{w+2}}$. Continuing in this manner, using a congruence from (i) and a congruence from (ii) with successive values of i, we are left with n satisfying either (i) or (ii) unless $n \equiv a+2(3^w+3^{w+1}+\cdots+3^{t-1}) \pmod{3^t}$. For such n, there is a $k \in \{0, 1, \ldots, p-1\}$ such that both $n \equiv k \pmod{p}$ and $n \equiv a + 2(3^w + 3^{w+1} + \cdots + 3^{t-k-1}) \pmod{3^{t-k}}$; the first of these congruences determines k and the second follows from $n \equiv a + 2(3^w + 3^{w+1} + \cdots + 3^{t-1}) \pmod{3^t}$. Thus, in this case, n satisfies a congruence in (iii). ∎

Proof of Theorem 4.1. Let $S = \{0, 1, 2, 4, 5, 8, 9, \ldots\}$ be the set of integers that are sums of two squares. We begin by using a single congruence to cover every element n of S that is divisible by 3. Lemma 4.2 implies that each such n satisfies $n \equiv 0 \pmod 9$. Hence, we cover these n by using the congruence

$$\text{(C1)} \qquad [\![\langle 0\rangle, \langle 9\rangle]\!];$$

here, and throughout the proof, we indicate congruences in our final covering of S by labelling them with (C$*$) with $*$ replaced by a number. Now, we use

$$\text{(C2)} \qquad [\![\langle 1\rangle, \langle 3\rangle]\!]$$

to cover those n in S that are 1 modulo 3. Thus, it remains to cover the elements of S that are 2 modulo 3.

We separate the remaining elements of S into three groups, depending on whether they are 2, 5 or 8 modulo 9. We work first with those $n \in S$ for which $n \equiv 2 \pmod 9$. These we break up into five groups depending on their residues modulo 5. The n congruent to 0, 1 or 2 modulo 5 (that also satisfy $n \equiv 2 \pmod 9$) are covered by the three congruences

$$\text{(C3)} \qquad [\![\langle 0\rangle, \langle 5\rangle]\!], \quad [\![\langle 2, 1\rangle, \langle 3, 5\rangle]\!], \quad [\![\langle 2, 2\rangle, \langle 9, 5\rangle]\!].$$

We separate the $n \in S$ for which $n \equiv 2 \pmod 9$ and $n \equiv 3 \pmod 5$, into seven groups depending on their residue classes modulo 7. We take advantage of Lemma 4.2 again to see that the $n \in S$ divisible by 7 satisfy $n \equiv 0 \pmod{49}$. We can therefore cover the n in all seven groups by using the congruences

$$\text{(C4)} \qquad \begin{aligned} &[\![\langle 0\rangle, \langle 49\rangle]\!], \quad [\![\langle 1\rangle, \langle 7\rangle]\!], \quad [\![\langle 2, 2\rangle, \langle 3, 7\rangle]\!], \quad [\![\langle 3, 3\rangle, \langle 5, 7\rangle]\!], \\ &[\![\langle 2, 3, 4\rangle, \langle 3, 5, 7\rangle]\!], \quad [\![\langle 2, 5\rangle, \langle 9, 7\rangle]\!], \quad [\![\langle 2, 3, 6\rangle, \langle 9, 5, 7\rangle]\!]. \end{aligned}$$

As of now, we are left with covering the $n \in S$ which satisfy $[\![\langle 2, 4\rangle, \langle 9, 5\rangle]\!]$, $[\![\langle 5\rangle, \langle 9\rangle]\!]$ or $[\![\langle 8\rangle, \langle 9\rangle]\!]$. We return to the first of these later in the argument.

Next, we cover the elements of S satisfying $[\![\langle 5\rangle, \langle 9\rangle]\!]$. We break these up into their five residue classes modulo 5. The first two congruences in (C3) will already cover the $n \in S$ for which $n \equiv 5 \pmod 9$ and n is either 0 or 1 modulo 5.

We cover the $n \in S$ that satisfy $[\![\langle 5, 2\rangle, \langle 9, 5\rangle]\!]$ next. For this, we use Lemma 4.4 with $a = 5$, $w = 2$, $r = 0$, $s = 1$, $b_1'' = 2$ and $m_1'' = 5$. The values of t and p do not play a significant role, though they will need to be

sufficiently large. We take $t = p = 53$. Thus, our congruences here are

$$\begin{aligned}
&[\![\langle 5 + 2(3^2 + 3^3 + \cdots + 3^{i-2})\rangle, \langle 3^i\rangle]\!] && \text{for } 3 \le i \le 53,\\
&[\![\langle 5 + 2(3^2 + 3^3 + \cdots + 3^{i-2}) + 3^{i-1}, 2\rangle, \langle 3^i, 5\rangle]\!] && \text{for } 3 \le i \le 53,\\
&[\![\langle 5 + 2(3^2 + 3^3 + \cdots + 3^{52-k}), k\rangle, \langle 3^{53-k}, 53\rangle]\!] && \text{for } 0 \le k \le 52.
\end{aligned} \tag{C5}$$

Next, we cover the integers in S satisfying $[\![\langle 5, 3\rangle, \langle 9, 5\rangle]\!]$ by grouping them into seven residue classes modulo 7. All integers in S divisible by 7 have been covered by the first congruence in (C4). For the integers satisfying $[\![\langle 5, 3\rangle, \langle 9, 5\rangle]\!]$ and that are either 1, 2, 3 or 4 modulo 7, we can use $[\![\langle 1\rangle, \langle 7\rangle]\!]$, $[\![\langle 2, 2\rangle, \langle 3, 7\rangle]\!]$, $[\![\langle 3, 3\rangle, \langle 5, 7\rangle]\!]$ and $[\![\langle 2, 3, 4\rangle, \langle 3, 5, 7\rangle]\!]$ from (C4). For the integers in $[\![\langle 5, 3\rangle, \langle 9, 5\rangle]\!]$ that are 5 modulo 7, we apply Lemma 4.4 with $a = 5$, $w = 2$, $r = 0$, $s = 2$, $b_1'' = 3$, $b_2'' = 5$, $m_1'' = 5$ and $m_2'' = 7$. We note that we can take $t = p = 53$ as before. For Lemma 4.4 here, we are reusing the congruences

$$\begin{aligned}
&[\![\langle 5 + 2(3^2 + 3^3 + \cdots + 3^{i-2})\rangle, \langle 3^i\rangle]\!] && \text{for } 3 \le i \le 53,\\
&[\![\langle 5 + 2(3^2 + 3^3 + \cdots + 3^{52-k}), k\rangle, \langle 3^{53-k}, 53\rangle]\!] && \text{for } 0 \le k \le 52,
\end{aligned}$$

which appear in (C5), and making use of the additional congruences

$$[\![\langle 5 + 2(3^2 + 3^3 + \cdots + 3^{i-2}) + 3^{i-1}, 3, 5\rangle, \langle 3^i, 5, 7\rangle]\!] \quad \text{for } 3 \le i \le 53. \tag{C6}$$

For the remaining integers in S satisfying $[\![\langle 5, 3\rangle, \langle 9, 5\rangle]\!]$ which are 6 modulo 7, we apply Lemma 4.4 again, this time with $a = 5$, $w = 2$, $r = 0$, $s = 1$, $b_1'' = 6$, $m_1'' = 7$, and $t = p = 53$. For this application of Lemma 4.4, after reusing congruences from (C5) as above, we additionally use

$$[\![\langle 5 + 2(3^2 + 3^3 + \cdots + 3^{i-2}) + 3^{i-1}, 6\rangle, \langle 3^i, 7\rangle]\!] \quad \text{for } 3 \le i \le 53. \tag{C7}$$

Thus far, we have covered all the integers in S satisfying $[\![\langle 5\rangle, \langle 9\rangle]\!]$ except for those that are 4 modulo 5. Combining what we now know, we are left with covering the $n \in S$ which satisfy $[\![\langle 2, 4\rangle, \langle 9, 5\rangle]\!]$, $[\![\langle 5, 4\rangle, \langle 9, 5\rangle]\!]$ or $[\![\langle 8\rangle, \langle 9\rangle]\!]$. We deal with the latter next.

We break up the integers in S satisfying $[\![\langle 8\rangle, \langle 9\rangle]\!]$ into groups depending on the residue class modulo 5. We use $[\![\langle 0\rangle, \langle 5\rangle]\!]$ and $[\![\langle 2, 1\rangle, \langle 3, 5\rangle]\!]$ from (C3) to cover those integers in S satisfying $[\![\langle 8\rangle, \langle 9\rangle]\!]$ that are 0 or 1 modulo 5. The remaining integers in S satisfying $[\![\langle 8\rangle, \langle 9\rangle]\!]$ must satisfy $[\![\langle 8, 2\rangle, \langle 9, 5\rangle]\!]$, $[\![\langle 8, 3\rangle, \langle 9, 5\rangle]\!]$ or $[\![\langle 8, 4\rangle, \langle 9, 5\rangle]\!]$.

We group those satisfying $[\![\langle 8, 2\rangle, \langle 9, 5\rangle]\!]$ into the seven residue classes modulo 7. We reuse the first three congruences in (C4) so that we are left with elements in S satisfying $[\![\langle 8, 2\rangle, \langle 9, 5\rangle]\!]$ that also satisfy one of

$$\begin{aligned}
&[\![\langle 8, 2, 3\rangle, \langle 9, 5, 7\rangle]\!], \quad [\![\langle 8, 2, 4\rangle, \langle 9, 5, 7\rangle]\!],\\
&[\![\langle 8, 2, 5\rangle, \langle 9, 5, 7\rangle]\!], \quad [\![\langle 8, 2, 6\rangle, \langle 9, 5, 7\rangle]\!].
\end{aligned}$$

We examine these in reverse order.

We group those integers in S satisfying $[\![\langle 8,2,6\rangle,\langle 9,5,7\rangle]\!]$ into their eleven residue classes modulo 11. Since $11 \equiv 3 \pmod 4$, Lemma 4.2 implies that

$$[\![\langle 0\rangle,\langle 121\rangle]\!] \tag{C8}$$

covers every integer in S divisible by 11. We cover nine further residue classes modulo 11, of the integers in S satisfying $[\![\langle 8,2,6\rangle,\langle 9,5,7\rangle]\!]$, using

$$\begin{aligned} &[\![\langle 1\rangle,\langle 11\rangle]\!], && [\![\langle 2,2\rangle,\langle 3,11\rangle]\!], && [\![\langle 8,3\rangle,\langle 9,11\rangle]\!],\\ &[\![\langle 2,4\rangle,\langle 5,11\rangle]\!], && [\![\langle 2,2,5\rangle,\langle 3,5,11\rangle]\!], && [\![\langle 8,2,6\rangle,\langle 9,5,11\rangle]\!],\\ &[\![\langle 6,7\rangle,\langle 7,11\rangle]\!], && [\![\langle 2,6,8\rangle,\langle 3,7,11\rangle]\!], && [\![\langle 8,6,9\rangle,\langle 9,7,11\rangle]\!]. \end{aligned} \tag{C9}$$

To cover the residue class of integers in S that are 10 modulo 11 and satisfy $[\![\langle 8,2,6\rangle,\langle 9,5,7\rangle]\!]$, we apply Lemma 4.4 with $a=8$, $w=2$, $r=1$, $s=2$, $b_1'=10$, $b_1''=6$, $b_2''=10$, $m_1'=11$, $m_1''=7$, $m_2''=11$ and $t=p=59$. This leads to

$$\begin{aligned} &[\![\langle 8+2(3^2+\cdots+3^{i-2}),10\rangle,\langle 3^i,11\rangle]\!] && \text{for } 3\le i\le 59,\\ &[\![\langle 8+2(3^2+\cdots+3^{i-2})+3^{i-1},6,10\rangle,\langle 3^i,7,11\rangle]\!] && \text{for } 3\le i\le 59,\\ &[\![\langle 8+2(3^2+\cdots+3^{58-k}),k\rangle,\langle 3^{59-k},59\rangle]\!] && \text{for } 0\le k\le 58. \end{aligned} \tag{C10}$$

Thus, the integers in S satisfying $[\![\langle 8,2,6\rangle,\langle 9,5,7\rangle]\!]$ will be covered by the congruences in (C8)–(C10).

Next, we turn to the integers in S satisfying $[\![\langle 8,2,5\rangle,\langle 9,5,7\rangle]\!]$. We split these up into congruence classes modulo 11 as well. Those congruent to $0,\dots,6 \pmod{11}$ are covered by (C8) and the first six congruences in (C9). Those congruent to 7, 8 or 9 modulo 11 are covered by one of

$$\begin{aligned} &[\![\langle 2,5,7\rangle,\langle 5,7,11\rangle]\!], \quad [\![\langle 2,2,5,8\rangle,\langle 3,5,7,11\rangle]\!],\\ &[\![\langle 8,2,5,9\rangle,\langle 9,5,7,11\rangle]\!]. \end{aligned} \tag{C11}$$

To cover those that are 10 modulo 11, we apply Lemma 4.4 with $a=8$, $w=2$, $r=1$, $s=2$, $b_1'=10$, $b_1''=2$, $b_2''=10$, $m_1'=11$, $m_1''=5$, $m_2''=11$ and $t=p=59$. For this, we reuse congruences from (C10). We are then left with the additional congruences

$$[\![\langle 8+2(3^2+\cdots+3^{i-2})+3^{i-1},2,10\rangle,\langle 3^i,5,11\rangle]\!] \quad \text{for } 3\le i\le 59. \tag{C12}$$

Our congruences then cover the integers in S satisfying $[\![\langle 8,2,5\rangle,\langle 9,5,7\rangle]\!]$.

Next, we turn to the integers in S satisfying $[\![\langle 8,2,4\rangle,\langle 9,5,7\rangle]\!]$. Again, consider their residue classes modulo 11 and use (C8) and the first six congruences in (C9) to cover those that are in the residue classes $0,\dots,6$ modulo 11. Furthermore, our use of Lemma 4.4 leading to (C12) covers the integers in S satisfying $[\![\langle 8,2,4\rangle,\langle 9,5,7\rangle]\!]$ that are 10 modulo 11. To finish covering the integers in S satisfying $[\![\langle 8,2,4\rangle,\langle 9,5,7\rangle]\!]$, we are left now with covering those which satisfy one of $[\![\langle 8,2,4,7\rangle,\langle 9,5,7,11\rangle]\!]$,

$[\![\langle 8,2,4,8\rangle,\langle 9,5,7,11\rangle]\!]$ and $[\![\langle 8,2,4,9\rangle,\langle 9,5,7,11\rangle]\!]$. To cover those satisfying $[\![\langle 8,2,4,7\rangle,\langle 9,5,7,11\rangle]\!]$, we break them up into the seven residue classes $4,11,18,\dots,46$ modulo 49. We cover these by using

$$\begin{aligned}&[\![\langle 2,4\rangle,\langle 3,49\rangle]\!],\quad [\![\langle 2,11\rangle,\langle 5,49\rangle]\!],\quad [\![\langle 8,18\rangle,\langle 9,49\rangle]\!],\\ &[\![\langle 2,2,25\rangle,\langle 3,5,49\rangle]\!],\quad [\![\langle 8,2,32\rangle,\langle 9,5,49\rangle]\!],\\ &[\![\langle 2,39,7\rangle,\langle 3,49,11\rangle]\!],\quad [\![\langle 2,46,7\rangle,\langle 5,49,11\rangle]\!].\end{aligned}\tag{C13}$$

The first five of these congruences also cover the integers in S satisfying $[\![\langle 8,2,4,8\rangle,\langle 9,5,7,11\rangle]\!]$ which are 4, 11, 18, 25 or 32 modulo 49. To cover the integers in S satisfying $[\![\langle 8,2,4,8\rangle,\langle 9,5,7,11\rangle]\!]$ which are 39 or 46 modulo 49, we use

$$[\![\langle 8,39,8\rangle,\langle 9,49,11\rangle]\!],\quad [\![\langle 2,2,46,8\rangle,\langle 3,5,49,11\rangle]\!].\tag{C14}$$

The first five of the congruences in (C13) also cover the integers in S satisfying $[\![\langle 8,2,4,9\rangle,\langle 9,5,7,11\rangle]\!]$ which are 4, 11, 18, 25 or 32 modulo 49. Those in the residue classes 39 and 46 modulo 49 satisfy one of

$$\begin{aligned}&[\![\langle 8,2,39,9\rangle,\langle 9,5,49,11\rangle]\!],\quad [\![\langle 8,46\rangle,\langle 27,49\rangle]\!],\\ &[\![\langle 17,2,46\rangle,\langle 27,5,49\rangle]\!],\qquad [\![\langle 26,2,46,9\rangle,\langle 27,5,49,11\rangle]\!].\end{aligned}\tag{C15}$$

We have now finished covering the integers in S satisfying $[\![\langle 8,2,4\rangle,\langle 9,5,7\rangle]\!]$.

We turn to the integers in S satisfying $[\![\langle 8,2,3\rangle,\langle 9,5,7\rangle]\!]$. We break up these integers into 13 residue classes modulo 13 and cover the integers in 12 of these residue classes using

$$\begin{aligned}&[\![\langle 0\rangle,\langle 13\rangle]\!],\quad [\![\langle 2,1\rangle,\langle 3,13\rangle]\!],\quad [\![\langle 8,2\rangle,\langle 9,13\rangle]\!],\quad [\![\langle 2,3\rangle,\langle 5,13\rangle]\!],\\ &[\![\langle 2,2,4\rangle,\langle 3,5,13\rangle]\!],\quad [\![\langle 8,2,5\rangle,\langle 9,5,13\rangle]\!],\quad [\![\langle 3,6\rangle,\langle 7,13\rangle]\!],\\ &[\![\langle 2,3,7\rangle,\langle 3,7,13\rangle]\!],\quad [\![\langle 8,3,8\rangle,\langle 9,7,13\rangle]\!],\quad [\![\langle 2,3,9\rangle,\langle 5,7,13\rangle]\!],\\ &[\![\langle 2,2,3,10\rangle,\langle 3,5,7,13\rangle]\!],\quad [\![\langle 8,2,3,11\rangle,\langle 9,5,7,13\rangle]\!].\end{aligned}\tag{C16}$$

For those in the residue class 12 modulo 13, we apply Lemma 4.4 with $a=8$, $w=2$, $r=1$, $s=2$, $b_1'=12$, $b_1''=2$, $b_2''=12$, $m_1'=13$, $m_1''=5$, $m_2''=13$ and $t=p=59$. We reuse the last set of congruences in (C10) and make use of the additional congruences

$$\begin{aligned}&[\![\langle 8+2(3^2+\cdots+3^{i-2}),12\rangle,\langle 3^i,13\rangle]\!] && \text{for } 3\le i\le 59,\\ &[\![\langle 8+2(3^2+\cdots+3^{i-2})+3^{i-1},2,12\rangle,\langle 3^i,5,13\rangle]\!] && \text{for } 3\le i\le 59.\end{aligned}\tag{C17}$$

The last set of congruences in (C10) and the congruences in (C16) and (C17) cover then the integers in S satisfying $[\![\langle 8,2,3\rangle,\langle 9,5,7\rangle]\!]$. Therefore we have now covered all the integers in S satisfying $[\![\langle 8,2\rangle,\langle 9,5\rangle]\!]$.

Next, we will cover the integers in S satisfying $[\![\langle 8,3\rangle,\langle 9,5\rangle]\!]$. Any of the previous congruences used can be applied here as long as they intersect the class 8 modulo 9 and 3 modulo 5. In particular, the first five congruences

in (C4) imply that we need only concern ourselves with integers in S satisfying $[\![\langle 8,3,5\rangle,\langle 9,5,7\rangle]\!]$ and $[\![\langle 8,3,6\rangle,\langle 9,5,7\rangle]\!]$. By combining this information with the congruences (C8)–(C10), what remains to be covered of the integers in S satisfying $[\![\langle 8,3\rangle,\langle 9,5\rangle]\!]$ are those satisfying one of

$$\begin{aligned}
&[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!], \quad [\![\langle 8,3,5,5\rangle,\langle 9,5,7,11\rangle]\!],\\
&[\![\langle 8,3,5,6\rangle,\langle 9,5,7,11\rangle]\!], \quad [\![\langle 8,3,5,7\rangle,\langle 9,5,7,11\rangle]\!],\\
&[\![\langle 8,3,5,8\rangle,\langle 9,5,7,11\rangle]\!], \quad [\![\langle 8,3,5,9\rangle,\langle 9,5,7,11\rangle]\!],\\
&[\![\langle 8,3,5,10\rangle,\langle 9,5,7,11\rangle]\!], \quad [\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!],\\
&[\![\langle 8,3,6,5\rangle,\langle 9,5,7,11\rangle]\!], \quad [\![\langle 8,3,6,6\rangle,\langle 9,5,7,11\rangle]\!].
\end{aligned}$$

Of these, the integers in S satisfying

$$[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!] \quad \text{and} \quad [\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!]$$

will be covered last.

To cover the integers in S satisfying $[\![\langle 8,3,5,5\rangle,\langle 9,5,7,11\rangle]\!]$, we break them up into residue classes modulo 19 and make use of the 24 divisors of $3^2\cdot 5\cdot 7\cdot 11$ to form the congruences we want. To specify, we use

$$\begin{aligned}
&[\![\langle 8,j\rangle,\langle 3^j,19\rangle]\!], && [\![\langle 8,3,j+3\rangle,\langle 3^j,5,19\rangle]\!],\\
&[\![\langle 8,5,j+6\rangle,\langle 3^j,11,19\rangle]\!], && [\![\langle 8,3,5,j+9\rangle,\langle 3^j,5,11,19\rangle]\!],\\
&[\![\langle 8,5,j+12\rangle,\langle 3^j,7,19\rangle]\!], && [\![\langle 8,3,5,j+15\rangle,\langle 3^j,5,7,19\rangle]\!],\\
&[\![\langle 5,5,18\rangle,\langle 7,11,19\rangle]\!], && \text{for } j\in\{0,1,2\},
\end{aligned} \tag{C18}$$

to cover the integers in S satisfying $[\![\langle 8,3,5,5\rangle,\langle 9,5,7,11\rangle]\!]$.

For the integers in S satisfying $[\![\langle 8,3,5,6\rangle,\langle 9,5,7,11\rangle]\!]$, we make use of

$$\begin{aligned}
&[\![\langle 0\rangle,\langle 17\rangle]\!], \quad [\![\langle 2,1\rangle,\langle 3,17\rangle]\!], \quad [\![\langle 3,2\rangle,\langle 5,17\rangle]\!],\\
&[\![\langle 8,3\rangle,\langle 9,17\rangle]\!], \quad [\![\langle 2,3,4\rangle,\langle 3,5,17\rangle]\!],\\
&[\![\langle 8,3,5\rangle,\langle 9,5,17\rangle]\!], \quad [\![\langle 6,6\rangle,\langle 11,17\rangle]\!],\\
&[\![\langle 2,6,7\rangle,\langle 3,11,17\rangle]\!], \quad [\![\langle 3,6,8\rangle,\langle 5,11,17\rangle]\!],\\
&[\![\langle 8,6,9\rangle,\langle 9,11,17\rangle]\!], \quad [\![\langle 2,3,6,10\rangle,\langle 3,5,11,17\rangle]\!],\\
&[\![\langle 8,3,6,11\rangle,\langle 9,5,11,17\rangle]\!], \quad [\![\langle 5,12\rangle,\langle 7,17\rangle]\!],\\
&[\![\langle 2,5,13\rangle,\langle 3,7,17\rangle]\!], \quad [\![\langle 3,5,14\rangle,\langle 5,7,17\rangle]\!],\\
&[\![\langle 8,5,15\rangle,\langle 9,7,17\rangle]\!], \quad [\![\langle 2,3,5,16\rangle,\langle 3,5,7,17\rangle]\!].
\end{aligned} \tag{C19}$$

Thus, these integers have been covered by breaking them up into their residue classes modulo 17.

We break up the integers in S satisfying $[\![\langle 8,3,5,7\rangle,\langle 9,5,7,11\rangle]\!]$ into their residue classes modulo 13. Observe that moduli with largest prime divisor 13 have been used in (C16) and (C17). Here, the moduli will be different in that the largest two prime divisors will be 11 and 13. We cover the residue

classes $0, 1, \ldots, 11$ modulo 13 by using

$$\begin{aligned}
&[\![\langle 7,0\rangle, \langle 11,13\rangle]\!], \quad [\![\langle 2,7,1\rangle, \langle 3,11,13\rangle]\!], \quad [\![\langle 8,7,2\rangle, \langle 9,11,13\rangle]\!],\\
&[\![\langle 3,7,3\rangle, \langle 5,11,13\rangle]\!], \quad [\![\langle 2,3,7,4\rangle, \langle 3,5,11,13\rangle]\!],\\
&[\![\langle 8,3,7,5\rangle, \langle 9,5,11,13\rangle]\!], \quad [\![\langle 5,7,6\rangle, \langle 7,11,13\rangle]\!],\\
&[\![\langle 2,5,7,7\rangle, \langle 3,7,11,13\rangle]\!], \quad [\![\langle 8,5,7,8\rangle, \langle 9,7,11,13\rangle]\!],\\
&[\![\langle 3,5,7,9\rangle, \langle 5,7,11,13\rangle]\!], \quad [\![\langle 2,3,5,7,10\rangle, \langle 3,5,7,11,13\rangle]\!],\\
&[\![\langle 8,3,5,7,11\rangle, \langle 9,5,7,11,13\rangle]\!].
\end{aligned} \tag{C20}$$

For the integers in S satisfying $[\![\langle 8,3,5,7\rangle, \langle 9,5,7,11\rangle]\!]$ and lying in the residue class 12 modulo 13, we apply Lemma 4.4 with $a = 8$, $w = 2$, $r = 1$, $s = 3$, $b_1' = 12$, $b_1'' = 3$, $b_2'' = 7$, $b_3'' = 12$, $m_1' = 13$, $m_1'' = 5$, $m_2'' = 11$, $m_3'' = 13$ and $t = p = 59$. Thus, we reuse congruences from (C10) and (C17) and add

$$[\![\langle 8 + 2(3^2 + 3^3 + \cdots + 3^{i-2}) + 3^{i-1}, 3, 7, 12\rangle, \langle 3^i, 5, 11, 13\rangle]\!] \quad \text{for } 3 \le i \le 59 \tag{C21}$$

to our collection of congruences.

To cover the integers in S satisfying $[\![\langle 8,3,5,8\rangle, \langle 9,5,7,11\rangle]\!]$, we can reuse the congruences in (C19) to cover those that fall into one of the residue classes $0, 1, \ldots, 5$ and $12, 13, \ldots, 16$ modulo 17. To cover those in the remaining residue classes modulo 17, we use

$$\begin{aligned}
&[\![\langle 8,3,5,6\rangle, \langle 9,5,7,17\rangle]\!], \quad [\![\langle 5,8,7\rangle, \langle 7,11,17\rangle]\!],\\
&[\![\langle 2,5,8,8\rangle, \langle 3,7,11,17\rangle]\!], \quad [\![\langle 3,5,8,9\rangle, \langle 5,7,11,17\rangle]\!],\\
&[\![\langle 8,5,8,10\rangle, \langle 9,7,11,17\rangle]\!], \quad [\![\langle 2,3,5,8,11\rangle, \langle 3,5,7,11,17\rangle]\!].
\end{aligned} \tag{C22}$$

Note that (C8) is the only congruence thus far involving a modulus divisible by 121. To cover the integers in S that satisfy the congruence $[\![\langle 8,3,5,9\rangle, \langle 9,5,7,11\rangle]\!]$, we break them up into 11 residue classes modulo 121. These integers are thus covered by

$$\begin{aligned}
&[\![\langle 2,9\rangle, \langle 3,121\rangle]\!], \quad [\![\langle 3,20\rangle, \langle 5,121\rangle]\!], \quad [\![\langle 8,31\rangle, \langle 9,121\rangle]\!],\\
&[\![\langle 2,3,42\rangle, \langle 3,5,121\rangle]\!], \quad [\![\langle 8,3,53\rangle, \langle 9,5,121\rangle]\!],\\
&[\![\langle 5,64\rangle, \langle 7,121\rangle]\!], \quad [\![\langle 2,5,75\rangle, \langle 3,7,121\rangle]\!],\\
&[\![\langle 3,5,86\rangle, \langle 5,7,121\rangle]\!], \quad [\![\langle 8,5,97\rangle, \langle 9,7,121\rangle]\!],\\
&[\![\langle 2,3,5,108\rangle, \langle 3,5,7,121\rangle]\!], \quad [\![\langle 8,3,5,119\rangle, \langle 9,5,7,121\rangle]\!].
\end{aligned} \tag{C23}$$

We cover the integers in S satisfying $[\![\langle 8,3,5,10\rangle, \langle 9,5,7,11\rangle]\!]$ by breaking them up into residue classes modulo 23. These are then covered by using

$$\begin{aligned}
&[\![\langle 8, j\rangle, \langle 3^j, 23\rangle]\!], \quad [\![\langle 8, 3, j+3\rangle, \langle 3^j, 5, 23\rangle]\!],\\
&[\![\langle 8, 5, j+6\rangle, \langle 3^j, 7, 23\rangle]\!], \quad [\![\langle 8, 10, j+9\rangle, \langle 3^j, 11, 23\rangle]\!],\\
&[\![\langle 8, 3, 5, j+12\rangle, \langle 3^j, 5, 7, 23\rangle]\!], \quad [\![\langle 8, 3, 10, j+15\rangle, \langle 3^j, 5, 11, 23\rangle]\!],\\
&[\![\langle 8, 5, 10, j+18\rangle, \langle 3^j, 7, 11, 23\rangle]\!], \quad [\![\langle 3, 5, 10, 21\rangle, \langle 5, 7, 11, 23\rangle]\!],\\
&[\![\langle 2, 3, 5, 10, 22\rangle, \langle 3, 5, 7, 11, 23\rangle]\!], \quad \text{for } j \in \{0, 1, 2\}.
\end{aligned} \tag{C24}$$

Next, we turn to covering integers in S satisfying $[\![\langle 8, 3, 6, 6\rangle, \langle 9, 5, 7, 11\rangle]\!]$. We break these up into residue classes modulo 17. The first 12 congruences from (C19) cover those integers in the residue classes $0, 1, \dots, 11$ modulo 17. To cover those that are 12, 13 or 14 modulo 17, we use

$$\begin{aligned}
&[\![\langle 8, 3, 6, 6, 12\rangle, \langle 9, 5, 7, 11, 17\rangle]\!], \quad [\![\langle 8, 13\rangle, \langle 27, 17\rangle]\!],\\
&[\![\langle 17, 3, 13\rangle, \langle 27, 5, 17\rangle]\!], \quad [\![\langle 26, 6, 13\rangle, \langle 27, 7, 17\rangle]\!],\\
&[\![\langle 8, 6, 14\rangle, \langle 27, 11, 17\rangle]\!], \quad [\![\langle 17, 3, 6, 14\rangle, \langle 27, 5, 7, 17\rangle]\!],\\
&[\![\langle 26, 3, 6, 14\rangle, \langle 27, 5, 11, 17\rangle]\!].
\end{aligned} \tag{C25}$$

For those integers in S satisfying $[\![\langle 8, 3, 6, 6\rangle, \langle 9, 5, 7, 11\rangle]\!]$ and lying in the residue class 15 modulo 17, we cover separately the three residue classes 8, 17 and 26 modulo 27 that they belong to, covering the first two directly and using Lemma 4.4 to cover the third. For Lemma 4.4, we want $a = 26$, $w = 3$, $r = 1$, $s = 2$, $b_1' = 15$, $b_1'' = 3$, $b_2'' = 15$, $m_1' = 17$, $m_1'' = 5$, $m_2'' = 17$, and $t = p = 59$. We reuse the last 59 congruences in (C10). This leads to the additional congruences

$$\begin{aligned}
&[\![\langle 8, 6, 6, 15\rangle, \langle 27, 7, 11, 17\rangle]\!], \quad [\![\langle 17, 3, 6, 6, 15\rangle, \langle 27, 5, 7, 11, 17\rangle]\!],\\
&[\![\langle 26 + 2(3^3 + \cdots + 3^{i-2}), 15\rangle, \langle 3^i, 17\rangle]\!] \quad \text{for } 4 \le i \le 59,\\
&[\![\langle 26 + 2(3^3 + \cdots + 3^{i-2}) + 3^{i-1}, 3, 15\rangle, \langle 3^i, 5, 17\rangle]\!] \quad \text{for } 4 \le i \le 59.
\end{aligned} \tag{C26}$$

For the remaining integers in S satisfying $[\![\langle 8, 3, 6, 6\rangle, \langle 9, 5, 7, 11\rangle]\!]$, which are 16 modulo 17, we break them up into residue classes modulo 13 and note that we have not used any moduli yet where the largest two prime divisors are 13 and 17. We are able then to cover these integers by using

$$\begin{aligned}
&[\![\langle 0, 16\rangle, \langle 13, 17\rangle]\!], \quad [\![\langle 2, 1, 16\rangle, \langle 3, 13, 17\rangle]\!], \quad [\![\langle 8, 2, 16\rangle, \langle 9, 13, 17\rangle]\!],\\
&[\![\langle 3, 3, 16\rangle, \langle 5, 13, 17\rangle]\!], \quad [\![\langle 2, 3, 4, 16\rangle, \langle 3, 5, 13, 17\rangle]\!],\\
&[\![\langle 8, 3, 5, 16\rangle, \langle 9, 5, 13, 17\rangle]\!], \quad [\![\langle 6, 6, 16\rangle, \langle 7, 13, 17\rangle]\!],\\
&[\![\langle 2, 6, 7, 16\rangle, \langle 3, 7, 13, 17\rangle]\!], \quad [\![\langle 8, 6, 8, 16\rangle, \langle 9, 7, 13, 17\rangle]\!],\\
&[\![\langle 6, 9, 16\rangle, \langle 11, 13, 17\rangle]\!], \quad [\![\langle 2, 6, 10, 16\rangle, \langle 3, 11, 13, 17\rangle]\!],\\
&[\![\langle 8, 6, 11, 16\rangle, \langle 9, 11, 13, 17\rangle]\!], \quad [\![\langle 3, 6, 12, 16\rangle, \langle 5, 7, 13, 17\rangle]\!].
\end{aligned} \tag{C27}$$

Now, we cover the integers in S satisfying $[\![\langle 8, 3, 6, 5\rangle, \langle 9, 5, 7, 11\rangle]\!]$ by breaking them up into their residue classes modulo 19 and beginning with congruences similar to the last case but with 17 replaced by 19. In particular,

(C18) covers those integers in S satisfying $[\![\langle 8,3,6,5\rangle, \langle 9,5,7,11\rangle]\!]$ that are $0, 1, \ldots, 10$ or 11 modulo 19. For those congruent to 12, 13 or 14 modulo 19, we use

$$\begin{aligned}
&[\![\langle 8,3,6,5,12\rangle, \langle 9,5,7,11,19\rangle]\!], \quad [\![\langle 8,13\rangle, \langle 27,19\rangle]\!],\\
&[\![\langle 17,3,13\rangle, \langle 27,5,19\rangle]\!], \quad [\![\langle 26,6,13\rangle, \langle 27,7,19\rangle]\!],\\
&[\![\langle 8,5,14\rangle, \langle 27,11,19\rangle]\!], \quad [\![\langle 17,3,6,14\rangle, \langle 27,5,7,19\rangle]\!],\\
&[\![\langle 26,3,5,14\rangle, \langle 27,5,11,19\rangle]\!].
\end{aligned} \tag{C28}$$

For those congruent to 15 modulo 19, we consider their three residue classes modulo 27, covering those in the first two residue classes directly and covering those in the third residue class using Lemma 4.4 with $a = 26$, $w = 3$, $r = 1$, $s = 2$, $b'_1 = 15$, $b''_1 = 3$, $b''_2 = 15$, $m'_1 = 19$, $m''_1 = 5$, $m''_2 = 19$, and $t = p = 59$. We again reuse the last collection of congruences in (C10). Thus, we make use of

$$\begin{aligned}
&[\![\langle 8,6,5,15\rangle, \langle 27,7,11,19\rangle]\!], \quad [\![\langle 17,3,6,5,15\rangle, \langle 27,5,7,11,19\rangle]\!],\\
&[\![\langle 26+2(3^3+\cdots+3^{i-2}),15\rangle, \langle 3^i,19\rangle]\!] \quad \text{for } 4 \le i \le 59,\\
&[\![\langle 26+2(3^3+\cdots+3^{i-2})+3^{i-1},3,15\rangle, \langle 3^i,5,19\rangle]\!] \quad \text{for } 4 \le i \le 59.
\end{aligned} \tag{C29}$$

For those that are 16 modulo 19, we consider their seven residue classes modulo 49 and use

$$\begin{aligned}
&[\![\langle 6,16\rangle, \langle 49,19\rangle]\!], \quad [\![\langle 2,13,16\rangle, \langle 3,49,19\rangle]\!],\\
&[\![\langle 8,20,16\rangle, \langle 9,49,19\rangle]\!], \quad [\![\langle 3,27,16\rangle, \langle 5,49,19\rangle]\!],\\
&[\![\langle 34,5,16\rangle, \langle 49,11,19\rangle]\!], \quad [\![\langle 2,3,41,16\rangle, \langle 3,5,49,19\rangle]\!],\\
&[\![\langle 8,3,48,16\rangle, \langle 9,5,49,19\rangle]\!].
\end{aligned} \tag{C30}$$

For those that are 17 modulo 19, we consider their eleven residue classes modulo 121 and use

$$\begin{aligned}
&[\![\langle 5,17\rangle, \langle 121,19\rangle]\!], \quad [\![\langle 2,16,17\rangle, \langle 3,121,19\rangle]\!],\\
&[\![\langle 8,27,17\rangle, \langle 9,121,19\rangle]\!], \quad [\![\langle 3,38,17\rangle, \langle 5,121,19\rangle]\!],\\
&[\![\langle 6,49,17\rangle, \langle 7,121,19\rangle]\!], \quad [\![\langle 2,3,60,17\rangle, \langle 3,5,121,19\rangle]\!],\\
&[\![\langle 8,3,71,17\rangle, \langle 9,5,121,19\rangle]\!], \quad [\![\langle 2,6,82,17\rangle, \langle 3,7,121,19\rangle]\!],\\
&[\![\langle 8,6,93,17\rangle, \langle 9,7,121,19\rangle]\!], \quad [\![\langle 2,3,6,104,17\rangle, \langle 3,5,7,121,19\rangle]\!],\\
&[\![\langle 8,3,6,115,17\rangle, \langle 9,5,7,121,19\rangle]\!].
\end{aligned} \tag{C31}$$

We break up the integers in S satisfying $[\![\langle 8,3,6,5\rangle, \langle 9,5,7,11\rangle]\!]$ which are 18 modulo 19 into residue classes modulo 13. Observe that we have not used moduli which have their two largest prime divisors 13 and 19. We can cover these integers with the congruences

$$\begin{aligned}
&[\![\langle 0,18\rangle, \langle 13,19\rangle]\!], \quad [\![\langle 2,1,18\rangle, \langle 3,13,19\rangle]\!],\\
&[\![\langle 8,2,18\rangle, \langle 9,13,19\rangle]\!], \quad [\![\langle 3,3,18\rangle, \langle 5,13,19\rangle]\!],
\end{aligned} \tag{C32}$$

$$\begin{array}{ll}(\text{C32})\\ [\text{cont.}]\end{array}\quad\begin{array}{l}[\![\langle 2,3,4,18\rangle,\langle 3,5,13,19\rangle]\!],\quad [\![\langle 8,3,5,18\rangle,\langle 9,5,13,19\rangle]\!],\\ [\![\langle 6,6,18\rangle,\langle 7,13,19\rangle]\!],\quad [\![\langle 2,6,7,18\rangle,\langle 3,7,13,19\rangle]\!],\\ [\![\langle 8,6,8,18\rangle,\langle 9,7,13,19\rangle]\!],\quad [\![\langle 3,6,9,18\rangle,\langle 5,7,13,19\rangle]\!],\\ [\![\langle 2,3,6,10,18\rangle,\langle 3,5,7,13,19\rangle]\!],\quad [\![\langle 8,3,6,11,18\rangle,\langle 9,5,7,13,19\rangle]\!],\\ [\![\langle 3,6,5,12,18\rangle,\langle 5,7,11,13,19\rangle]\!].\end{array}$$

Of the integers in S satisfying $[\![\langle 8,3\rangle,\langle 9,5\rangle]\!]$, we are now left with those which satisfy one of

$$[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!],\quad [\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!].$$

We handle those satisfying $[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!]$ next by considering the different residue classes modulo 29. There are 24 moduli that we can use here of the form $29d$ where $d\,|\,(9\cdot 5\cdot 7\cdot 11)$, and we use all of them to cover those integers in 24 of the 29 residue classes. Since $[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!]$ is equivalent to

$$x\equiv 2798 \pmod{9\cdot 5\cdot 7\cdot 11},$$

we can express these congruences as

$$(\text{C33})\qquad [\![\langle 2798,j\rangle,\langle d_j,29\rangle]\!],\quad \text{where } 0\le j\le 23 \text{ and where } \{d_i : 0\le i\le 23\}=\{d\in\mathbb{Z}^+ : d\,|\,(9\cdot 5\cdot 7\cdot 11)\}.$$

Note that the order of the divisors d_i in (C33) does not matter. We cover the integers in S satisfying $[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!]$ in four more residue classes modulo 29 by applying Lemma 4.4 four times. For those congruent to 24 modulo 29, we apply Lemma 4.4 with $a=8$, $w=2$, $r=1$, $s=2$, $b'_1=24$, $b''_1=3$, $b''_2=24$, $m'_1=29$, $m''_1=5$, $m''_2=29$, and $t=p=59$. By the last line of congruences in (C10), this gives the additional congruences

$$(\text{C34})\qquad \begin{array}{ll}[\![\langle 8+2(3^2+\cdots+3^{i-2}),24\rangle,\langle 3^i,29\rangle]\!] & \text{for } 3\le i\le 59,\\ [\![\langle 8+2(3^2+\cdots+3^{i-2})+3^{i-1},3,24\rangle,\langle 3^i,5,29\rangle]\!] & \text{for } 3\le i\le 59.\end{array}$$

For those congruent to 25 modulo 29, we apply Lemma 4.4 with $a=8$, $w=2$, $r=2$, $s=2$, $b'_1=5$, $b'_2=25$, $b''_1=4$, $b''_2=25$, $m'_1=7$, $m'_2=29$, $m''_1=11$, $m''_2=29$, and $t=p=59$. In this case, with the congruences from (C10), we need only make use of the additional congruences

$$(\text{C35})\qquad \begin{array}{ll}[\![\langle 8+2(3^2+\cdots+3^{i-2}),5,25\rangle,\langle 3^i,7,29\rangle]\!] & \text{for } 3\le i\le 59,\\ [\![\langle 8+2(3^2+\cdots+3^{i-2})+3^{i-1},4,25\rangle,\langle 3^i,11,29\rangle]\!] & \text{for } 3\le i\le 59.\end{array}$$

For the integers in S satisfying $[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!]$ that are 26 modulo 29, we apply Lemma 4.4 with $a=8$, $w=2$, $r=3$, $s=3$, $b'_1=3$, $b'_2=5$, $b'_3=26$, $b''_1=3$, $b''_2=4$, $b''_3=26$, $m'_1=5$, $m'_2=7$, $m'_3=29$, $m''_1=5$, $m''_2=11$, $m''_3=29$, and $t=p=59$. In this case, we additionally get

$$\text{(C36)}\qquad \begin{aligned} &[\![\langle 8+2(3^2+\cdots+3^{i-2}),3,5,26\rangle,\langle 3^i,5,7,29\rangle]\!] && \text{for } 3\le i\le 59,\\ &[\![\langle 8+2(3^2+\cdots+3^{i-2})+3^{i-1},3,4,26\rangle,\langle 3^i,5,11,29\rangle]\!] && \text{for } 3\le i\le 59. \end{aligned}$$

For the integers in S satisfying $[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!]$ that are 27 modulo 29, we apply Lemma 4.4 with $a=8$, $w=2$, $r=3$, $s=4$, $b'_1=5$, $b'_2=4$, $b'_3=27$, $b''_1=3$, $b''_2=5$, $b''_3=4$, $b''_4=27$, $m'_1=7$, $m'_2=11$, $m'_3=29$, $m''_1=5$, $m''_2=7$, $m''_3=11$, $m''_4=29$, and $t=p=59$. In this case, we additionally get

$$\text{(C37)}\qquad \begin{aligned} &[\![\langle 8+2(3^2+\cdots+3^{i-2}),5,4,27\rangle,\langle 3^i,7,11,29\rangle]\!] && \text{for } 3\le i\le 59,\\ &[\![\langle 8+2(3^2+\cdots+3^{i-2})+3^{i-1},3,5,4,27\rangle,\langle 3^i,5,7,11,29\rangle]\!] && \\ & && \text{for } 3\le i\le 59. \end{aligned}$$

For the integers in S satisfying $[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!]$ that are 28 modulo 29, we consider their residue classes modulo 37. There are 48 divisors of $9\cdot 5\cdot 7\cdot 11\cdot 29$. If these divisors are ordered from least to greatest, the 37th divisor is 2233. The congruence

$$[\![\langle 8,3,5,4,28\rangle,\langle 9,5,7,11,29\rangle]\!]$$

is equivalent to

$$x\equiv 6263 \pmod{9\cdot 5\cdot 7\cdot 11\cdot 29}.$$

Therefore we can obtain a covering of these integers in the residue class 28 modulo 29 with the congruences

$$\text{(C38)}\qquad [\![\langle 6263,j\rangle,\langle d'_j,37\rangle]\!],\quad \text{where } 0\le j\le 36 \text{ and where}$$
$$\{d'_i : 0\le i\le 36\}=\{d\in\mathbb{Z}^+ : d\,|\,(9\cdot 5\cdot 7\cdot 11\cdot 29),\ d\le 2233\}.$$

Analogously to the situation in (C33), the order of the d'_i in (C38) can be arbitrary.

Next, we describe a covering of the integers in S satisfying

$$[\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!].$$

We can replace the congruences which we just listed for integers in S satisfying $[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!]$ by congruences which cover 29 residue classes modulo 31 instead of residue classes modulo 29. The congruence $[\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!]$ is equivalent to

$$x\equiv 818 \pmod{9\cdot 5\cdot 7\cdot 11},$$

so this will lead to some changes needed in the congruences. For the first 24 residue classes modulo 31, we use

$$\text{(C39)}\qquad [\![\langle 818,j\rangle,\langle d_j,31\rangle]\!],\quad \text{where } 0\le j\le 23 \text{ and the } d_j \text{ are as in (C33).}$$

We make use of Lemma 4.4 and the last line of congruences from (C10) again to cover the integers that are 24 modulo 31. This leads to the additional congruences

$$\text{(C40)}\quad \begin{aligned} &[\![\langle 8+2(3^2+\cdots+3^{i-2}),24\rangle,\langle 3^i,31\rangle]\!] && \text{for } 3\le i\le 59,\\ &[\![\langle 8+2(3^2+\cdots+3^{i-2})+3^{i-1},3,24\rangle,\langle 3^i,5,31\rangle]\!] && \text{for } 3\le i\le 59. \end{aligned}$$

Recalling our application of Lemma 4.4 to obtain (C35), we want here to use the same information except $b_1'=6$ and $m_2'=m_2''=31$. Reusing congruences in (C10), we cover the integers in S satisfying $[\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!]$ that are in 25 modulo 31 with the additional congruences

$$\text{(C41)}\quad \begin{aligned} &[\![\langle 8+2(3^2+\cdots+3^{i-2}),6,25\rangle,\langle 3^i,7,31\rangle]\!] && \text{for } 3\le i\le 59,\\ &[\![\langle 8+2(3^2+\cdots+3^{i-2})+3^{i-1},4,25\rangle,\langle 3^i,11,31\rangle]\!] && \text{for } 3\le i\le 59. \end{aligned}$$

Similarly, for the integers in S satisfying $[\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!]$ that are 26 modulo 31, we mirror what we did to obtain (C36) and use additionally

$$\text{(C42)}\quad \begin{aligned} &[\![\langle 8+2(3^2+\cdots+3^{i-2}),3,6,26\rangle,\langle 3^i,5,7,31\rangle]\!] && \text{for } 3\le i\le 59,\\ &[\![\langle 8+2(3^2+\cdots+3^{i-2})+3^{i-1},3,4,26\rangle,\langle 3^i,5,11,31\rangle]\!] && \\ & && \text{for } 3\le i\le 59. \end{aligned}$$

We cover the integers in S satisfying $[\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!]$ that are 27 modulo 31 by applying Lemma 4.4 as in (C37) but with $b_1'=6$, $b_2''=6$ and $m_3'=m_4''=31$, by using congruences in (C10), and additionally

$$\text{(C43)}\quad \begin{aligned} &[\![\langle 8+2(3^2+\cdots+3^{i-2}),6,4,27\rangle,\langle 3^i,7,11,31\rangle]\!] && \text{for } 3\le i\le 59,\\ &[\![\langle 8+2(3^2+\cdots+3^{i-2})+3^{i-1},3,6,4,27\rangle,\langle 3^i,5,7,11,31\rangle]\!] && \\ & && \text{for } 3\le i\le 59. \end{aligned}$$

The remaining integers in S satisfying $[\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!]$ are 28, 29 or 30 modulo 31. The integers in each of these residue classes can be covered using a list of congruences similar to (C38) but with 29 replaced by 31, and 37 replaced by 41, 43 and 47. Observe that

$$\begin{aligned} &[\![\langle 8,3,6,4,28\rangle,\langle 9,5,7,11,31\rangle]\!], \quad [\![\langle 8,3,6,4,29\rangle,\langle 9,5,7,11,31\rangle]\!],\\ &[\![\langle 8,3,6,4,30\rangle,\langle 9,5,7,11,31\rangle]\!] \end{aligned}$$

are equivalent to

$$\begin{aligned} &x\equiv 38933 \pmod{9\cdot 5\cdot 7\cdot 11\cdot 31}, \quad x\equiv 7748 \pmod{9\cdot 5\cdot 7\cdot 11\cdot 31},\\ &x\equiv 83978 \pmod{9\cdot 5\cdot 7\cdot 11\cdot 31}, \end{aligned}$$

respectively. We cover the integers in S satisfying these congruences then by using

$$\text{(C44)}\quad \begin{aligned} &[\![\langle 38933,j\rangle,\langle d_j'',41\rangle]\!], && \text{where } 0\le j\le 40,\\ &[\![\langle 7748,j\rangle,\langle d_j'',43\rangle]\!], && \text{where } 0\le j\le 42,\\ &[\![\langle 83978,j\rangle,\langle d_j'',47\rangle]\!], && \text{where } 0\le j\le 46 \text{ and where}\\ & && \{d_0'',d_1'',\dots,d_{47}''\}=\{d\in\mathbb{Z}^+ : d\,|\,(9\cdot 5\cdot 7\cdot 11\cdot 31)\}. \end{aligned}$$

The order of the divisors d''_j does not matter, but we take $d''_0 < d''_1 < \cdots < d''_{47}$ to be explicit.

We have now completely covered all the integers in S which satisfy $[\![\langle 8,3\rangle, \langle 9,5\rangle]\!]$. We still need congruences that cover the $n \in S$ satisfying one of $[\![\langle 2,4\rangle, \langle 9,5\rangle]\!]$, $[\![\langle 5,4\rangle, \langle 9,5\rangle]\!]$ and $[\![\langle 8,4\rangle, \langle 9,5\rangle]\!]$, or equivalently the n that satisfy $[\![\langle 2,4\rangle, \langle 3,5\rangle]\!]$. Of significance is that in every one of the 2210 congruences appearing in (C1)–(C44), no modulus is divisible by 5^2. We set $r = 1169$, which is the number of moduli appearing in (C1)–(C44) which are not divisible by 5; and we set $s = 1041$, the number of moduli divisible by 5. We apply Lemma 4.3 with $p = 5$. Recall that after the statement of Lemma 4.3, we showed that the set S of integers that are sums of two squares satisfies the condition in the second sentence of the lemma. As noted above, every modulus appearing in (C1)–(C44) can be expressed in the form given by the elements of C_1 in Lemma 4.3 or of the form given by the elements of C_2. Also, the congruences in $C = C_1 \cup C_2$ cover the set of integers in S that belong to one of the congruence classes 0, 1, 2 and 3 modulo 5. We take $q = t = 61$. Note that the congruences in C_1 correspond to the congruences given in (i) of Lemma 4.3 and the congruences in C_2 correspond to those in (ii) with $i = 1$. Hence, Lemma 4.3 now implies that we can cover every element of S by combining these congruences with

$$\text{(C45)}\qquad \begin{array}{ll} [\![\langle 5^{i-1} - 1 + b_j 5^{i-1}, b_j\rangle, \langle 5^i, m'_j\rangle]\!] & \text{for } 2 \le i \le 61 \text{ and } 1 \le j \le 1041, \\ [\![\langle j, -1\rangle, \langle 61, 5^{61-j}\rangle]\!] & \text{for } 0 \le j \le 60. \end{array}$$

Thus, from (C1)–(C45), we obtain a set of 64731 congruences, with distinct odd moduli > 1, that cover the set of integers that are sums of two squares, completing the proof of Theorem 4.1. ∎

5. Concluding remarks. The recent works by B. Hough [9] and by B. Hough and P. Nielsen [10] establish that certain conditions on the moduli (that the moduli are all distinct and large or the moduli are > 1 and relatively prime to 6) ensure a system of congruences cannot cover the integers. Motivated by this, we have provided here some initial insights into the notion of using a set of congruences to cover subsets of the integers. As noted at the end of the introduction, there are many questions in this direction that are still unanswered, which we hope will provide a source of future investigations.

Acknowledgements. The authors are grateful to the National Security Agency for funding during research for this paper. In addition, the authors express their gratitude to the referee for some helpful remarks on exposition in this paper.

References

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

[2] M. Filaseta, C. Finch and M. Kozek, *On powers associated with Sierpiński numbers, Riesel numbers and Polignac's conjecture*, J. Number Theory 128 (2008), 1916–1940.

[3] M. Filaseta, K. Ford, S. Konyagin, C. Pomerance and G. Yu, *Sieving by large integers and covering systems of congruences*, J. Amer. Math. Soc. 20 (2007), 495–517.

[4] M. Filaseta, M. Kozek, C. Nicol and J. Selfridge, *Composites that remain composite after changing a digit*, J. Combin. Number Theory 2 (2010), 25–36.

[5] R. L. Graham, *A Fibonacci-like sequence of composite numbers*, Math. Mag. 37 (1964), 322–324.

[6] A. Granville, private communication, December 13, 2016.

[7] R. K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Problem Books in Math., Springer, New York, 2004.

[8] J. Harrington, *Two questions concerning covering systems*, Int. J. Number Theory 11 (2015), 1739–1750.

[9] B. Hough, *Solution of the minimum modulus problem for covering systems*, Ann. of Math. 181 (2015), 361–382.

[10] B. Hough and P. Nielsen, *Covering systems with restricted divisibility*, arXiv:1703.02133 (2017).

[11] L. Jones, *When does appending the same digit repeatedly on the right of a positive integer generate a sequence of composite integers?*, Amer. Math. Monthly 118 (2011), 153–160.

[12] C. E. Krukenberg, *Covering sets of the integers*, doctoral dissertation, Univ. of Illinois at Urbana-Champaign, IL, 1971.

[13] P. P. Nielsen, *A covering system whose smallest modulus is 40*, J. Number Theory 129 (2009), 640–666.

[14] T. Owens, *A covering system with minimum modulus 42*, master's thesis, Brigham Young Univ., Provo, UT, 2014 http://scholarsarchive.byu.edu/etd/4329.

[15] H. Riesel, *Några stora primtal*, Elementa 39 (1956), 258–260.

[16] A. Schinzel, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. 13 (1967), 91–101.

[17] W. Sierpiński, *Sur un problème concernant les nombres* $k \cdot 2^n + 1$, Elem. Math. 15 (1960), 73–74.

[18] K. Zsigmondy, *Zur Theorie der Potenzreste*, Monatsh. Math. Phys. 3 (1892), 265–284.

Michael Filaseta
Department of Mathematics
University of South Carolina
Columbia, SC 29208, U.S.A.
E-mail: filaseta@math.sc.edu

Wilson Harvey
Walker 3-33
University of Louisiana at Monroe
Monroe, LA 71209, U.S.A.
E-mail: harvey@ulm.edu

Abstract (will appear on the journal's web site only)

A number of results are established showing that certain subsets of the integers can be covered by congruences with distinct moduli satisfying various restrictions. For example, the primes, the powers of 2, the Fibonacci numbers, and the sums of two squares can each be covered by congruences with distinct odd moduli > 1.