2017

Covering Subsets of the Integers and a Result on Digits of Fibonacci Numbers

Wilson Andrew Harvey
University of South Carolina

Covering Subsets of the Integers and a Result on Digits of Fibonacci Numbers

by

Wilson Andrew Harvey

Bachelor of Science
Presbyterian College, 2012

Submitted in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy in

Mathematics

College of Arts and Sciences

University of South Carolina

2017

Accepted by:

Michael Filaseta, Major Professor

Ognian Trifonov, Major Professor

Matthew Boylan, Committee Member

Alexander Duncan, Committee Member

Marco Valtorta, Committee Member

Cheryl L. Addy, Vice Provost and Dean of the Graduate School

ABSTRACT

A covering system of the integers is a finite system of congruences where each integer satisfies at least one of the congruences. Two questions in covering systems have been of particular interest in the mathematical literature. First is the minimum modulus problem, whether the minimum modulus of a covering system of the integers with distinct moduli can be arbitrarily large, and the second is the odd covering problem, whether a covering system of the integers with distinct moduli can be constructed with all moduli odd. We consider these and similar questions for subsets of the integers, such as the set of prime numbers, the Fibonacci numbers, and numbers that are the sums of two squares. For example, we show that there does exist an odd covering of the integers that are the sums of two squares, and that the minimum modulus problem can be answered in the affirmative for the Fibonacci numbers.

We also define a block of digits in an integer m written in base b as a successive sequence of equal digits of maximal length and define $B(m, b)$ as the number of blocks of m base b. Integers m with $B(m, b) = 1$ are referred to as base b repdigits and have been studied by a number of authors in relationship to recursive sequences, the most famous of which is the Fibonacci sequence. The Fibonacci numbers F_n are defined by $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. In particular, Florian Luca was able to show that the largest Fibonacci number which is a base 10 repdigit is $F_{10} = 55$. We expand upon this idea for all integer bases $b \geq 2$, and show that $B(F_n, b)$ tends to infinity as n goes to infinity.

Table of Contents

CHAPTER 1

INTRODUCTION

A covering system of the integers is defined as a finite collection of congruences $x \equiv a_j \pmod{m_j}$ such that every integer satisfies at least one of the congruences in the collection. A simple example of a covering system of the integers is the following collection of congruences:

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

$$x \equiv 1 \pmod{4}$$

$$x \equiv 0 \pmod{3}$$

$$x \equiv 5 \pmod{6}$$

$$x \equiv 7 \pmod{12}$$

To see that this is a covering system of the integers, notice that the least common multiple of the moduli $2, 3, 4, 6$, and 12 is 12. Using the Euclidean Algorithm, we may write any integer in the form $12q + r$ for integers q and r with $r \in \{0, 1, \ldots, 11\}$. Thus, by checking that each element in the set $\{0, 1, \ldots, 11\}$ satisfies at least one of the congruences above, we establish that the collection is a covering system of the integers.

In 1950, P. Erdős [6] 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

$$n \equiv 0 \pmod{2} \implies 2^n \equiv 1 \pmod{3}$$

$$n \equiv 0 \pmod{3} \implies 2^n \equiv 1 \pmod{7}$$

$$n \equiv 1 \pmod 4 \implies 2^n \equiv 2 \pmod 5$$

$$n \equiv 3 \pmod 8 \implies 2^n \equiv 8 \pmod{17}$$

$$n \equiv 7 \pmod{12} \implies 2^n \equiv 11 \pmod{13}$$

$$n \equiv 23 \pmod{24} \implies 2^n \equiv 121 \pmod{241}$$

where the congruences on the left form a covering of the integers. 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 N satisfies all of the following

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

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 $p \in \{3, 5, 7, 13, 17, 241\}$. What Erdős had in mind to handle the case that $p \in \{3, 5, 7, 13, 17, 241\}$ 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 $\{3, 5, 7, 13, 17, 241\}$. More precisely, the condition $N \equiv 1 \pmod 3$ implies $N - 2^n \equiv 0$ or $2 \pmod 3$, and the condition $N \equiv 1 \pmod 7$ implies $N - 2^n \equiv 0, 4$ or $6 \pmod 7$. As no prime p in $\{3, 5, 7, 13, 17, 241\}$ satisfies both $p \equiv 0$ or $2 \pmod 3$ and $p \equiv 0, 4$ or $6 \pmod 7$, the result of Erdős follows.

Covering systems have found other applications in number theory; one such application is the proof of the existence of Sierpiński numbers, defined as positive odd integers k satisfying the condition that $k \cdot 2^n + 1$ is composite for all positive integers n. In [25] W. Sierpiński uses the covering system

$$x \equiv 1 \pmod 2$$

$$x \equiv 2 \pmod 4$$

$$x \equiv 4 \pmod 8$$

$$x \equiv 8 \pmod{16}$$

$$x \equiv 16 \pmod{32}$$

$$x \equiv 32 \pmod{64}$$

$$x \equiv 0 \pmod{64}$$

to show that there are infinitely many Sierpiński numbers given by

$$k \equiv 15511380746462593381 \pmod{2 \cdot 3 \cdot 5 \cdot 17 \cdot 257 \cdot 65537 \cdot 641 \cdot 6700417}.$$

Coverings of the integers have found a number of other interesting applications; for example, see [8, 10, 11, 16, 23, 24]. There has in particular been a great deal of interest in two old problems on the subject. The first, recently resolved by Bob Hough [15], is whether the minimum modulus of a covering system of the integers consisting of congruences with distinct moduli can be arbitrarily large. Bob Hough [15] has shown that this minimum modulus is $\leq 10^{16}$. In the other direction, Pace Nielsen [21] has shown that the minimum modulus can be as large as 40, and later his ideas were extended by Tyler Owens [22] 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 of distinct odd moduli > 1. This problem remains open. The non-existence of coverings with distinct moduli all $> 10^{16}$, however, leads to some doubt that other coverings of the integers, like one where all moduli are distinct odd numbers > 1, which have eluded construction over the years, exist. 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.

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

- There is a covering of the set of primes using only distinct odd moduli > 1.

- There is a covering of the numbers that are sums of two squares using only distinct odd moduli > 1.
- There is an exact covering of the powers of 2 consisting of distinct moduli > 1 only divisible by primes larger than any prescribed amount 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 distinct moduli > 1 only divisible by primes larger than any prescribed amount 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 using distinct moduli > 1.

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 amount. 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 distinct large moduli, but we show that this is not in general true in the next section. More precisely, we show that there are sets $\mathcal{N}$ for which the n_j increase as fast as one wants, which cannot be covered by congruences with distinct moduli all $> 10^{16}$. An analogous result is obtained for odd coverings of subsets of the integers provided no odd covering with distinct moduli > 1 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 the sum of two squares that uses only distinct moduli that are greater than an arbitrary fixed bound M? Does there exist a covering of the set of squarefree numbers using distinct odd moduli > 1? Does there exist a covering of the set of squarefree numbers using distinct 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 a covering of S_f using distinct odd moduli > 1? Although it will be clear that some of our approach for Fibonacci numbers generalizes to other recursive sequences, we have not obtained a result for arbitrary recursive sequences in the integers.

Another topic we investigate in this dissertation is “blocks" of digits in an integer sequence. For a positive integer m, let $d_r d_{r-1} \dots d_1 d_0$ be the base b representation of m. We define a block (of digits) of m base b as a successive sequence of equal digits $d_j d_{j-1} \dots d_k$ of maximal length. For example, the base 10 number 888005255 consists of 5 blocks: 888, 00, 5, 2, and 55. We denote the number of blocks of m base b as $B(m, b)$. In the previous example, we have $B(888005255, 10) = 5$.

One would expect that, for an integer a that is not a power of the base b, $B(a^n, b)$ would grow larger and larger as n tends to infinity. In [3], R. Blecksmith, M. Filaseta, and C. Nicol are able to show that this intuition is true. They show that

$$\lim_{n\to\infty} B(a^n, b) = \infty$$

if and only if $\log a / \log b$ is irrational for integers a and $b \geq 2$.

We will be working with the Fibonacci numbers, and throughout the dissertation will denote the nth Fibonacci number as F_n so that $F_0 = 0$, $F_1 = 1$, and $F_n = F_{n-1} + F_{n-2}$ for $n \geq 2$. In Chapter 3, we will show that

$$\lim_{n\to\infty} B(F_n, b) = \infty,$$

mirroring the result found in [3].

We include here some numerical data to point toward the two results given above. In Table 1.1, we exhibit the largest $n \leq 50000$ such that the 2^n has the prescribed number of blocks base 10. In Table 1.2, we similarly exhibit the largest $n \leq 50000$ such that the nth Fibonacci number F_n has the prescribed number of blocks base 10. It may also be

Table 1.1: Blocks of digits in 2^n for $n \leq 50000$

$B(2^n, 10)$	Largest $n \leq 50000$	2^n
1	3	8
2	6	64
3	9	512
4	16	65536
5	25	33554432
6	24	16777216
7	26	67108864
8	27	134217728
9	41	2199023255552
10	38	274877906944

Table 1.2: Blocks of digits in F_n for $n \leq 50000$

$B(F_n, 10)$	Largest $n \leq 50000$	F_n
1	10	55
2	14	377
3	22	17711
4	20	6765
5	29	514229
6	35	9227465
7	43	433494437
8	49	7778742049
9	66	27777890035288
10	56	225851433717

of interest to note that, again for $n \leq 50000$, the largest $B(2^n, 10) = 13631$ occurs for $n = 49997$ and the largest $B(F_n, 10) = 9452$ occurs for $n = 49884$.

Another area of interest has been to consider representations of Fibonacci and Lucas numbers in different bases b other than $b = 10$. In [5], Y. Bugeaud, M. Ciphu, and M. Mignotte are able to produce a finite list of Fibonacci and Lucas numbers with at most four non-zero digits in their base 2 representation, the largest of which is $F_{18} = 2584$. The authors also use techniques established by C. L. Stewart in [26] to establish a lower bound on $B(m, a) + B(m, b)$ for two multiplicatively independent integer bases a and b (and an integer $m > 25$). The authors summarize their results by writing that "in two unrelated number systems, two miracles cannot happen simultaneously for large integers."

Integers m satisfying $B(m, b) = 1$ are of particular interest; such an integer m is referred to as a base b repdigit. The number $F_{10} = 55$ is an example of a Fibonacci number which is a base 10 repdigit. In [19], F. Luca proves that the largest n for which F_n is a base 10 repdigit is $n = 10$. There have been a number of other papers focusing on repdigits and their relationships to recursive sequences, such as [4], [7], and [20]. We can view our result on blocks of digits in the Fibonacci numbers as extending and generalizing the results found in [3] and [19].

Chapter 2

Covering Subsets of the Integers by Congruences

2.1 Preliminary Results

Definition 1. A *covering* of a set $S \subset \mathbb{Z}$ is a finite set of congruences $\{x \equiv a_j \pmod{m_j} : 1 \le j \le r\}$ (or equivalently a set of pairs (a_j, m_j) representing these congruences) such that each $s \in S$ satisfies at least one of the congruences $x \equiv a_j \pmod{m_j}$ with $1 \le j \le r$. An *odd covering* of a set $S \subset \mathbb{Z}$ is a covering $C = \{x \equiv a_j \pmod{m_j} : 1 \le j \le r\}$ of S where each m_j is odd. An *exact covering* of a set $S \subset \mathbb{Z}$ is a covering $C = \{x \equiv a_j \pmod{m_j} : 1 \le j \le r\}$ of S for which each $s \in S$ satisfies exactly one of the congruences $x \equiv a_j \pmod{m_j}$ with $1 \le j \le r$. If $S = \mathbb{Z}$, these are referred to as a *covering of the integers*, as an *odd covering of the integers*, and as an *exact covering of the integers*, respectively.

The idea of covering subsets of the integers is not really new. For example, the motivating paper by Erdős [6] 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 distinct odd 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 [6]. Analogous to (1.1) providing a covering of the powers of 2, A. Granville [12] has pointed out that

$$\begin{gathered} x \equiv 1 \pmod{2}, \quad x \equiv 0 \pmod{3}, \quad x \equiv 1 \pmod{7}, \\ x \equiv 0 \pmod{17}, \quad x \equiv 2 \pmod{19}, \quad x \equiv 15 \pmod{23} \end{gathered} \tag{2.1}$$

provides a covering of the Fibonacci numbers. As in (1.1), the moduli in (2.1) are distinct primes. It is also of interest to note that the sum of the reciprocals of the moduli appearing in (1.1) is $0.816\ldots < 1$ and the sum of the reciprocals of the moduli appearing in (2.1) 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. [9]) using a complex variable shows that an exact covering of the integers with moduli > 1 necessarily has the largest modulus appearing as the modulus for two of the congruences in the covering. This is certainly not necessarily the case when we turn to covering subsets of the integers.

Next, 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 [14] and [15].

Proposition 1. *If there is no odd covering of the integers with distinct moduli > 1, then there is no odd covering of the odd integers with distinct moduli > 1.*

Proof. Suppose there exists a covering C of the odd integers with distinct odd moduli > 1. Thus, $C = \{x \equiv a_i \pmod{m_i} : 1 \leq i \leq r\}$, where each m_i is odd and $1 < m_1 < m_2 < \ldots < m_r$. 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 n is either 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 $k \in \{1, 2, \ldots, r\}$ and some $\varepsilon \in \{0, 1\}$. But $m_k | M$, so $n \equiv n + \varepsilon M \equiv a_k \pmod{m_k}$. Thus, n necessarily satisfies a congruence from C, completing the proof. □

Lemma 1. *Let $t \in \mathbb{Z}$. Given a covering $C = \{x \equiv a_k \pmod{m_k} : 1 \leq k \leq r\}$ of $S \subseteq \mathbb{Z}$, the set $C_t = \{x \equiv a_k + t \pmod{m_k} : 1 \leq k \leq r\}$ is a covering of the set $S_t = \{s + t : s \in S\}$.*

Proof. Fix an arbitrary integer $x_0 \in S_t$. Since $x_0 \in S_t$, we may write $x_0 = s_0 + t$ for some $s_0 \in S$. Since C is a covering of S, there exists $k_0 \in \{1, \ldots, r\}$ with $s_0 \equiv a_{k_0} \pmod{m_{k_0}}$.

Further, we have $x_0 = s_0 + t \equiv a_{k_0} + t \pmod{m_{k_0}}$, so x_0 is covered by a congruence from C_t. Thus, C_t is a covering of S_t. □

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

Corollary 1. *If there is no odd covering of the integers with distinct moduli > 1, then there is no odd covering of the even integers with distinct moduli > 1.*

Along the lines of basic results like Lemma 1, 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. 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 $f(x) \to \infty$ as $x \to \infty$, there exists a set S, depending on $f(x)$, 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 1. *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 any finite set C of congruences from $\mathcal{N}$, with each modulus appearing in C at most r times, is not a covering of $\mathbb{Z}$. Then there exist arbitrarily thin sets $S \subset \mathbb{Z}^+$ such that no covering C of S exists using congruences from $\mathcal{N}$ where each modulus appears in C at most r times.*

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

$$C = \{x \equiv a_k \pmod{m_k} : 1 \le k \le s\} \subseteq \mathcal{N}, \quad \text{with } m_1 m_2 \cdots m_s \le M.$$

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 countable.

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, each C_j is not a covering of the integers. For each $k \geq 1$, choose an integer n_k not covered by C_k. Then the set $S = \{n_1, n_2, \ldots\}$ is not covered by a subset $C \subseteq \mathcal{N}$ where each modulus appears in C at most r times.

Observe that if a number n is not covered by some C_k, then neither is 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. $\square$

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 we take $\mathcal{N}$ equal to 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. *There are arbitrarily thin sets $S \subset \mathbb{Z}$ for which no covering of S exists using only distinct moduli greater than 10^{16}.*

Corollary 3. *If there is no odd covering of the integers using distinct moduli > 1, then there are arbitrarily thin sets $S \subset \mathbb{Z}$ for which no odd covering of S, using distinct moduli > 1, exists.*

There is an alternative approach to establishing Corollary 2 and Corollary 3. They both follow as a consequence of the following.

Theorem 2. *There exist arbitrarily thin sets $S \subset \mathbb{Z}^+$ satisfying the property that if C is a set of congruences that forms a covering of 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 $S \subset \mathbb{Z}^+$ 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 we deduce that $u^{2^{u-1}} \leq x$ 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 u so that u is a prime 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 modulus 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 modulus 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 1, 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 makes use of the result by B. Hough [15] 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 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. *Let $S \subseteq \mathbb{Z}^+$ satisfy*

$$\limsup_{X\to\infty} \frac{|\{s \in S : s \leq X\}|}{X} = 1. \tag{2.2}$$

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

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

$$C = \{x \equiv a_j \pmod{m_j} : 1 \le j \le r\}, \quad \text{where } 10^{16} < m_1 < m_2 < \ldots < m_r,$$

is a covering of S. From [15], we know that C is not a covering system 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 the moduli $m_1, \ldots, m_r$ (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

$$\liminf_{X \to \infty} \frac{\left|\left\{x \in \mathbb{Z}^+ : x \le X, x \not\equiv a_j \pmod{m_j} \text{ for all } j \in \{1, 2, \ldots, r\}\right\}\right|}{X} \ge \frac{1}{L}.$$

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 (2.2) is at most $1 - (1/L) < 1$. The proposition follows. □

In connection to 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 amount. 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 [14].

Proposition 3. *There exists a covering of the prime numbers which consists of moduli that are distinct odd numbers* > 1.

Proof. In [14], J. Harrington established the existence of a covering C of the integers where the moduli are all odd and > 1, the modulus 3 is used exactly twice, and no other modulus is repeated. By Lemma 1 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 C is a covering of the integers, 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 the congruence $x \equiv 0 \pmod 3$ 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 $x \equiv 3 \pmod m$ is satisfied by the prime 3 and the other congruences in C' cover the remaining primes. □

2.2 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 odd exact covering of the Fibonacci numbers.

Theorem 3. *Let* $P \geq 2$, $M \geq 2$, *and* $\varepsilon > 0$. *There exists a finite set of congruences*

$$x \equiv a_j \pmod{m_j}, \quad \text{for } 1 \leq j \leq r, \tag{2.3}$$

that satisfies each of the following:

(i) For each $n \geq 0$, *the number* 2^n *satisfies exactly one of the congruences in* (2.3). *(Thus, the congruences form an exact covering of the powers of* 2.*)*

(ii) The moduli m_j are all distinct and each prime divisor of each m_j is $> P$. (In particular, the congruences form an odd covering of the powers of 2*.)*

(iii) Each $m_j > M$. (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. Given that each $m_j > 1$ (a consequence of (iii)), the fact that the minimum modulus can be arbitrarily large is a consequence of (ii).

Proof. Define $A(n) = 2^{2^n} - 1$ and $B(n) = 2^{2^n} + 1$. As a consequence of K. Zsigmondy's Theorem [27], for each $n \geq 1$, there is a prime p dividing $A(n)$ that does not divide $A(k)$ for each integer $k \in [0, n)$. Alternatively, we can use that

$$A(n) = B(n-1)A(n-1) = B(n-1)B(n-2)\cdots B(0) \text{ and } B(n-1) - A(n-1) = 2 \tag{2.4}$$

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 integer $k \in [0, n)$. For $n \geq 1$, we fix d_n to be such a divisor of $A(n)$, that is some divisor > 1 that is relatively prime to each $A(k)$ with $0 \leq k < n$. 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 sequence of powers of 2 repeat modulo d_n with period 2^n. To clarify, first, if $r = 2^n$, then

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

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, we observe that the minimum positive integer r for which $2^r \equiv 1 \pmod{d_n}$ holds, 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 $\leq 2^n$. 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 $0 \leq k < n$. Thus, the period of the sequence of 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 $0 \leq i < 2^n$ are distinct modulo D.

The coprimality of d_n and d_k for $0 \leq k < n$ 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 $k \in \mathbb{Z}^+$ with the property that every d_n with $n \geq k$ has each of its prime divisors $> P$ and with the property that $d_n > M$ for each $n \geq k$. In particular, from (2.4), the $n - k + 1$ numbers

$$d_k, d_{k+1}, \ldots, d_{n-1}, d_n \tag{2.5}$$

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 (2.5). 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 1 congruence formed from the 1 element of S_k, and this congruence covers 2^m for m in this 1 residue class modulo 2^k. This 1 residue class modulo 2^k corresponds to 2 residue classes modulo 2^{k+1}. We then take $n = k + 1$ and cover 2 more residue classes modulo 2^{k+1}. Thus, at this point 4 different residue classes are covered modulo 2^{k+1}. A straight forward 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 $j \in \{0, 1, \ldots, J\}$, 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), (ii) and (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. Taking $d_n = B(n-1) = 2^{2^{n-1}} + 1$, the sum of the reciprocals of all moduli in our covering of the powers of 2 is then

$$\le \sum_{j=0}^{2^k-1} \frac{2^j}{2^{2^{k+j-1}} + 1} \le \sum_{j=k}^{\infty} \frac{2^j}{2^{2^{j-1}} + 1}. \tag{2.6}$$

The series

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

converges, for example, by using a comparison with 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 then that the last series in (2.6) tends to 0 as k tends to infinity. Thus, by choosing k sufficiently large in our construction, 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 $n \geq 0$. Our next lemma easily follows from these identities, and we omit the proof.

Lemma 2. *Let u and v denote integers with $u \geq v \geq 0$. 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. *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 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 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 $L_v = L_{2^j}$. This implies the lemma. $\square$

Lemma 4. *If j and k are distinct non-negative integers, then* $\gcd(L_{2^j}, L_{2^k}) = 1$.

Proof. Since $L_1 = 1$, it follows from Lemma 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 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 lemma follows. $\square$

The following are consequences of the previous two lemmas.

Corollary 4. *Let* $P = L_{2^{a_1}} L_{2^{a_2}} \cdots L_{2^{a_k}}$ *for some integer* $k > 0$ *and some* a_j *satisfying* $1 \le a_1 < a_2 < \cdots < a_k$*. The Fibonacci numbers modulo* P *are periodic with period dividing* 2^{a_k+2}.

Corollary 5. *The minimum prime divisor of* L_{2^j} *tends to infinity with* j.

Our next lemma is an easy consequence of Lemma 2 (b) and induction, and we leave out further details of its proof.

Lemma 5. *For every positive integer* j*, we have* $L_{2^j} \ge 10^{2^{j-3}} + 1$.

Theorem 4. *Let* $P \ge 2$*,* $M \ge 2$*, and* $\varepsilon > 0$*. There exists a finite set of congruences*

$$x \equiv a_j \pmod{m_j}, \quad \textit{for } 1 \le j \le r, \tag{2.7}$$

that satisfies each of the following:

(i) For each $n \ge 0$*, the Fibonacci number* F_n *satisfies at least one of the congruences in* (2.7)*. (Thus, the congruences form a covering of the Fibonacci numbers.)*

(ii) The moduli m_j *are all distinct and each prime divisor of each* m_j *is* $> P$*. (In particular, the congruences form an odd covering of the Fibonacci numbers.)*

(iii) Each $m_j > M$*. (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. From Corollary 5, there is a $k \in \mathbb{Z}^+$ with the property that for every integer $j \ge k$, L_{2^j} has each of its prime divisors $> P$. Momentarily, we fix such a $k \ge 3$, and consider $n \ge k$. In the end, we will want to choose k large. Observe that Lemma 2 (a) with $u = v$ implies

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

Combining the above with Lemma 4, we see that the Lucas numbers

$$L_{2^k}, L_{2^{k+1}}, \ldots, L_{2^{n-1}}, L_{2^n} \tag{2.8}$$

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 (2.8). 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 4, 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 1 congruence which covers the set of F_m for m from at least 1 residue class modulo 2^{k+2}. This 1 residue class modulo 2^{k+2} corresponds to 2 residue classes, say r_1 and r_2, modulo 2^{k+3}. We then select $a \in [0, 2^{k+3})$ in creating the 2 congruences $x \equiv F_a \pmod{D}$ for C_{k+1} so that each of these a's do not belong to either of the residue classes r_1 and r_2 modulo 2^{k+3}. Thus, $C_k \cup C_{k+1}$ covers the integers belonging to a total of 4 residue classes modulo 2^{k+3}. Similarly, we create 4 congruences for C_{k+2} that cover F_m for m from at least 4 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 $C_k \cup C_{k+1} \cup \cdots \cup C_{k+J}$ 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 $C = C_k \cup C_{k+1} \cup \cdots \cup C_{k+J}$ that satisfy (i) and (ii).

By taking 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 obtain from Lemma 5 that the sum of the reciprocals of the moduli in C is bounded above by

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

Thus, taking k sufficiently large, we can also assure that (iv) holds, establishing the theorem. □

Observe that Theorem 3 establishes the existence of an exact covering of the powers of 2 whereas Theorem 4 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 4 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. We simply document here, in the first column of Table 2.1 below, such a covering and leave the details of the verification that the covering given is an exact odd covering of the Fibonacci numbers to the reader. The second column clarifies the Fibonacci numbers covered by each congruence in the first column.

2.3 Sums of Two Squares

In this section, we prove

Theorem 5. *There is a covering of the set of integers which are sums of two squares that uses only distinct odd moduli* > 1.

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

Table 2.1: An exact odd covering of the Fibonacci numbers

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

Lemma 6. *A positive integer n is the sum of two squares if and only if each prime $p \equiv 3 \pmod{4}$ satisfies $p^e \| n$ for some even nonnegative integer e.*

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

$$x \equiv a_1 \pmod{m_1}, \quad x \equiv a_2 \pmod{m_2}, \ldots, \quad x \equiv a_r \pmod{m_t}.$$

Again, we are interested only in the case where the m_j are positive pairwise relatively prime integers. Note that, 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 [17].

Lemma 7. *Let p be a prime. Let $S \subseteq \mathbb{Z}^+$ have the property that given any integers m 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*

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

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 not divisible by p^2 (and, hence, exactly divisible by p). Suppose that C is a covering for the set

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

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* $1 \le j \le r$,

(ii) $[\![\langle p^{i-1} - 1 + b_j p^{i-1}, b_j \rangle, \langle p^i, m'_j \rangle]\!]$, *for* $1 \le i \le t$ *and* $1 \le j \le s$,

(iii) $[\![\langle j, -1 \rangle, \langle q, p^{t-j} \rangle]\!]$, *for* $0 \le j \le q-1$,

where q is an arbitrary fixed prime such that $q \nmid (pm'_1 \cdots m'_s)$ and where $t \in \mathbb{Z}$ satisfies $t \ge q$.

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 a sum 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 a sum of two squares can be used for S in Lemma 7.

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 a sum of two squares can be used for S in Lemma 7 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 $u \in \{0, 1, \ldots, p-1\}$. If $s_1 = 0$, then we define $v = 1$. If $s_1 \neq 0$, we define v as a positive integer with the property that if $q^e | s_1$ 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 $q^e \| d$, then $q^e \| s_1$. From Lemma 6, we see that since s_1 and m^{2v} are each the 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

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

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 $4 | m'$. 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, $4 | m'$, $s' \equiv 1 \pmod{4}$ and there is an ℓ such that

$s' + k_0m' + p^2m'\ell$ 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 then that s_2 is 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 have 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 so 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 7, we note that if $m_1, \ldots, m_r$ are distinct and $m'_1, \ldots, m'_s$ are distinct, then the various moduli appearing in (i), (ii) and (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. To prove Lemma 7, for each $u \in \{0, 1, \ldots, p-1\}$, we define

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

We begin by showing that for each $u \neq p - 1$, the set $C_1 \cup C_2^{(u)}$ covers the set S.

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

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

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

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

Since C covers the integers in S that are u modulo p, either $n_0 \equiv a_j \pmod{m_j}$ for some $j \in \{1, 2, \dots, r\}$ or $n_0 \equiv b_j \pmod{pm'_j}$ for some $j \in \{1, 2, \dots, s\}$. 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 $j \in \{1, 2, \dots, s\}$. 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, $C_1 \cup C_2^{(u)}$ covers the integers in S.

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

$$n \equiv -1 \pmod{p^\ell} \quad \text{and} \quad n \not\equiv -1 \pmod{p^{\ell+1}}. \tag{2.9}$$

First, we consider $n \neq -1$ and the case in (2.9) 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 $C_1 \cup C_2^{(u)}$ is a covering of S, 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 have that n satisfies a congruence in (i) or (ii) provided $n \neq -1$ and the value of ℓ in (2.9) satisfies $\ell \leq t-1$. Now, suppose $n = -1$ or ℓ in (2.9) 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 $j = k$. This completes the proof. $\square$

Lemma 8. *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* $[\![\langle a, b_1, \ldots, b_\ell\rangle, \langle 3^w, m_1, \ldots, m_\ell\rangle]\!]$*. Then* n *satisfies at least one of the following congruences:*

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

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

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

where empty sums are interpreted as equal to 0*.*

Proof. Let n be an integer satisfying the congruence $[\![\langle a, b_1, \ldots, b_\ell\rangle, \langle 3^w, m_1, \ldots, m_\ell\rangle]\!]$. 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 n satisfies both $n \equiv k \pmod{p}$ and $n \equiv a + 2(3^w + 3^{w+1} + \cdots + 3^{t-k-1}) \pmod{3^{t-k}}$, where 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), completing the proof. □

Proof of Theorem 5. Let $S = \{0, 1, 2, 4, 5, 8, 9, \ldots\}$ be the set of integers that are a sum of two squares. We begin by using a single congruence to cover every element n of S that is divisible by 3. Lemma 6 implies that each such n satisfies $n \equiv 0 \pmod{9}$. Hence, we cover these n by using the congruence

$$[\![\langle 0\rangle, \langle 9\rangle]\!], \tag{C1}$$

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

$$[\![\langle 1\rangle, \langle 3\rangle]\!] \tag{C2}$$

to cover those n in S that are are 1 modulo 3. Thus, what remains is for us 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 in turn break up into 5 groups depending on what they are congruent to 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

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

We seperate the $n \in S$ for which $n \equiv 2 \pmod 9$ and $n \equiv 3 \pmod 5$, into 7 groups depending on what residue class they belong to modulo 7. We take advantage of Lemma 6 again to see that the $n \in S$ divisible by 7 satisfy $n \equiv 0 \pmod{49}$. We therefore can cover the n in all 7 of the groups by using the congruences

$$\begin{gathered}[\![\langle 0\rangle, \langle 49\rangle]\!], \quad [\![\langle 1\rangle, \langle 7\rangle]\!], \quad [\![\langle 2,2\rangle, \langle 3,7\rangle]\!], \quad [\![\langle 3,3\rangle, \langle 5,7\rangle]\!], \\ [\![\langle 2,3,4\rangle, \langle 3,5,7\rangle]\!], \quad [\![\langle 2,5\rangle, \langle 9,7\rangle]\!] \quad \text{and} \quad [\![\langle 2,3,6\rangle, \langle 9,5,7\rangle]\!].\end{gathered} \tag{C4}$$

As of now, we are left with covering the $n \in S$ which satisfy one of the congruences $[\![\langle 2,4\rangle, \langle 9,5\rangle]\!]$, $[\![\langle 5\rangle, \langle 9\rangle]\!]$ and $[\![\langle 8\rangle, \langle 9\rangle]\!]$. 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 5 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 the congruence $[\![\langle 5,2\rangle, \langle 9,5\rangle]\!]$ next. For this, we use Lemma 8 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

$$\llbracket \langle 5 + 2(3^2 + 3^3 + \cdots + 3^{i-2}) \rangle, \langle 3^i \rangle \rrbracket, \text{ for } 3 \le i \le 53,$$

$$\llbracket \langle 5 + 2(3^2 + 3^3 + \cdots + 3^{i-2}) + 3^{i-1}, 2 \rangle, \langle 3^i, 5 \rangle \rrbracket, \text{ for } 3 \le i \le 53, \tag{C5}$$

$$\text{and} \quad \llbracket \langle 5 + 2(3^2 + 3^3 + \cdots + 3^{52-k}), k \rangle, \langle 3^{53-k}, 53 \rangle \rrbracket, \text{ for } 0 \le k \le 52.$$

Next, we cover the integers in S satifying $\llbracket \langle 5, 3 \rangle, \langle 9, 5 \rangle \rrbracket$ by grouping them into 7 different residue classes modulo 7. All integers in S divisible by 7 have been covered by the first congruence in (C4). For the integers satisfying $\llbracket \langle 5, 3 \rangle, \langle 9, 5 \rangle \rrbracket$ and that are either 1, 2, 3 or 4 modulo 7, we can use the congruences $\llbracket \langle 1 \rangle, \langle 7 \rangle \rrbracket$, $\llbracket \langle 2, 2 \rangle, \langle 3, 7 \rangle \rrbracket$, $\llbracket \langle 3, 3 \rangle, \langle 5, 7 \rangle \rrbracket$ and $\llbracket \langle 2, 3, 4 \rangle, \langle 3, 5, 7 \rangle \rrbracket$ from (C4). For the integers in $\llbracket \langle 5, 3 \rangle, \langle 9, 5 \rangle \rrbracket$ that are 5 modulo 7, we apply Lemma 8 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 8 here, we are reusing the congruences

$$\llbracket \langle 5 + 2(3^2 + 3^3 + \cdots + 3^{i-2}) \rangle, \langle 3^i \rangle \rrbracket, \text{ for } 3 \le i \le 53,$$

$$\text{and} \quad \llbracket \langle 5 + 2(3^2 + 3^3 + \cdots + 3^{52-k}), k \rangle, \langle 3^{53-k}, 53 \rangle \rrbracket, \text{ for } 0 \le k \le 52,$$

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

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

For the remaining integers in S satisfying $\llbracket \langle 5, 3 \rangle, \langle 9, 5 \rangle \rrbracket$ which are 6 modulo 7, we apply Lemma 8 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 8, after reusing congruences from (C5) as above, we use the additional congruences

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

Thus far, we have covered the integers in S satisfying the congruence $\llbracket \langle 5 \rangle, \langle 9 \rangle \rrbracket$ except for those that are 4 modulo 5. Combining what we now know, we are left with covering the

$n \in S$ which satisfy one of the congruences $[\![\langle 2,4\rangle,\langle 9,5\rangle]\!]$, $[\![\langle 5,4\rangle,\langle 9,5\rangle]\!]$ and $[\![\langle 8\rangle,\langle 9\rangle]\!]$. We deal with the integers in S satisfying $[\![\langle 8\rangle,\langle 9\rangle]\!]$ next.

We break up the integers in S satisfying $[\![\langle 8\rangle,\langle 9\rangle]\!]$ into groups depending on the residue class they belong to modulo 5. We use the congruences $[\![\langle 0\rangle,\langle 5\rangle]\!]$ 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 one of the congruences $[\![\langle 8,2\rangle,\langle 9,5\rangle]\!]$, $[\![\langle 8,3\rangle,\langle 9,5\rangle]\!]$ and $[\![\langle 8,4\rangle,\langle 9,5\rangle]\!]$.

We group those satisfying $[\![\langle 8,2\rangle,\langle 9,5\rangle]\!]$ into the 7 residue classes modulo 7. The first 3 congruences in (C4) we reuse so that we are left with elements in S satisfying $[\![\langle 8,2\rangle,\langle 9,5\rangle]\!]$ that also satisfy one of the congruences

$$[\![\langle 8,2,3\rangle,\langle 9,5,7\rangle]\!],\quad [\![\langle 8,2,4\rangle,\langle 9,5,7\rangle]\!],\quad [\![\langle 8,2,5\rangle,\langle 9,5,7\rangle]\!]\quad\text{and}\quad [\![\langle 8,2,6\rangle,\langle 9,5,7\rangle]\!].$$

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 11 residue classes modulo 11. Since $11 \equiv 3 \pmod 4$, Lemma 6 implies that the congruence

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

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

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

To cover the residue class of integers that are 10 modulo 11 that are in S and satisfy the congruence $[\![\langle 8,2,6\rangle,\langle 9,5,7\rangle]\!]$, we apply Lemma 8, 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 the additional congruences

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

$$[\![\langle 8+2(3^2+3^3+\cdots+3^{i-2})+3^{i-1},6,10\rangle,\langle 3^i,7,11\rangle]\!],\ \text{for } 3\le i\le 59, \tag{C10}$$

$$\text{and}\quad [\![\langle 8+2(3^2+3^3+\cdots+3^{58-k}),k\rangle,\langle 3^{59-k},59\rangle]\!],\ \text{for } 0\le k\le 58.$$

Thus, the integers in S satisfying $[\![\langle 8,2,6\rangle,\langle 9,5,7\rangle]\!]$ will be covered by the congruences given 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 congruences 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

$$[\![\langle 2,5,7\rangle,\langle 5,7,11\rangle]\!],\quad [\![\langle 2,2,5,8\rangle,\langle 3,5,7,11\rangle]\!]\quad \text{and}\quad [\![\langle 8,2,5,9\rangle,\langle 9,5,7,11\rangle]\!]. \tag{C11}$$

To cover those that are 10 modulo 11, we apply Lemma 8, 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

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

Our congruences thus far cover then 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 8 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 integers in S which satisfy one of the congruences $[\![\langle 8,2,4,7\rangle,\langle 9,5,7,11\rangle]\!]$, $[\![\langle 8,2,4,8\rangle,\langle 9,5,7,11\rangle]\!]$ 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 7 residue classes 4, 11,

$18, \ldots, 46$ they belong to modulo 49. We cover these in turn by using the congruences

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

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

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

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

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

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

We turn to congruences to cover 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 the congruences

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

For those in the residue class 12 modulo 13, we apply Lemma 8, 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

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

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

Next, we will cover the the integers in S satisfying $[\![\langle 8,3\rangle,\langle 9,5\rangle]\!]$. Any of the previous congruences used can be used here as long as they intersect the class 8 modulo 9 and 3 modulo 5. In particular, the first 5 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 $[\![\langle 8,3,6\rangle,\langle 9,5,7\rangle]\!]$. Combining this information with the congruences (C8), (C9) and (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

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

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

$$[\![\langle 8,3,5,10\rangle,\langle 9,5,7,11\rangle]\!],\quad [\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!],$$

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

Of these, the integers in S satisfying $[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!]$ and $[\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!]$ 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 up these integers 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 the congruences

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

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 the congruences

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

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 the congruences

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

For the integers in S satisfying $[\![\langle 8,3,5,7\rangle,\langle 9,5,7,11\rangle]\!]$ and that lie in the residue class 12 modulo 13, we apply Lemma 8, 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 the additional congruences

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

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 the congruences

$$[\![\langle 8, 3, 5, 6\rangle, \langle 9, 5, 7, 17\rangle]\!], \quad [\![\langle 5, 8, 7\rangle, \langle 7, 11, 17\rangle]\!],$$
$$[\![\langle 2, 5, 8, 8\rangle, \langle 3, 7, 11, 17\rangle]\!], \quad [\![\langle 3, 5, 8, 9\rangle, \langle 5, 7, 11, 17\rangle]\!], \quad \text{(C22)}$$
$$[\![\langle 8, 5, 8, 10\rangle, \langle 9, 7, 11, 17\rangle]\!] \quad \text{and} \quad [\![\langle 2, 3, 5, 8, 11\rangle, \langle 3, 5, 7, 11, 17\rangle]\!].$$

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 the congruences

$$[\![\langle 2, 9\rangle, \langle 3, 121\rangle]\!], \quad [\![\langle 3, 20\rangle, \langle 5, 121\rangle]\!], \quad [\![\langle 8, 31\rangle, \langle 9, 121\rangle]\!], \quad [\![\langle 2, 3, 42\rangle, \langle 3, 5, 121\rangle]\!],$$
$$[\![\langle 8, 3, 53\rangle, \langle 9, 5, 121\rangle]\!], \quad [\![\langle 5, 64\rangle, \langle 7, 121\rangle]\!], \quad [\![\langle 2, 5, 75\rangle, \langle 3, 7, 121\rangle]\!],$$
$$[\![\langle 3, 5, 86\rangle, \langle 5, 7, 121\rangle]\!], \quad [\![\langle 8, 5, 97\rangle, \langle 9, 7, 121\rangle]\!],$$
$$[\![\langle 2, 3, 5, 108\rangle, \langle 3, 5, 7, 121\rangle]\!] \quad \text{and} \quad [\![\langle 8, 3, 5, 119\rangle, \langle 9, 5, 7, 121\rangle]\!]. \quad \text{(C23)}$$

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 the congruences

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

Next, we turn to covering the 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 $0,1,\ldots,11$ modulo 17. To cover those integers in the residue classes 12, 13 and 14 modulo 17, we use the congruences

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

For those integers in S satisfying $[\![\langle 8,3,6,6\rangle,\langle 9,5,7,11\rangle]\!]$ and in the residue class 15 modulo 17, we cover separately the 3 residue classes 8, 17 and 26 modulo 27 that they belong to, covering the first two directly and using Lemma 8 to cover the third. For Lemma 8, 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

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

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 their 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 the congruences

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

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 there replaced by 19 here. In particular, we use (C18) to cover those integers in S satisfying $[\![\langle 8,3,6,5\rangle,\langle 9,5,7,11\rangle]\!]$ that lie in one of the residue classes $0,1,\dots,10$ and 11 modulo 19. For those congruent to 12, 13 or 14 modulo 19, we use the congruences

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

For those congruent to 15 modulo 19, we consider their 3 residue classes modulo 27, covering those in the first two residue classes directly and covering those in the third residue class using Lemma 8 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 the congruences

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

For those that are 16 modulo 19, we consider their 7 residue classes modulo 49 and use the congruences

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

For those that are 17 modulo 19, we consider their 11 residue classes modulo 121 and use the congruences

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

We break up the integers in S satisfying $[\![\langle 8,3,6,5\rangle,\langle 9,5,7,11\rangle]\!]$ which are in the residue class 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

$$
\begin{gathered}
[\![\langle 0,18\rangle,\langle 13,19\rangle]\!],\quad [\![\langle 2,1,18\rangle,\langle 3,13,19\rangle]\!],\quad [\![\langle 8,2,18\rangle,\langle 9,13,19\rangle]\!],\\
[\![\langle 3,3,18\rangle,\langle 5,13,19\rangle]\!],\quad [\![\langle 2,3,4,18\rangle,\langle 3,5,13,19\rangle]\!],\\
[\![\langle 8,3,5,18\rangle,\langle 9,5,13,19\rangle]\!],\quad [\![\langle 6,6,18\rangle,\langle 7,13,19\rangle]\!],\\
[\![\langle 2,6,7,18\rangle,\langle 3,7,13,19\rangle]\!],\quad [\![\langle 8,6,8,18\rangle,\langle 9,7,13,19\rangle]\!],\\
[\![\langle 3,6,9,18\rangle,\langle 5,7,13,19\rangle]\!],\quad [\![\langle 2,3,6,10,18\rangle,\langle 3,5,7,13,19\rangle]\!],\\
[\![\langle 8,3,6,11,18\rangle,\langle 9,5,7,13,19\rangle]\!]\quad\text{and}\quad [\![\langle 3,6,5,12,18\rangle,\langle 5,7,11,13,19\rangle]\!].
\end{gathered}
\tag{C32}
$$

Of the those integers in S satisfying $[\![\langle 8,3\rangle,\langle 9,5\rangle]\!]$, we are now left with those which satisfy one of $[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!]$ and $[\![\langle 8,3,6,4\rangle,\langle 9,5,7,11\rangle]\!]$. We handle those satisfying $[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!]$ next by considering the different residue classes they belong to 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

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

Note that the order of the divisors d_i in (C33) does not matter. We cover integers in S satisfying $[\![\langle 8,3,5,4\rangle,\langle 9,5,7,11\rangle]\!]$ in 4 more residue classes modulo 29 by applying Lemma 8 four times. For those congruent to 24 modulo 29, we apply Lemma 8 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 $t=p=59$. Using the last line of congruences in (C10), this gives the additional congruences

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

For those congruent to 25 modulo 29, we apply Lemma 8 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

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

For the integers in S satisfying $[\![\langle 8, 3, 5, 4\rangle, \langle 9, 5, 7, 11\rangle]\!]$ that are congruent to 26 modulo 29, we apply Lemma 8 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 get the additional congruences

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

For the integers in S satisfying $[\![\langle 8, 3, 5, 4\rangle, \langle 9, 5, 7, 11\rangle]\!]$ that are in the residue class 27 modulo 29, we apply Lemma 8 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 get the additional congruences

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

For the integers in S satisfying $[\![\langle 8, 3, 5, 4\rangle, \langle 9, 5, 7, 11\rangle]\!]$ that are in the residue class 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

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

Analogous 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

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

We make use of Lemma 8 and the last line of congruences from (C10) again to cover the integers that are 24 modulo 31. This leads to the additional congruences

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

Recalling our application of Lemma 8 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 the residue class 25 modulo 31 with the additional congruences

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

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

$$[\![\langle 8+2(3^2+3^3+\cdots+3^{i-2}),3,6,26\rangle,\langle 3^i,5,7,31\rangle]\!],\ \text{for } 3\le i\le 59,$$

$$\text{and}\ \ [\![\langle 8+2(3^2+3^3+\cdots+3^{i-2})+3^{i-1},3,4,26\rangle,\langle 3^i,5,11,31\rangle]\!],\ \text{for } 3\le i\le 59. \tag{C42}$$

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

$$[\![\langle 8+2(3^2+3^3+\cdots+3^{i-2}),6,4,27\rangle,\langle 3^i,7,11,31\rangle]\!],\ \text{for } 3\le i\le 59,$$

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

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

$$[\![\langle 8,3,6,4,28\rangle,\langle 9,5,7,11,31\rangle]\!],\quad [\![\langle 8,3,6,4,29\rangle,\langle 9,5,7,11,31\rangle]\!]$$

$$\text{and}\quad [\![\langle 8,3,6,4,30\rangle,\langle 9,5,7,11,31\rangle]\!]$$

are equivalent to $x\equiv 38933 \pmod{9\cdot 5\cdot 7\cdot 11\cdot 31}$, $x\equiv 7748 \pmod{9\cdot 5\cdot 7\cdot 11\cdot 31}$, and $x\equiv 83978 \pmod{9\cdot 5\cdot 7\cdot 11\cdot 31}$, respectively. We cover the integers in S satisfying these congruences then by using

$$\begin{aligned}&[\![\langle 818,j\rangle,\langle d_j'',41\rangle]\!],\ \text{where } 0\le j\le 40,\\ &[\![\langle 818,j\rangle,\langle d_j'',43\rangle]\!],\ \text{where } 0\le j\le 42,\\ &[\![\langle 818,j\rangle,\langle d_j'',47\rangle]\!],\ \text{where } 0\le j\le 46,\ \text{and where}\end{aligned} \tag{C44}$$

$$\{d_0'',d_1'',\ldots,d_{47}''\}=\{d\in\mathbb{Z}^+ : d|(9\cdot 5\cdot 7\cdot 11\cdot 31)\}.$$

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 the integers in S that satisfy $[\![\langle 8,3\rangle,\langle 9,5\rangle]\!]$. We are still needing congruences that cover the $n \in S$ which satisfy one of the congruences $[\![\langle 2,4\rangle,\langle 9,5\rangle]\!]$, $[\![\langle 5,4\rangle,\langle 9,5\rangle]\!]$ and $[\![\langle 8,4\rangle,\langle 9,5\rangle]\!]$, or equivalently which satisfy the congruence $[\![\langle 2,4\rangle,\langle 3,5\rangle]\!]$. 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 7 with $p = 5$. Recall that after the statement of Lemma 7, we showed that the set S of integers that are a sum 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 7 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 7 and the congruences in C_2 correspond to the congruences in (ii) with $i = 1$. Hence, Lemma 7 now implies that we can cover every element of S by combining these congruences with

$$\begin{gathered}[\![\langle 5^{i-1}-1+b_j 5^{i-1}, b_j\rangle,\langle 5^i, m'_j\rangle]\!],\ \text{ for } 2 \le i \le 61 \text{ and } 1 \le j \le 1495,\\ \text{and}\quad [\![\langle j,-1\rangle,\langle 61, 5^{61-j}\rangle]\!],\ \text{ for } 0 \le j \le 60.\end{gathered} \tag{C45}$$

Thus, from (C1)-(C45), we obtain a set of 64731 congruences, with distinct odd moduli > 1, that cover the set of integers that are a sum of two squares, completing the proof. □

2.4 Concluding Remarks

The recent work of B. Hough [15] establishes that certain conditions on the moduli (that the moduli are all distinct and large) ensure a system of congruences cannot cover the integers and further suggests other conditions (like the moduli being distinct, > 1 and odd) may impose similar restrictions on what sets of integers can be covered. 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.

CHAPTER 3

BLOCKS OF DIGITS IN FIBONACCI NUMBERS

3.1 INTRODUCTION

Our interest here is to expand on the idea of base-b repdigits for Fibonacci numbers and to consider not just the case that $B(F_n, b) = 1$ but to consider instead the more general case of $B(F_n, b)$ and show that this expression tends to infinity with n. The idea for such a result was inspired in part by work of R. Bleckmith, M. Filaseta, and C. Nicol [3] showing that

$$\lim_{n\to\infty} B(a^n, b) = \infty$$

if and only if $\log a/\log b$ is irrational for integers a and $b \geq 2$. In this chapter, we apply similar techniques to those in [3] to prove the following result.

Theorem 6. *Let F_n represent the nth Fibonacci number, and $b \in \mathbb{Z}$ be ≥ 2. Then*

$$\lim_{n\to\infty} B(F_n, b) = \infty.$$

It would be relatively easy to modify the approach in the chapter to show Theorem 6 holds for the Lucas numbers, but we do not know if a general result of this type applies to an arbitrary linear recursion. The methods used in the chapter are effective, so that constants can be made precise. For example, one could find N such that $n > N$ implies F_n has $B(F_n, 10) \geq 10$, but this would be more difficult to do and we have not considered such an undertaking. It would be of interest further to have explicit constants $c_0, n_0 \in \mathbb{R}^+$, depending on b, such that $B(F_n, b) \geq c_0 f(n)$ for all integers $n > n_0$ and for some explicit function $f(x) \to \infty$ as $x \to \infty$. We note that G. Barat, R. F. Tichy, and R. Tijdeman in [2] show the existence of such constants for $B(a^n, b)$ with $f(n) = \log n / \log\log n$ where the constants depend on both a and b and with $\log a / \log b$ irrational.

3.2 Proof of Theorem 6 assuming Lemma 9

We begin our proof of Theorem 6 with the following lemma.

Lemma 9. *Let $b \in \mathbb{Z}$ be ≥ 2. Let $a_1, a_2, \ldots, a_m$ be arbitrary integers. Then there are finitely many $(m+1)$-tuples $(k_1, k_2, \ldots, k_m, n)$ of non-negative integers satisfying*

(i) $k_1 < k_2 < \cdots < k_m$,

(ii) $\sum_{j=r}^{m} a_j b^{k_j} > 0$ *for* $1 \leq r \leq m$, *and*

(iii) $\sum_{j=1}^{m} a_j b^{k_j} = (b-1)F_n$.

We will first prove Theorem 6 assuming Lemma 9, and then proceed to prove Lemma 9.

Proof of Theorem 6. It suffices to show that for any $M \in \mathbb{Z}^+$, there are only finitely many n for which $B(F_n, b) \leq M$. Fix such an M, and consider any n with $B(F_n, b) \leq M$. Write $m = B(F_n, b) + \varepsilon$, where $\varepsilon = 0$ if $b | F_n$ and $\varepsilon = 1$ otherwise. Define d_1 to be the first right-most nonzero digit of F_n base b, and take k_1 to be the number of right-most consecutive zero digits of F_n. Let d_2 be the next right-most digit of F_n satisfying $d_2 \neq d_1$ and continue in the same manner, defining d_{j+1} as the next digit of F_n with $d_{j+1} \neq d_j$, until d_{m-1} has been defined. Then there exist positive integers $l_2, \ldots, l_m$ with $l_2 < l_3 < \cdots < l_m$ such that

$$F_n = b^{k_1} \left[(d_1 - d_2) \frac{b^{l_2} - 1}{b - 1} + \cdots + (d_{m-2} - d_{m-1}) \frac{b^{l_{m-1}} - 1}{b - 1} + d_{m-1} \frac{b^{l_m} - 1}{b - 1} \right].$$

Condition (iii) of Lemma 9 holds with $a_1 = -d_1, a_j = d_{j-1} - d_j$ for $2 \leq j \leq m-1$, $a_m = d_{m-1}$, and $k_j = k_1 + l_j$ for $2 \leq j \leq m$. Regardless of the value of n, we have $a_j \neq 0$ and $|a_j| \leq b - 1$ for every $1 \leq j \leq m$. So each n produces a solution to at most one of

$(2b-2)^m \leq (2b-2)^{M+1}$ equations of the form in (iii). Further, with k_j and a_j defined as above, condition (i) is satisfied and condition (ii) holds since $a_m = d_{m-1} \geq 1$ and

$$\sum_{j=r}^{m} a_j b^{k_j} \geq b^{k_m} - \sum_{j=r}^{m-1} |a_j| b^{k_j} \geq b^{k_m} - \sum_{j=r}^{m-1} (b-1) b^{k_j} > 0.$$

Applying Lemma 9, we deduce that there are only finitely many n for which $B(F_n, b) \leq M$. Theorem 6 follows. □

3.3 PRELIMINARIES

Lemma 10 (Baker, 1979)**.** *Let $\alpha_1, \alpha_2, \ldots, \alpha_r$ be non-zero algebraic numbers with degrees at most d and heights at most A. Let $\beta_0, \beta_1, \ldots, \beta_r$ be algebraic numbers with degrees at most d and heights at most $B > 1$. Suppose that*

$$\Lambda = \beta_0 + \beta_1 \log \alpha_1 + \cdots + \beta_r \log \alpha_r \neq 0.$$

Then there are numbers $C = C(r, d) > 0$ and $w = w(r) \geq 1$ such that

$$|\Lambda| > B^{-C(\log A)^w}.$$

Lemma 11 (Lengyel, 1995)**.** *Fix a prime p and a positive integer n. If $p^e || F_n$ and $p^f || n$ for nonnegative $e, f \in \mathbb{Z}$, then $e \leq f + c_p$ for some constant c_p that depends only on p.*

For the next lemma, we define

$$\alpha = \frac{1+\sqrt{5}}{2} \quad \text{and} \quad \beta = \frac{1-\sqrt{5}}{2}.$$

Consider the sequence of numbers

$$\left\{ \left(\frac{\beta}{\alpha} \right)^n \right\}_{n=1}^{\infty}.$$

We have that

$$\frac{\beta}{\alpha} = \frac{1-\sqrt{5}}{1+\sqrt{5}} < 0.$$

Further, $|\beta| < |\alpha|$, so $|\beta/\alpha| < 1$. For positive integers n, we see that $(\beta/\alpha)^n$ is smallest (most negative) for $n = 1$, and largest (most positive) for $n = 2$. Then we have

$$1 - \left(\frac{\beta}{\alpha}\right)^n \leq 1 - \frac{\beta}{\alpha} < 1 + \frac{1}{2} = \frac{3}{2}$$

for $n \geq 1$. We also have

$$1 - \left(\frac{\beta}{\alpha}\right)^n \geq 1 - \left(\frac{\beta}{\alpha}\right)^2 > \frac{1}{2}.$$

Lemma 12. *For any positive integer* n*, we have*

$$n \log \alpha - \frac{1}{2}\log 5 + \log\frac{1}{2} \leq \log F_n \leq n \log \alpha - \frac{1}{2}\log 5 + \log\frac{3}{2}.$$

Proof. Write

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} = \frac{\alpha^n}{\sqrt{5}}\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right).$$

Taking logarithms of both sides gives us

$$\log F_n = n \log \alpha - \frac{1}{2}\log 5 + \log\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right) \leq n \log \alpha - \frac{1}{2}\log 5 + \log\frac{3}{2}.$$

We also have

$$\log F_n = n \log \alpha - \frac{1}{2}\log 5 + \log\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right) \geq n \log \alpha - \frac{1}{2}\log 5 + \log\frac{1}{2},$$

completing the proof. □

3.4 Proof of Lemma 9

Proof of Lemma 9. We begin by showing that we can add the additional condition (iv) below to Lemma 9:

(iv) $\sum_{j=1}^{r} a_j b^{k_j} \neq 0$ for $1 \leq r \leq m$.

To justify that we may do so, we show that Lemma 9 with condition (iv) implies Lemma 9 without condition (iv). Suppose that Lemma 9 with condition (iv) holds. If $(k_1, k_2, \ldots, k_m, n)$ satisfies conditions (i), (ii), and (iii) of Lemma 9, but not (iv), then fix $r \in \{1, 2, \ldots, m\}$ as large as possible with $\sum_{j=1}^{r} a_j b^{k_j} = 0$. By condition (ii) of Lemma 9, we have $r < m$. Now we have that $(k_{r+1}, k_{r+2}, \ldots, k_m, n)$ satisfies $k_{r+1} < k_{r+2} < \cdots < k_m$, $\sum_{j=t}^{m} a_j b^{k_j} > 0$ for $r+1 \le t \le m$, $\sum_{j=r+1}^{m} a_j b^{k_j} = (b-1)F_n$, and $\sum_{j=r+1}^{t} a_j b^{k_j} \neq 0$ for $r+1 \le t \le m$. We may then apply Lemma 9 with condition (iv) to conclude that there are only finitely many such $(k_{r+1}, k_{r+2}, \ldots, k_m, n)$. But for each such solution $(k_{r+1}, k_{r+2}, \ldots, k_m, n)$, there are only a finite number of choices for $(k_1, k_2, \ldots, k_r)$ satisfying $0 \le k_1 < \cdots < k_r < k_{r+1}$. Since there are at most $m-1$ possible values of r, we conclude that if Lemma 9 holds with condition (iv), then it holds true in general.

Assume that the tuple $(k_1, k_2, \ldots, k_m, n)$ satisfies conditions (i)-(iv). First, we will prove that $k_m \ll n+1$, where here and elsewhere in the proof all constants, implied or otherwise, may depend on b, m, and the a_j's. For a fixed $r \in \{2, 3, \ldots, m\}$, we have as a consequence of (i), (ii), and (iii) that

$$(b-1)F_n = \sum_{j=1}^{m} a_j b^{k_j} = \left(\sum_{j=r}^{m} a_j b^{k_j - k_r}\right) b^{k_r} + \sum_{j=1}^{r-1} a_j b^{k_j}$$

$$\ge b^{k_r} - \left(\sum_{j=1}^{r-1} |a_j|\right) b^{k_{r-1}} \ge b^{k_r - k_{r-1}} - \sum_{j=1}^{r-1} |a_j|,$$

assuming that the final expression is positive. If it is nonpositive, we conclude that $b^{k_r - k_{r-1}} \ll 1$, so that in either case we have

$$k_r - k_{r-1} \ll n+1 \quad \text{ for } r \in \{2, 3, \ldots, m\}.$$

Thus $k_m - k_1 = (k_m - k_{m-1}) + (k_{m-1} - k_{m-2}) + \cdots + (k_2 - k_1) \ll n+1$. Using (iii), we have $b^{k_1} | F_n$, so $k_1 \ll n$. Thus we conclude that $k_m \ll n+1$.

Observe that since $k_m \ll n+1$, it suffices now to show that n is bounded above, since then (i) implies there are finitely many $(m+1)$-tuples $(k_1, k_2, \ldots, k_m, n)$. To complete the proof, we therefore assume n is sufficiently large, that is

$$n \ge n_0 = n_0(b, m, a_1, \ldots, a_m).$$

Our goal is to show that with $n \ge n_0$, there are no solutions to (i)-(iv).

Next, we show that $n \ll k_m$. Set

$$M = \sum_{j=1}^{m} |a_j| \geq 1.$$

We have

$$\frac{\alpha^n - \beta^n}{\sqrt{5}} = F_n = \sum_{j=1}^{m} \frac{a_j b^{k_j}}{b-1} \leq \left| \sum_{j=1}^{m} a_j b^{k_j} \right| \leq \sum_{j=1}^{m} |a_j| b^{k_j} \leq M b^{k_m}.$$

Taking logarithms and applying Lemma 12 gives us

$$n \log \alpha - \frac{1}{2} \log 5 + \log \frac{1}{2} \leq \log F_n \leq k_m \log b + \log M,$$

so

$$n \log \alpha \leq k_m \log b + \log M + \frac{1}{2} \log 5 - \log \frac{1}{2}.$$

Thus, $n \ll k_m$, since $\log \alpha, \log b, \log M, \log 5$, and $\log(1/2)$ are all constants. We will extend this and show $n \ll k_m - k_1$.

Fix a prime $p|b$ and nonnegative $e, f \in \mathbb{Z}$ with $p^e || F_n$ and $p^f || n$. Note that the possibilities for p, e, and f only depend on b which is fixed in the lemma. Observe that $k_1 \leq e$, since $b^{k_1} | F_n$ and thus $p^{k_1} | F_n$. By Lemma 11, we have $k_1 \leq e \leq f + c_p$ for some constant c_p that depends only on p. Since n is sufficiently large and

$$f \leq \frac{\log n}{\log p} \leq \frac{\log n}{\log 2} \leq 2 \log n,$$

we obtain

$$k_1 \leq 2 \log n + c_p \leq 3 \log n.$$

From above, we have $n \ll k_m$, so there is a positive constant C' with $n \leq C' k_m$. Since n is sufficiently large, we have

$$n + 6C' \log n \leq 2C' k_m \implies n + 2C' k_1 \leq 2C' k_m,$$

so

$$n \leq 2C'(k_m - k_1) \ll k_m - k_1,$$

which is what we set out to show.

What we now want to do is to improve these estimates using Lemma 10. In particular, we consider $n > 2$ and show that

$$k_{m-i+1} - k_{m-i} \ll (\log n)^{w^{i-1}i} \tag{3.1}$$

for $1 \leq i \leq m-1$, where $w = w(5)$ is as in Lemma 10. This will imply that

$$n \ll k_m - k_1 = (k_m - k_{m-1}) + (k_{m-1} - k_{m-2}) + \cdots + (k_2 - k_1) \ll (\log n)^{w^{m-1}m}.$$

Since m and w are fixed, we can conclude that n is bounded. This will give us that all of the k_i are bounded, completing the proof.

We prove (3.1) by induction on i. Assume $n > 2$ and consider the case when $i = 1$. Using (ii) of Lemma 9 with $r = m$, we have that $a_m > 0$. Setting

$$D = \sum_{j=1}^{m-1} \frac{a_j}{a_m} b^{k_j - k_m}$$

and using (iii), we get

$$a_m b^{k_m}(1 + D) = (b-1)F_n. \tag{3.2}$$

Further, using (i), we have

$$|D| = \left| \sum_{j=1}^{m-1} \frac{a_j}{a_m} b^{k_j - k_m} \right| \leq M b^{k_{m-1} - k_m},$$

where as before $M = \sum_{j=1}^{m} |a_j| \geq 1$. If $k_m - k_{m-1} \leq \log(2M)/\log b$, then since $n \geq 3$, we have that

$$k_m - k_{m-1} \leq \frac{\log(2M)}{(\log b)(\log 3)} \cdot \log n \ll \log n,$$

which is what is to be shown for $i = 1$. So suppose that $k_m - k_{m-1} > \log(2M)/\log b$. This gives $|D| < 1/2$. We use that

$$\log(1 + x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots \qquad \text{for } |x| < 1 \tag{3.3}$$

to deduce

$$|\log(1 + D)| \leq \sum_{j=1}^{\infty} \frac{|D|^j}{j} \leq |D| + \frac{|D|^2}{2(1 - |D|)} < (1 + |D|)|D| < \frac{3}{2}|D| \ll b^{k_{m-1} - k_m}.$$

Define

$$\Lambda = \log a_m + k_m \log b - \log(b-1) + \frac{1}{2}\log 5 - n\log\alpha$$

and rewrite

$$F_n = \frac{\alpha^n - \beta^n}{\sqrt{5}} = \frac{\alpha^n}{\sqrt{5}}\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right).$$

From (3.3), we obtain

$$\left|\log\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right)\right| \le \left|\frac{\beta}{\alpha}\right|^n + \left|\frac{\beta}{\alpha}\right|^{2n} + \left|\frac{\beta}{\alpha}\right|^{3n} + \cdots = \frac{\left|\frac{\beta}{\alpha}\right|^n}{1 - \left|\frac{\beta}{\alpha}\right|^n} < 2\left(\frac{1}{2}\right)^n,$$

since $|\beta/\alpha| < 1/2$. Taking the logarithm of both sides of (3.2) gives

$$\begin{aligned}|\Lambda| &= |\log a_m + k_m \log b - \log(b-1) + \frac{1}{2}\log 5 - n\log\alpha| \\ &\le |\log(1+D)| + \left|\log\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right)\right| \\ &\le |\log(1+D)| + 2\left(\frac{1}{2}\right)^n \ll b^{k_{m-1}-k_m} + \left(\frac{1}{2}\right)^n.\end{aligned}$$

Using Lemma 10 with $d = 2$, $r = 5$, $A = \max\{a_m, b, 5\} \ll 1$, and $B = \max\{k_m, n\} \ll n$, we have

$$|\Lambda| \gg B^{-C(\log A)^w},$$

where $C = C(5,2)$ and $w = w(5)$. Thus, for a constant value t,

$$n^{-t} \ll b^{k_{m-1}-k_m} + \left(\frac{1}{2}\right)^n.$$

So, for some constant $C'' > 0$, we have

$$n^{-t} \le C'' b^{k_{m-1}-k_m} + C''\left(\frac{1}{2}\right)^n \implies \frac{1}{n^t} - C''\left(\frac{1}{2}\right)^n \le C'' b^{k_{m-1}-k_m}.$$

Since n is sufficiently large, we have $\log C'' + t\log n + \log 2 \le n\log 2$ implies $C'' n^t \le 2^{n-1}$, so $C''(1/2)^n \le 1/(2n^t)$. Thus,

$$\frac{1}{2n^t} \le C'' b^{k_{m-1}-k_m} \implies n^{-t} \le 2C'' b^{k_{m-1}-k_m}.$$

Taking logarithms above gives us that $k_m - k_{m-1} \ll \log n$, proving that (3.1) holds for $i = 1$.

Now fix i' with $2 \leq i' \leq m-1$ and suppose that (3.1) holds for each positive integer $i < i'$. Then from (iii) we have that

$$D_1 b^{k_{m-i'+1}}(1+D_2) = (b-1)F_n, \tag{3.4}$$

where

$$D_1 = a_m b^{k_m - k_{m-i'+1}} + a_{m-1} b^{k_{m-1} - k_{m-i'+1}} + \cdots + a_{m-i'+1}$$

and

$$D_2 = \sum_{j=1}^{m-i'} \frac{a_j}{D_1} b^{k_j - k_{m-i'+1}}.$$

From (i) and from (ii) with $r = m - i' + 1$, we have

$$1 \leq D_1 \ll b^{k_m - k_{m-i'+1}} \quad \text{and} \quad |D_2| \leq M b^{k_{m-i'} - k_{m-i'+1}} \ll b^{k_{m-i'} - k_{m-i'+1}}.$$

From the induction hypothesis, we have

$$k_m - k_{m-i'+1} = (k_m - k_{m-1}) + \cdots + (k_{m-i'+2} - k_{m-i'+1}) \ll (\log n)^{w^{i'-2}(i'-1)},$$

and thus

$$\log D_1 \ll (\log n)^{w^{i'-2}(i'-1)}. \tag{3.5}$$

If $k_{m-i'+1} - k_{m-i'} \leq \log(2M)/\log b$, then $k_{m-i'+1} - k_{m-i'} \ll (\log n)^{w^{i'-1}i'}$, which is what we want to prove. So suppose $k_{m-i'+1} - k_{m-i'} > \log(2M)/\log b$. Like the $i = 1$ case above, we have $|D_2| < 1/2$, so that $|\log(1+D_2)| < 3|D_2|/2$. Taking logarithms in (3.4) we have

$$\log D_1 + k_{m-i'+1} \log b + \log(1+D_2) = \log(b-1) + n \log \alpha + \log\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right) - \frac{1}{2}\log 5.$$

Thus,

$$\begin{aligned}
&\left|\log D_1 + k_{m-i'+1} \log b - \log(b-1) - n \log \alpha + \frac{1}{2}\log 5\right| \\
&\qquad = \left|-\log(1+D_2) + \log\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right)\right| \leq |\log(1+D_2)| + \left|\log\left(1 - \left(\frac{\beta}{\alpha}\right)^n\right)\right|
\end{aligned}$$

$$\leq |\log(1+D_2)| + 2\left(\frac{1}{2}\right)^n \ll b^{k_{m-i'}-k_{m-i'+1}} + \left(\frac{1}{2}\right)^n.$$

We apply Lemma 10 with $d = 2, r = 5, A = \max\{D_1, b, 5\}$, and $B = \max\{k_{m-i'+1}, n\}$. Observe that $B \leq c_0 n$ for some $c_0 > 0$. We deduce

$$|\log D_1 + k_{m-i'+1}\log b - \log(b-1) - n\log\alpha + \frac{1}{2}\log 5| \gg B^{-C(\log A)^w},$$

where $C = C(5,2)$ and $w = w(5)$. Therefore, either $B^{-C(\log A)^w} \ll (1/2)^n$ or $B^{-C(\log A)^w} \ll b^{k_{m-i'}-k_{m-i'+1}}$. If $B^{-C(\log A)^w} \ll (1/2)^n$, then

$$\frac{1}{B^{C(\log A)^w}} \ll \frac{1}{2^n},$$

so

$$2^n \ll B^{C(\log A)^w}.$$

Taking logarithms, and noting (3.5) gives us $\log A \ll (\log n)^{w^{i'-2}(i'-1)}$, we have

$$\begin{aligned} n &\ll \frac{C}{\log 2}(\log A)^w \log B \ll (\log A)^w \log n \\ &\ll ((\log n)^{w^{i'-2}(i'-1)})^w \log n = (\log n)^{w^{i'-1}(i'-1)} \cdot \log n \\ &= (\log n)^{w^{i'-1}(i'-1)+1} \ll (\log n)^{w^{i'-1}i'} \ll (\log n)^{w^{m-1}m}. \end{aligned}$$

This is a contradiction for n large since w and m are fixed positive numbers. Therefore, we deduce that $B^{-C(\log A)^w} \ll b^{k_{m-i'}-k_{m-i'+1}}$ from which we obtain

$$b^{k_{m-i'+1}-k_{m-i'}} \ll B^{C(\log A)^w}.$$

Taking logarithms gives

$$\begin{aligned} k_{m-i'+1} - k_{m-i'} &\ll \frac{C}{\log b}(\log A)^w \log B \ll (\log A)^w \log n \ll ((\log n)^{w^{i'-2}(i'-1)})^w \log n \\ &= (\log n)^{w^{i'-1}(i'-1)} \cdot \log n = (\log n)^{w^{i'-1}(i'-1)+1} \ll (\log n)^{w^{i'-1}i'}, \end{aligned}$$

completing the induction and the proof. □

BIBLIOGRAPHY

[1] A. Baker, Transcendental Number Theory, Cambridge Univ. Press, Cambridge, 1979.

[2] G. Barat, R. F. Tichy, and R. Tijdeman, *Digital blocks in linear numeration systems*, Number theory in progress, Vol. 2 (Zakopane-Kościelisko, 1997), de Gruyter, Berlin, 1999, 607–631.

[3] R. Blecksmith, M. Filaseta, and C. Nicol, *A result on the digits of* a^n, Acta Arith. 64 (1993), 331–339.

[4] J. J. Bravo and F. Luca, *On a conjecture about repdigits in* k*-generalized Fibonacci Sequences*, Publ. Math. Debrecen 82 (2013), 623–639.

[5] Y. Bugeaud, M. Ciphu, and M. Mignotte, *On the representation of Fibonacci and Lucas numbers in an integer base*, Ann. Math. Qué. 37 (2013), 31–43.

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

[7] B. Faye and F. Luca, *Pell and Pell-Lucas numbers with only one distinct digit*, Ann. Math. Inform. 45 (2015), 55–60.

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

[9] 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), 495–517.

[10] Michael Filaseta, Mark Kozek, Charles Nicol and John Selfridge, *Composites that remain composite after changing a digit*, J. Comb. Number Theory 2 (2010), 25–36.

[11] Ron Graham, *A Fibonacci-Like Sequence of Composite Numbers*, Math. Mag. 37 (1964), 322–324.

[12] Andrew Granville, private communication, December 13, 2016.

[13] Richard K. Guy, *Unsolved Problems in Number Theory*, 3rd ed., Problem Books in Math., Springer-Verlag, New York, 2004.

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

[15] Bob Hough, *Solution of the minimum modulus problem for covering systems*, Annals of Math 181 (2015), 361–382.

[16] Lenny 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.

[17] Claire Emil Krukenberg, Covering Sets of the Integers, Doctoral Dissertation, University of Illinois at Urbana-Champaign, 1971.

[18] T. Lengyel, *The order of the Fibonacci and Lucas numbers*, Fib. Quart. 33 (1995), 234–239.

[19] F. Luca, *Fibonacci and Lucas numbers with only one distinct digit*, Portugaliae Mathematica 57 (2000), 243–254.

[20] D. Marques and A. Togbé, *On terms of linear recurrence sequences with only one distinct block of digits*, Colloq. Math. 124 (2011), 145–155.

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

[22] Tyler Owens, *A covering system with minimum modulus* 42, Masters Thesis, 2014, All Theses and Dissertations, Paper 4329, http://scholarsarchive.byu.edu/etd/4329.

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

[24] Andrzej Schinzel, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. 13 (1967/1968), 91–101.

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

[26] C. L. Steward, *On the representation of an integer in two different bases*, J. Reine Angew. Math. 319 (1980), 63–72.

[27] Karl Zsigmondy, *Zur Theorie der Potenzreste*, Monatshefte für Mathematik und Physik 3 (1892), 265–284.