Université de Montréal

Covering systems

par

Jonah Klein

Département de mathématiques et de statistique
Faculté des arts et des sciences

Mémoire présenté en vue de l'obtention du grade de
Maître ès sciences (M.Sc.)
en Mathématiques

May 15, 2023

Université de Montréal

Faculté des arts et des sciences

Ce mémoire intitulé

Covering systems

présenté par

Jonah Klein

a été évalué par un jury composé des personnes suivantes :

Andrew Granville
(président-rapporteur)

Dimitris Koukoulopoulos
(directeur de recherche)

Matilde Lalín
(membre du jury)

Résumé

Un système couvrant est un ensemble fini de progressions arithmétiques avec la propriété que chaque entier appartient à au moins une des progressions. L'étude des systèmes couvrants a été initié par Erdős dans les années 1950, et il posa dans les années qui suivirent plusieurs questions sur ces objets mathématiques. Une de ses questions les plus célèbres est celle du plus petit module : est-ce que le plus petit module de tous les systèmes couvrants avec modules distinct est borné uniformément?

En 2015, Hough a montré que la réponse était affirmative, et qu'une borne admissible est 10^{16}. En se basant sur son travail, mais en simplifiant la méthode, Balister, Bollobás, Morris, Sahasrabudhe et Tiba on réduit cette borne a $616,000$. Leur méthode a menée a plusieurs applications supplémentaires. Entre autres, ils ont compté le nombre de système couvrant avec un nombre fixe de module.

La première partie de ce mémoire vise a étudier une question similaire. Nous allons essayer de compter le nombre de système couvrant avec un ensemble de module fixé. La technique que nous utiliserons nous mènera vers l'étude des symmétries de système couvrant.

Dans la seconde partie, nous répondrons à des variantes du problème du plus petit module. Nous regarderons des bornes sur le plus petit module d'un système couvrant de multiplicité s, c'est-à-dire un système couvrant dans lequel chaque module apparait au plus s fois. Nous utiliserons ensuite ce résultat afin montrer que le plus petit module d'un système couvrant de multiplicité 1 d'une progression arithmétique est borné, ainsi que pour montrer que le n-eme plus petit module dans un système couvrant de multiplicité 1 est borné.

Mots clés : Système couvrant, Translation, Groupe symmétrique, Borne, Plus petit module, Méthode des distortions, Théorie des nombres analytique

Abstract

A covering system is a finite set of arithmetic progressions with the property that every integer belongs to at least one of them. The study of covering systems was started by Erdős in the 1950's, and he asked many questions about them in the following years. One of the most famous questions he asked was if the minimum modulus of a covering system with distinct moduli is bounded uniformly.

In 2015, Hough showed that it is at most 10^{16}. Following on his work, but simplifying the method, Balister, Bollobás, Morris, Sahasrabudhe and Tiba showed that it is at most $616,000$. Their method led them to many further applications. Notably, they counted the number of covering systems with a fixed number of moduli.

The first part of this thesis seeks to study a related question, that is to count the number of covering systems with a given set of moduli. The technique developped to do this for some sets will lead us to look at symmetries of covering systems.

The second part of this thesis will look at variants of the minimum modulus problem. Notably, we will be looking at bounds on the minimum modulus of a covering system of multiplicity s, that is a covering system in which each moduli appears at most s times, as well as bounds on the minimum modulus of a covering system of multiplicity 1 of an arithmetic progression, and finally look at bounds for the n-th smallest modulus in a covering system.

Key words : Covering system, Translations, Symmetric group, Bound, Smallest modulus, Distortion method, Analytic number theory

Contents

List of tables

List of figures

List of abbreviations and accronyms

CS	Covering system
AP	Arithmetic progression
lcm	Least common multiple
gcd	Greatest common divisor

Prerequisites

Prerequisites from elementary number theory

In this section, we go over some well known definitions and results from elementary number theory that we will be using throughout the thesis. We denote by $\mathbb{Z}$ the set of integers, that is

$$\mathbb{Z} = \{\ldots, -3, -2, -1, 0, 1, 2, 3, \ldots\}.$$

We say an integer d divides another integer n, usually denoted $d|n$ if there exists some integer k such that $dk = n$. If d does not divide n, we will write $d \nmid n$.

For example, $6 = 2 \cdot 3$, and so $2|6$ and $3|6$. A prime number, usually denoted by p, is a positive integer who's only positive divisors are 1 and itself. A fundamental result about prime numbers is that any positive integer can be written uniquely as a product of prime numbers up to ordering. This is known as the fundamental theorem of arithmetic. For a positive integer a, we will say that $p^a \| n$ if $p^a | n$ but $p^{a+1} \nmid n$.

The gcd, or *greatest common divisor* of two integers a and b is the largest integer d that divides both a and b. The lcm, or *least common multiple* of two integers a and b, is the smallest positive integer m such that $a|m$ and $b|m$.

The *arithmetic progression*, $a \pmod m$ is the set of integers

$$a \pmod m = \{a + km : k \in \mathbb{Z}\}.$$

We will often say the *congruence class* $a \pmod m$ to denote the same set. We say an integer n is *square-free* if n is not divisible by the square of any prime, that is if $p^2 \nmid n$ for every prime p.

We say an integer n is *y-smooth* if every prime factor of n is $\leq y$. Denote the k-th prime by p_k. Then the *primorial* of p_k is

$$P_k = \prod_{i=1}^{k} p_i.$$

Finally, the *Euler totient function* of an integer n, $\phi(n)$, is the number of integers $k \in [1,n]$ such that $(n,k) = 1$.

Prerequisites from group theory

A group is composed of a set G and an associative binary operation that is denoted by $+$ when the group is additive, and by $\cdot$ when the group is multiplicative. For example, the integers modulo p form a group under addition, usually denoted by $\mathbb{Z}/p\mathbb{Z}$, and non-zero integers modulo p form a group under multiplication, usually denoted by $(\mathbb{Z}/p\mathbb{Z})^*$. In particular, any integer that is not divisible by p is invertible modulo p, or again for each $n \in \{1,2,...,p-1\}$, there exists an integer $n^{-1} \in \{1,2,\ldots,p-1\}$ such that $n \cdot n^{-1} \equiv 1 \pmod p$.

Another important family of groups that we will be using are the symmetric groups. The symmetric group over the set of n elements $E = \{1,2,\ldots,n\}$, usually denoted by S_n, is the set of bijective functions from E to E, with function composition as the binary operation. The group has order $n!$, that is the number of elements in S_n is $n!$.

The last result we need from group theory concerns generating symmetric groups.

Proposition 0.1. *The symmetric group S_n is generated by transpositions. That is, any element $\sigma \in S_n$ can be written as $\sigma = (i_1 i_2)(i_3 i_4) \cdots (i_k i_{k+1})$ for some integer k, where the transposition (ij) is understood to be the bijection of $\{1,2,\cdots,n\}$ that sends i onto j, j onto i, and sends each other k, with $k \notin \{i,j\}$ onto itself.*

Prerequisites from analytic number theory

In this section, we go through some results from analytic number theory that we will need in order to prove our bound on the minimum modulus of a covering system of multiplicity s. We first introduce some notation that will be used in what follows.

Definition 0.1. We say that a function $f(x)$ *has smaller or equal order of magnitude* in I than $g(x)$, or that $f(x)$ is *big-Oh* of g(x) in I, denoted by

$$f(x) = O(g(x)) \quad (x \in I),$$

if there exists some positive constant c such that $|f(x)| \leq cg(x)$ for all $x \in I$. When the set I we are dealing with is clear from the context, we will simply write $f(x) = O(g(x))$. We will also write

$$f(x) \ll g(x) \quad (x \in I),$$

which can be read $f(x)$ is *less than less than* $g(x)$, to say the same thing.

Definition 0.2. We say that a function $f(x)$ *has the same order of magnitude* in I as $g(x)$, denoted by

$$f(x) \asymp g(x) \quad (x \in I),$$

if $f(x)$ has smaller or equal order of magnitude in I than $g(x)$ and $g(x)$ has smaller or equal order of magnitude in I than $f(x)$.

Definition 0.3. We denote by $\pi(x)$ the *prime counting function*, that is

$$\pi(x) = |\{n \leq x : n \text{ is prime}\}|.$$

The first result we will look at is Chevyshev's estimate. For a proof of this result, see chapter 2 in [**20**].

Theorem 0.2. *(Chebyshev's estimate)*

$$\pi(x) \asymp \frac{x}{\log(x)}$$

.

The next result we look at is Merten's three estimates. For a proof of this result, see chapter 3 in [**20**].

Theorem 0.3. *(Merten's three estimates) There are constants c and γ such that for $x \geq 2$, we have that :*

(1)

$$\sum_{p \leq x} \frac{\log p}{p} = \log x + O(1),$$

(2)

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + c + O(1/\log x),$$

(3)

$$\prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x}\left(1 + O\left(\frac{1}{\log x}\right)\right).$$

Finally, we will require Theorem 16.3 from [**20**] to estimate inverse smooth number sums.

Theorem 0.4. *Let f be a multiplicative function such that $0 \leq f \leq \tau_k$ for some $k \in \mathbb{Z}_{\geq 1}$. Let $x \geq y \geq 3$, and $u = \log(x)/\log(y)$. If $y \geq (\log(x))^{2+\delta}$ for some $\delta > 0$, then*

$$\sum_{n \in \mathcal{S}(y), n > x} \frac{f(n)}{n} \leq \frac{e^{O_{k,\delta}(u)}}{(u\log(2u))^u} \cdot \exp\left\{\sum_{p \leq y} \frac{f(p)}{p}\right\}.$$

Acknowledgements

I would first like to thank my advisor, Dimitris Koukoulopoulos, for our weekly meetings, in which his patience, insight, and breadth of knowledge made this thesis possible. I would also like to thank him for his financial support, as well as FRQNT and CICMA for their scholarship and bursaries.

I would like to thank my parents, Louise and Allan, my sister Emilie, and my friends Julien, Cédric, Olivier, Emma, Alex, Camille, Hugo, Gabriel and Antoine for their support throughout my endeavors.

I would like to thank my fellow students and friends for all the interesting conversations we had about mathematics and the world. A particular thanks to Simon, with whom I spent a summer working on covering systems, in which we came up with some of the ideas we present here.

Finally, I would like to thank Mrs. Nimbus, whose support proved invaluable throughout this project.

Chapter 1

Introduction

1.1. Definitions and origin

We learn at a very young age that every integer is either odd or even. In other terms, we say that every integer is either divisible by 2, or not. Another way of rephrasing this is that any integer is either congruent to 0 (mod 2) or to 1 (mod 2), or again that

$$\mathbb{Z} = A_1 \cup A_2,$$

where A_1 is the arithmetic progression 0 (mod 2) and A_2 is the arithmetic progression 1 (mod 2). This is a particular case of what we call a covering system. Before defining what a covering system, it will be useful to define what it is to cover an integer, or again what it is for an integer to be covered.

Definition 1.1. We say an integer n is *covered* by a finite set of arithmetic progressions

$$\{a_1 \pmod{m_1}, a_2 \pmod{m_2}, ..., a_k \pmod{m_k}\},$$

or that the set of arithmetic progressions *covers* the number n, if there is some $1 \leq i \leq k$ such that $n \equiv a_i \pmod{m_i}$.

Definition 1.2. A *covering system* is a finite set of arithmetic progressions that covers every integer.

Normally, covering systems are described as a finite set of arithmetic progressions for which each integer belongs to at least one of them. We decompose this definition here because it will be useful later on to talk about integers that are covered by some arithmetic progressions, and so it will improve readibility of certain proofs.

The covering system described above is simply a way of classifying the integers according to their residue modulo 2. In a first class of discrete mathematics, we realise that 2 is pretty arbitrary in this type of construction; we may instead classify the integers according to their residue modulo n, for any integer n. Another way of saying this is that

$$\{0 \pmod n), 1 \pmod n), ..., n-1 \pmod n)\}$$

is a covering system.

However interesting these above covering systems may be, the main focus of our investigations will be on what is called covering systems of multiplicity s.

Definition 1.3. Let $\mathcal{A} = \{a_1 \pmod{d_1}, a_2 \pmod{d_2}, \ldots, a_n \pmod{d_n}\}$ be a set of congruences. We define the *multiplicity* of $\mathcal{A}$ to be the number

$$\mathcal{M}(\mathcal{A}) := \max_{d \in \mathbb{N}} \#\{1 \le j \le n : d_j = d\}.$$

If C is a covering system, we define the *multiplicity* of C to be $\mathcal{M}(C)$, and if $\mathcal{M}(C) = s$, we say that C is a *covering system of multiplicity* s.

For example,

$$\{1 \pmod 2), 1 \pmod 3), 2 \pmod 4), 4 \pmod 8), 8 \pmod{12}), 0 \pmod{24})\}$$

is a covering system of multiplicity 1. We will look at how to verify that this is indeed a covering system in the following section.

The concept of a covering system of multiplicity 1 was first introduced by Erdős [**10**] in 1950, where he used the above covering system of multiplicity 1 to answer a question of Romanoff about integers of the form $2^k + p$. We show here a proof of Erdős's result.

Theorem 1.1. *There exists an arithmetic progression of odd numbers, no term of which is of the form $2^k + p$, where k is a positive integer and p is a prime.*

Proof. Note that the periods of the powers of 2 for the primes 3,5,7,13,17,241 are 2,4,3,12,8,24 respectively. The following table gives this information in a clear and concise way.

Table 1.1. Periods of powers of 2 for various primes

Primes	Periods
3	2
5	4
7	3
13	12
17	8
241	24

If we choose n to be simultaneously $-2^1 \pmod 3$, $-2^2 \pmod 5$, $-2^1 \pmod 7$, $-2^8 \pmod{13}$, $-2^4 \pmod{17}$, and $-2^0 \pmod{241}$, then $2^k + n$ is always composite. Indeed, we know that any integer k belongs to at least one of the arithmetic progressions

$$\{1 \pmod 2, 1 \pmod 3, 2 \pmod 4, 4 \pmod 8, 8 \pmod{12}, 0 \pmod{24}\}.$$

If $k \equiv 1 \pmod 2$, then $2^k \equiv 1 \pmod 3$, and so $2^k + n \equiv 0 \pmod 3$, and similarly for each other prime we mentionned above. □

Notice that if we take the above covering system and add some random arithmetic progression, it remains a covering system. For example,

$$\{1 \pmod 2, 1 \pmod 3, 2 \pmod 4, 4 \pmod 8, 8 \pmod{12}, 0 \pmod{24}, 2 \pmod 5\}$$

is also a covering system. However, the arithmetic progression that we added is *redundant*; it may be removed from the set and the remaining arithmetic progressions still form a covering system. For this reason, we define the concept of a minimal covering system.

Definition 1.4. We say a covering system

$$C = \{a_1 \pmod{m_1}, \ldots, a_n \pmod{m_n}\}$$

is *minimal* if for each $a_i \pmod{m_i}$ in C, there exists some integer k such that $k \equiv a_i \pmod{m_i}$, but $k \not\equiv a_j \pmod{m_j}$ for each $j \neq i$. Another way of saying this is that a covering system C is minimal if there does not exists a proper subset of C that is also a covering system, or again that there exists no *proper subcover* of C.

The study of non-minimal covering systems can get hard, as we can artificially insert arithmetic progressions into a covering system to create another one that is not minimal, but can then have certain properties that we did not have before. We will see how important minimality is in the study of certain problems in the following sections. Some results that we can prove true for minimal covering systems are much harder to prove, or may even be false, if we leave the assumption of minimality behind.

For an example of minimality, let us show the covering system used by Erdős is minimal. It suffices to find for each arithmetic progression an integer that is in that arithmetic progression, but that is not in any of the others. The following table gives us such integers for each arithmetic progression in the covering system.

Although it was quite easy here to show that the covering system was minimal as we have few arithmetic progressions, it can get quite hard to show in practice when we have a large number of progressions, or to show that certain families of covering sytems are minimal. We will be building some tools in the following sections that will help us show minimality when certain conditions are met.

Table 1.2. Minimality of Erdós's covering system

Arithmetic progression	Integer
1 (mod 2)	3
1 (mod 3)	16
2 (mod 4)	2
4 (mod 8)	12
8 (mod 12)	8
0 (mod 24)	0

1.2. Structure and symmetry in covering systems

The first part of this thesis will focus on covering systems and their transformations. Notably, we will be looking at various ways to take a covering system and transform it into another covering system that has the same moduli, but different arithmetic progressions. For example, we may translate each arithmetic progression in a covering system by a fixed integer t, and the resulting set of arithmetic progressions is a covering system. We may also dilate each arithmetic progression in a covering system by a fixed integer λ, and under certain conditions, the resulting set of arithmetic progressions is a covering system.

In search for more general ways to transform covering systems, we will show that if C is a covering system, $p_1, \ldots, p_\ell$ are the distinct prime factors of $\operatorname{lcm}(C)$, and $\eta^*(C)$ is the set of minimal covering systems that have the same moduli as C, then the group $S_1 \times \ldots \times S_{p_\ell}$ acts on $\eta^*(C)$ in a very natural way. Using this, we will prove the following proposition.

Proposition 1.2. *Let C be a minimal covering system of multiplicity 1, and suppose p_1,...,p_ℓ are the distinct prime divisors of the* lcm *of the moduli in C. Denote by $H^*(C)$ the number of minimal covering systems with the same moduli as C. Then*

$$p_1! \cdots p_\ell! | H^*(C).$$

We will also show how to construct infinitely many covering systems C for which this divisibility condition is sharp, that is for which $p_1! \cdots p_\ell! = H^*(C)$, as well as how to construct infinitely many covering systems for which this is not sharp, that is for which $p_1! \cdots p_\ell! < H^*(E)$.

1.3. The minimum modulus problem

Notice that the smallest modulus in the covering system used by Erdős above is 2. Naturally, the larger the smallest modulus in a covering system of multiplicity 1 is, the more there will be arithmetic progressions in the system. Indeed, through a union bound, we have that if a set of arithmetic progressions

$$\{a_1 \pmod{m_1}, a_2 \pmod{m_2}, \ldots, a_n \pmod{m_n}\}$$

covers the integers, then

$$\sum_{i=1}^{n} \frac{1}{m_i} \geq 1.$$

This led Erdős to ask [**10**] if there could be covering systems of multiplicity 1 with arbitrarily large smallest modulus, or again if the smallest modulus in a covering system of multiplicity 1 is bounded, which led many mathematicians to look for covering systems of multiplicity 1 with large smallest moduli, see for example [**6**], [**21**], [**5**], [**22**], [**16**], [**23**] and [**24**]. The following table gives a history of the search for these covering systems.

Table 1.3. History of the largest smallest modulus

Minimum modulus	Discovered by	Year
9	Churchhouse	1968
18	Krukenberg	1971
20	Choi	1971
24	Morikawa	1981
25	Gibson	2006
40	Nielsen	2007
42	Owens	2014

Owens was a student of Nielsen when he found the covering system with minimum modulus 42, and used a very similar method. Note that after so many years of research, the largest known minimum modulus of a covering system of multiplicity 1 remains very small. This led Nielsen to suggest [**23**] that the answer to Erdős's question was negative, that is that the minimum modulus is bounded. It did not take very long after that for the answer to come. The answer to this question is that it is bounded, as proven by Hough [**18**] in 2015, who showed that it is smaller than 10^{16}. A few years later, in 2018, Balister, Bollobás, Morris, Sahasrabudhe and Tiba [**4**] simplified Hough's proof, and in doing this reduced the bound on the minimum modulus to 616,000.

Many similar questions to the minimum modulus problem can arise. For example, since we know that the smallest modulus is bounded, we may wonder if the second smallest modulus is also bounded, or in general if the n-th smallest modulus is bounded. Since the minimum modulus is bounded, it is very natural to conjecture that the answer here is yes, that is that the n-th minimum modulus should be bounded. Interestingly enough, it was proved recently by Cummings, Filaseta and Trifonov that the n-th minimum modulus is bounded [**8**]. The bounds that come from their method, however, are of tower type. In the same article, they also managed to reduce Hough's bound to 118 in the special case where all the moduli are square-free.

Another natural question is to ask if the minimum modulus of a partial covering system with certain properties is bounded. For example, one may wonder if the minimum modulus of a covering system of some arithmetic progression $a \pmod{m}$ is bounded.

One last possible question we will consider here is the problem of the minimum modulus of a covering system of multiplicity s. One may ask if the minimum modulus of a covering system of multiplicity s is bounded. It would be natural to conjecture that it is, since it is the case that the minimum modulus of a covering system of multiplicity 1 is bounded, as we mentionned above.

In the last chapter of this thesis, we will give an answer to all these questions. In joint work with Dimitris Koukoulopoulos and Simon Lemieux [**19**], we showed the following three theorems. Our first theorem is about bounding the minimum modulus for covering system of multiplicity s.

Theorem 1.3. *The minimum modulus of a covering system of multiplicity s is bounded. More precisely, there exists a constant c such that the minimum modulus in a covering system of multiplicity s is smaller than*

$$\exp\left(c\frac{\log^2(s+1)}{\log\log(s+2)}\right).$$

An immediate consequence of Theorem 1.3 is the following theorem about the minimum modulus in a covering system of some arithmetic progression.

Theorem 1.4. *The minimum modulus of a covering system of multiplicity 1 of the arithmetic progression $a \pmod{m}$ is bounded. More precisely, there exists a constant c such that the minimum modulus in a covering system of multiplicity 1 of the arithmetic progression $a \pmod{m}$ is smaller than*

$$\exp\left(c\frac{\log^2(m+1)}{\log\log(m+2)}\right).$$

The trick to proving this theorem from the previous one will be to construct from our covering system of multiplicity 1 of $a \pmod{m}$ a covering system of multiplicity m that has the same minimum modulus. The result then follows immediately. This is actually why we considered the problem of the minimum modulus for covering system of multiplicity s in the first place. Finally, using a similar trick, that is constructing some covering system of multiplicity s with a suitable minimum modulus and a suitable value of s, we can prove the following theorem about the j-th minimum modulus in a covering system.

Theorem 1.5. *The n-th minimum modulus in a minimal covering system of multiplicity 1 is bounded. More precisely, there exists a constant c such that the n-th minimum modulus in a minimal covering system of multiplicity 1 is smaller than*

$$\exp\left(c\frac{n^2}{\log(n+1)}\right).$$

The trick will be to construct a covering system of multiplicity s from our covering system in which we remove the $n-1$ arithmetic progressions with smallest moduli. This can always be done with s lesser or equal to the lcm of the first $n-1$ moduli. Indeed, we have by minimality that the first $n-1$ moduli are not a covering system, hence there is at least one integer modulo their lcm that is not covered by them. This implies that the remaining moduli cover this arithmetic progression, which in turn using the previous theorem would give us a bound, assuming the lcm is bounded. However, by induction, the lcm of the first few moduli is bounded. Indeed, it is bounded for $n = 2$ by the minimum modulus problem, and then taking the product of our first $n-1$ bounds gives us a bound for the lcm at step n.

However, using this value of s would yield bounds that are far from the ones we obtain here. To get the above result, we need to find a value of s that does not depend on the first $n-1$ moduli. We will discuss this further in the last chapter of this thesis. We do not know if the way we use the trick is optimal, and even if in the case of this particular trick it is optimal, we do not know if the asymptotic bounds we found are optimal, as there could be some other way of viewing the problem that bypasses this trick completely. However, we do know that the j-th largest modulus can grow at least exponentially, as the following proposition shows.

Proposition 1.6. *For each $j \geq 5$, there exists a minimal covering system with the following j distinct moduli placed in increasing order:*

$$2 < 2^2 < 2^3 < \cdots < 2^{j-4} < 3\cdot 2^{j-5} < 2^{j-3} < 3\cdot 2^{j-4} < 3\cdot 2^{j-3}.$$

Proof. Fix $j \geq 5$, and let

$$\mathcal{C}_j = \{1 \mod 2, 2 \mod 4, \ldots, 2^{j-4} \mod 2^{j-3}, A_0, A_1, A_2\},$$

where A_k is the intersection of the congruence classes $k \mod 3$ and $0 \mod 2^{j-5+k}$. We claim that $\mathcal{C}_j$ is a covering system.

Indeed, for each integer n, either $2^{j-3}|n$ or $2^{j-3} \nmid n$. In the former case, let $k \in \{0,1,2\}$ be such that $n \equiv k \mod 3$. In particular, we have $n \in A_k$, and thus n is covered by $\mathcal{C}_j$. Let us now consider the case when $2^{j-3} \nmid n$. Then, there must exist some $i \in \{1,2\ldots,j-3\}$ such that $2^{i-1}|n$ and $2^i \nmid n$. Hence, $n \equiv 2^{i-1} \mod 2^i$, so that n is covered again by $mathcalC_j$.

We have thus proven that $\mathcal{C}_j$ is a covering system. Clearly, its list of moduli is the one prescribed in the statement of the theorem. Lastly, $\mathcal{C}_j$ is a minimal covering system: the arithmetic progressions $2^{i-1} \mod 2^i$ with $i = 1, \ldots, j-3$ are disjoint and cover exactly the integers not divisible by 2^{j-3}. On the other hand, the arithmetic progressions A_0,A_1,A_2 are disjoint and are all needed to cover the integers in $0 \mod 2^{j-3}$. This completes the proof of the proposition. □

Chapter 2

Structure and symmetry in covering systems

2.1. Some examples of covering systems

In this section we will look at a few examples of covering system of multiplicity 1. We start off showing a useful result that gives a simple algorithm which allows to verify if a set of arithmetic progressions is a covering system in a fairly easy way. We first need to define the least common multiple of a covering system. This definition will come back a lot, and it is one of the principal invariants of a covering system that we will use to study them.

Definition 2.1. Let

$$C = \{a_1 \pmod{m_1}, ..., a_k \pmod{m_k}\}$$

be a set of arithmetic progressions. We define the *least common multiple of* C to be the lcm of the moduli in C, that is

$$\operatorname{lcm}(C) = \operatorname{lcm}(m_1, m_2, ..., m_k).$$

We are now ready to give an easy to use criterion to verify if a set of arithmetic progressions is a covering system. Since all the moduli in a covering system divide the lcm of the covering system, a set of arithmetic progressions covers all integers if it covers all integers modulo the lcm. We give the following proposition as a rigorous way to use the above discussion in practice.

Proposition 2.1. *Let*

$$C = \{a_1 \pmod{m_1}, a_2 \pmod{m_2}, ..., a_n \pmod{m_n}\}$$

be a set of arithmetic progressions, and let $M = \operatorname{lcm}(C)$*. Then* C *is a covering system if and only if there exists some interval of* M *consecutive integers that is covered by progressions in* C*.*

Proof. If C is a covering system, then any integer belongs to one of the arithmetic progressions in C, and so any interval of M consecutive integers is covered by C. In partiular, there exists one interval of M consecutive integers that are covered by progressions in C.

On the other hand, suppose there is some interval of M consecutive integers that is covered by arithmetic progressions in C, say $k+1$,$k+2$,...,$k+M$. We must show that any integer belongs to one of the arithmetic progressions in C. Take an integer a. Choose an integer ℓ so that $a-\ell M \in [k+1,k+M]$. By assumption, we know that $a-\ell M \equiv a_i \pmod{m)_i}$ for some arithmetic progression $a_i \pmod{m_i}$ in C. Since $m_i|M$, $a-\ell M \equiv a \pmod{m_i}$, hence $a \equiv a_i \pmod{m_i}$. This gives us the result. □

In practice, we will usually verify that any integer in $[1,M]$ is covered by some arithmetic progression in C. The following example illustrates the use of this lemma.

We now verify that

$$C = \{1 \pmod 2, 1 \pmod 3, 2 \pmod 4, 4 \pmod 8, 8 \pmod{12}, 0 \pmod{24}\},$$

the covering system used by Erdős in his proof, is indeed a covering system. Notice that the lcm of this set of arithmetic progressions is

$$M = \text{lcm}(C) = \text{lcm}(2,3,4,8,12,24) = 24,$$

and so by our previous lemma, to show that C is a covering system, it suffices to show that any integer in the interval [1,24] belongs to one of the above arithmetic progressions. Any odd integer in [1,24] is covered by 1 (mod 2). The even integers can then be split into those that are 0 (mod 4) and those that are 2 (mod 4). The arithmetic progression 2 (mod 4) takes care of half of these, and we are left with the integers $\equiv 0 \pmod 4$. We can split these into those that are 0 (mod 8) and those that are 4 (mod 8). Any integer that is $\equiv 4 \pmod 8$ is covered by 4 (mod 8), and so we are left to cover the integers that are 0 (mod 8). There are exactly 3 of these in [1,24], which are 8, 16, and 24. 8 is covered by 8 (mod 12), 16 is covered by 1 (mod 3) and 24 is covered by 0 (mod 24). We conclude that the set of arithmetic progressions used by Erdős is indeed a covering system of multiplicity 1. Since we showed earlier that it was minimal, it is in fact a minimal covering system of multiplicity 1.

Another way of using this lemma to show that a set of arithmetic progressions

$$C = \{a_1 \pmod{m_1},...,a_k \pmod{m_k}\}$$

is indeed covering is to write down all the integers in $[1, \text{lcm}(C)]$, and then cross out recursively all the integers congruent to $a_1 \pmod{m_1}$, then to $a_2 \pmod{m_2}$, all the way till $a_k \pmod{m_k}$. If all the integers in $[1, \text{lcm}(C)]$ are crossed out, then the set of arithmetic progressions is a covering system. Doing this can give us a good way to look at how a covering system covers step by step, as well as a good way to implement an algorithm to verify if sets of arithmetic progressions are covering systems. For example, we can illustrate via a graph how the above covering system covers.

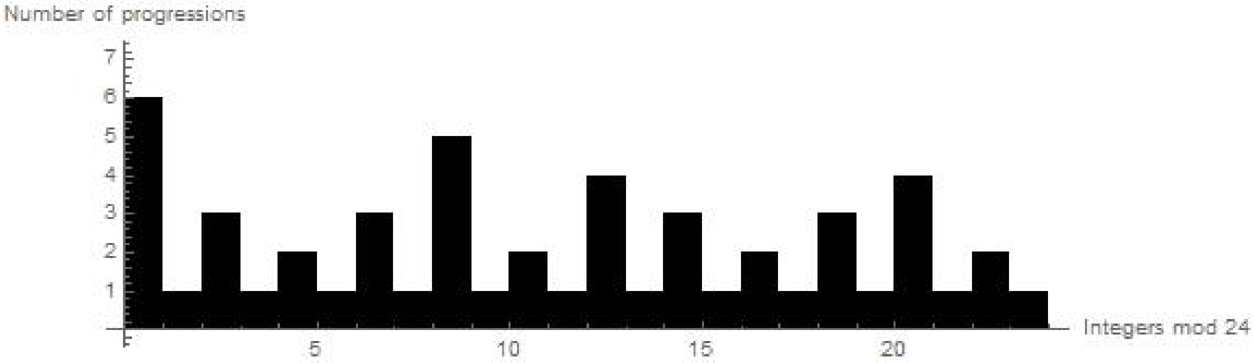


Fig. 2.1. Verifying that the set covers

In this figure, the lowest line shows all the integers modulo 24 as black squares, and the subsequent lines show in black the integers remaining after sieving out the first few arithmetic progressions. If the highest line in the graphic is all white, it means all the integers in our interval have been covered, and hence that our set of arithmetic progressions is a covering system.

The system used by Erdős in his proof is not the simplest covering system of multiplicity 1. Indeed, Krukenberg [**21**] showed that if the minimum modulus of a covering system of multiplicity 1 is 2, then the largest modulus is at least 12, and a widely known example of a covering system of multiplicity 1 with minimum modulus 2 and largest modulus 12 is

$$C = \{0 \pmod 2, 0 \pmod 3, 1 \pmod 4, 1 \pmod 6, 11 \pmod{12}\}.$$

We offer below a proof by graphic that this set of arithmetic progressions is indeed a covering system.

The last example of a covering system we look at here is the simplest square-free covering system of multiplicity 1. We first define what a square-free covering system is.

Definition 2.2. We say that a covering system C is *square-free* if all the moduli appearing in C are square-free.

As it is sometimes the case in number theory, where the square-free case of a problem is often simpler than the original problem, it turns out that the study of square-free covering systems is easier than that of general covering system.

A recently famous example of this that concerns covering systems is that of the Erdős-Selfridge problem. The first mention of this problem seems to be in 1965 [**13**], where Erdős asked if there exists a covering system of multiplicity 1 in which all the moduli are odd (and greater than 1). A few years later [**14**], Erdős went further and conjectured that there does

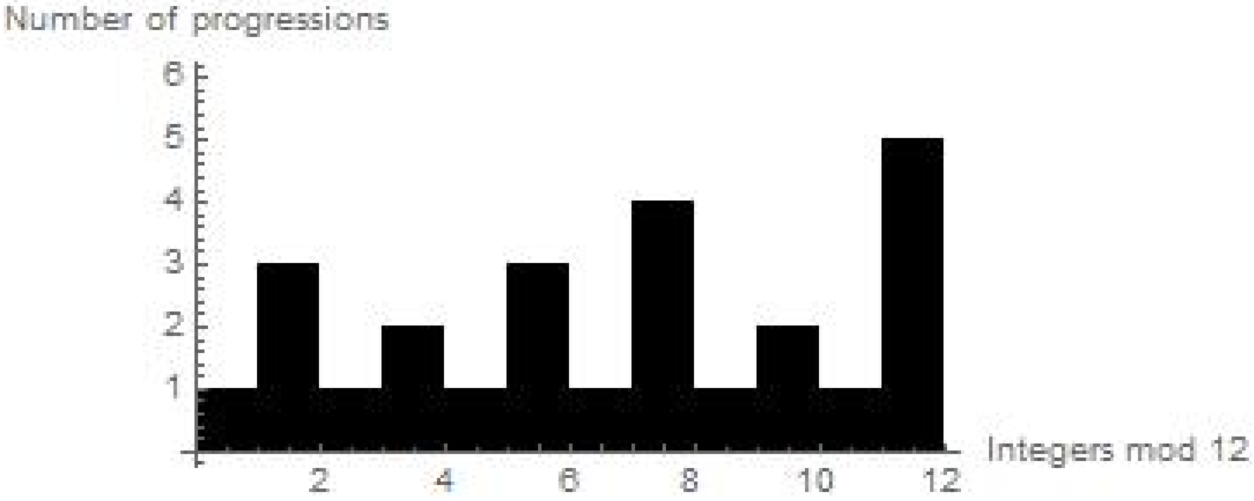


Fig. 2.2. Verifying that the set covers

in fact exist such a system. In 1977, Erdős went even further, and conjectured [**9**] that there exists square-free covering systems with the prime factors of the moduli arbitrarily large, which would imply the existence of a square-free covering system with only odd moduli. We know that the last conjecture is false, of course, by the solution to the minimum modulus problem.

Selfridge, on the other hand, believed that covering systems of multiplicity 1 with only odd moduli do not exist. This is perhaps why the problem has become known as the Erdős-Selfridge problem. In any case, it took until 2019 for a solution to this problem to come for the square-free case. In [**3**], Balister, Bollobás, Morris, Sarahsrabudhe and Tiba, building upon their methods in [**4**], showed that there cannot be a square-free covering system of multiplicity 1 with only odd moduli. The answer to the general Erdős-Selfridge problem, however, remains unknown.

For these reasons, we will direct most of our attention for the rest of this chapter to the study of square-free covering systems. We initiate this with our first example of a square-free covering system. As we will see, there are many covering systems with the set of square-free moduli

$$\{2,3,5,6,7,10,15,30,14,21,35,42,70,105\}.$$

Here is an example of one.

$$\begin{aligned} C = \{&0 \pmod 2, 0 \pmod 3, 0 \pmod 5, 1 \pmod 6, 0 \pmod 7, 1 \pmod{10}, \\ &8 \pmod{15}, 17 \pmod{30}, 1 \pmod{14}, 17 \pmod{21}, 19 \pmod{35}, 23 \pmod{42}, \\ &39 \pmod{70}, 104 \pmod{105}\}. \end{aligned} \tag{2.1.1}$$

We say one of the many because there exists more than one covering system with the same moduli as the above covering system. In fact, there are exactly 7,257,600 covering systems with these moduli. We have verified this using a computer. However, we will be proving this is the following sections, and in doing so will develop an approach to unravel patterns of symmetry and structure in square-free covering systems. The following graphic shows that the above set of arithmetic progressions is indeed a covering system.

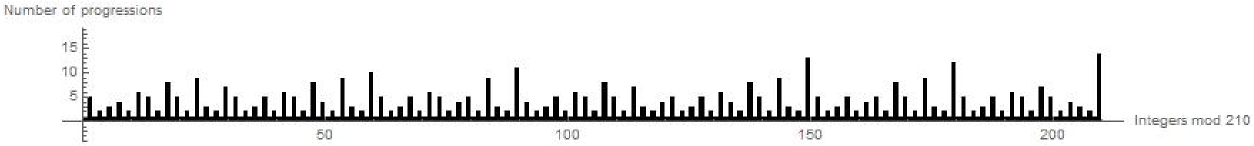


Fig. 2.3. Verifying that the set covers

Krukenberg [**21**] showed that if the smallest modulus in a square-free covering system of multiplicity 1 is 2, then the largest is at least 105. The above covering system shows that it is indeed possible to construct a square-free covering system of multiplicity 1 with minimum modulus 2 and largest modulus 105. In the following sections, we will work towards a new proof that this is the simplest square-free covering system of multiplicity 1, and use the results we build along the way to analyse other properties of this covering system and other covering systems that have similar structures. Later, we will show that all 7,257,600 covering systems with the moduli set above are minimal. In order to demonstrate that the naive argument for proving minimality gets quite complicated, we explain how it works in the case of the covering system 2.1.1. To show minimality, we give, for each $a \pmod{m}$ in C, an arithmetic progression modulo $210 = \text{lcm}(C)$ that belongs to that progression but no others in C. The notation used in this table is described in the following section.

2.2. The p-valuation and hyperplane notation

We introduce in this section here some notation that will be useful when dealing with square-free covering systems.

As in [**3**], we may view square-free covering system in a purely geometric way. Indeed, consider a covering system

$$C = \{a_1 \pmod{m_1}, ..., a_k \pmod{m_k}\},$$

with

$$\text{lcm}(C) = p_1 \cdots p_\ell.$$

Let $S_i = \{1, 2, ..., p_i\}$. We say that $(x_1, \ldots, x_\ell)$ is a *hyperplane* if $x_i \in S_i \cup \{\star\}$. This hyperplane is to be thought of as the arithmetic progression corresponding to the intersection of the

Table 2.1. Minimality of the square-free covering system

a (mod m)	Progression mod 210
(0)	(0,2,3,1)
($\star$,0)	(1,0,3,3)
(1,1)	(1,1,3,6)
($\star$, $\star$,0)	(1,2,0,5)
(1, $\star$,1)	(1,2,1,4)
($\star$,2,2)	(1,2,2,5)
(1,2,3)	(1,2,3,4)
($\star$, $\star$, $\star$,0)	(1,2,4,0)
(1, $\star$, $\star$,1)	(1,2,4,1)
($\star$,2, $\star$,2)	(1,2,4,2)
(1,2, $\star$,3)	(1,2,4,3)
($\star$, $\star$,4,4)	(1,2,4,4)
(1, $\star$,4,5)	(1,2,4,5)
($\star$,2,4,6)	(1,2,4,6)

arithmetic progressions x_i (mod p_i) for each $x_i \neq \star$, and $1 \leq i \leq \ell$. By the Chinese Remainder Theorem we may consider the covering system C as covering the set $S_1 \times S_2 \times \ldots \times S_\ell$ by hyperplanes. We say two hyperplanes $(x_1,\ldots,x_\ell)$ and $(y_1,\ldots,y_\ell)$ are *parallel* when $x_i = \star$ if, and only if, $y_i = \star$. In other words, parallel hyperplanes are hyperplanes for which the corresponding arithmetic progressions have the same modulus. A covering system of multiplicity 1 is then a covering by hyperplanes for which no two hyperplanes are parallel.

For practical purposes, as we will be using hyperplane notation to define covering systems, we will use the following slightly easier to work with notation for hyperplanes. Let p_j denote the j-th prime, so that $p_1 = 2$, $p_2 = 3$, etc.. We wish to construct a function that, for an arithmetic progression a (mod m) with square-free moduli, would give us the j-th coordinate of a (mod m) in hyperplane notation. To do so, we define the p-valuation of an arithmetic progression with square-free moduli.

Definition 2.3. Let a (mod m) be an arithmetic progression with m square-free. We will denote the *p-valuation* of a (mod m) to be

$$[a \text{ (mod } m)]_p := \begin{cases} \min\{n \in \mathbb{Z}_{\geq 0} : n \equiv a \text{ (mod } m)\} & \text{if p|m,} \\ \star & \text{if } p \nmid m. \end{cases}$$

Let p_k be the largest prime dividing m. We will denote

$$a \text{ (mod } m) = ([a \text{ (mod } m)]_2,[a \text{ (mod } m)]_3,\ldots,[a \text{ (mod } m)]_{p_k}).$$

For example, 0 (mod 2) = (0), 1 (mod 21) = ($\star$,1, $\star$,1) and 29 (mod 30) = (1,2,4).

Using this notation, we may rewrite the square-free covering system (2.1.1) described above in the following way.

$$\begin{aligned}C =&\{0 \pmod 2), 0 \pmod 3, 0 \pmod 5, 1 \pmod 6, 0 \pmod 7, 1 \pmod{10},\\ &8 \pmod{15}, 17 \pmod{30}, 1 \pmod{14}, 17 \pmod{21}, 19 \pmod{35}, 23 \pmod{42},\\ &39 \pmod{70}, 104 \pmod{105}\}\\ =&\{(0),(\star,0),(\star,\star,0),(1,1),(\star,\star,\star,0),(1,\star,1),(\star,2,3),(1,2,2),\\ &(1,\star,\star,1),(\star,2,\star,3),(\star,\star,4,5),(1,2,\star,2),(1,\star,4,4),(\star,2,4,6)\}.\end{aligned}$$

The usefulness of this notation will become clear once we start defining very large square-free covering systems of multiplicity 1.

2.3. Divisibility conditions on the moduli in covering systems

Notice that for the covering system

$$\begin{aligned}C =&\{0 \pmod 2, 0 \pmod 3, 0 \pmod 5, 1 \pmod 6, 0 \pmod 7, 1 \pmod{10},\\ &8 \pmod{15}, 17 \pmod{30}, 1 \pmod{14}, 17 \pmod{21}, 19 \pmod{35}, 23 \pmod{42},\\ &39 \pmod{70}, 104 \pmod{105}\},\end{aligned}$$

there are exactly seven moduli that are divisible by 7, and the 7-valuation of these moduli form a complete set of residues modulo 7. Also, if we look at the moduli that are divisible by 5, we also have that their 5-valuations contain a complete set of residues modulo 5, and the same happens when we look at the moduli divisible by 3, as well as those divisible by 2. We show here that this is a special case of a more general result. We first introduce the concept of relevant congruences for an arithmetic progression.

Definition 2.4. Let C be a set of arithmetic progressions, and p be a prime dividing $M = \operatorname{lcm}(C)$. We define the set of *relevant congruences* for the arithmetic progression $y \pmod p$ to be the set $C_p(y) := \{a \pmod m \in C : p|m, a \equiv y \pmod p\}$.

Why exactly we call this set the set of relevant congruences for the arithmetic progression $y \pmod p$ is because these are the congruences that intersect in a non-trivial manner with $y \pmod p$. The following lemma shows that the pattern we noted above is actually something that always happens in minimal covering systems.

Lemma 2.2. *Let C be a minimal covering system, let $M = \operatorname{lcm}(C)$, and let p be a prime dividing M. Then for each $y \in \{0,...,p-1\}$, $C_p(y)$ is non-empty.*

PROOF. Suppose that C is a covering system for which there is some prime $p|\operatorname{lcm}(C)$ and some integer $y \in \{0,1,\dots,p-1\}$ such that $C_p(y)$ is empty. We claim that $C' = \{a \pmod{m} \in C : p \nmid m\}$ is a covering system. Denote by $L = \operatorname{lcm}(C')$. To show that C' is a covering system, we will show that for each $n \in \{1,\dots,L\}$, there is a progression $a \pmod{m}$ in C' for which $n \equiv a \pmod{m}$. Indeed, fix $n \in \{1,\dots,L\}$. Since $C_p(y)$ is empty, we know that any integer congruent to $y \pmod{p}$ is covered by some progression in C'. In particular, the least non-negative integer that lies in the arithmetic progression $n \pmod{L} \cap y \pmod{p}$ is covered by some progression $a \pmod{m}$ in C'. However, since $p \nmid m$, this implies that $n \equiv a \pmod{m}$, and so n is covered by a congruence in C'. Since n can be any integer in $\{1,\dots,L\}$, we deduce the result. □

One consequence we find from this result is that if for some covering system C, there is some prime $p|\operatorname{lcm}(C)$ and some integer y for which $C_p(y)$ is empty, then C is not a minimal covering system. This will be useful to us later. Another corollary of this result is that if C is a minimal covering system, and $p|\operatorname{lcm}(C)$, then there are at least p arithmetic progressions in C whose moduli are divisible by p. This is a special case of a more general result of Krukenberg.

To show that the square-free covering system

$$\{0 \pmod{2}, 0 \pmod{3}, 1 \pmod{4}, 1 \pmod{6}, 11 \pmod{12}\}$$

is the simplest covering system of multiplicity 1 with minimum modulus 2, as well as many other similar results, Krukenberg [**21**] used the following theorem.

Theorem 2.3. *Let*

$$C = \{a_1 \pmod{m_1},\dots,a_k \pmod{m_k}\}$$

be a minimal covering system, and suppose $M = \operatorname{lcm}(C)$. *Let* p *be a prime that divides* M*, and suppose* p^α *is the largest power of* p *that divides* M. *If* β *is an integer such that* $1 \le \beta \le \alpha$*, then* p^β *divides at least* $p + (p-1)(\alpha - \beta)$ *distinct* m_i.

PROOF. Write $M = p^\alpha N$, with $(N,p) = 1$. Note that p^α must divide at least one modulus in C, say m_j with $j \in \{1,\dots,k\}$. By possibly reindexing the elements of C, we may assume that $j = 1$.

By minimality of our covering system, there is at least one integer $n \in [1,M]$ that is covered only by $a_1 \pmod{m_1}$, and not by any of the other arithmetic progressions in C. By translating our covering system by $-n$ if necessary, we may suppose $n = 0$, which gives us that $n \equiv 0 \pmod{p^\alpha}$ and $n \equiv 0 \pmod{N}$.

We claim that the residue class $0 \pmod{N}$ must then be covered only by arithmetic progressions with modulus divisible by p. Indeed, if there were some progression with modulus not divisible by p that intersects non-trivially with $0 \pmod{N}$, then the modulus would divide N, hence it would cover all of 0 (mod N), contradicting the fact that 0 is covered only by 0 (mod m_1) in C.

For the remainder of the proof we consider only the integers $\equiv 0 \pmod N$. We shift our attention towards how the congruence classes modulo p^α are covered within this class. The congruence classes $ip^{\alpha-1} \pmod{p^\alpha}$, for $i \in \{0,1,\ldots,p-1\}$, must be covered by progressions with modulus divisible by p^α, for or else the progression would cover all of 0 (mod p^α), contradicting our assumption about 0 (mod m_1), hence we must have at least p different classes divisible by p^α.

By a similar argument, all integers $x \equiv 0 \pmod{p^{\alpha-2}}$ such that $x \not\equiv 0 \pmod{p^{\alpha-1}}$ are covered by arithmetic progressions with moduli divisible by $p^{\alpha-1}$. Since $x \not\equiv 0 \pmod{p^{\alpha-1}}$, these arithmetic progressions must be distinct from the ones considered before. Hence, we have $p-1$ new arithmetic progressions whose moduli are divisible by $p^{\alpha-1}$. Continuing in this fashion, we find that there are disjoint sets $C_1,\ldots,C_\alpha \subset C$ such that all moduli in C_j are divisible by p^j and $|C_j| \geq 1_{j=\alpha} + p - 1$. To complete the proof, note that the set $\bigcup_{j\geq\beta} C_j$ contains $1 + (\alpha-\beta)(p-1)$ elements all of whose moduli are divisible by p^β. □

Remark 2.1. For the case $\beta = 0$, we recover the corollary of our lemma mentionned above.

2.4. How Krukenberg used the result

Krukenberg proved the above result in order to show that if the minimum modulus of a covering system is 2, then the largest is at least 12, and similar results when the minimum modulus is 3 or 4. We include the proof in the case of the minimum modulus 2 here.

We first start by proving a crucial corollary of Krukenberg's result.

Proposition 2.4. *Let C be a minimal covering system, and let p be a prime. Suppose the largest modulus in C is m. If $(p+1)p^a > m$, then p^a is not a divisor of any modulus in C.*

Proof. The first two positive integers divisible by p^{a+1} are p^{a+1} and $2p^{a+1}$. Since $m_k < (p+1)p^a < 2p^{a+1}$, Theorem 2.3 gives us that p^{a+1} cannot divide any modulus in the covering system. Therefore, the first p available moduli divisible by p^a are $p^a, 2p^a, \ldots, (p+1)p^a$. However, $(p+1)p^a > m_k$, hence we cannot have p moduli divisible by p^a, and so by Theorem 2.3, p^a is not a divisor of any modulus in C. This gives us the result. □

Using this result, we can now show Krukenberg's result about the minimum modulus 2 problem.

Proposition 2.5. *If the smallest moduli in a covering system of multiplicity 1 is* 2*, then the largest moduli is at least* 12.

Proof. Suppose it is not. Then the largest is lesser than or equal to 11. Note that $(11+1)\cdot 11 > 11$, hence 11 cannot be in the cover, and any divisors of it either. Similarly, $(7+1)\cdot 7 > 11$, $(5+1)\cdot 5 > 11$, and $(3+1)\cdot 3 > 11$, and $(2+1)\cdot 2^2 > 11$, hence no moduli divisible by 3,4,5,7 can be used in the covering system. Only 2 remains as a possible modulus in our covering system, and clearly we cannot cover the integers with a single arithmetic progression modulo 2. This gives us the result. □

A similar reasoning gives us that if the minimum modulus is 3, then the largest is at least 36, and if the minimum modulus is 4, then the largest is at least 120. The details in these proofs, however, are not of interest to what we will be doing henceforth, and so we do not include the proofs of these results here.

2.5. The number of covering systems with a prescribed set of moduli

In [**3**], Balister, Bollobás, Morris, Sahasrabudhe, and Tiba study the number of covering systems with exactly n moduli. In the following sections, we study a related problem.

Question 2.1. If E is a multiset of moduli, how many covering systems can we construct whose multiset of moduli is precisely E?

To work towards an answer to this question, we use the following definitions that will make the rest easier to read.

Definition 2.5. Let E be a multiset of integers. We define $\eta(E)$ to be the set of covering systems whose multiset of moduli is E, and $H(E) := |\eta(E)|$. By a slight abuse of notation, if C is a covering system, we define $\eta(C)$ to be the set of covering systems with exactly the same moduli as C, and $H(C) := |\eta(C)|$. We also define $\eta^*(E)$ to be the set of minimal covering systems in $\eta(E)$, $H^*(E) := |\eta^*(E)|$, $\eta^*(C)$ to be the set of minimal covering systems in $\eta(C)$, and $H^*(C) := |\eta^*(C)|$.

Let us look at some examples of this.

Example 2.1. If $E = \{2,2\}$, then $H(E) = 1$. If $E = \{2,3,4,6,12\}$, a quick check with a computer shows that $H(E)$=24. Note that $\mathrm{lcm}(E) = 12$, and that $12|24$. We will see shortly that this is not a coincidence. Finally, if $E = \{2,3,5,6,7,10,15,30,14,21,35,42,70,105\}$, we have mentionned above that $H(E) = 7{,}257{,}600$. Notice here also that $2\cdot 3\cdot 5\cdot 7|H(E)$. Once again, this is not a coincidence.

To study $H(E)$, we will see that it is useful to look at automorphisms of $\eta(E)$. This leads us to look at ways to transform a covering system with a given set of moduli into another one with the same set of moduli. One very natural way to do this is to look at translations of covering systems. We will in fact be using translations in our proof of Theorem 1.5, and it is through studying these that we came with the results that follow in this section.

Definition 2.6. Let

$$C = \{a_1 \pmod{m_1}, a_2 \pmod{m_2}, ..., a_n \pmod{m_n}\}$$

be a covering system. We define the translate of C by t to be

$$C + t := \{a_1 + t \pmod{m_1}, a_2 + t \pmod{m_2}, ..., a_n + t \pmod{m_n}\}.$$

It is easy to see that the translate of a covering system is also a covering system. We now show how different translations induce different covering systems, and how certain translations yield the same covering systems.

Lemma 2.6. *Let C be a covering system of multiplicity 1, let $M = \text{lcm}(C)$, and let t_1,$t_2 \in \mathbb{Z}$. We have that $C + t_1 = C + t_2$ if, and only if, $t_1 \equiv t_2 \pmod{M}$.*

Proof. If $t_1 \equiv t_2 \pmod{M}$, then clearly $C + t_1 = C + t_2$. Let us now prove the converse. It suffices to show that if $t_1 \not\equiv t_2 \pmod{M}$, then $C + t_1 \neq C + t_2$. If $t_1 \not\equiv t_2 \pmod{M}$, then there is some prime power $p^\alpha \| M$ for which $t_1 \not\equiv t_2 \pmod{p^\alpha}$. Since p^α is the highest power of p that divides M, there must be some arithmetic progression $a \pmod{m}$ in C for which $p^\alpha | m$, for p^α would not divide M if this were not the case. For this progression, we have that $a + t_1 \not\equiv a + t_2 \pmod{m}$. Since we supposed all the moduli were distinct, this gives us that $C + t_1 \neq C + t_2$. □

Using these results, we can now prove that the observation we made earlier that $12|24$ is indeed a general phenomenon.

Proposition 2.7. *Let E be set of moduli, and $M = \text{lcm}(E)$. Then $M|H(E)$.*

Proof. Define an equivalency relation on $\eta(E)$ by $C \sim C'$ if there exists some integer k for which $C = C' + k$. By our previous Lemma, the equivalency classes each have cardinality M, hence $M|H(E)$. □

Another very natural operation that we may perform on a covering system is a dilation of it.

Definition 2.7. Let

$$C = \{a_1 \pmod{m_1}, a_2 \pmod{m_2}, \ldots, a_n \pmod{m_n}\}$$

be a covering system. For any integer λ, we define the *dilation* of C by λ to be

$$\lambda C := \{\lambda a_1 \pmod{m_1}, \lambda a_2 \pmod{m_2}, \ldots, \lambda a_n \pmod{m_n}\}.$$

Unlike for translations, not any dilation of a covering system gives us another covering system. The following propositions shows us when it is.

Proposition 2.8. *Let C be a covering system, and $M = \operatorname{lcm}(C)$. Whenever $(\lambda,M) = 1$, λC is a covering system.*

Proof. Let $b \in \mathbb{Z}$. We wish to find some $\lambda a \pmod{m} \in \lambda C$ such that $b \equiv \lambda a \pmod{m}$. Since $(\lambda,M) = 1$, $(\lambda,m) = 1$ for all moduli m in C. We know that there is some $a \pmod{m}$ in C such that $\lambda^{-1}b \equiv a \pmod{m}$, and so $b \equiv \lambda a \pmod{m}$, hence b is covered in λC. As b was an arbitrary integer, we deduce that all integers must be covered. □

We can now prove that λC is a covering system only if $(\lambda,M) = 1$. However, in the case of this result, we need minimality. Indeed, if we did not have minimality, we could construct a counter-example, by taking a minimal covering system C, then adding in a modulus coprime to all the moduli is C, and then dilating out by one of the new primes that we introduced with our extra coprime modulus. In light of this observation, we show the following result.

Proposition 2.9. *Let C by a minimal covering system, and let $\operatorname{lcm}(C) = M$. If $(\lambda,M) > 1$, then λC is not a covering system.*

Proof. Suppose by contradiction that this is not the case. Then there exists a minimal covering system C with $\operatorname{lcm}(C) = M$, and an integer λ with $(\lambda,M) > 1$, such that λC is a covering system. Let $p_1, \ldots, p_k$ be the distinct prime divisors of M that divide λ. Since $(\lambda,M) > 1$, we know that such primes exist, that is that $k \geq 1$.

Let p denote one of the p_i, $i \in \{1, \ldots, k\}$. We will look at what happens to the sets $C_p(y)$ when we dilate by λ. Since $p|\lambda$, these sets are all sent onto a new set $(\lambda C)_p(0)$, and so $(\lambda C)_p(1)$, for example, must be empty. By our arguments about the non-emptiness of $C_p(y)$ in the proof of Lemma 2.2, we know that this implies that the prime p is redundant in λC, that is we can remove all moduli divisible by p, and λC will remain a covering system.

Doing this over each of the p_i, $i \in \{1, \ldots, k\}$, we find a new covering system D with $\operatorname{lcm}(D)$ not divisible by any of the p_i's. Let $j = \lambda/(\lambda,M)$. Notice that $(\operatorname{lcm}(D),j) = 1$, hence j is invertible modulo $\operatorname{lcm}(D)$. Let j^{-1} denote it's inverse.

Then $j^{-1}D$ is also a covering system. However, notice that by construction, it is a proper subcover of C, contradicting the minimality of C. We deduce the result. $\square$

From these two lemma, we may deduce the following result.

Lemma 2.10. *Let C be a minimal square-free covering system of multiplicity 1, let $M = \mathrm{lcm}(C)$, and let $\lambda_1,\lambda_2 \in \mathbb{Z}$. Suppose $(\lambda_1\lambda_2,M) = 1$. Then $\lambda_1 C = \lambda_2 C$ if, and only if, $\lambda_1 \equiv \lambda_2 \pmod{M}$.*

Proof. If $\lambda_1 \equiv \lambda_2 \pmod{M}$, then clearly $\lambda_1 C = \lambda_2 C$. We are left to prove to converse. Suppose $\lambda_1 \not\equiv \lambda_2 \pmod{M}$. Then there is some prime $p|M$ such that $\lambda_1 \not\equiv \lambda_2 \pmod{p}$. By minimality of C, we know that $C_p(1)$ is non-empty, hence there is some congruence $a \pmod{m}$ in C such that $p|m$ and $a \not\equiv 0 \pmod{p}$. Then $\lambda_1 a \not\equiv \lambda_2 a \pmod{m}$, hence $\lambda_1 C \neq \lambda_2 C$. $\square$

We are now ready to prove another proposition about $H^*(E)$.

Proposition 2.11. *Let E be a set of square-free integers that are greater than 1, and let $M = \mathrm{lcm}(E)$. Then $\phi(M)|H^*(E)$.*

Proof. Define an equivalency relation on $\eta^*(E)$ by $C \sim C'$ if there exists some integer λ, with $(\lambda,M) = 1$, such that $C = \lambda C'$. By the previous lemma, this partitions $\eta^*(E)$ into sets of size $\phi(M)$, hence the result. $\square$

We saw in this section that we can translate and dilate covering systems to create new covering systems with the same set of moduli. This leads us to the following question.

Question 2.2. What other operations can we perform on covering systems that give us other covering systems with the same set of moduli?

The aim of the following sections will be to answer this question.

2.6. Generalising a result of Hammer, Harrington and Marotta

In this section we will look at an operation we can perform on covering systems that can be seen in some sense as the most basic operation that can be performed on all covering systems. We will see in the following sections that translations and dilations are special cases of this operation. We will start by looking at a lemma from Hammer, Harrington and Marotta [**17**]. It is by looking for a generalisation of this lemma that the ideas that follow came.

Lemma 2.12. *Let C be a covering system, $M = \operatorname{lcm}(C)$, and p be a prime that divides M. Let a_1,a_2 be integers, with $0 \leq a_1$,$a_2 \leq p-1$. Suppose that $a_2 \pmod p$ is in C, but that $a_1 \pmod p$ is not. Then there exists a covering system C' with the following properties :*

(1) C' has the same moduli as C,

(2) $a_1 \pmod p$ is in C',

(3) $a_2 \pmod p$ is not in C',

(4) If $a \pmod p$ is in C, with $a \not\equiv a_2 \pmod p$, then $a \pmod p$ is in C',

(5) Any arithmetic progression with modulus coprime to p in C is also in C'.

Proof. Let
$$T = C_p(a_1) = \{a \pmod m \in C : p|m, a \equiv a_1 \pmod p\}.$$
Write $M = p^t N$, with $p^t \| M$. Since $(N,p) = 1$, N is invertible modulo p, and so we may choose an integer k such that
$$kN \equiv a_2 - a_1 \pmod p.$$
Let
$$T' = \{a + kN \pmod m : a \pmod m \in T\}.$$
We claim that
$$C' = \left(C \setminus (T \cup a_2 \pmod p)\right) \cup a_1 \pmod p \cup T'$$
is a covering system. Since C is a covering system, we need to show that what was covered by $T \cup a_2 \pmod p$ is now covered by either $C \setminus (T \cup a_2 \pmod p)$ or by $a_1 \pmod p \cup T'$. By what we noticed about T and $a_1 \pmod p$, we know that whatever was covered by T is now covered by $a_1 \pmod p$. We are left to find what covers $a_2 \pmod p$ in C'.

Let b be an integer such that $b \equiv a_2 \pmod p$. Since C is a covering system, we know that $b - kn \equiv a \pmod m$ for some $a \pmod m \in C$. Then $b \equiv a + kN \pmod m$. If $p \nmid m$, then $a + kN \equiv a \pmod m$, as $m|N$, and so b is still covered in C'. If $p|m$, then $a \pmod m \in T$, and so $a + kN \in T'$, and so b is also still covered in C'. We deduce that C' is a covering system. It is easy to see from the definition of C' that it satisfies the conditions in the lemma, and so we have the result. □

This lemma seems generalisable, and indeed we will see that it is. We would like to be able to change $a \pmod m$ for $a' \pmod m$ in any covering system C, where m is not necessarily prime, while changing as little as possible on the rest of the covering system. However, there need to be restrictions on when and how we can do this, as we will see.

To do so, we make use of the following lemma, which is a very slight generalisation of the previous one, but as we will see it leads us exactly to the generalisation we are looking for. Notice while looking at the proof that it is almost exactly the same as that of the previous lemma.

Lemma 2.13. *Let C be a covering system, $M = \operatorname{lcm}(C)$, and p be a prime dividing M. Let $0 \leq a_1 < a_2 \leq p-1$ be integers, and for $\alpha \in \{0,1,\ldots,p-1\}$, let*

$$C_p(\alpha) = \{a \pmod{m} \in C : p|m, a \equiv \alpha \pmod{p}\}.$$

Let t be an integer such that $t \equiv 1_{q=p} \cdot (a_2 - a_1) \mod q^{v_q(M)}$ for every prime $q|M$. Then

$$C' = \Big(C \setminus (C_p(a_1) \cup C_p(a_2))\Big) \cup (C_p(a_1) + t) \cup (C_p(a_2) - t)$$

is a covering system.

Remark 2.2. In the hyperplane notation for arithmetic progressions we introduced earlier, we have that the progressions in C' differ from those in C precisely when their p-valuation is either a_1 or a_2, and the operation we just described corresponds to changing the p-valuation of each progression in C with p-valuation a_1 to a_2, and similarly changing the p-valuation of each progression with p-valuation a_2 to a_1.

Proof. Let $b \in \mathbb{Z}$. If b is covered by

$$C \setminus (C_p(a_1) \cup C_p(a_2))$$

in C, then b is still covered in C'. If b is covered by $C_p(a_1)$ in C, we look at what covers $b+t$ in C. If it is covered by some element in $C \setminus (C_p(a_1) \cup C_p(a_2))$, then $b+t \equiv a \pmod{m}$, and $p \nmid m$. Indeed, if $p|m$, then $a \pmod{m}$ is in $C_p(a_2)$, which contradicts our assumption about $a \pmod{m}$. Hence $b+t \equiv b \pmod{m}$, and so b is covered by $a \pmod{m}$ in C'. If it was covered by some element in $C_p(a_2)$, then $b+t \equiv a_2 \pmod{m}$, and so $b \equiv a_2 - t \pmod{m}$, which is in $C_p(a_2) - t$, and so b is still covered in C'.

We now look at the mirror case, that is if b is covered by $C_p(a_2)$. We look at what covers $b-t$ in C. If it is in $C \setminus (C_p(a_1) \cup C_p(a_2))$, then by our previous argument, it is still covered in C'. If it is covered by some congruence in $C_p(a_1)$, then $b-t \equiv a \pmod{m}$, and so $b \equiv a+t$, hence b is covered by $C_p(a_1)+t$ in C'. Since b was an arbitrary integer, we deduce that C' is a covering system. □

We now look at a couple of examples of this lemma. First off, consider the covering system discussed earlier

$$C = \{0 \pmod{2}, 0 \pmod{3}, 1 \pmod{4}, 1 \pmod{6}, 11 \pmod{12}\}.$$

Take 3 as our prime, and take $a_1 = 1$ and $a_2 = 2$. Then

$$C_3(1) = \{a \pmod{m} \in C : 3|m, a \equiv 1 \pmod{3}\} = \{1 \pmod{6}\},$$

and

$$C_3(2) = \{a \pmod{m} \in C : 3|m, a \equiv 2 \pmod{3}\} = \{11 \pmod{12}\}.$$

We have that $\mathrm{lcm}(C) = 12$, and we can write it as $3^1 \cdot 4$. We then have that there is some integer k, namely $k = 1$, such that $4k \equiv a_2 - a_1 \pmod 3$. Indeed, $a_2 - a_1 \equiv 2 - 1 \equiv 1 \pmod 3$, and $4 \cdot 1 \equiv 4 \equiv 1 \pmod 3$. We can then take $t = 4$ in our lemma, and so we replace $1 \pmod 6$ by $5 \pmod 6$ and $11 \pmod{12}$ by $7 \pmod{12}$. Our lemma guarantees that this is a covering system.

Our next example will deal with the square-free covering system

$$\begin{aligned} C =& \{0 \pmod 2, 0 \pmod 3, 0 \pmod 5, 1 \pmod 6, 0 \pmod 7, 1 \pmod{10}, \\ & 8 \pmod{15}, 17 \pmod{30}, 1 \pmod{14}, 17 \pmod{21}, 19 \pmod{35}, \\ & 23 \pmod{42}, 39 \pmod{70}, 104 \pmod{105}\} \\ =& \{(0),(\star,0),(\star,\star,0),(1,1),(\star,\star,\star,0),(1,\star,1),(\star,2,3),(1,2,2), \\ & (1,\star,\star,1),(\star,2,\star,3),(\star,\star,4,5),(1,2,\star,2),(1,\star,4,4),(\star,2,4,6)\}. \end{aligned}$$

We will see here why the hyperplane notation for square-free arithmetic progressions comes in handy. In terms of this notation, our lemma can be seen as choosing some coordinate of our hyperplane, say the third, which corresponds to the prime 5, then choose two residues modulo 5, say 1 and 2. We then replace all the progressions which have a 1 in the third component by the same hyperplane with 1 replaced by 2, and all those with a 2 in the third component by the same hyperplane with a 2 replaced by a 1. The lemma says that this remains a covering system. Indeed, translating out by t in our lemma can be seem as simply switching the residues modulo p without changing the residues modulo any other prime, which corresponds to changing the residues modulo p, and that is exactly what we described above.

For our example, take $p = 5$, $a_1 = 1$ and $a_2 = 4$. Then $C_5(1)$ is the set of progressions that have a 1 as their third component, and $C_5(4)$ is the set of progressions that have a 4 as their third component. Hence

$$C_5(1) = \{(1,\star,1)\},$$

and

$$C_5(4) = \{(\star,\star,4,5),(1,\star,4,4),(\star,2,4,6)\}.$$

Our new sets are

$$C_5(1) + t = \{(1,\star,4)\}$$

and

$$C_5(4) - t = \{(\star,\star,1,5),(1,\star,1,4),(\star,2,1,6)\}.$$

The lemma guarantees that the covering system C' which replaces our $C_5(1)$ by $C_5(1) + t$ and $C_5(4)$ by $C_5(4) - t$ is indeed a covering system. This example perfectly illustrates the usefullness of the hyperplane notation for arithmetic progressions. It makes using the lemma easier.

2.7. The p-automorphisms of covering systems

We start out this section with a lemma that looks at how to apply Lemma 2.13 successively.

Lemma 2.14. *Let C be a minimal covering system. Let $M = \mathrm{lcm}(C)$, and let p be a prime that divides M. Let σ be a permutation in S_p. Then there is a unique covering system $C' \in \eta(C)$ such that :*

(1) For each $y \in \{1, \ldots ,p\}$, $C'_p(y) = C_p(y) + t$, where $t \equiv 1_{q=p}(\sigma(y) - y) \pmod{q^{\nu_q(M)}}$ for each prime $q|M$,

(2) If $a \pmod m$ is an arithmetic progression in C and $(m,p) = 1$, then $a \pmod m$ is also in C'.

Proof. By Proposition 0.1, there exists some transpositions $\tau_1, \ldots ,\tau_k \in S_p$ such that $\sigma = \tau_1 \cdots \tau_k$. For $i \in \{1, \ldots ,p\}$, we may write $\tau_i = (n_{i,1}n_{i,2})$. Note that since C is minimal, we have that $C_p(y)$ is non-empty for each prime $p|M$ and $y \in \{1, \ldots ,p\}$. We may then apply Lemma 2.13 onto C with $a_1 = n_{1,1}$ and $a_2 = n_{1,2}$. Call the resulting covering system C_1. We then apply Lemma 2.13 onto C_1 with $a_1 = n_{2,1}$ and $a_2 = n_{2,2}$. Call the resulting covering system C_2. In general, let C_j be the covering system we get after doing this process j times, using the lemma on C_{l-1} with $a_1 = n_{\ell,1}$ and $a_2 = n_{\ell,2}$ at step ℓ, for $1 \leq \ell \leq j$. We claim that $C' := C_k$ respects (a) and (b).

At each application of the lemma, we only change arithmetic whose moduli are divisible by p, hence C' has property (b). For property (a), we look at what happens to a specific $C_p(y)$ after the multiple applications of the lemma. Note that since $\tau_1 \cdots \tau_k = \sigma$, we have that $C_p(y)$ is sent on to a corresponding set of arithmetic progressions for which the residue mod p is $\sigma(y)$, and the residues modulo any other prime are left unchanged. This is exactly what property (a) describes, hence (a) is also satisfied by C'. The fact that C' is unique follows from the fact that we describe exactly what happens to each progression in C to get C'. We deduce the result. □

Remark 2.3. Notice that if C is a covering system of multiplicity 1, and if σ is not the identity in S_p, then the C' we find in Lemma 2.14 is distinct from C, and so by applying the lemma with all permutations in S_p, we get $p!$ different covering systems. Doing this for all the distinct prime divisors $p_1, \ldots ,p_\ell$ of M, we get $p_1! \cdots p_\ell!$ different covering systems.

Definition 2.8. Let C be a minimal covering system, and let $M = \mathrm{lcm}(C)$. Let p be a prime such that $p|M$, and let $\sigma \in S_p$. We define the *p-automorphism* of C for the permutation σ to be the covering system C' described in the above lemma, and we denote it by $T_{p,\sigma}(C)$.

Proposition 2.15. *Let E be a set of positive integers that are greater than 1, and let*

$$\operatorname{lcm}(E) = M = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$$

be the prime factorisation of M, with $p_1 < \ldots < p_\ell$. Then

$$p_1!p_2! \cdots p_\ell! | H^*(E).$$

Proof. Define an equivalency relation on $\eta^*(E)$ by $C \sim C'$ if there exists some p-automorphisms T_{p_1,σ_1}, $T_{p_2,\sigma_2}, \ldots, T_{p_\ell,\sigma_\ell}$ such that

$$C' = T_{p_1,\sigma_1} \circ T_{p_2,\sigma_2} \circ \cdots \circ T_{p_\ell,\sigma_\ell}(C).$$

This partitions $\eta^*(E)$ into sets of size $p_1! \cdots p_\ell!$, hence the result. □

This leads us to a few questions :

(1) Are there sets E for which $H(E)$ is equal to $p_1! \cdots p_\ell!$, where $\operatorname{lcm}(E) = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$?

(2) Are there sets E for which $H(E)$ is greater than $p_1! \cdots p_\ell!$, where $\operatorname{lcm}(E) = p_1^{\alpha_1} \cdots p_\ell^{\alpha_\ell}$?

(3) Does there exist a set of moduli E for which there are both minimal and non-minimal covering systems with this set of moduli?

We already noted that for the set

$$E = \{2,3,4,6,12\},$$

$H(E) = 24$, whereas $\operatorname{lcm}(E) = 12 = 2^2 \cdot 3$, so $2!3! = 12 < 24$. However, we may still wonder if this can happen if E is instead a set of square-free integers. In the following sections, we will show that there are infinitely many square-free sets E that respect (a), as well as infinitely many that respect (b).

Note that in the case (b), we can in fact construct sets of square-free integers for which $H(E)$ is an arbitrarily large multiple of $p_1! \cdots p_\ell!$, where $\operatorname{lcm}(E) = p_1 \cdots p_\ell$. We will mention how to construct such sets at the end of the chapter.

Finally, we give a lemma that hints towards a possible answer to question (c).

Lemma 2.16. *Let C be a covering system, let $M = \operatorname{lcm}(C)$, and let p be a prime dividing M. Let σ be a permutation in S_p. If C is a minimal covering system, then $T_{p,\sigma}(C)$ is also minimal.*

Proof. Suppose by contradiction that there is some minimal covering system C and some that does not satisfy this condition, so that there is some $p| \operatorname{lcm}(C)$, and some $0 \leq x < y \leq p-1$ such that the covering system

$$D = T_{p,(xy)}(C)$$

is not minimal. Since D is not minimal, there exists some proper subcover of D, call it D'. Then $T_{p,(xy)}(D')$ is a proper subcover of C, contradicting the fact that C was minimal. We deduce the result. □

Note that this lemma is very interesting on its own. Since

$$T_{p,(xy)}(T_{p,(xy)}(C)) = C,$$

it in fact shows that a covering system is minimal if and only if $T_{p,((xy)}(C)$ is, for all appropriate p,x,y. It also says that the minimal covering systems with a given set of moduli E group together through our p-automorphisms. So if E is a set of integers, with $\mathrm{lcm}(E) = p_1^{\alpha_1}...p_\ell^{\alpha_\ell}$, then $p_1! \cdots p_\ell!$ divides not only $H(E)$, but also $H^*(E)$. It remains unclear, for now, if for some set E, there can be minimal covering systems with moduli set E, as well as non-minimal covering system with the same set of moduli. This remains a question we would like to find a solution to.

2.8. A square-free covering system

In this section, we show that the square-free covering system described earlier respects property (a) mentionned above. The following lemma shows an interesting property about how arithmetic progressions divisible by some prime p in a covering system tend to group into certain arithmetic progressions. Since we will only need the lemma for the square-free case, we will only prove it for the square-free case, but we note that it remains true even when we are dealing with covering systems that are not square-free.

Lemma 2.17. *Let C be a square-free covering system, and let $M = \mathrm{lcm}(C)$. Let p be some prime dividing M, $C_p = \{a \pmod{m} \in C : p|m\}$ and $N = M/p$. If some progression $b \pmod{N}$ is covered only by progressions in C_p, then for each $y \in \{0,1,\ldots,p-1\}$, there is an arithmetic progression in $C_p(y)$ that intersects with $b \pmod{N}$.*

Proof. Since the progressions in C_p cover all of $b \pmod{N}$, then at least one progression in C_p must intersect with $(y \pmod{p}) \cap (b \pmod{N})$. Since this progression is in C_p and it intersects with $y \pmod{p}$, it must in fact be in $C_p(y)$. □

We remind here that we proved earlier that each $C_p(y)$ is non-empty if C is a minimal covering system. We will use this result in the following lemma. For technical reasons, we first need to show that any covering system with moduli set

$$\{2,3,5,6,7,10,15,30,14,21,35,42,70,105\}$$

is minimal. This leads us to the following lemma.

Lemma 2.18. *If C is a covering system with moduli set*

$$E = \{2,3,5,6,7,10,15,30,14,21,35,42,70,105\},$$

then C is a minimal covering system.

Proof. Suppose by contradiction that this is not the case, so that there exists some covering system C with this set of moduli that is not minimal. Let D be a minimal proper subcover of C. Since there are exactly seven progressions with moduli divisible by 7 in C, or again that $|C_7| = 7$, by minimality of D and Lemma 2.2, we have two possible cases :

(1) All progressions in C_7 are in D

(2) No progressions in C_7 are in D.

In case (b), notice that there are only four moduli in C that are divisible by 5 but not by 7. Since D is minimal, if $5 | \operatorname{lcm}(D)$, then $|D_5| \geq 5$ or $|D_5| = 0$. Since it is impossible to have five progressions in D_5, we deduce that there must be none. The possible moduli in D are now reduced to those that are 3-smooth, that is $\{2,3,6\}$. Once again, there are only two moduli divisible by 3 here, hence there can not be any of those. Therefore, D can only have a single progressions modulo 2, and clearly this can not be a covering system. We deduce that case (b) is impossible.

We now direct our study towards case (a). Note that the set of progressions in D not divisible by 7, that is those that are 5-smooth, cover some set of residues modulo 30, and cannot cover them all by the minimality of D. We therefore have that the seven progressions in D_7 cover some arithmetic progressions modulo 30. By minimality of D, note that $D_7(a)$ is a singleton for each a. Furthermore, we know that all seven progressions in D_7 must intersect with any progression modulo 30 that they cover. However, by the Chinese Remainder Theorem, the progressions modulo $2 \cdot 7$ and modulo $15 \cdot 7$ can only intersect in one progression modulo 30, and so our seven progressions in D_7 can only cover one progression modulo 30. This implies that our 5-smooth arithmetic progressions must cover all twenty-nine others. However, we need all of the 5-smooth progressions to do this. Indeed, suppose we can do it with some proper subset of them. Taking one we do not have in our proper subset, we can cover the remaining progression modulo 30. But then, we would have a covering system with the 5-smooth moduli, which we showed was impossible when studying case (b). Therefore, D must have all the same arithmetic progressions as C, which contradicts the fact that D was a proper subcover. We deduce that all the covering systems with the set of moduli E are minimal. □

We are now ready to show that we have exactly 2!3!5!7! covering systems with the moduli set E as described above.

Proposition 2.19. *Let*

$$E = \{2,3,5,6,7,10,15,30,14,21,35,42,70,105\}.$$

Then $H(E) = 2!3!5!7!$.

Proof. Let C be the square-free covering system described above, that is

$$\begin{aligned} C =&\{0 \pmod 2, 0 \pmod 3, 0 \pmod 5, 1 \pmod 6, 0 \pmod 7, 1 \pmod{10},\\ &8 \pmod{15}, 17 \pmod{30}, 1 \pmod{14}, 17 \pmod{21}, 19 \pmod{35}, 23 \pmod{42},\\ &39 \pmod{70}, 104 \pmod{105}\}\\ =&\{(0),(\star,0),(\star,\star,0),(1,1),(\star,\star,\star,0),(1,\star,1),(\star,2,3),(1,2,2),\\ &(1,\star,\star,1),(\star,2,\star,3),(\star,\star,4,5),(1,2,\star,2),(1,\star,4,4),(\star,2,4,6)\}. \end{aligned}$$

Let C' be some covering system in $\eta(E)$. Note that by our previous lemma, C' is minimal. We will show that we can reach C from C' by a sequence of p-automorphisms. As there are exactly $2!3!5!7!$ such automorphisms, we will deduce the result.

We analyse the covering system prime by prime, starting with the prime 2. Whatever the progression modulo 2 we have in C', we can via a 2-automorphism bring it back to $0 \pmod 2$.

We then look at the prime 3. Via a 3-automorphism, we may suppose we have $0 \pmod 3$. Since p-automorphisms preserve minimality, we know that our progression modulo 6 has to be either $1 \pmod 6$ or $5 \pmod 6$. Via a 3-automorphism, we may suppose we have $1 \pmod 6$.

By minimality, all the remaining progressions must intersect with $5 \pmod 6$, which means that their 2-valuation (see definition 2.3) is either 1 or $\star$, and their 3-valuation is either 2 or $\star$.

We now look at the prime 5. The only thing we do not know about the new progressions introduced at this stage is their 5-valuation. However, we know that they must all have different 5-valuation. Indeed, they can each cover at most one of the remaining residues modulo 30, for all 5 residues left to cover modulo 30 are incongruent modulo 5, and if their 5-valuation were the same, they would cover the same residue, which would give us a non-minimal covering system where one could be removed. Hence they must all have different 5-valuation, and so via a series of 5-automorphisms we may suppose their 5-valuations are as in C.

Finally, we are left to deal with the prime 7. We introduce at this stage exactly 7 progressions, and they must all intersect with $29 \pmod{30}$ by minimality, hence they must cover $29 \pmod{30}$. By Lemma 2.17, we must therefore have that they all have a different 7-valuation, and that their 2,3 and 5-valuations are respectively either 1 or $\star$, 2 or $\star$ and 4 or $\star$. Via a series of 7-automorphisms, we may then suppose that their 7-valuations are exactly as in C. This gives us the result. □

We end this section with some graphs that show the structure of our covering system C and some of its p-automorphisms. We will construct the graphs prime by prime, and a branch that ends signifies that the arithmetic progression corresponding to the intersection of the different prime arithmetic progressions that compose its sub branches is covered.

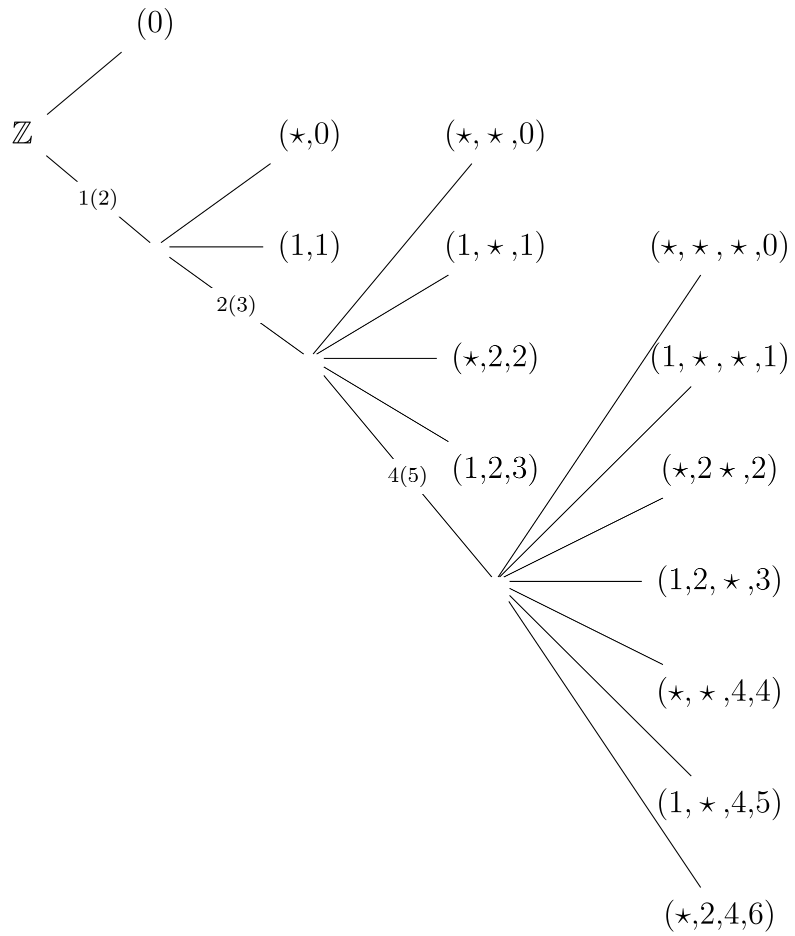


Fig. 2.4. A graph of the square-free covering system

We now discuss this graph a little. We wonder how the p-automorphisms will affect the structure of the branches. It turns out that they affects them in a very simple way. Applying the 2-automorphism $T_{2,(01)}$ onto C will simply switch how the two first branches cover, that is we will have the structure that covers 1 (mod 2) covers 0 (mod 2) instead, and the structure that covers 0 (mod 2) now cover 1 (mod 2) instead.

We can see that the structure of the covering system is, in essence, the same as before, just that the roles of 1 (mod 2) and 0 (mod 2) have been switched. This is exactly what the p-automorphisms do : they give us a new covering system, but the structure of the system remains essentially the same. If we were to look at 3-automorphisms of our covering system, the resulting graph would simply change the roles of the three branches modulo 3, and similarly if we were to look at 5-automorphisms and 7-automorphisms.

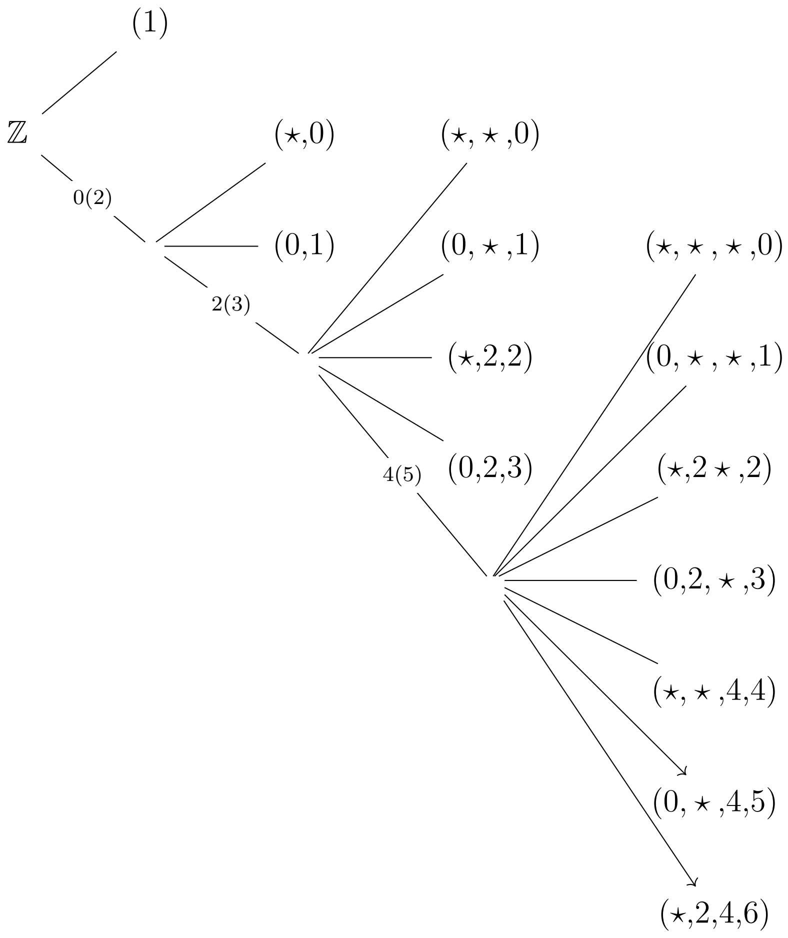


Fig. 2.5. A graph of $T_{2,(01)}(C)$

2.9. An infinite family of covering systems with the same property

In the previous section, we showed our covering system had the desired property. This property essentially came from the way our graph branches out in a nice way, as well as some technical features. We wish to reproduce this. Let p_k denote the k-th prime. The idea will be to construct covering systems whose corresponding graphs have a similar structure as the graph above. Notably we will, for $j \geq 4$, construct covering systems C^j that have

$$\operatorname{lcm}(C^j) = \prod_{k=1}^{j} p_k,$$

and such that their corresponding sets of moduli E^j have the property that

$$H(E^j) = H^*(E^j) = \prod_{k=1}^{j} p_k!.$$

We will construct these covering systems prime by prime, that is we look at the 2-smooth moduli, then the 3-smooth, and so on. We start with the case $j = 4$. Although the covering system we will construct will be precisely the square-free covering system we just talked about, it will be useful to look at how exactly we construct it to see how we will do it for the subsequent ones.

We start with the progression modulo 2. Since we know by a 2-automorphism that it does not really matter what we choose, we take (0). We then look at the 3-smooth moduli that have not been used yet, that is 3 and 6. We know that by a 3 automorphism it does not really matter what we take modulo 3, and so we take ($\star$,0). We want our covering system to be minimal, and so we are left with either (1,1) or (1,2) for our progression modulo 6. By a 3-automorphism, our choice does not really matter, so we take (1,1).

We now look at the 5-smooth moduli that are not 3-smooth. Since we want a minimal covering system, and we are left to cover 5 (mod 6), we note that the 3-valuation of any of these new progressions is either 2 or $\star$, and the 2-valuation of these is either 1 or $\star$. We therefore only have a choice on the 5-valuation of these progressions that are 5-smooth and divisible by 5. We are in fact even restricted among the 5-valuations : to have a minimal covering system, they must all be distinct, for if two were to have the same 5-valuation, then one of them would be redundant. By 5-automorphisms, our choice for the 5-valuations does not really matter. We therefore add in the progressions ($\star, \star$,0), (1, $\star$,1), ($\star$,2,2) and (1,2,3). We are left to cover (1,2,4).

To do this, we take seven progressions divisible by 7. By a similar reasoning as with the moduli divisible by 5 that were 5-smooth, the only choice we have for these progressions is their 7-valuation. By p-automorphisms, it does not matter which progression divisible by 7 takes which 7-valuation, hence taking the progressions ($\star, \star$, $\star$,0),(1, $\star$, $\star$,1),($\star$,2, $\star$,3), ($\star, \star$,4,5),(1,2, $\star$,2),(1, $\star$,4,4),($\star$,2,4,6) gives us our covering system.

Note that we proved in the previous section that this covering system C^4 satisfies our desired property. We now construct C^5.

To do so, we take the same progressions as in C^4, except for the last one we added in, in this case ($\star$,2,4,6). We are now left to cover the progression (1,2,4,6). To do so, we use progressions that are divisible by 11. We have access to sixteen of these, but we only need eleven for our covering system. We choose any of these sixteen for our eleven, so long as their are 2 of the progressions $a_1 \pmod{m_1}$ and $a_2 \pmod{m_2}$ such that $m_1 m_2 = 11^2 \cdot 2 \cdot 3 \cdot 5 \cdot 7$. This is a technical detail that makes our proof much easier, and it can easily be done. We then have a covering system, if each of the eleven new progressions has a different 11-valuation, which we take to be the case. We then construct our C^j, for $j \geq 6$, inductively.

Suppose C^{j-1} is defined. We define C^j as follows. First take C^{j-1} and remove the progression that is divisible by p_{j-1} and has p_{j-1}-valuation $p_{j-1} - 1$. Then take any p_j of the

2^{j-1} square-free moduli available that are divisible by p_j, so long as there are two of them, $a_1 \pmod{m_1}$ and $a_2 \pmod{m_2}$, that have the property that $m_1m_2 = p_j^2 \cdot P_{j-1}$.

We now need to choose a residue for each of these p_j moduli. For each of these moduli m, we take their p_k-valuation to be $p_k - 1$ if $k < j$ and $p_k|m$, and $\star$ if $p_k \nmid m$. We then take any p_j-valuation for them, so long as they are all distinct. This gives us a covering system. Indeed, let us prove that any sequence C^j of covering systems constructed in this way are indeed covering systems. Before delving into the proof, let us first look at the key properties of our C^j's.

(1) C^j has exactly p_j moduli divisible by p_j,
(2) The p_j-valuation of these arithmetic progressions form a complete set of residues modulo p_j,
(3) The p_k-valuation of these arithmetic progressions is either $\star$ or $p_k - 1$, for $1 \le k < j$,
(4) There are at least two moduli divisible by p_j with product $p_j^2 \cdot P_{j-1}$.

With this in mind, let us show that our C^j are indeed covering systems.

Proposition 2.20. *Any sequence of collections of arithmetic progressions C^j constructed as above are all covering systems.*

Proof. We prove the result by induction on $j \ge 4$. The case $j = 4$ is a covering system, as we have already verified. Suppose C^j is a covering system for some $j \ge 4$. We wish to prove that C^{j+1} is also a covering system. Note that when we remove the progression with modulus divisible by p_j and that has p_j-valuation $p_j - 1$, we are left with only the progression $(1,2,4,\ldots,p_i - 1,\ldots,p_j - 1)$ to cover. To cover this progression, we simply need p_{j+1} moduli divisible by p_{j+1}, that each have a different residue modulo p_{j+1}, but all intersect with $(1,2,4,...,p_i - 1,...,p_j - 1)$. This is exactly what we do in our inductive definition, hence we have a covering system. □

2.10. The covering systems C^j have the desired property

The goal of this section is to show that the covering systems C^j have moduli set E^j with

$$H(E^j) = \prod_{k=1}^{j} p_k!.$$

The proof will be quite similar to the proof for the case $j = 4$.

Lemma 2.21. *Let $\{C^j\}_{j\ge4}$ be a sequence of covering systems constructed as above, and let E^j be the set of moduli appearing in C^j. Then for each $j \ge 4$, all the covering systems in $\eta(E^j)$ are minimal.*

Proof. We will show the result by induction on j. We already covered the base case $j = 4$. Suppose the result is true for some j. We will show that the result is also true for $j + 1$. Suppose by contradiction that the result is not true for $j + 1$, that is that there is some covering system C in $\eta(E^{j+1})$ that is not minimal. Let D be a proper minimal subcover of C. Since there are exactly p_{j+1} progressions in $C_{p_{j+1}}$, we have by Lemma 2.2 and the minimality of D two possibilities :

(1) All progressions in $C_{p_{j+1}}$ are in D.

(2) No progressions in $C_{p_{j+1}}$ are in D.

The second case is impossible, as the moduli appearing in D would then be a proper subset of E^j, contradicting our induction hypothesis.

We will show that the first case is also impossible. Note that the progressions that are in $D \setminus D_{p_{j+1}}$ cover a set of residues modulo P_j, and cannot cover them all by minimality. We therefore have that the progressions in $D_{p_{j+1}}$ cover at least one arithmetic progression modulo P_j. However, by Lemma 2.17, we know that all of them must intersect with any progression modulo P_j that they cover. We know that there are two progressions in $D_{p_{j+1}}$, $a_1 \pmod{m_1}$ and $a_2 \pmod{m_2}$ such that $m_1 m_2 = p_{j+1}^2 P_j$. By the Chinese Remainder Theorem, these two progressions can only intersect in one progression modulo P_j, hence the moduli in $D_{p_{j+1}}$ cover only one progression modulo P_j. This implies that the progressions in $D \setminus D_{p_{j+1}}$ must cover the $P_j - 1$ other progressions modulo P_j. However, to do this, we need all the progressions in C that are not in $C_{p_{j+1}}$. Indeed, if we could do it without all of them, then taking one we did not use, we could construct a covering system, contradicting once again our induction hypothesis. Hence the moduli in D are the same as the moduli in C, which contradicts the fact that D was a proper subcover of C. Hence, all of the covering systems in $\eta(E^j)$ are minimal. □

We are now ready to prove our result.

Proposition 2.22. *Let C^j and E^j be defined as above. Then*

$$H(E^j) = \prod_{k=1}^{j} p_k!.$$

Proof. Fix $j \geq 4$. We will show the result for j. Let C' be some covering system in $\eta(E^j)$. Note that by our previous lemma, C' is minimal. We will show that we can reach C^j from C' by a sequence of p-automorphisms. As there are exactly $\prod_{k=1}^{j} p_k!$ such automorphisms, we will deduce the result.

We analyse C' prime by prime, starting with 2. Whatever the progression modulo 2 we have in C', we can bring it back to $0 \pmod 2$ via a 2-automorphism. We then look at the prime 3. Via 3-automorphism, we can suppose we have $0 \pmod 3$. We know our covering system is still minimal as p-automorphisms conserve minimality, hence we have either 1 (mod 6) or 5 (mod 6). Via a 3-automorphism, we may suppose we have 1 (mod 6). By minimality, all the remaining progressions must intersect with 5 (mod 6), which means that their 2-valuation is either 1 or $\star$, and their 3-valuation is either 2 or $\star$. We now look at our four new progressions that are divisible by 5 and are 5-smooth. Since their 2-valuations and 3-valuations are already set, we need only look at their 5-valuations, and since by minimality they must all be distinct, we may, by a sequence of 5-automorphisms, suppose they are exactly as in C.

For the k-th prime, we have a similar argument. We are left to cover the arithmetic progression $P_{k-1} - 1 \pmod{P_{k-1}}$. Therefore, all the new progressions divisible by p_k must intersect with this arithmetic progression by minimality, and so the only thing we may choose about them is their p_k-valuation. However, since they must all have distinct p_k-valuations, we may, via a sequence of p_k-automorphisms, have them exactly as in C^j.

Iterating this argument all the way up to p_j gives us that we can reach C^j by C' through a series of p-automorphisms, which in turn gives us our result. □

2.11. A troublesome covering system

In this section, we construct a square-free covering system C of multiplicity 1 with moduli set E such that

$$\mathrm{lcm}(C) = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 11,$$

but

$$H(E) > \prod_{k=1}^{5} p_k!.$$

We construct our covering system prime by prime. For the first level, we take

$$0 \pmod 2 = (0).$$

We are left to cover (1) = 1 (mod 2). For the second level, we take

$$(\star,0),(1,1).$$

We are left to cover (1,2) = 5 (mod 6). For the third level, we take

$$(\star,\star,0),(1,\star,1),(\star,2,2),(1,2,3).$$

We are left to cover (1,2,4) = 29 (mod 30). For the fourth, we take

$$(\star,\star,\star,0),(1,\star,\star,1),(1,2,\star,2),(\star,2,\star,3),(\star,\star,4,4).$$

Notice that after this level, we are left to cover $(1,2,4,x,y)$, for all $x \in \{5,6\}$ and $y \in \{0,1,\ldots,10\}$. We will cover $(1,2,4,x,y)$ $x \in \{5,6\}$ and $y \in \{0,1,\ldots,7\}$ with the first eight progressions, and (1,2,4,x,y) for $x \in \{5,6\}$ and $y \in \{8,9,10\}$ with the last six, using one to cover each of the six available congruences. For the fifth level, we take

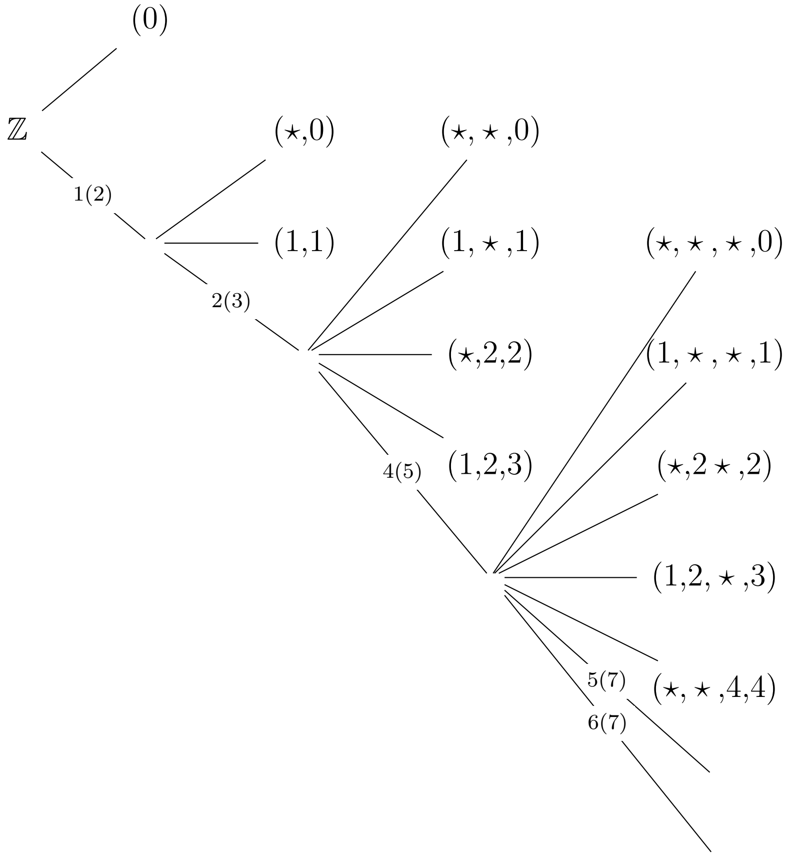
$$(\star,\star,\star,\star,0),(1,\star,\star,\star,1),(\star,2,\star,\star,2),(\star,\star,4,\star,3),(1,2,\star,\star,4),(1,\star,4,\star,5),(\star,2,4,\star,6),(1,2,4,\star,7)$$

and

$$(\star,\star,\star,5,8),(1,\star,\star,6,8),(\star,2,\star,5,9),(\star,\star,4,6,9),(1,2,\star,5,10),(1,\star,4,6,10).$$

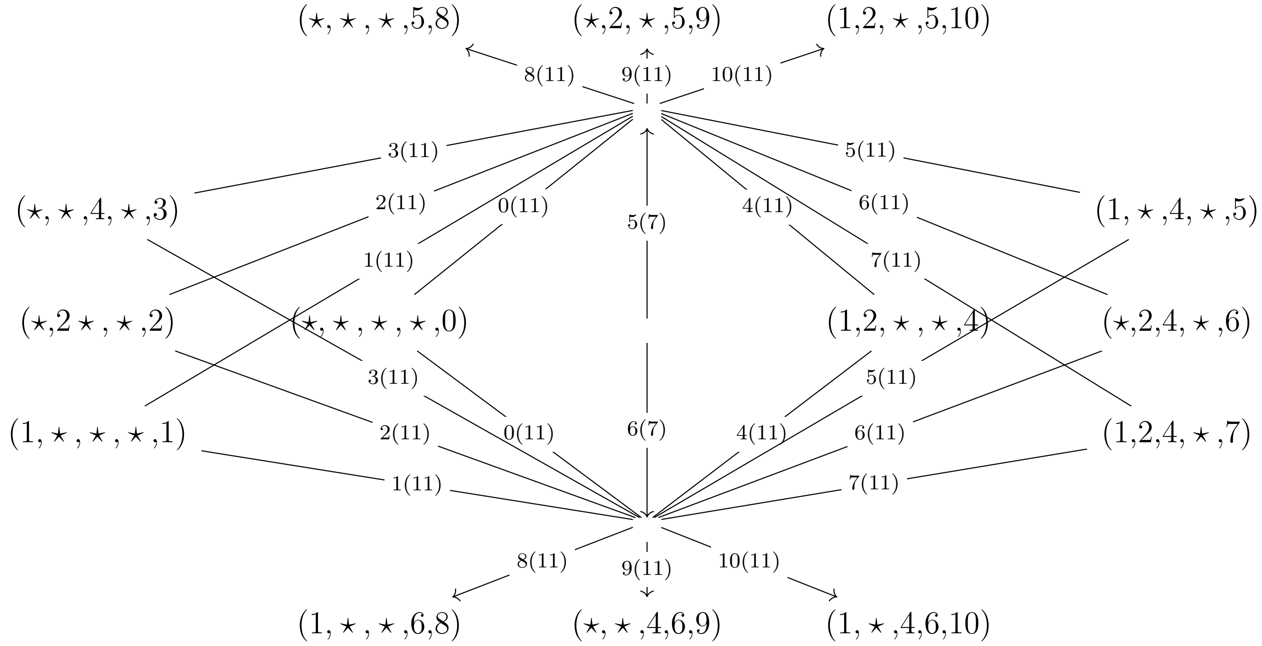
This is a covering system. Notice that the structure of this covering system is fundamentally different than the C^j covering systems we constructed earlier. This leads us to notice that we may replace $(1,2,\star,5,10)$ and $(1,\star,4,6,10)$ by $(1,2,\star,6,10)$ and $(1,\star,4,5,10)$, and the system remains a covering system. However, this is not a p-automorphism, as the sets $C_7(5)$ and $C_7(6)$ contain three elements each. This is a change of only one element in each of these sets. Here is a graph of the covering system to illustrate why the structure of this covering system is different than that of the previous square-free covering systems we studied.

Fig. 2.6. The first 4 primes in our covering system



This first graph shows what happens on the first 4 levels of our covering system. We separate the last level into another graph as it is much more complex, and it is where the structure really breaks down.

Fig. 2.7. The prime 11 in our covering system



The main problem here is that the arithmetic progressions (1,2,4,5,x) and (1,2,4,6,x), for $x = 8,9,10$ are covered by two different arithmetic progressions, whereas the arithmetic progressions (1,2,4,5,x) and (1,2,4,6,x) for $x \in \{1,2,3,4,5,6,7\}$ are covered by only one progression. It is where they are covered by two different arithmetic progressions that our previous argument for counting $H(E)$ breaks down, and it is the fundamental difference in between the structure of this covering system and the previous ones. We would in fact conjecture that in our case,

$$H(E) = 2^3 \prod_{i=1}^{5} p_i!.$$

2.12. An infinite family of similar covering systems

Let p_j denote the j-th prime. We construct here a sequence C^j, $j \geq 5$, of square-free covering systems of multiplicity 1, such that the moduli set E^j of C^j has $\operatorname{lcm}(E^j) = p_1 \cdots p_j$, but

$$H(E^j) > \prod_{i=1}^{j} p_j!.$$

The idea will be to mimic the structure of the last level of the covering system from the previous section, but to do it for a larger and larger last prime.

Instead of constructing the covering systems explicitly, we will give the idea of how to construct these covering systems by constructing such a system with 13 as our largest prime.

We start out with a very similar approach as the sequence of square-free covering systems that we constructed earlier. For the later stage, we will simultaneously cover two progressions modulo 11 in our first few progressions divisible by 13 by taking them to be coprime to 11, but cover the last couple of residues modulo 13 with progressions divisible by 11. This will mimic the structure of the last covering system we defined.

We construct our covering systems level by level, startig with the prime 2. We take (0). We are left to cover (1). For the next level, we take $(\star,0)$ and (1,1), and we are left to cover (1,2). For the prime 5, we take $(\star,\star,0)$, $(1,\star,1)$, $(\star,2,2)$, (1,2,3). We are left to cover (1,2,4). For the prime 7, we take $(\star,\star,\star,0)$, $(1,\star,\star,1)$, $(\star,2,\star,2)$, $(1,2,\star,3)$, $(\star,2,4,4)$ and $(1,\star,4,5)$. We are left to cover (1,2,4,6). For the prime 11, we take $(\star,\star,\star,\star,0)$, $(1,\star,\star,\star,1)$, $(\star,2,\star,\star,2)$, $(1,2,\star,\star,3)$, $(\star,\star,3,\star,4)$, $(1,2,4,\star,5)$, $(\star,\star,\star,6,6)$, $(\star,2,4,\star,7)$ and $(1,\star,4,\star,8)$. We are left to cover (1,2,4,6,9) and (1,2,4,6,10). To do this, we use the prime 13. We start by taking $(\star,\star,\star,\star,\star,0)$, $(1,\star,\star,\star,\star,1)$, $(\star,2,\star,\star,\star,2)$, $(1,2,\star,\star,\star,3)$, $(\star,\star,4,\star,\star,4)$, $(1,2,4,\star,\star,5)$, $(\star,\star,\star,6,\star,6)$, $(1,2,\star,6,\star,7)$, $(1,2,4,6,\star,8)$, $(\star,2,4,\star,\star,9)$ and $(\star,\star,4,6,\star,10)$. We are left to cover (1,2,4,6,9,11), (1,2,4,6,9,12), (1,2,4,6,10,11) and (1,2,4,6,10,12).

To do this, we use four progressions that are divisible by 11 and 13. We take $(\star,\star,\star,\star,9,11)$, $(1,\star,\star,\star,9,12)$, $(1,2,\star,\star,10,11)$ and $(\star,2,\star,\star,10,12)$. This constructs our covering system.

To see that this covering system respects the desired property, note that we may change out $(\star,\star,\star,\star,9,11)$ and $(1,2,\star,\star,10,11)$ by $(\star,\star,\star,\star,10,11)$ and $(1,2,\star,\star,9,11)$. However, doing this is not a p-automorphism, as part of $C_{11}(9)$ and $C_{11}(10)$ remains unchanged, while part of them changes. If we denote the covering system described above by C, this gives us that

$$H(C) > \prod_{i=1}^{j} p_j!.$$

We now mention how to generalise this construction. We start in a similar manner, covering all but one progression modulo 2, then all but one progression modulo $2 \cdot 3$, all the way till we cover all but one progression modulo P_k. Then, for the $(k+1)$-th prime, we cover all but two progressions. Finally, to cover our two remaining progression modulo P_{k+1}, we first take $p_{k+2}-2$ arithmetic progressions that are divisible by p_{k+2}, but coprime to p_{k+1} to cover the first $p_{k+2}-2$ progressions modulo p_{k+2} intersected with both missing progressions modulo p_{k+1}, and we take four progressions divisible by $p_{k+1}p_{k+2}$ to cover the remaining progressions. This gives us the desired property, in the exact same way as with our previous example.

We should mention that as our primes get very large, the number of available moduli also grows very large, so that we may, instead of leaving only two progressions uncovered at the before last level, leave k progressions uncovered. We can then cover these k progressions with progressions of our next prime, and in doing so get our number $H(E)$ to be an arbitrarily large multiple of $\prod_{i=1}^{k} p_k!$, so that not only can we get covering systems that have more automorphisms than the p-automorphisms, we can in fact get covering systems with an arbitrarily large number of other automorphisms.

Chapter 3

The j-th smallest modulus in a covering system

3.1. An overview of the argument

Before getting into the technical details of our argument, we offer an overview of what we will be doing throughout this chapter. Our goal is to bound the j-th smallest modulus in a minimal covering system of multiplicity 1.

To do this, we will need two key results. The first is offered in the next section, which says that any set of n arithmetic progressions that is not a covering system does not cover some integer in the interval $[1,2^n]$. The first proof of this result was given by Crittenden and Vanden-Eynden [**7**] in 1969. We offer here instead a more modern proof of this result [**1**] that was given by Balister, Bollobás, Morris, Sahasrabudhe and Tiba in 2019.

The second result we need is a bound on the minimum modulus of a covering system of multiplicity s. To obtain this, we adapt the ideas of Balister, Bollobás, Morris, Sahasrabudhe and Tiba in [**4**]. Note that while adapting their ideas, there is really not much difference with the original argument. The reader is encouraged to go look at their exposition of the argument in their new article from november 2022 [**2**], or again to go look at their original exposition of the argument in [**4**]. Notice that in our adaptation for covering systems of multiplicity s, all we really need is a couple of union bounds, so that the proof of our bound for the minimum modulus of a covering system of multiplicity s follows from the method they use for the minimum modulus of a covering system of multiplicity 1.

To put these ideas together, we consider a minimal covering system. From this covering system, we remove the first $j-1$ moduli. Since by minimality they do not form a covering system, they do not cover at least one integer in any interval of length 2^{j-1}, hence there is at least one integer in any interval of length 2^{j-1} that is covered by the remaining moduli. This allows us to construct a covering system of multiplicity 2^{j-1} for which the minimum modulus is the j-th minimum modulus of our original covering system. Our bound on the

j-th minimum modulus of a minimal covering system of multiplicity 1 then follows from our bound on the minimum modulus for covering system of multiplicity s. With this in mind, we get into the technical details of our proof.

3.2. A result of Crittenden and Vanden-Eynden

In this section we give a proof of the result of Crittenden and Vanden-Eynden [**7**] that we use for the translation argument in our proof of the bound on the j-th smallest modulus in a covering system. They proved the following theorem.

Theorem 3.1. *Any n arithmetic progressions that cover the first 2^n integers form a covering system.*

In 2019 , Balister, Bollobás, Morris, Sahasrabudhe, and Tiba [**1**] gave another proof of the result of Crittenden and Vanden-Eynden, using some group theory. We offer their proof here instead of the original one of Crittenden and Vanden-Eynden, as it is much simpler.

Theorem 3.2. *Let*

$$A = \{A_1, \dots, A_k\} = \{a_1 \pmod{m_1}, \dots, a_k \pmod{m_k}\}$$

be a set of k arithmetic progressions. If A covers 2^k consecutive integers, then it covers all of $\mathbb{Z}$.

Proof. Let a be an integer, and let

$$I = \{a+1, a+2, \dots, a+2^k\}.$$

Suppose by contradiction that there is some set

$$A = \{A_1, \dots, A_k\} = \{a_1 \pmod{m_1}, \dots, a_k \pmod{m_k}\}$$

of k arithmetic progressions that covers all of I, but that does not cover the integers. By a translation of A by $-a$, we may assume $a = 0$. Let $q = \operatorname{lcm}(A)$. Since A does not cover the integers, there exists an integer c, with $0 < c \le q$, that is not covered by A. Since the first 2^k positive integers are covered by our assumption, we have in fact that $2^k < c \le q$. Denote by s the smallest such integer. Let $\omega = \exp(2\pi i/q)$, and let Ω be the multiplicative group of order q generated by ω. Let $\phi : \mathbb{Z} \to \Omega$, $\phi(n) = \omega^n$, and note that ϕ is a homomorphism.

Now, let

$$Z_i = \phi(a_i \pmod{m_i}) = \{\omega^{a_i}, \omega^{a_i+m_i}, \dots, \omega^{a_i+(q/m_i-1)m_i}\},$$

and notice that $|\phi(A_i)| = q/m_i$. Let $Z = Z_1 \cup Z_2 \cup \dots \cup Z_k$. Note that $\{\omega^j : 1 \le j \le 2^k\} \subset Z$, and that $\omega^s \notin Z$. We can see that Z is the set of zeroes of the polynomial

$$P(z) := \prod_{i=1}^{k}\left(z^{q/m_i} - \omega^{a_i q/m_i}\right).$$

Expanding this polynomial into a sum of monomials, we find that

$$P(z) = \sum_{J\subset\{1,\dots,k\}} c_J z^{\sum_{j\in J} q/m_j} = \sum_{J\subset\{1,\dots,k\}} c_J z^{\alpha_J},$$

where the c_J's are complex numbers and $\alpha_J = \sum_{j\in J} q/m_j$.

Denote by W the linear span of the z^{α_J} over $\mathbb{C}$, and note that the dimension of W is at most 2^k, and that $P(z) \in W$.

To reach a contradiction, we will show that there are $2^k + 1$ linearly independent polynomials in W, which will contradict the fact that the dimension of W is at most 2^k.

For $m \in \mathbb{Z}$, denote by

$$P_m(z) := P(\omega^{-m} z).$$

Note that

$$P_m(z) = \sum_{S\subset\{1,\dots,k\}} c_J \omega^{-m\alpha_J} z^{\alpha_J},$$

and so $P_m(z) \in W$. We now show that $P_0(z)$,$P_1(z)$,...,$P_{2^k}(z)$ are linearly independent. To do so, we will show that for each $0 \le l \le 2^k$, we have that if

$$\sum_{m=\ell}^{2^k} \lambda_m P_m(z) = 0, \tag{3.2.1}$$

then $\lambda_\ell = 0$. Recall that by our definition of s, we have that $P(\omega^s) \neq 0$, and so $P_\ell(\omega^{s+\ell}) = P(\omega^s) \neq 0$. However, if $\ell < m \le 2^k$, then $P_m(\omega^{s+\ell}) = P(\omega^{s+\ell-m}) = 0$, as $0 < s + \ell - m < s$, and s was minimal. This and (3.2.1) imply that $\lambda_\ell P_\ell(\omega^s) = 0$, and so that $\lambda_\ell = 0$. This gives us the result. □

3.3. Constructing covering systems of multiplicity s

In this section, we prove a key lemma that we will use to bound the j-th smallest modulus in a covering system. The idea is that we may construct a covering system of multiplicity s from our original covering system from which we removed the $j-1$ first moduli. The following lemma shows precisely how we will do this.

Lemma 3.3. *Let $C = \{a_1 \pmod{m_1}, a_2 \pmod{m_2}, \dots, a_k \pmod{m_k}\}$ be a minimal covering system of multiplicity 1, and suppose $m_1 < m_2 < \dots < m_k$. Let $C_j = \{a_j \pmod{m_j}, a_{j+1} \pmod{m_{j+1}}, \dots, a_k \pmod{m_k}\}$. Then the set*

$$C' = \bigcup_{\ell=1}^{2^{j-1}}\left(C_j + \ell\right)$$

is a covering system of multiplicity $\leq 2^{j-1}$ *with minimum modulus* m_j.

Proof. By Theorem 3.2, we know that any n arithmetic progressions that do not cover the integers do not cover at least one integer in $[1,2^n]$. By minimality, $\{a_1 \pmod{m_1},\ldots,a_{j-1} \pmod{m_{j-1}}\}$ is a set of $j-1$ arithmetic progressions that do not cover the integers, and so we know that they do not cover at least one integer in $[1,2^{j-1}]$. In fact, we have that they do not cover at least one integer in any interval of the form $[x,x+2^{j-1}-1]$, where x is an integer. Indeed, if this were not the case, then $a_1 - x + 1 \pmod{m_1},\ldots,a_{j-1} - x + 1 \pmod{m_{j-1}}$ would be a set of $j-1$ arithmetic progressions that do not cover the integers, but cover all the integers in $[1,2^{j-1}]$. This means that C_j covers at least one integer in any interval of length 2^{j-1}.

Suppose now that C' is not a covering system. Then there exists some integer x that is not covered by C'. This means that for each $\ell \in \{1,\ldots,2^{j-1}\}$, x is not covered by $C_j + \ell$, which in turn implies that C_j does not cover $x - l$, for $\ell \in \{1,\ldots,2^{j-1}\}$. This contradicts the fact that C_j covers at least one integer in any inverval of length 2^{j-1}, and so C' is a covering system. The fact that it is 2^{j-1}-distinct and that it has minimum modulus m_j follows from the definition. □

In general, we only need to find some value of s for which there exists a covering system of multiplicity s with the same minimum modulus as the j-th minimum modulus in our covering system. We do not know if the way we did this in the lemma above is the best way to do this. Indeed, we could possibly introduce into our covering system of multiplicity s some moduli which do not appear in the original covering system, but that are greater than the j-th smallest modulus, in order to get a smaller value of s. However, this can get very complicated, which is why we opted for the simpler method here that yields a bound in a fairly easy manner.

3.4. Towards covering systems of multiplicity s

In this section, we slightly modify the definitions in [**4**] to allow for covering systems of multiplicity s, instead of simply distinct.

We start with a finite set of arithmetic progressions $\mathcal{A} = \{a_1 \pmod{d_1},\ldots,a_n \pmod{d_n}\}$. Denote by $D = D(\mathcal{A})$ the multiset of moduli m that appear in $\mathcal{A}$. Our goal is to show that the density of the set of uncovered integers

$$R = \mathbb{Z} \setminus \mathcal{A}$$

is greater than 0. Instead of immediately considering all the progressions, we instead let them appear according to the primes that divide them. Let $Q = \operatorname{lcm}[D]$, and let $p_1,\ldots,p_J$

be the distinct prime divisors of Q. We may write

$$Q = \prod_{k=1}^{J} p_k^{\nu_k},$$

where ν_k is the p_k-adic valuation of Q. For $j \in \{1,2,\ldots,J\}$, we define

$$Q_j := \prod_{k=1}^{j} p_k^{\nu_k},$$

and

$$\mathcal{A}_j := \{a \pmod{m} \in \mathcal{A} : m | Q_j\}.$$

We adopt the convention that $Q_0 = 1$ and that $\mathcal{A}_0 = D_0 = \emptyset$. We also define

$$D_j := \{d \in D : d | Q_j\},$$

and

$$R_j := \mathbb{Z} \setminus \mathcal{A}_j.$$

Denote by $N_j = D_j \setminus D_{j-1}$, and

$$\mathcal{B}_j = \mathcal{A}_j \setminus \mathcal{A}_{j-1} = \bigcup_{\substack{1 \le i \le n \\ P^+(d_i) = p_j}} \Big\{a \mod Q : a \equiv a_i \mod d_i\Big\},$$

so that $R_j = R_{j-1} \setminus B_j$. We may view R_j as a subset of $\mathbb{Z}/Q_j\mathbb{Z}$, or even of $Z/Q\mathbb{Z}$, and it will be useful to do so, as the density of R_j is the measure of R_j in the uniform probability measure over Z_{Q_j}.

The most crucial definition is that of certain probability measures $\mathbb{P}_0, \mathbb{P}_1, \ldots, \mathbb{P}_J$ on $\mathbb{Z}/Q\mathbb{Z}$, which we construct exactly as in [**4**] in terms of some free parameters $\delta_1, \ldots, \delta_J \in [0,1/2]$.

Let $\pi_j : \mathbb{Z}/Q\mathbb{Z} \to \mathbb{Z}/Q_j\mathbb{Z}$ be the natural projection for all $j \in \{0,1,\ldots,J\}$, where $Q_0 = 1$. In addition, let

$$F_j(x) := \{x' \in \mathbb{Z}/Q\mathbb{Z} : \pi_j(x') = \pi_j(x)\},$$

so that $|F_j(x)| = Q/Q_j$. The measure $\mathbb{P}_j$ will be Q_j*-measurable* by construction, meaning that it will have the property that

$$\mathbb{P}_j(x) = \mathbb{P}_j(x') \quad \text{whenever } \pi_j(x') = \pi_j(x).$$

Let

$$\alpha_j(x) := \frac{|F_{j-1}(x) \cap \mathcal{B}_j|}{|F_{j-1}(x)|} \qquad \text{for all } x \in \mathbb{Z}/Q\mathbb{Z},$$

and note that α_j is a Q_{j-1}-measurable function, meaning that $\alpha_j(x') = \alpha_j(x)$ if $\pi_{j-1}(x') = \pi_{j-1}(x)$. We then define $\mathbb{P}_j$ on the congruence class $x \in \mathbb{Z}/Q\mathbb{Z}$ as follows:

- If $\alpha_j(x) < \delta_j$, we let

$$\mathbb{P}_j(x) := \mathbb{P}_{j-1}(x) \cdot \frac{1_{x \notin \mathcal{B}_j}}{1 - \alpha_j(x)}.$$

- If $\alpha_j(x) \geq \delta_j$, we let

$$\mathbb{P}_j(x) := \mathbb{P}_{j-1}(x) \cdot \begin{cases} \dfrac{\alpha_j(x) - \delta_j}{\alpha_j(x)(1-\delta_j)} & \text{if } x \in \mathcal{B}_j, \\ \\ \dfrac{1}{1-\delta_j} & \text{if } x \notin \mathcal{B}_j. \end{cases}$$

Note that the probability measures are constructed so that $\mathbb{P}_i(B_i)$ is small, but without changing the measure of B_j, for $j < i$. It follows that the measure of what is covered by our arithmetic progressions is at most $\sum_i \mathbb{P}_i(B_i)$, and so if this quantity is less than 1, our set of arithmetic progressions do not form a covering system. Instead of doing this directly, we will instead be using the method of moments, which we expand upon in more detail in the following section.

We now show a couple of simple lemmas that will be useful for what follows.

Lemma 3.4. *If S is a union of congruence classes modulo Q_{i-1}, then $\mathbb{P}_i(S) = \mathbb{P}_{i-1}(S)$.*

Proof. Let $x \in \mathbb{Z}/Q_{i-1}\mathbb{Z}$. We do a simple computation starting from the definition, where we separate the $x \in \mathbb{Z}/Q_{i-1}\mathbb{Z}$ into two categories :

(1) $\alpha_i(x) \leq \delta_i$,

(2) $\alpha_i(x) > \delta_i$.

In both cases, we may write $\mathbb{P}_i(x) = \sum_{y \in F_i(x)} \mathbb{P}_i(y)$. For the first case :

$$\mathbb{P}_i(x) = \left(\alpha_i(x) \cdot 0 + (1-\alpha_i(x)) \cdot \frac{1}{1-\alpha_i(x)} \cdot \right)\mathbb{P}_{i-1}(x) = \mathbb{P}_{i-1}(x).$$

In the second case :

$$\mathbb{P}_i(x) = \left(\alpha_i(x) \cdot \frac{\alpha_i(x) - \delta_i}{\alpha_i(x)(1-\delta_i)} + (1-\alpha_i(x))\frac{1}{1-\delta_i}\right)\mathbb{P}_{i-1}(x) = \mathbb{P}_{i-1}(x).$$

Summing these over all $x \in S$, we get the desired result. □

We then look at our second lemma.

Lemma 3.5. *For any $S \subset \mathbb{Z}/Q\mathbb{Z}$, we have that*

$$\mathbb{P}_i(S) \leq \frac{1}{1-\delta_i} \cdot \mathbb{P}_{i-1}(S).$$

Furthermore, if $S \subset \mathcal{B}_i$, we have that

$$\mathbb{P}_i(S) \leq \mathbb{P}_{i-1}(S).$$

PROOF. Both results follow directly from the definition when $S = \{y\}$, and so for any S by additivity. $\square$

Given a function $f : \mathbb{Z}_Q \to \mathbb{R}_{\geq 0}$, we define the expected value of f in relation to $\mathbb{P}_i$ to be

$$\mathbb{E}_i[f(x)] = \sum_{x \in \mathbb{Z}_Q} f(x)\mathbb{P}_i(x).$$

We can deduce a couple of results immediately on these expected values by using the two previous lemma. First of all,

$$\mathbb{E}_i[f(x)] \leq \frac{1}{1-\delta_i}\mathbb{E}_{i-1}[f(x)].$$

Furthermore, if f has support over $\mathcal{B}_i$, then $\mathbb{E}_i[f(x)] \leq \mathbb{E}_{i-1}[f(x)]$, and if f is Q_{i-1}-measurable, then $\mathbb{E}_i[f(x)] = \mathbb{E}_{i-1}[f(x)]$.

3.5. Bounding the moments is sufficient

In this section, we offer a proof of a theorem in section 3 of [**4**]. We put ourselves in the context of the previous section, in the sense that we suppose that we have a system $\mathcal{A}$ of arithmetic progressions, and $\mathcal{M}(\mathcal{A}) = s$. We let δ_1,...,δ_J be some parameters that will be chosen later to either optimise or simplify some computations. Finally, we suppose that the α_i and the $\mathbb{P}_i$ are defined as above.

We now introduce a few new definitions. We will denote by

$$M_i^{(1)} := \mathbb{E}_i[\alpha_i(x)] \quad \text{and} \quad M_i^{(2)} := \mathbb{E}_i[\alpha_i(x)^2].$$

We also introduce the following multiplicative function, which is defined over the factors d of Q.

$$\nu(d) = \prod_{p_k | d}\left(\frac{1}{1-\delta_k}\right).$$

Our goal for the rest of the section is to prove the following lemma.

Lemma 3.6. *Let $\mathcal{A}$ be a finite set of arithmetic progressions, and let δ_1,.., $\delta_n \in [0,1/2]$. If*

$$\eta := \sum_{i=1}^{n} \min\left\{M_{i-1}^{(1)}, \frac{M_{i-1}^{(2)}}{4\delta_i(1-\delta_i)}\right\} < 1,$$

then $\mathcal{A}$ is not a covering system. Furthermore, the uncovered set R has density at least

$$\mathbb{P}_0(R) \geq (1-\eta)\exp\left(-\frac{2}{1-\eta}\sum_{d\in D}\frac{\nu(d)}{d}\right).$$

3.5.1. Proof of Lemma 3.6

We start of this section with a few lemmas that will be usefull in proving our lemma. First off, Lemma 3.3 from [**4**] follows as is :

Lemma 3.7.

$$\mathbb{P}_i(\mathcal{B}_i) \leq \min\left\{M_{i-1}^{(1)}, \frac{M_{i-1}^{(2)}}{4\delta_i(1-\delta_i)}\right\}$$

Proof. We show that the left hand side of the equation is always smaller than either of the parts of the right hand side. For the first, we have the result directly from the definition of the α_i's and Lemma 3.5. For the second, we use the fact that $\frac{a^2}{4d} \geq \max\{0,a-d\}$, which can be seen to hold for all $a,d > 0$ by rearranging the terms in the inequality $(a-2d)^2 \geq 0$. We then find by the definitions of α_i and $\mathbb{P}_i$ that

$$\begin{aligned}\mathbb{P}_i(\mathcal{B}_i) &= \sum_{x \in \mathbb{Z}_{Q_{i-1}}} \max\left\{0, \frac{\alpha_i(x)-\delta_i}{\alpha_i(x)(1-\delta_i)}\right\} \cdot \mathbb{P}_{i-1}(F_i(x) \cap \mathcal{B}_i) \\ &= \frac{1}{1-\delta_i} \sum_{x \in \mathbb{Z}_{Q_{i-1}}} \max\{0, \alpha_i(x)-\delta_i\} \cdot \mathbb{P}_{i-1}(x) \\ &\leq \frac{1}{1-\delta_i} \sum_{x \in \mathbb{Z}_{Q_{i-1}}} \frac{\alpha_i(x)}{4\delta_i} \cdot \mathbb{P}_{i-1}(x) = \frac{M_{i-1}^{(2)}}{4\delta_i(1-\delta_i)},\end{aligned}$$

which gives us the result. □

The ease in the use of the previous lemma in showing the first part of Lemma 3.6 comes from the fact that we suppose that this quantity is lesser than or equal to 1. In practice, the larger s get, the larger our minimum modulus needs to be to assure that we have this condition. We also use Lemma 3.4 and 3.5 from [**4**] as they are.

Lemma 3.8. *For each $0 \leq i \leq n$, and all $b,d \in \mathbb{Z}$ such that $d|Q$, we have that*

$$\mathbb{P}_i(b + d\mathbb{Z}) \leq \frac{1}{d} \prod_{p_k|d, k \leq i} \frac{1}{1-\delta_k} = \frac{\nu((d,Q_i))}{d}.$$

Proof. We prove this by induction on i. Since $\mathbb{P}_0$ is the uniform measure, $\mathbb{P}_0(b+d\mathbb{Z}) = 1/d$. Let $1 \leq i \leq n$, and suppose the result is true for $\mathbb{P}_{i-1}$. We analyse two cases : either $p_i|d$, either not. In the first case, by Lemma 3.5 and our induction hypothesis, we find that

$$\mathbb{P}_i(b + d\mathbb{Z}) \leq \frac{1}{1-\delta_i}\mathbb{P}_{i-1}(b + d\mathbb{Z}) \leq \frac{1}{d} \prod_{p_k|d, k \leq i} \frac{1}{1-\delta_k}$$

In the second case, we write $d = m\ell$, where $m = (d,Q_i) = (d,Q_{i-1})$. We then have that

$$\mathbb{P}_i(b+d\mathbb{Z}) = \frac{\mathbb{P}_i(b+m\mathbb{Z})}{\ell} = \frac{\mathbb{P}_{i-1}(b+m\mathbb{Z})}{\ell} \leq \frac{1}{\ell m}\prod_{p_k|d,k<i}\frac{1}{1-\delta_k} = \frac{1}{d}\prod_{p_k|d,k\leq i}\frac{1}{1-\delta_k},$$

Which gives us the desired result. □

We define the distorsion $\Delta_i(x)$ of a point $x \in \mathbb{Z}_{Q_i}$ by

$$\Delta_i(x) := \max\left\{0, \log\left(\frac{\mathbb{P}_i(x)}{\mathbb{P}_0(x)}\right)\right\}.$$

We then find the following bound on the average distortion.

Lemma 3.9. *For each $0 \leq i \leq n$, we have that*

$$\mathbb{E}_i[\Delta_i(x)] \leq 2\sum_{d\in D_i}\frac{\nu(d)}{d}.$$

Proof. We first show that

$$\log\left(\frac{\mathbb{P}_k(x)}{\mathbb{P}_{k-1}(x)}\right) \leq 2\cdot\alpha_k(x).$$

Indeed, we have this result, as $\frac{\mathbb{P}_{k-1}(x)}{\mathbb{P}_k(x)} \geq \max\{1-\alpha_k(x),1-\delta_k\}$, and $-\log(1-z) \leq 2z$ for all $z \leq 1/2$. It follows that

$$\mathbb{E}_i[\Delta_i(x)] \leq \sum_{k=1}^{i}\mathbb{E}_i\left[\max\left\{0,\log\left(\frac{\mathbb{P}_k(x)}{\mathbb{P}_{k-1}(x)}\right)\right\}\right] \leq 2\cdot\sum_{k=1}^{i}\mathbb{E}_i[\alpha_k(x)].$$

Now, for each $1 \leq k \leq i$,

$$\mathbb{E}_i[\alpha_k(x)] = \mathbb{E}_{k-1}[\alpha_k(x)] = \mathbb{P}_{k-1}(\mathcal{B}_k),$$

since α_k is Q_{k-1}-measurable. Furthermore, by the previous lemma and a union bound, we find that

$$\mathbb{P}_{j-1}(\mathcal{B}_j) \leq \sum_{A\in\mathcal{B}_k}\mathbb{P}_{k-1}(A) \leq \sum_{d\in N_k}\frac{\nu((d,Q_{k-1})}{d} \leq \sum_{d\in N_k}\frac{\nu(d)}{d},$$

and so we have that

$$\mathbb{E}_i[\Delta_i(x)] \leq 2\cdot\sum_{k=1}^{i}\sum_{d\in N_k}\frac{\nu(d)}{d} \leq 2\cdot\sum_{d\in D_i}\frac{\nu(d)}{d}.$$

This gives us the result. □

We are now ready to prove Lemma 3.6.

Proof. The first part of our lemma follows immediately from a union bound, Lemma 3.4, Lemma 3.7 and the definition of η. Indeed,

$$1 - \mathbb{P}_n(R) \leq \sum_{i=1}^{n} \mathbb{P}_n(\mathcal{B}_i) \leq \sum_{i=1}^{n} \mathbb{P}_i(\mathcal{B}_i) \leq \eta,$$

and so, since $\eta < 1$, we have that

$$\mathbb{P}_n(R) \geq 1 - \eta > 0$$

The second part of the lemma uses 3.9, as well as the convexity of the exponential function. We first find that by the definition of $\Delta_n(x)$,

$$\mathbb{P}_0(R) = \mathbb{E}_0[1_{x\in\mathbb{R}}] \geq \mathbb{E}_n[1_{x\in\mathbb{R}} \exp(-\Delta_n(x))],$$

and so by convexity and since $\omega = \mathbb{P}_n(R) \cdot \mathbb{E}_n[\Delta_n(x)|x \in \mathbb{R}] \leq \mathbb{E}_n[\Delta_n(x)]$, we get that

$$\mathbb{E}_n[1_{x\in\mathbb{R}} \exp(-\Delta_n(x))] = \omega \geq \mathbb{P}_n(R) \cdot \exp(-\mathbb{E}_n[\Delta_n(x)|x \in \mathbb{R}) \geq \mathbb{P}_n(R) \cdot \exp\left(- \frac{\mathbb{E}_n[\Delta_n(x)]}{\mathbb{P}_n(R)} \right).$$

Then by Lemma 3.9, and since $\mathbb{P}_n(R) \geq 1 - \eta$, we find that

$$\mathbb{P}_0(R) \geq (1 - \eta) \exp\left(- \frac{2}{1-\eta} \sum_{d\in D} \frac{\nu(d)}{d} \right),$$

which gives us the lemma. □

3.5.2. Bounding the first and second moments

We now proceed with bounding $M_j^{(1)}$ and $M_j^{(2)}$. Doing so is the context of Theorem 3.2 in [**4**], but this result is only valid for systems of congruences of multiplicity 1. We thus need to generalize it. This is rather straightforward, and we describe how to do it below.

Lemma 3.10. *Assume the above notation. For $x \in \mathbb{Z}/Q\mathbb{Z}$ and $j \in \{1,2,\ldots,J\}$, we have*

$$\alpha_j(x) \leq \sum_{r=1}^{\nu_j} \sum_{g|Q_{j-1}} \sum_{\substack{1\leq i\leq n \\ d_i = gp_j^r}} \frac{1_{x\subseteq a_i+g\mathbb{Z}}}{p_j^r}.$$

Proof. Note that $|F_{j-1}(x)| = Q/Q_{j-1}$ and that we may write $x = c + Q\mathbb{Z}$ for some $c \in \mathbb{Z}$. Hence,

$$\alpha_j(x) = \frac{|F_{j-1}(x) \cap \mathcal{B}_j|}{Q/Q_{j-1}} \leq \frac{Q_{j-1}}{Q} \sum_{\substack{1\leq i\leq n \\ P^+(d_i)=p_j}} \sum_{\substack{a \mod Q \\ a\equiv c \mod Q_{j-1} \\ a\equiv a_i \mod d_i}} 1,$$

by the union bound. For each i with $P^+(d_i) = p_j$ we may write uniquely $d_i = gp_j^r$ with $g|Q_{j-1}$ and $1 \leq r \leq \nu_j$. We thus find that

$$\alpha_j(x) \leq \frac{Q_{j-1}}{Q_j} \sum_{r=1}^{\nu_j} \sum_{g|Q_{j-1}} \sum_{\substack{1\leq i\leq n \\ d_i = gp_j^r}} \sum_{\substack{a \mod Q \\ a\equiv c \mod Q_{j-1} \\ a\equiv a_i \mod d_i}} 1.$$

For the congruences $a \equiv a_i \mod d_i$ and $a \equiv c \mod Q_{j-1}$ to be compatible, we must have $c \equiv a_i \mod d_i$ or, equivalently, that x is a subset of $a_i + g\mathbb{Z}$. Under this assumption, a lies in some congruence class mod $Q_{j-1}p_j^r$, so there are $Q/(Q_{j-1}p_j^r)$ choices for $a \mod Q$. This completes the proof of the lemma. □

Lemma 3.11. *Assume the above notation, let $s = m(\mathcal{A})$, and let $j \in \{1,2,\dots,J\}$.*

(1) If $\delta_i = 0$ for $i \in \{1,\dots,j-1\}$, then

$$M_j^{(1)} \leq s \sum_{\substack{d\geq d_1 \\ P^+(d)=p_j}} \frac{1}{d}.$$

(2) We have

$$M_j^{(2)} \ll \frac{s^2(\log p)^6}{p^2}.$$

Proof. We treat both parts simultaneously for now. Let $k \in \{1,2\}$ and let us write $p = p_j$ for simplicity. By Lemma 3.10, we have

$$\mathbb{E}_{j-1}[\alpha_j^k] \leq \sum_{1\leq r_1,\dots,r_k\leq\nu_j} \sum_{g_1,\dots,g_k|Q_{j-1}} \sum_{\substack{1\leq i_1,\dots,i_k\leq n \\ d_{i_\ell}=g_\ell p^{r_\ell}\ \forall\ell}} \frac{\mathbb{P}_{j-1}\Big(\bigcap_{\ell=1}^k (a_{i_\ell} + g_\ell\mathbb{Z})\Big)}{p^{r_1+\cdots+r_k}}.$$

Since $d_i \geq d_1$ for all i, we must have $g_\ell p^{r_\ell} \geq d_1$ for all ℓ. Given $r_1,\dots,r_k$ and $g_1,\dots,g_k$, there are at most s^k choices for $i_1,\dots,i_k$ with $d_{i_\ell} = g_\ell p^{r_\ell}$ (because we have assumed that $\mathcal{A}$ has multiplicity s). For each such choice of $i_1,\dots,i_k$, the Chinese Remainder Theorem implies that the set $\bigcap_{\ell=1}^k (a_{i_\ell} + g_\ell\mathbb{Z})$ is either empty, or an arithmetic progression modulo $[g_1,\dots,g_k]$. Hence, Lemma 3.8 implies that

$$\mathbb{P}_{j-1}\bigg(\bigcap_{\ell=1}^k (a_{i_\ell} + g_\ell\mathbb{Z})\bigg) \leq \frac{\prod_{p_i|[g_1,\dots,g_k]}(1-\delta_i)^{-1}}{[g_1,\dots,g_k]}, \tag{3.5.1}$$

for each of the $\leq s^k$ possible values of $i_1,\dots,i_k$. We thus conclude that

$$\mathbb{E}_{j-1}[\alpha_j^k] \leq s^k \sum_{1\leq r_1,\dots,r_k\leq\nu_j} \sum_{\substack{g_1,\dots,g_k|Q_{j-1} \\ g_\ell p^{r_\ell}\geq d_1\ \forall\ell}} \frac{\prod_{p_i|[g_1,\dots,g_k]}(1-\delta_i)^{-1}}{[g_1,\dots,g_k]p^{r_1+\cdots+r_k}}.$$

When $k = 1$ and $\delta_i = 0$ for all $i < j$, this readily proves part (a) of the lemma.

Now, let us consider the case when $k = 2$ and prove part (b). Here, there are no conditions on the parameters δ_i except for knowing that $\delta_i \in [0,1/2]$ for all i. In particular, $\prod_{p_i|[g_1,g_2]}(1-\delta_i)^{-1} \le 2^{\omega([g_1,g_2])}$. Therefore,

$$\mathbb{E}_{j-1}[\alpha_j^2] \le s^2 \sum_{1\le r_1,r_2\le \nu_j} \sum_{g_1,g_2|Q_{j-1}} \frac{2^{\omega([g_1,g_2])}}{[g_1,g_2]p^{r_1+r_2}} \le \frac{s^2}{(p-1)^2} \sum_{g_1,g_2|Q_{j-1}} \frac{2^{\omega([g_1,g_2])}}{[g_1,g_2]}.$$

The function $\mathbb{N} \ni m \to \#\{(g_1,g_2) \in \mathbb{N}^2 : [g_1,g_2] = m\}$ is multiplicative and takes the value $2\nu+1$ on each ν-th prime power. Hence,

$$\sum_{g_1,g_2|Q_{j-1}} \frac{2^{\omega([g_1,g_2])}}{[g_1,g_2]} = \prod_{i<j}\left(1+\frac{6}{p_i}+O\left(\frac{1}{p_i^2}\right)\right) \le \exp\left\{\sum_{i<j}\frac{6}{p_i}+O\left(\frac{1}{p_i^2}\right)\right\} \ll (\log p)^6$$

by the inequality $1+t\le e^t$ and the second part of Theorem 0.3 . This completes the proof of part (b) of the lemma too. □

3.5.3. Proof of Theorem 1.3

It remains to prove Theorem 1.3. We will need the following simple consequence of Theorem 16.3 in [**20**]:

Lemma 3.12. *Let $x \ge y \ge 2$ be such that $y \ge (\log x)^3$, and let $u = \log x/\log y$. Then we have that*

$$\sum_{\substack{d>y^u \\ P^+(d)\le y}} \frac{1}{d} \ll \frac{\log y}{u^u}.$$

Now, let us complete the proof of Theorem 1.3. In the notation of the previous sections, we must show that if $d_1 > \exp(c\log^2(s+1)/\log\log(s+2))$, then $\mathcal{A}$ that does not cover $\mathbb{Z}$. In view of Lemma 3.6, it suffices to show that

$$\eta := \sum_{1\le j\le J} \min\left\{M_j^{(1)}, \frac{M_j^{(2)}}{4\delta_j(1-\delta_j)}\right\} < 1.$$

Let $y = Cs^3$, where C is a constant that will be chosen to be large enough, and let $k = \max\{j \in [1,J]\cap\mathbb{Z} : p_j \le y\}$. We set $\delta_i = 0$ for $i \le k$ and $\delta_i = 1/2$ for $i > k$, so that

$$\eta \le \sum_{1\le j\le k} M_j^{(1)} + \sum_{k<j\le J} M_j^{(2)} =: \eta_1 + \eta_2.$$

Then, Lemma 3.11(b) and Chebyshev's estimate [**20**, Theorem 2.4] imply that

$$\eta_2 \ll \sum_{p>y} \frac{s^2(\log p)^6}{p^2} \asymp \frac{s^2(\log y)^5}{y}.$$

If C is large enough, then $\eta_2 < 1/2$. From now on, we fix such a choice of C.

It remains to bound η_1. Applying Lemma 3.11(a) and our assumption that

$$d_1 > x := \exp\{c\log^2(s+1)/\log\log(s+2)\},$$

we find that

$$\eta_1 \leq s \sum_{\substack{d>x \\ P^+(d)\leq y}} \frac{1}{d}.$$

If c is large enough compared to C (which we have already fixed), then Lemma 3.12, applied with

$$u = \frac{\log x}{\log y} = \frac{c\log^2(s+1)}{\log(Cs^3)\log\log(s+2)} \sim \frac{c\log s}{\log\log s} \quad \text{when } s\to\infty,$$

implies that the sum over d is $< 1/(2s)$. Hence, $\eta_1 < 1/2$, and thus $\eta \leq \eta_1 + \eta_2 < 1$, as needed. This shows that if $d_1 > x$, then $\mathcal{A}$ does not cover $\mathbb{Z}$, thus completing the proof of Theorem 1.3.

3.6. Minimum modulus theorems

In this section, we prove the three theorems we discussed in the introduction of this thesis. Firstly, from what we proved in the previous sections, we get our first theorem.

Theorem 3.13. *The minimum modulus of a covering system of multiplicity s is bounded. More precisely, there exists a constant c such that the minimum modulus in a covering system of multiplicity s is smaller than*

$$\exp\left(c\frac{\log^2(s+1)}{\log\log(s+2)}\right).$$

Using this theorem, we can deduce the following theorem.

Theorem 3.14. *The minimum modulus of a covering system of multiplicity 1 of the arithmetic progression $a \pmod m$ is bounded. More precisely, there exists a constant C such that the minimum modulus in a covering system of multiplicity 1 of the arithmetic progression $a \pmod m$ is smaller than*

$$\exp\left(C\frac{\log^2(m+1)}{\log\log(m+2)}\right).$$

Proof. Let C be a covering system of multiplicity 1 of the arithmetic progression $a \pmod m$. Notice that

$$C' = \bigcup_{i=0}^{m-1}\left(C+i\right)$$

is an m-covering system of multiplicity 1 of the integers. Indeed, let $b \in \mathbb{Z}$ be an integer. Then there exists some i, $0 \le i \le m-1$ such that $b - i \equiv a \pmod{m}$. Then $b - i$ is covered in C, so that there exists some progression $a_1 \pmod{m_1} \in C$ such that $b - i \equiv a_1 \pmod{m_1}$. But then $b \equiv a_1 + i \pmod{m_1}$, and so b is covered by a congruence in $C + i$, which is also a congruence in C'. To see that it is m-distinct, it suffices to notice that each moduli in C appears exactly m times in C' by definition.

Therefore, by our previous theorem, the minimum modulus in C' is bounded by

$$\exp\left(c\frac{\log^2(m+1)}{\log\log(m+2)}\right)$$

for some constant c. However, the minimum modulus in C' is also the minimum modulus in C, hence we get the result. □

The proof of our next theorem will follow in a similar fashion.

Theorem 3.15. *The n-th minimum modulus in a minimal covering system of multiplicity 1 is bounded. More precisely, there exists a constant c such that the n-th minimum modulus in a minimal covering system of multiplicity 1 is smaller than*

$$\exp\left(c\frac{n^2}{\log(n+1)}\right).$$

Proof. By Lemma 3.3, we know that the n-th minimum modulus of a minimal covering system of multiplicity 1 is the minimum modulus of some covering system of multiplicity 2^{n-1}. Hence, there is a constant c such that this modulus is bounded by

$$\exp\left(c\frac{\log(2^{n-1}+1)^2}{\log\log(2^{n-1}+2)}\right).$$

However,

$$\exp\left(c\frac{\log^2(2^{n-1}+1)}{\log\log(2^{n-1}+2)}\right) \le \exp\left(c'\frac{n^2}{\log(n+1)}\right)$$

for an appropriate choice of c', which gives us the result. □

References

[1] P. Balister, B. Bollobás, R. Morris, J. Sahasrabudhe, and M. Tiba. Covering intervals with arithmetic progressions. *Acta Math. Hungar.*, 161(1):197–200, 2020.

[2] P. Balister, B. Bollobás, R. Morris, J. Sahasrabudhe, and M. Tiba. Erdös covering systems. *Acta Math. Hungar.*, 161(2):540–549, 2020.

[3] Paul Balister, Béla Bollobás, Robert Morris, Julian Sahasrabudhe, and Marius Tiba. The Erdös-Selfridge problem with square-free moduli. *Algebra Number Theory*, 15(3):609–626, 2021.

[4] Paul Balister, Béla Bollobás, Robert Morris, Julian Sahasrabudhe, and Marius Tiba. On the Erdös covering problem: the density of the uncovered set. *Invent. Math.*, 228(1):377–414, 2022.

[5] S. L. G. Choi. Covering the set of integers by congruence classes of distinct moduli. *Math. Comp.*, 25:885–895, 1971.

[6] R. F. Churchhouse. Covering sets and systems of congruences. In *Computers in Mathematical Research*, pages 20–36. North-Holland, Amsterdam, 1968.

[7] R. B. Crittenden and C. L. Vanden Eynden. Any n arithmetic progressions covering the first 2^n integers cover all integers. *Proc. Amer. Math. Soc.*, 24:475–481, 1970.

[8] Maria Cummings, Michael Filaseta, and Ognian Trifonov. An upper bound for the minimum modulus in a covering system with squarefree moduli. *Arxiv*, page 25, 2022.

[9] Paul Erdős. Problems and results on combinatorial number theory. III. In *Number theory day (Proc. Conf., Rockefeller Univ., New York, 1976)*, Lecture Notes in Math., Vol. 626, pages 43–72. Springer, Berlin, 1977.

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

[11] P. Erdös and R. L. Graham. *Old and new problems and results in combinatorial number theory*, volume 28 of *Monographies de L'Enseignement Mathématique [Monographs of L'Enseignement Mathématique]*. Université de Genève, L'Enseignement Mathématique, Geneva, 1980.

[12] Paul Erdös. Remarks on number theory. IV. Extremal problems in number theory. I. *Mat. Lapok*, 13:228–255, 1962.

[13] Paul Erdös. Some recent advances and current problems in number theory. In *Lectures on Modern Mathematics, Vol. III*, pages 196–244. Wiley, New York, 1965.

[14] Paul Erdös. Some recent advances and current problems in number theory. In *Lectures on Modern Mathematics, Vol. III*, pages 196–244. Wiley, New York, 1965.

[15] 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(2):495–517, 2007.

[16] Donald Jason Gibson. A covering system with least modulus 25. *Math. Comp.*, 78(266):1127–1146, 2009.

[17] Joshua Harrington, Yewen Sun, and Tony W. H. Wong. Covering systems with odd moduli. *Discrete Math.*, 345(8):Paper No. 112936, 12, 2022.

[18] Bob Hough. Solution of the minimum modulus problem for covering systems. *Ann. of Math. (2)*, 181(1):361–382, 2015.

[19] Jonah Klein, Dimitris Koukoulopoulos, and Simon Lemieux. On the j-th smallest modulus in a covering system with distinct moduli. *Arxiv*, page 7, 2022.

[20] Dimitris Koukoulopoulos. *The distribution of prime numbers*, volume 203 of *Graduate Studies in Mathematics*. American Mathematical Society, Providence, RI, [2019] ©2019.

[21] Claire Emil Krukenberg. *COVERING SETS OF THE INTEGERS*. ProQuest LLC, Ann Arbor, MI, 1971. Thesis (Ph.D.)–University of Illinois at Urbana-Champaign.

[22] Ryozo Morikawa. Some examples of covering sets. *Bull. Fac. Liberal Arts Nagasaki Univ.*, 21(2):1–4, 1981.

[23] Pace P. Nielsen. A covering system whose smallest modulus is 40. *J. Number Theory*, 129(3):640–666, 2009.

[24] Tyler Owens. *A covering system with minimum modulus 42*. BYU ScholarsArchive, 2014. Thesis (M.Sc.)–Brigham Young University.

[25] J. Barkley Rosser and Lowell Schoenfeld. Approximate formulas for some functions of prime numbers. *Illinois J. Math.*, 6:64–94, 1962.