Spring 2023

Extreme Covering Systems, Primes Plus Squarefrees, and Lattice Points Close to a Helix

Jack Robert Dalton

Extreme Covering Systems, Primes Plus Squarefrees, and Lattice Points Close to a Helix

by

Jack Robert Dalton

Bachelor of Science
University of Massachusetts Dartmouth 2006

Master of Science
University of Vermont 2017

Submitted in Partial Fulfillment of the Requirements

for the Degree of Doctor of Philosophy in

Mathematics

College of Arts and Sciences

University of South Carolina

2023

Accepted by:

Ognian Trifonov, Major Professor

Michael Filaseta, Committee Member

Alexander Duncan, Committee Member

Matthew Boylan, Committee Member

Karl Gregory, Committee Member

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

Acknowledgments

First and foremost, to my advisor, Oggie: Thank you for taking me as a student, for the courses you taught, for agreeing to the independent studies, and all of the guidance and encouragement you provided along the way.

Grace, thank you for making the past five years the best of my life (so far... more great things to come). I don't know if I could have done it without you. I will be forever grateful to this program for helping our paths to cross. Thanks also for convincing me to bring two wonderful goons into my house, and then agreeing that the third fit too well with our family to give away; relaxing in the yard with the four of you helped keep me sane.

Mom, thank you for your belief in me, and your love and support. You say I'm the luckiest person you know, but if that is true, it is only because I have you as my mom.

Sara, thanks for teaching me math when I was little, bringing me to your math class at community college, helping me learn the ropes at UMassD, and showing me that getting a doctoral degree is possible.

Kay and Mark, thank you for inspiring me to creative and intellectual endeavours.

Dad, thanks for employing me while I figured out that higher math is where I wanted to be, and for teaching me that international travel is a lot of fun.

Heather, thanks for being an awesome sister and taking care of dad while I left to get back into math.

Thanks to whoever invented the Fluid Dynamics "seminar." It helped me make and became closer to friends, and it is indirectly how I met Grace. And thanks to

everyone who came out when I was Captain! Yarrr.

Thanks to all the friends I made during my time at UVM and USC: Gabby, Logan, McKenzie, Corey, Tamang, Shelby, Abby, David, Rob, Harsh, Hays, Ann, Blake, Tyler, Sophie, Ada, Ryan, Kewang, Garvin, Christelle, Peter, Victoria, Josiah, Jeremiah, Joe, Jacob, and Trevor.

Thank you to my classmates and friends Cuyler, Drew, and Demmas for forming our study group for quals and comps. I laughed so hard at you guys arguing about analysis that summer that I cried; a much needed comic relief. Also, thanks for rescuing me from our original "office" in the Coliseum; You don't need a PhD in math to know that the four of us would never have fit in a hallway with three desks and one electrical outlet.

Thank you to all the great math teachers I have had in my life, whom I finally feel comfortable calling by their first names: Stephen Swiniarski, Gary Davis, Stephen Hegedus, Richard Foote, Sean Yee, Ognian Trifonov, Michael Filaseta, Jonathan Sands, Frank Thorne, George Androulakis, Michael Wilson, Jae-Hun Jung, Louis Bianco, Taylor Dupuy, Matt Boylan, Alex Duncan, Gary Martin, Richard Faulkenberry, Greg Warrington, Jeff Dinitz, Saeja Kim, Dana Fine, Sigal Gottlieb, and Steve Leon.

To Karl, thanks for being an awesome committee member!

Lastly, thank you to the wonderful administrative faculty who helped me during my graduate career! You do so much for us, but specifically thank you for helping me get all my paperwork in on time!

Abstract

This dissertation considers three different topics.

In the first part, we prove that if the least modulus of a distinct covering system is 4, its largest modulus is at least 60; also, if the least modulus is 3, the least common multiple of the moduli is at least 120; finally, if the least modulus is 4, the least common multiple of the moduli is at least 360. The constants 60, 120, and 360 are best possible, they cannot be replaced by larger constants. We also show that there do not exist distinct covering systems with all of the moduli in the interval $[n, 9n]$ for $n \geq 3$.

In the second part, we obtain a lower bound for the maximum distance between any three distinct points in an affine lattice which are close to a helix with small curvature and torsion. This is a generalization of analogous results in two dimensions.

In the final part, we prove that every positive integer n which is not equal to 1, 2, 3, 6, 11, 30, 155, or 247 can be represented as a sum of a squarefree number and a prime not exceeding $\sqrt{n}$.

Table of Contents

List of Tables

List of Figures

Chapter 1

Extreme Covering Systems

1.1 Introduction

A *covering system* $\mathcal{C}$ is a finite set of congruences $x \equiv r_i \pmod{n_i}$, $i = 1, \ldots, k$, such that every integer satisfies at least one of the congruences. Without loss of generality, we can assume that $1 \leq n_1 \leq \cdots \leq n_k$. A covering system is distinct if further $1 < n_1 < n_2 < \ldots < n_k$. Note that we allow 1 to be a modulus for a covering system in this paper but do not allow 1 to be a modulus for a distinct covering system. Throughout the paper we will denote the least modulus n_1 of the covering by m, the largest modulus n_k by M, and the least common multiple of all moduli by $L(\mathcal{C}) = L$. For example,

$$x \equiv 1 \pmod{2},\ x \equiv 2 \pmod{4},\ x \equiv 0 \pmod{3},\ x \equiv 4 \pmod{6},\ \text{and } x \equiv 8 \pmod{12} \tag{1.1}$$

is a distinct covering system with $m = 2$, $M = 12$, and $L = 12$.

Erdős [10] introduced the use of covering systems in number theory in the 1950s. He constructed a distinct covering system with least modulus 3 and largest modulus 120. Erdős [10] wrote, "It seems likely that for every c there exists such a system all the moduli of which are $> c$." Proving or disproving this statement became *the minimum modulus problem*. For decades many mathematicians believed that indeed, it is possible to construct covering systems with arbitrarily large least modulus.

Swift [34] (1954) found a distinct covering with $m = 4$ and later on with $m = 6$. This was improved throughout the years by Churchhouse [7] with $m = 9$ (1968), Krukenberg [26] with $m = 18$ (1971), Choi [6] with $m = 20$ (1971), and Morikawa

[29] with $m = 24$ (1981). Twenty-five years later, Gibson [20] constructed a distinct covering with $m = 25$. In 2009, Nielsen [30] introduced the use of recursion in covering systems and constructed a distinct covering whose smallest modulus is 40. In the same paper Nielsen wrote, "The method further demonstrates some of the difficulty in answering Erdős' minimum modulus problem, and leads the author to believe that it has a negative solution." Owens [31] refined Nielsen's approach and constructed a distinct covering system with minimum modulus 42.

In 1980, Erdős and Graham [12] investigated systems of congruences with all moduli in $[n, cn]$, where $c > 0$ is a fixed constant. They conjectured that for each $c > 0$ there exists $n(c)$ and $\epsilon(c) > 0$, such that for each set of congruences with moduli $n_1 < \cdots < n_k$ all in $[n, cn]$, the density of the uncovered set is at least $\epsilon(c)$ provided n is sufficiently large, $n \geq n(c)$.

Erdős and Graham's conjecture was proved in 2007 by Filaseta, Ford, Konyagin, Pomerance, and Yu [19]. Building on the work of Filaseta et al., Hough [22] made a real breakthrough and solved *the minimum modulus problem*. He showed that the minimum modulus in any distinct covering system does not exceed 10^{16}.

Erdős and Selfridge posed another famous problem, *the odd covering problem*. The problem is to determine whether there exists a distinct covering with all moduli odd integers. Erdős was convinced [13] that such coverings exist and offered \$25 for a proof that no such covering exists. Selfridge, as recounted from [16], was convinced that no such covering exists and offered \$2000 for the first example of an odd covering.

Work of Balister, Bolobas, Morris, Sahasrabudhe, and Tiba brings us the closest to solving the odd covering problem. Balister et al. [1] show that if $\mathcal{C}$ is a distinct covering, then either $2|L(\mathcal{C})$, or $9|L(\mathcal{C})$, or $15|L(\mathcal{C})$. The authors also show that the least modulus of a distinct covering system does not exceed $616,000$, and that [2] there is no distinct covering system in which all moduli are odd, squarefree integers.

So, in the last fifteen years several remarkable papers concerning coverings with

large minimum modulus appeared. In 1971, Krukenberg [26] wrote a Ph.D. dissertation where he did an extensive study of covering systems with relatively small minimum modulus and obtained a number of interesting results. Unfortunately, none of these results were published in mathematical journals. We outline the main results of Krukenberg's dissertation.

Krukenberg investigated the following problem. Suppose the least modulus m of a distinct covering system is fixed. What is the least possible value of the largest modulus M of the covering system? The covering system (1.1) with $m = 2$ and $M = 12$ has been well-known for many years and Krukenberg constructed a distinct covering system with $m = 3$ and $M = 36$ and proved the following theorem.

Theorem 1 (Krukenberg)**.** *(i) If the minimum modulus of a distinct covering system is* 2*, then its largest modulus is at least* 12*;*

(ii) If the minimum modulus of a distinct covering system is 3*, then its largest modulus is at least* 36*.*

Krukenberg also found a distinct covering system with $m = 4$ and $M = 60$. Krukenberg notes that the value of $M = 60$ is least possible when $m = 4$ and writes "but this result will not be proved here." When $m = 5$, Krukenberg constructed a distinct covering system with $M = 108$ and conjectured that 108 is the least possible value of M in this case.

Krukenberg also provided a complete description of all distinct covering systems with least common multiple of the moduli of the form $L = 2^a 3^b$ with a and b positive integers.

Theorem 2 (Krukenberg)**.** *Let $\mathcal{C}$ be a distinct covering system with least common multiple of the moduli of the form $L = 2^a 3^b$ with a and b positive integers and least modulus m. Then*

(i) $m \leq 4$;

(ii) if $m = 3$, *then* $a \geq 3$, *and* $b \geq 2$;

(iii) if $m = 3$ *and* $a = 3$, *then* $b \geq 3$;

(iv) there exist distinct coverings with $m = 3$ *for each* $L \in \{2^4 3^2, 2^3 3^3\}$;

(v) if $m = 4$, *then* $a \geq 5$ *and* $b \geq 3$;

(vi) there exist distinct coverings with $m = 4$ *for each* $L \in \{2^7 3^3, 2^6 3^4, 2^5 3^5\}$;

(vii) there is no distinct covering with $m = 4$ *and* $L \in \{2^6 3^3, 2^5 3^4\}$.

Krukenberg also constructed a distinct covering system where all moduli are squarefree integers and the system does not use the modulus 3. The problem whether there exists a distinct covering system with all moduli squarefree integers and least modulus 3, is still open. Finally, for m between 3 and 18 with the exception of $m = 7$, Krukenberg constructed distinct covering systems with least modulus m while trying to keep the least common multiple L of all moduli small. Having L small is an advantage. It is much easier to understand the structure of the covering system when L is small and to modify the covering system to obtain a covering system with different properties. Below is a table comparing L in the systems constructed by Churchhouse [7] to the systems constructed by Krukenberg when m is between 3 and 9.

Table 1.1 Comparison of L in the Systems Constructed by Churchhouse to the Systems Constructed by Krukenberg When $m \in [3, 9]$

m	L (Churchhouse)	L (Krukenberg)
3	$2^3 \times 3 \times 5$	$2^3 \times 3 \times 5$
4	$2^4 \times 3^2 \times 5$	$2^3 \times 3^2 \times 5$
5	$2^3 \times 3^2 \times 5 \times 7$	$2^5 \times 3^2 \times 5$
6	$2^5 \times 3^2 \times 5 \times 7$	$2^4 \times 3^2 \times 5 \times 7$
7	$2^5 \times 3^3 \times 5 \times 7$	
8	$2^4 \times 3^3 \times 5^2 \times 7$	$2^5 \times 3^2 \times 5^2 \times 7$
9	$2^7 \times 3^3 \times 5^2 \times 7$	$2^5 \times 3^3 \times 5^2 \times 7$

In the table above there is no entry in the third column for $m = 7$ since Krukenberg modified the covering with $m = 6$ to jump straight to one with $m = 8$.

As a result of the work of Krukenberg, we have an almost complete understanding of distinct covering systems when $m = 3$ and $m = 4$. In this paper we tie a few loose ends left when $m = 3, 4$ and lay the groundwork to extend Krukenberg's work to larger m.

Filaseta, Trifonov, and Yu showed in a research seminar in 2006 that for each integer $n \geq 3$ there is no distinct covering system with all moduli in the interval $[n, 6n]$. We prove the result with a larger constant.

Theorem 3. *For each integer $n \geq 3$, there is no distinct covering system with all moduli in the interval $[n, 9n]$.*

In the fifty years since the Ph.D. thesis of Krukenberg, no proof of Krukenberg's claim that if $m = 4$, then $M \geq 60$ has appeared. We supply a proof.

Theorem 4. *If the minimum modulus in a distinct covering system is 4, then its largest modulus is at least 60.*

Recall that Churchhouse found a covering with $m = 3$ and $L = 120$ and Krukenberg found one with $m = 4$ and $L = 360$. Can one replace the constants 120 and 360 by smaller constants? We show that this is not the case.

Theorem 5. *(i) If the minimum modulus in a distinct covering is 3, then the least common multiple of all the moduli is at least 120;*

(ii) If the minimum modulus in a distinct covering is 4, then the least common multiple of all the moduli is at least 360.

This chapter is organized as follows. In Section 1.2, we introduce new notation which makes analyzing coverings easier, and refine an approach of Krukenberg on reducing the number of congruences in a covering. In Section 1.3, we introduce another tool, 'reduction of a covering' and prove Theorem 4. In Section 1.4, we prove Theorem 3. In Section 1.5, we prove Theorem 5. In Section 1.6, we formulate some

open problems and indicate possible extensions of Krukenberg's work. Finally, in Section 1.7, we give a construction of a distinct covering with a congruence modulo 180 and the remaining moduli in $[4, 56]$.

1.2 Reducing the Number of Congruences in a Covering System

First, we introduce a notation for congruences which is convenient when dealing with covering systems.

Assume we are considering a covering with least common multiple of the moduli $L = p_1^{b_1} \cdots p_k^{b_k}$ (unless specified otherwise, p_k will be the kth prime number). Consider the congruence $x \equiv r \pmod{n}$, where $n > 1$ has prime factorization $n = p_1^{a_1} \cdots p_k^{a_k}$. For the moment, we suppose $a_l \geq 1$ for $l = 1, \ldots, k$. Next, we find the remainders $r_1, r_2, \ldots, r_k$ when r is divided by $p_1^{a_1}, \ldots, p_k^{a_k}$ respectively. Let d_1 be the base p_1 - representation of r_1 with its base p_1 digits written in **reverse** order. Define similarly, $d_2, \ldots, d_k$. Then, $x \equiv r \pmod{n}$ is written $(d_1|\ \ldots|\ d_k)$ in our notation.

For example, consider the congruence $x \equiv 6 \pmod{120}$. It is equivalent to the system of congruences $x \equiv 6 \pmod{8}$, $x \equiv 0 \pmod{3}$, and $x \equiv 1 \pmod{5}$. Thus, for $x \equiv 6 \pmod{120}$ we have $120 = 2^3 \times 3 \times 5$, $r_1 = 6$, $r_2 = 0$, $r_3 = 1$, and $d_1 = 011$, $d_2 = 0$, $d_3 = 1$ (since 6 is 110 in base 2). So, $x \equiv 6 \pmod{120}$ is written $(011|\ 0|\ 1)$.

A technical note on the above notation is that if we consider a congruence modulo $p_1^{a_1} \cdots p_k^{a_k}$, we make sure that in the new notation we have a_1 base p_1 digits in the first component, a_2 base p_2 digits in the second component, and so on. For example, $x \equiv 0 \pmod{360}$ will be $(000|\ 00|\ 0)$, and not $(0|\ 0|\ 0)$ (the congruence $(0|\ 0|\ 0)$ is $x \equiv 0 \pmod{30}$).

The reason we reverse the order of the digits is as follows. Imagine all nonnegative integers organized as a tree with all integers at a vertex at the top, branching to two vertices, one with even integers to the left labeled (0) in our notation, and one with odd integers to the right labeled (1). Next, each of these two vertices branches into two vertices, so we get vertices (00) and (01) on the left, and vertices (10) and (11)

on the right. Having the base 2 digits in reverse order makes it faster to find our path in this tree.

Furthermore, if one or more of the exponents a_l in the factorization $n = p_1^{a_1} \cdots p_k^{a_k}$ is zero, then we put $*$ in the lth position of the notation for the congruence. For example, $x \equiv 1 \pmod{10}$ is written $(1|\ *\ |\ 1)$.

Sometimes, it will be possible to write several residue classes in a more compact way. For example, suppose that at a certain stage of constructing a covering, the uncovered set consists of the residue classes $x \equiv 0 \pmod 6$ and $x \equiv 4 \pmod 6$. In this case, we will denote the uncovered set by $(0|\ 0, 1)$.

Finally, for brevity we truncate trailing $*$s. For example, if $L = 60$, the congruence $x \equiv 0 \pmod 2$ will be written as (0) rather than $(0|\ *\ |\ *)$.

For a final example on this notation, let us analyze the distinct covering system given in (1.1). The first two congruences are (1) and (01) leaving a congruence class modulo 4, namely (00), uncovered. We split it into three classes modulo 12, namely $(00|\ 0, 1, 2)$ which is our way of writing the three congruences given by $(00|\ 0)$, $(00|\ 1)$, and $(00|\ 2)$. We cover $(00|\ 0)$ by a congruence modulo 3, $(*|\ 0)$; we cover $(00|\ 1)$ by a congruence modulo 6, $(0|\ 1)$; finally, we cover $(00|\ 2)$ by a congruence modulo 12, $(00|\ 2)$.

We refer to the representation of a residue class we just introduced as a coordinate representation. This notation is in line with the geometric approach to covering systems of Simpson and Zeilberger [33]. In the case when L is squarefree, congruences correspond to points and hyperplanes in a certain k dimensional box.

If p is a prime, a is a nonnegative integer, and n is a positive integer, then $p^a||n$ will mean that $p^a|n$ and $p^{a+1} \nmid n$.

Next, we define two operations on residue classes - splitting modulo p and reducing modulo p.

Assume that p is a prime, a is a nonnegative integer, n is a positive integer, and

$p^a||n$. Splitting the residue class $r \pmod n$ modulo p means that we replace it by p residue classes modulo np (fibers) by consecutively appending the base-p digits $0, 1, \ldots, p-1$ in the position corresponding to p^{a+1} in the coordinate representation of the residue class. We denote the lth fiber described above by $(r \pmod n)_{p,l}$. For example, if we split $(1|\ 1|\ 4)$ modulo 3, we obtain the three fibers $(1|\ 10, 11, 12|\ 4)$.

Similarly, assume that p is a prime, a and n are positive integers, and $p^a||n$. Reducing the residue class $r \pmod n$ modulo p means that we delete the base-p digit in the position corresponding to p^a in the coordinate representation of the residue class. For example, if we reduce $(0|\ 21|\ 34)$ modulo 5 we get $(0|\ 21|\ 3)$.

Our first tool is the following lemma which builds on ideas of Krukenberg [26].

Lemma 6. *Let $\mathcal{C}$ be a covering system with least common multiple of the moduli L. Assume $p^a||L$ for some prime p and a positive integer a. Denote by $\mathcal{C}_0$ the subset of congruences in $\mathcal{C}$ whose moduli are not divisible by p^a; also, let $\mathcal{C}_1$ be the subset of congruences in $\mathcal{C}$ whose moduli are divisible by p^a.*

Next, for $l = 0, \ldots, p-1$, define B_l as the subset of congruences in $\mathcal{C}_1$ whose congruence class has base-p digit corresponding to p^a (in coordinate notation) equal to l.

Finally, let D_l be the set of congruences in B_l reduced modulo p.

Then, one can replace the congruences in $\mathcal{C}_1$ by $D = \bigcap_{l=0}^{p-1} D_l$ and we will still have a covering; that is, $\mathcal{C}_0 \cup D$ is a covering system.

To clarify, what we do is sort the congruences with moduli divisible by p^a by the base-p digit corresponding to p^a in bins B_l. Next, we delete the base-p digits corresponding to p^a from all congruences in the bins. Finally, we take the intersection of the union of the reduced congruences in each bin. Note that the intersection of unions of sets can be written as a union of intersections. Also, the intersection of the sets covered by several congruences is either an empty set or the set covered by a single congruence with modulus the least common multiple of the moduli of the

congruences we intersect. The claim is that we can replace the congruences in $\mathcal{C}_1$ by the congruences we obtain by the process described above.

For example, if we apply Lemma 6 with $p = 3$ to the covering in (1.1), the bins are $B_0 = \{(*|\ 0)\}$, $B_1 = \{(0|\ 1)\}$, and $B_2 = \{(00|\ 2)\}$. Reducing modulo 3 we get $D_0 = \{(*|\ *)\}$, $D_1 = \{(0|\ *)\}$, and $D_2 = \{(00|\ *)\}$. So, $D = \{(00|\ *)\}$. We claim that replacing the congruences with moduli 3, 6, and 12 by a single congruence modulo 4 still leaves us with a covering. Indeed, (1), (01), and (00) is a covering.

Proof. Let R be the set uncovered by the congruences in $\mathcal{C}_0$. Note that the least common multiple of the moduli in $\mathcal{C}_0$ divides $L_1 = L/p$. Therefore, R can be expressed as a union of residue classes modulo L_1 and $p^{a-1}||L_1$.

Let $r \pmod{L_1}$ be one of the uncovered residue classes in R. We split it modulo p. Consider the fiber $(r \pmod{L_1})_{p,0}$. It does not satisfy any of the congruences in $\mathcal{C}_0$ or in bins $B_1, \ldots, B_{p-1}$. We say that a set of congruences C covers a certain set of integers S if every integer in S satisfies at least one congruence in C. Then, since $\mathcal{C}$ is a covering, the congruences in bin B_0 cover $(r \pmod{L_1})_{p,0}$.

Reducing modulo p we get that the congruences in bin D_0 cover $r \pmod{L_1}$. Since this is true for each residue class in R, we get that the congruences in bin D_0 cover R.

Similarly, we get that the congruences in bin D_l cover R for each $l = 1, \ldots, p-1$. Therefore, $D = \bigcap_{l=0}^{p-1} D_l$ covers R, so we can replace $\mathcal{C}_1$ by D and will still have a covering. □

Corollary 7. *Let $\mathcal{C}$ be a covering such that $p^a|L$ for some prime p and integer $a \geq 1$. Suppose that there are k congruences in $\mathcal{C}$ whose moduli are divisible by p^a. Then, if $k < p$, we can discard from $\mathcal{C}$ all congruences whose moduli are divisible by p^a and will still have a covering.*

Proof. First, we justify that we need only consider the case $a = \nu_p(L)$, where $\nu_p(m)$

for $m \in \mathbb{N}$ is the integer for which $p^{\nu_p(m)}||m$. Suppose we have established the result for the case $a = \nu_p(L)$. With k as stated in the corollary, k is an upper bound on the number of congruences in $\mathcal{C}$ with moduli divisible by p^j for all $j \in \mathbb{Z}$ with $a \leq j \leq \nu_p(L)$. Then by applying the corollary for a replaced by $\nu_p(L)$ to obtain a new covering and then applying the corollary over and over again, one arrives at the covering $\mathcal{C}$ with all congruences having moduli divisible by p^a removed, proving the corollary. So, we suppose now $a = \nu_p(L)$.

Now, let $a = \nu_p(L)$. Since $k < p$, we see that there is an $l \in \{0, 1, \ldots, p-1\}$ in Lemma 6 such that $B_l \neq \emptyset$. Therefore, D_l and, hence, D is $\emptyset$. The corollary now follows from Lemma 6. □

Corollary 8 (Krukenberg)**.** *Let $\mathcal{C}$ be a distinct covering with all moduli in the interval $[c, d]$. If p is a prime and a is a positive integer such that $p^a(p+1) > d$, then we can discard all congruences whose moduli are multiples of p^a and still have a covering.*

Proof. First, since $p^a(p+1) < 2p^{a+1}$, there is at most one multiple of p^{a+1} in $[c, d]$ so by Corollary 7 we can discard the congruence with modulus p^{a+1} (if there is one). This leaves us with at most $p-1$ multiples of p^a in $[c, d]$, namely $p^a \cdot 1, \ldots, p^a \cdot (p-1)$. By applying Corollary 7 again, we can discard all moduli divisible by p^a. □

Corollary 9 (Krukenberg)**.** *Let $\mathcal{C}$ be a covering such that $p^a||L$ for some prime p and integer $a \geq 1$. Let $\mathcal{C}_1$ be the subset of $\mathcal{C}$ consisting of congruences whose moduli are divisible by p^a. Suppose $|\mathcal{C}_1| = p$ and the moduli of the congruences in $\mathcal{C}_1$ are $p^a m_1, \ldots, p^a m_p$. Then,*

(i) one can replace the congruences in $\mathcal{C}_1$ by a single congruence with modulus

$$p^{a-1}\mathrm{lcm}(m_1, \ldots, m_p)$$

and the resulting set will still be a covering.

(ii) if two of the above p congruences are in the same class modulo p^a we can discard all p congruences and the resulting set will still be a covering.

Proof. (i) Again, we use Lemma 6. Now, we split the p congruences into p bins B_l, with $l \in \{0, 1, \ldots, p-1\}$, as in Lemma 6. The only case when $D \neq \emptyset$ is when there is exactly one congruence in each bin and when the system of the p congruences reduced modulo p with moduli $p^{a-1}m_1, \ldots, p^{a-1}m_p$ has a solution. By a generalization of the Chinese remainder theorem, if a finite system of congruences has a solution, the system of congruences is equivalent to a single congruence whose modulus is the least common multiple of the congruences in the finite system. Lemma 6 now implies *(i)*.

(ii) Here we note that since a bin contains two or more congruences, at least one of the remaining bins will be empty, so $D = \emptyset$ in this case. Then the conclusion of Lemma 6 implies *(ii)*. □

Next, we define a *minimal covering system*. A minimal covering system $\mathcal{C}$ is a covering such that no proper subset of $\mathcal{C}$ is a covering system. Clearly, by discarding one by one redundant congruences, after a finite number of steps, any finite covering system can be reduced to a minimal covering system in at least one way.

1.3 Reduction of a covering

Our second tool is *reduction of a covering*. We start with an example.

Consider the covering (1.1). Let $a \in \{0, 1, 2\}$. Since (1.1) is a covering, the residue class $3m + a$ is covered by the congruences in (1.1).

Substituting $3m + a$ for x in each of the congruences of (1.1) and solving for m we get a new covering system. When $a = 0$ we get $m \equiv 1 \pmod 2$, $m \equiv 2 \pmod 4$, $m \equiv 0 \pmod 1$, and two congruences have no solution; when $a = 1$ we obtain $m \equiv 0 \pmod 2$, $m \equiv 3 \pmod 4$, $m \equiv 1 \pmod 2$, and two congruences have no solution; finally, when $a = 2$ we have $m \equiv 1 \pmod 2$, $m \equiv 0 \pmod 4$, $m \equiv 2 \pmod 4$, and two congruences have no solution.

In general, let $\mathcal{C}$ be a covering system and let p be a prime. Let $\mathcal{C}_0$ be the subset of $\mathcal{C}$ of congruences whose moduli are not divisible by p. Let $\mathcal{M}_0$ be the list of the moduli of the congruences in $\mathcal{C}_0$. Similarly, let $\mathcal{C}_1$ be the subset of $\mathcal{C}$ of congruences whose

moduli are divisible by p, and let $\mathcal{M}_1$ be the list of the moduli of the congruences in $\mathcal{C}_1$.

To reduce the covering modulo p for each $a \in \{0, 1, \ldots, p-1\}$ we substitute $pm+a$ for x in each of the congruences of $\mathcal{C}$ and solve for m to get a new covering. This way we end up with p coverings in which each modulus in $\mathcal{M}_0$ is used in all p coverings. However, if m is a modulus in $\mathcal{M}_1$ it gets replaced by m/p and it is used in just one of the p coverings.

Indeed, if $x \equiv r \pmod{n}$ is a congruence in $\mathcal{C}_0$ (so $p \nmid n$), substituting $mp + a$ for x and solving for m, we get $m \equiv p^{-1}(r - a) \pmod{n}$.

However, if $x \equiv r \pmod{n}$ is a congruence in $\mathcal{C}_1$ (so $p|n$), substituting $mp + a$ for x, we get the congruence $mp + a \equiv r \pmod{n}$. The last congruence has a solution if and only if $r \equiv a \pmod{p}$, in which case we get $m \equiv (r - a)/p \pmod{n/p}$.

Next, we say that two congruences are in the same class modulo a positive integer q, if the integers covered by the congruences all belong to one class modulo q. In other words, if the two congruences are $x \equiv r_1 \pmod{n_1}$ and $x \equiv r_2 \pmod{n_2}$, we say that they are in the same class modulo q if $q|n_1$, $q|n_2$, and $r_1 \equiv r_2 \pmod{q}$.

Assume two congruences $x \equiv r_1 \pmod{n_1}$ and $x \equiv r_2 \pmod{n_2}$, both in $\mathcal{C}_0$ are in the same class modulo q with $p \nmid qn_1n_2$. After reduction modulo p, we get $mp \equiv (r_1-a) \pmod{n_1}$ and $mp \equiv (r_2-a) \pmod{n_2}$. Suppose that the reduced congruences are $m \equiv r_1' \pmod{n_1}$ and $m \equiv r_2' \pmod{n_2}$. Then, $mp \equiv r_1'p \equiv (r_1 - a) \pmod{n_1}$ and $mp \equiv r_2'p \equiv (r_2 - a) \pmod{n_2}$. Since $q|n_1$, $q|n_2$, we obtain $r_1'p \equiv r_2'p \pmod{q}$. Furthermore, $p \nmid q$, so $r_1' \equiv r_2' \pmod{q}$. Therefore, the reduced congruences are still in the same class modulo q. Conversely, arguing in the same way one gets that if the two congruences $x \equiv r_1 \pmod{n_1}$ and $x \equiv r_2 \pmod{n_2}$, both in $\mathcal{C}_0$ are *not* in the same class modulo q with $p \nmid qn_1n_2$, then after reduction, the reduced congruences are *not* in the same class modulo q.

To summarize, we showed that the following lemma holds.

Lemma 10. *Let $\mathcal{C}$ be a covering system and let p be a prime. Let $\mathcal{C}_0$ be the subset of $\mathcal{C}$ of congruences whose moduli are not divisible by p. Let $\mathcal{M}_0$ be the list of the moduli of the congruences in $\mathcal{C}_0$. Similarly, let $\mathcal{C}_1$ be the subset of $\mathcal{C}$ of congruences whose moduli are divisible by p, and let $\mathcal{M}_1$ be the list of the moduli of the congruences in $\mathcal{C}_1$.*

Reducing the covering $\mathcal{C}$ modulo p produces p coverings where

(i) each modulus in $\mathcal{M}_0$ is used in each of the p coverings but each modulus n in $\mathcal{M}_1$ is replaced by n/p and is used in just one of the p coverings, and

(ii) if two congruences in $\mathcal{C}_0$ are in the same class modulo a positive integer q, then after reduction they are in the same class modulo q in each of the p coverings; furthermore, if two congruences in $\mathcal{C}_0$ are not in the same class modulo a positive integer q, then after reduction they are not in the same class modulo q.

With the risk of stating the obvious and erring on the side of clarity, we state the following lemma.

Lemma 11. *Let $r_1 \pmod{m_1}$ and $r_2 \pmod{m_2}$ be two congruence (residue) classes with $m_1 \mid m_2$. If there is an integer which belongs to both congruence classes, then every integer in the congruence class $r_2 \pmod{m_2}$ is in the congruence class $r_1 \pmod{m_1}$.*

Proof. Assume that there is an integer r in both $r_1 \pmod{m_1}$ and $r_2 \pmod{m_2}$. Then, $r \equiv r_1 \pmod{m_1}$ and $r \equiv r_2 \pmod{m_2}$. Since $m_1 \mid m_2$, $r \equiv r_2 \pmod{m_2}$ implies $r \equiv r_2 \pmod{m_1}$. Thus, $r_1 \equiv r \equiv r_2 \pmod{m_1}$. Let m be an integer in the residue class $r_2 \pmod{m_2}$, that is, $m \equiv r_2 \pmod{m_2}$. Then, $m \equiv r_2 \pmod{m_1}$ and since $r_1 \equiv r_2 \pmod{m_1}$, we obtain $m \equiv r_1 \pmod{m_1}$, so m is in the residue class $r_1 \pmod{m_1}$. Therefore, if the residue classes $r_1 \pmod{m_1}$ and $r_2 \pmod{m_2}$ intersect, then every element of $r_2 \pmod{m_2}$ is an element of $r_1 \pmod{m_1}$. □

We will be using the above lemma as follows. Suppose $x \equiv r_1 \pmod{m_1}$ and $x \equiv r_2 \pmod{m_2}$ are two congruences in a certain distinct covering $\mathcal{C}$ and $m_1 \mid m_2$. If the sets of integers covered by the two congruences intersect, then by Lemma 11, every integer covered by $x \equiv r_2 \pmod{m_2}$ is covered by $x \equiv r_1 \pmod{m_1}$. Thus, we can discard the congruence $x \equiv r_2 \pmod{m_2}$ from the covering and we will still have a covering. Now, if we add a congruence to a covering, we still have a covering, so we can change r_2 to r_2' so that the two congruences do not intersect. In fact, if the congruences in $\mathcal{C}$ with moduli which are proper divisors of m_2 do not form a covering, without loss of generality, we can assume that the congruence $x \equiv r_2 \pmod{m_2}$ does not intersect any of these congruences. For example, in a distinct covering, without loss of generality, we can assume that a congruence modulo 16 does not cover any integers covered by the congruences modulo 4 and 8.

Next, we prove that there is no distinct covering system with moduli in the interval $[4, 59]$ using a proof by contradiction. Our proof proceeds as follows. First, we will use Corollary 8 and Corollary 9 to reduce the list of possible moduli in the covering to 17 integers. Next, we reduce the covering modulo 3. We explore all ways in which it is possible to construct the three coverings from Lemma 10 which satisfy condition (i) of the lemma. It turns out, this can be done in two ways. In both cases, we obtain a contradiction by showing condition (ii) of Lemma 10 with $q = 5$ is violated.

The reason the details of the proof of Theorem 4 are somewhat complicated is that using moduli in $[4, 59]$ one can get very close to a covering; more precisely, one can cover 179 out of 180 classes modulo 180. In Section 1.7 we give an example of a distinct covering system using congruences with moduli in $[4, 56]$ and a congruence modulo 180.

Proof of Theorem 4. Assume that there exists a distinct covering $\mathcal{C}$ with all moduli in $[4, 59]$. Since every covering contains a subset which is a minimal covering, without loss of generality, we can assume that $\mathcal{C}$ is a minimal covering. Let $\mathcal{M}$ be the set of

the moduli of the congruences in $\mathcal{C}$. Also, let L be the least common multiple of the moduli in $\mathcal{M}$.

By Corollary 8, if $p^a(p+1) > 59$ for some prime p and a positive integer a, then p^a does not divide any modulus in $\mathcal{M}$, so $p^a \nmid L$. Since, $2^5 \cdot 3 > 59$, $3^3 \cdot 4 > 59$, $7^2 \cdot 8 > 5^2 \cdot 6 > 59$, and $p(p+1) > 59$ for $p \geq 11$, we get $L \mid (2^4 \cdot 3^2 \cdot 5 \cdot 7)$. Therefore,

$$\mathcal{M} \subseteq \{4, 8, 16, 6, 12, 24, 48, 9, 18, 36, 5, 10, 20, 40, 15, 30, 45, 7, 14, 21, 28, 35, 42, 56\}.$$

Without loss of generality, we can assume that

$$\mathcal{M} = \{4, 8, 16, 6, 12, 24, 48, 9, 18, 36, 5, 10, 20, 40, 15, 30, 45, 7, 14, 21, 28, 35, 42, 56\}.$$

Indeed, for each modulus m is in the displayed set above which is not in $\mathcal{M}$, we simply add a congruence $x \equiv 0 \pmod{m}$ to $\mathcal{C}$.

When analyzing or constructing a covering using a given set of moduli, following Krukenberg [26], Nielsen [30], Balister et al. [2], we use the moduli in increasing order of arithmetic complexity. For example, above we first list powers of 2, next, powers of 2 times 3, etc. and we do not introduce moduli which are multiples of a not yet used prime p, until moduli with all prime divisors less than p are used.

Next, by Corollary 9 we can replace the seven congruences in $\mathcal{C}$ with moduli divisible by 7 by a single congruence modulo $120 = \operatorname{lcm}(1, 2, 3, 4, 5, 6, 8)$ and still have a covering. Also, by Corollary 9 we can replace the two congruences with moduli $16, 48$ by a single congruence modulo 24 and still have a covering. Denote the resulting covering by $\mathcal{C}'$ and denote the *list* of the moduli of the congruences in $\mathcal{C}'$ by $\mathcal{M}'$. Then, $\mathcal{M}'$ is the list $[4, 8, 6, 12, 24, 24, 9, 18, 36, 5, 10, 20, 40, 15, 30, 120, 45]$, where $[\ldots]$ is used to emphasize that $\mathcal{M}'$ is a list. Note that 24 appears twice in the last list meaning that we have two congruences modulo 24 in $\mathcal{C}'$.

This concludes the first part of the proof.

Next, we reduce the covering $\mathcal{C}'$ modulo 3 and obtain three coverings, say $\mathcal{C}'_0$, $\mathcal{C}'_1$, $\mathcal{C}'_2$, whose moduli are $\mathcal{M}'_0$, $\mathcal{M}'_1$, $\mathcal{M}'_2$, respectively. By Lemma 10 the moduli in

$\mathcal{M}_0 = \{4, 8, 5, 10, 20, 40\}$ can be used in all three coverings, and each modulus in

$$\mathcal{M}_1 = [2*, 4*, 8*, 8*, 3*, 6*, 12*, 5*, 10*, 40*, 15*]$$

can be used in just one of the coverings. We use * to the right of a modulus to indicate that it can be used in at most one of the three coverings $\mathcal{C}'_0$, $\mathcal{C}'_1$, $\mathcal{C}'_2$.

After relabeling, we can assume that $2*$ is in $\mathcal{M}'_0$.

Moreover, by Corollary 7, we can take congruences with moduli $3*, 6*, 12*, 15*$ in only one of $\mathcal{C}'_0$, $\mathcal{C}'_1$, $\mathcal{C}'_2$. (If we have just one or two congruences with moduli divisible by 3 in a covering, we can discard them.)

It is relatively easy to see that we can take $3*, 6*, 12*, 15*$ to be in $\mathcal{M}'_1$ or $\mathcal{M}'_2$. Indeed, $2*, 4, 8$ are already in $\mathcal{M}'_0$. If $8*$ is also in $\mathcal{M}'_0$, no additional congruences are needed to construct the covering $\mathcal{C}'_0$. Note that the congruences with moduli $3*, 6*, 12*$ can cover a congruence class modulo 4 (and some integers outside of it). If $8*$ is in $\mathcal{M}'_1$ or $\mathcal{M}'_2$ and $3*, 6*, 12*, 15*$ are in $\mathcal{M}'_0$, we can swap the congruences with moduli $3*, 6*, 12*, 15*$ and the congruence modulo $8*$ and we will still have three coverings.

Thus, after relabeling we can assume that $3*, 6*, 12*, 15*$ are in $\mathcal{M}'_1$.

Next, we analyze how to allocate the moduli $5*, 10*, 40*$. We claim that $\mathcal{M}'_2$ contains at least one of the moduli $5*, 10*, 40*$. Otherwise,

$$\mathcal{M}'_2 \subseteq [4, 8, 5, 10, 20, 40, 4*, 8*, 8*].$$

Using Corollary 7 we discard any of $5, 10, 20, 40$ from $\mathcal{M}'_2$, leaving us with the impossible task of constructing a covering using only congruences with moduli $4, 8, 4*, 8*, 8*$.

So, we allocated 5 out of 11 moduli in $\mathcal{M}_1$ and have partial information about three of the remaining six moduli. It is possible to allocate the moduli $4*, 8*, 8*, 5*, 10*, 40*$ and to construct the three coverings. However, we will show that it cannot be done without violating condition (ii) of Lemma 10. To this end, we consider two cases.

Case I: The congruences with moduli 20 and 40 in $\mathcal{C}'$ are not in the same class modulo 5.

By Lemma 10 the congruences with moduli 20 and 40 are not in the same class modulo 5 in $\mathcal{C}'_0$, $\mathcal{C}'_1$, and $\mathcal{C}'_2$, as well.

First, note that currently $\mathcal{M}'_0$ contains $\{2*, 4, 8, 5, 10, 20, 40\}$ which is not sufficient to construct a covering. (Discard $5, 10, 20, 40$ using Corollary 7 and we are left only with moduli $2*, 4, 8$.) We assign $40*$ to $\mathcal{M}'_0$, so that covering is possible with moduli from $\mathcal{M}'_0$. All the remaining five moduli $4*, 8*, 8*, 5*, 10*$ are divisors of $40*$, so the remaining two coverings cannot benefit from us assigning a different modulus instead of 40 to $\mathcal{M}'_0$.

Next, we concentrate on allocating $5*, 10*$. We proved above that $\mathcal{M}'_2$ contains at least one of the moduli $5*, 10*$ (since $40*$ is already allocated to $\mathcal{M}'_0$). There are two subcases.

Subcase A: Exactly one of the moduli $5*, 10*$ is in $\mathcal{M}'_2$.

In this subcase,

$$\mathcal{M}'_2 \subseteq [4, 8, 5, 10, 20, 40, 4*, 8*, 8*, 5*],$$

or

$$\mathcal{M}'_2 \subseteq [4, 8, 5, 10, 20, 40, 4*, 8*, 8*, 10*].$$

By Corollary 9 we can replace $5, 10, 20, 40$, and one of $5*$ and $10*$ by a congruence modulo 8. Now, we need to construct a covering using moduli $4, 8, 8$ and some of $4*, 8*, 8*$. The covering $\mathcal{C}'_2$ can be completed only if all three moduli $4*, 8*, 8*$ are in $\mathcal{M}'_2$.

Without loss of generality, we may assume we are left with

$$\mathcal{M}'_1 = [4, 8, 5, 10, 20, 40, 3*, 6*, 12*, 15*, 5*].$$

We finish this subcase by proving the following lemma.

Lemma 12. *There is no covering with congruences whose moduli form the list*

$$[4, 8, 3, 6, 12, 5, 5, 10, 20, 40, 15],$$

such that the congruence with modulus 20 *and the congruence with modulus* 40 *are not in the same class modulo* 5*.*

Proof. We assume that there is such a covering and use Lemma 10 to reduce the covering modulo 3. We get three coverings where each has moduli in the list

$$[4, 8, 5, 5, 10, 20, 40]$$

and each of the moduli in $[1*, 2*, 4*, 5*]$ is used in exactly one covering. Consider one of the three coverings, say $\mathcal{C}''$, which does not use the moduli $1*$ and $2*$. The moduli of $\mathcal{C}''$ are in the list $[4, 4*, 8, 5, 5, 5*, 10, 20, 40]$. Next, we apply Lemma 6 with $p = 5$ to the congruences with moduli $5, 5, 5*, 10, 20, 40$. After reduction modulo 5 we need to place the reduced congruences with moduli $1, 1, 1, 2, 4, 8$ in five bins and take the intersection of the congruences in the five bins. Consider a bin which does not contain a congruence with modulus one of $1, 1, 1, 2$. This bin contains the congruence modulo 4 or the congruence modulo 8 but not both, since 4 and 8 are not in the same bin (the congruences with moduli 20 and 40 are not in the same class modulo 5). So, D is inside a residue class modulo 4. Thus, we can replace the congruences with moduli $5, 5, 5*, 10, 20, 40$ by a single congruence modulo 4. This is a contradiction because it requires building a covering with congruences with moduli $4, 4, 4, 8$. □

Subcase B: Both moduli $5*, 10*$ are in $\mathcal{M}_2'$.

Here

$$\mathcal{M}_2' \subseteq [4, 8, 5, 10, 20, 40, 4*, 8*, 8*, 5*, 10*].$$

We apply Lemma 6 with $p = 5$ to the congruences with moduli $5, 10, 20, 40, 5*, 10*$. Proceeding word for word as in the proof of Lemma 12 we get that we can replace the congruences with moduli $5, 10, 20, 40, 5*, 10*$ by a single congruence modulo 4.

Now, we need to construct a covering using moduli $4, 8, 4$ and some of the moduli $4*, 8*, 8*$. This can be done only if $4*$ and at least one $8*$ are in $\mathcal{M}'_2$.

This leaves

$$\mathcal{M}'_1 = [4, 8, 5, 10, 20, 40, 8*, 3*, 6*, 12*, 15*].$$

Next, by using Corollary 9 we replace the congruences with moduli $5, 10, 20, 40, 15*$ by a single congruence modulo 24. So, we need to construct a covering using moduli $4, 8, 8, 3, 6, 12, 24$. Assume there is such a covering and reduce it modulo 3. We get three new coverings with common moduli $4, 8, 8$ and moduli to be used by just one of the three coverings: $1*, 2*, 4*, 8*$. Consider the covering which does not contain $1*, 2*$. The moduli of the congruences of this covering are at most $4, 8, 8, 4*, 8*$, which is a contradiction.

This completes Case I.

Case II: The congruences with moduli 20 and 40 in $\mathcal{C}'$ are in the same class modulo 5.

First, we claim that $\mathcal{M}'_2$ contains at least two of the moduli $5*, 10*, 40*$. Assume otherwise. Then, $\mathcal{M}'_2$ contains at most the moduli $4, 8, 5, 10, 20, 40, 4*, 8*, 8*$ and one of the moduli $5*, 10*, 40*$. By Corollary 9 we can discard from $\mathcal{C}'_2$ the congruences with moduli $5, 10, 20, 40$ and the congruence with modulus $5*$, $10*$, or $40*$ since two of these congruences are in the same class modulo 5. This leaves us at most with moduli $4, 8, 4*, 8*, 8*$ which are not sufficient to construct a covering, proving the claim.

Thus, $\mathcal{M}'_0$ contains at most one of the moduli $5*, 10*, 40*$. Allocating just one of $5*, 10*, 40*$ to $\mathcal{M}'_0$ does not help construct $\mathcal{C}'_0$. For example, if $5*$ is in $\mathcal{M}'_0$ and $10*, 40*$ are not in $\mathcal{M}'_0$, again, using Corollary 9 we can discard from $\mathcal{C}'_0$ the congruences with moduli $5, 10, 20, 40, 5*$. To complete $\mathcal{C}'_0$ we need to assign to $\mathcal{M}'_0$ one of the moduli $4*, 8*, 8*$. It is possible to construct the covering $\mathcal{C}'_0$ by assigning to it one congruence modulo $8*$ and it is the efficient way to do it. (The coverings $\mathcal{C}'_1$ and $\mathcal{C}'_2$ cannot benefit

from swapping with $\mathcal{C}'_0$ a congruence modulo 4 with a congruence modulo 8.) So, one modulus $8*$ is allocated to $\mathcal{M}'_0$.

Next, we analyze how to split the moduli $5*, 10*, 40*$ among $\mathcal{M}'_1$ and $\mathcal{M}'_2$.

We claim that both moduli $5*$ and $10*$ are in $\mathcal{M}'_2$. Assume otherwise. Then, $\mathcal{M}'_2$ contains at most the moduli $4, 8, 5, 10, 20, 40, 4*, 8*, 40*$ and one of the moduli $5*, 10*$. Apply Lemma 6 to the congruences in the above list which are multiples of 5. Note that in Case II, 4 and 8 are in the same bin and we have either 1 or 2 in a bin depending on whether $5*$ or $10*$ is in $\mathcal{M}'_2$. The only way that D is a nonempty set is when we have

$$|1|2|4,8|1|8| \quad \text{or} \quad |1|2|4,8|2|8|$$

in the five bins (here we use | as a separator between the bins and for brevity, instead of writing 'the congruence modulo 2 is in a certain bin' we just write '2 is in the bin'). Thus, we can replace the congruences with moduli which are multiples of 5 by a single congruence modulo 8. Now, we need to construct a covering with moduli from the list $4, 8, 4*, 8*, 8$ which is impossible.

Thus, we need to allocate both $5*$ and $10*$ to $\mathcal{M}'_2$. There are two subcases depending on how we allocate $40*$.

Subcase A: The modulus $40*$ is in $\mathcal{M}'_1$.

In this subcase $\mathcal{M}'_2$ contains the moduli $4, 8, 5, 10, 20, 40,\ 5*$, and $10*$ and some of the moduli $4*, 8*$. We apply Lemma 6 again to the congruences with moduli $5, 10, 20, 40, 5*$, and $10*$. In this case D is nonempty only if we have $|1|2|4,8|1|2|$ in the bins (again, 4 and 8 must be in the same bin). Therefore, we can replace the congruences with moduli $5, 10, 20, 40,\ 5*$, and $10*$ by two congruences with moduli $4, 8$ respectively. Now, we are left with moduli $4, 8, 4, 8$ and some of $4*, 8*$. So, we need to allocate $4*$ to $\mathcal{M}'_2$. This leaves for $\mathcal{M}'_1$ the moduli $4, 8, 5, 10, 20, 40, 3*, 6*, 12*, 15*, 8*, 40*$. We apply Lemma 6 again, this time to the congruences with moduli $5, 10, 20, 40, 15*, 40*$. Again, D is nonempty only if the con-

tent of the bins is $|1|2|4,8|3|8|$ (in some order). Thus, we can replace the congruences with moduli $5, 10, 20, 40, 15*, 40*$ by a single congruence modulo 24. We are left with moduli $4, 8, 3*, 6*, 12*, 24*, 8*$. We already proved in Case 1, Subcase B that it is not possible to construct a covering with moduli from the last list. The same proof works word for word here, too, so we are done with this subcase.

Subcase B: The modulus $40*$ is in $\mathcal{M}_2'$.

In this subcase, $\mathcal{M}_2'$ contains the moduli $4, 8, 5, 10, 20, 40, 5*, 10*, 40*$ and some of the moduli $4*, 8*$. We apply Lemma 6 again to the congruences with moduli divisible by 5. The congruences reduced modulo 5 have moduli $1, 2, 4, 8, 1, 2, 8$ respectively. We need to place seven congruences in five bins, so at least one bin will contain only one congruence modulo $2, 4$, or 8. Thus, one can replace the congruences with moduli $5, 10, 20, 40, 5*, 10*, 40*$ by a single congruence modulo 2. This leaves $\mathcal{M}_2'$ with moduli $2, 4, 8$ and some of $4*, 8*$, so we allocate $8*$ to $\mathcal{M}_2'$. Now, $\mathcal{M}_1' = [4, 8, 5, 10, 20, 40, 3*, 6*, 12*, 15*, 4*]$. We apply Corollary 9 to the congruences with moduli $5, 10, 20, 40, 15*$. Since the congruences with moduli 20 and 40 in $\mathcal{C}'$ are in the same class modulo 5, we can discard the congruences with moduli $5, 10, 20, 40, 15*$. This leaves us the moduli $4, 8, 3, 6, 12, 4$. We apply Corollary 9 again to replace the congruences with moduli $3, 6, 12$ by a single congruence modulo 4. Finally, we are left with moduli $4, 8, 4, 4$ which is not sufficient to construct a covering.

Having exhausted all cases, we obtain the proof of the theorem. □

1.4 The nonexistence of distinct covering systems with moduli in $[m, 9m]$ for $m \geq 3$

Next, we use Lemma 6 to prove Theorem 3.

Proof of Theorem 3. Assume that for some integer $m \geq 3$ there is a distinct covering $\mathcal{C}$ with all moduli in the interval $[m, 9m]$. Let $\mathcal{C}_m$ be a minimal covering which is a subset of $\mathcal{C}$. Consider the least common multiple L of the moduli of the congruences

in $\mathcal{C}_m$. By Corollary 7, if $p^a|L$ for some prime p and a positive integer a, then the interval $[m, 8m]$ contains at least p multiples of p^a that are not multiples of p^{a+1}. Since one of every p consecutive multiples of p^a is divisible by p^{a+1}, we deduce that the interval $[m, 9m]$ contains at least $p+1$ multiples of p^a.

Denote by $\mathcal{M} \subseteq [m, 9m]$ the set of moduli from the congruences in $\mathcal{C}_m$. Let $p \geq \sqrt{8m+1}$ be a prime. The number of multiples of p in the interval $[m, 9m]$ is

$$n_p := \left\lfloor \frac{9m}{p} \right\rfloor - \left\lfloor \frac{m-1}{p} \right\rfloor = \frac{8m+1}{p} - \left\{ \frac{9m}{p} \right\} + \left\{ \frac{m-1}{p} \right\},$$

where $\{x\}$ denotes the fractional part of x. Since for each x, $0 \leq \{x\} < 1$, we get

$$n_p < \frac{8m+1}{p} + 1 \leq \sqrt{8m+1} + 1 \leq p + 1.$$

Thus, for each $p \geq \sqrt{8m+1}$, there are less than $p+1$ multiples of p in the interval $[m, 9m]$. Therefore, if n is a modulus of one of the congruences in $\mathcal{C}_m$ (that is $n \in \mathcal{M}$), then all the prime divisors of n are less than $\sqrt{8m+1}$. Since the density of integers covered by a congruence modulo n is $1/n$ and $\mathcal{C}_m$ is a covering, we get

$$\sum_{\substack{m \leq n \leq 9m \\ P(n) < \sqrt{8m+1}}} \frac{1}{n} \geq \sum_{n \in \mathcal{M}} \frac{1}{n} \geq 1, \tag{1.2}$$

where $P(n)$ denotes the largest prime divisor of n.

Let

$$S_m = \sum_{n \in \mathcal{M}} \frac{1}{n} \quad \text{and} \quad T_m = \sum_{\substack{m \leq n \leq 9m, \\ P(n) < \sqrt{8m+1}}} \frac{1}{n}.$$

We checked by direct computation and by using the inequality $T_{m-1} \leq T_m + \frac{1}{m-1}$ that $T_m < 1$ for all $m \in [70, 616000]$. Since Balister et al. [1] showed that the minimum modulus of a distinct covering system does not exceed 616000, Theorem 3 holds when $m \geq 51$.

Here we provide some details on how we showed that $T_m < 1$ for all m in $[70, 616000]$.

Using the methods below, we only needed to calculate 23 values of T_m in the interval $[99, 616000]$.

First, we computed and stored $P(n)$, which denotes the largest prime divisor of n, for all n from 2 to $9 \cdot 616000$.

Next note that $T_{m-1} \leq T_m + a_{m-1}$, where we define a_{m-1} to be $\frac{1}{m-1}$ when $P(m-1) < \sqrt{8m-7}$, and we define a_{m-1} to be 0 when $P(m-1) \geq \sqrt{8m-7}$.

Indeed,

$$T_{m-1} = \sum_{\substack{m-1 \leq n \leq 9m-9 \\ P(n) < \sqrt{8m-7}}} \frac{1}{n} = a_{m-1} + \sum_{\substack{m \leq n \leq 9m-9 \\ P(n) < \sqrt{8m-7}}} \frac{1}{n} \leq a_{m-1} + \sum_{\substack{m \leq n \leq 9m \\ P(n) < \sqrt{8m+1}}} \frac{1}{n}.$$

So, we computed $T_{616000} = 0.7377315135995607\ldots$,and then using the inequality $T_{m-1} \leq T_m + a_{m-1}$ we get that $T_{615999} \leq T_{616000} + a_{615999}$. Iterating this method, we backtracked down to the last value of m where the sum is less than 1, which got us to 327067. Thus, because

$$\sum_{m=327067}^{615999} a_m + T_{616000} = 0.99999801282458\ldots < 1,$$

we get that $T_m < 1$ for all $m \in [327067, 616000]$. Next, we computed

$$T_{327066} = 0.7457686535160482\ldots,$$

and backtracked again; we got

$$\sum_{m=178357}^{327066} a_m + T_{327067} = 0.9999963760059897\ldots < 1.$$

Through these jumps, we confirmed that $T_m < 1$ for each m in the intervals

$$[327067, 616000], [178357, 327066], [98613, 178356], [56006, 98612], [32297, 56005],$$
$$[19027, 32296], [11422, 19026], [6993, 11421], [4397, 6992], [2821, 4396], [1847, 2820],$$
$$[1273, 1846], [855, 1272], [612, 854], [441, 611], [331, 440], [254, 330], [205, 253],$$
$$[155, 204], [125, 154], [116, 124], [99, 115].$$

We had to compute 23 values of T_m to get to $m = 99$. We then computed directly all values of T_m for $m \in [3, 98]$.

Also, since Krukenberg showed that there is no distinct covering system with moduli in $[3, 35]$, Theorem 3 holds when $m = 3$.

Furthermore, given Theorem 4, there is no distinct covering system with moduli in $[4, 59]$; therefore Theorem 3 holds when $m = 4$, 5, and 6.

There are 34 occasions when $m \in [7, 98]$ and $T_m \geq 1$. They are shown below.

Table 1.2 Values of $m \in [7, 98]$ Where $T_m \geq 1$

m	7	8	9	10
T_m	1.39261054...	1.29355301...	1.20673202...	1.11863678...
m	11	12	14	16
T_m	1.039257527...	1.068040596...	1.017905675...	1.100318617...
m	17	18	19	20
T_m	1.051288005...	1.070204351...	1.026661782...	1.043613442...
m	22	23	24	25
T_m	1.144971586...	1.104517040...	1.118716267...	1.090503785...
m	26	27	28	37
T_m	1.059106294...	1.033058879...	1.00807173...	1.003611508...
m	38	39	40	46
T_m	1.012487455...	1.021109052...	1.003887834...	1.056792532...
m	47	48	49	50
T_m	1.063969675...	1.070968433...	1.054675401...	1.040984046...
m	51	52	54	67
T_m	1.027553480...	1.012246891...	1.003429288...	1.010436485...
m	68	69		
T_m	1.015368102...	1.003895902...		

So far, we have used Corollary 7 only with $a = 1$. Next, we use Corollary 8 for all $a \geq 1$.

Define

$$L_m = \begin{cases} 5040 = 2^4 \cdot 3^2 \cdot 5 \cdot 7 \text{ if } m \in \{7, 8, 9, 10\} \\ 10080 = 2^5 \cdot 3^2 \cdot 5 \cdot 7 \text{ if } m = 11 \\ 30240 = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \text{ if } m \in \{12, 14\} \\ 332640 = 2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 11 \text{ if } m = 16 \\ 1663200 = 2^5 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \text{ if } m \in \{17, 18, 19, 20\} \\ 43243200 = 2^6 \cdot 3^3 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \text{ if } m \in \{22, 23, 24, 25, 26, 27, 28\} \\ 2205403200 = 2^6 \cdot 3^4 \cdot 5^2 \cdot 7 \cdot 11 \cdot 13 \cdot 17 \text{ if } m \in \{37, 38, 39, 40\} \\ 586637251200 = 2^7 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \text{ if } m \in [46, 52] \\ 13492656777600 = 2^7 \cdot 3^4 \cdot 5^2 \cdot 7^2 \cdot 11 \cdot 13 \cdot 17 \cdot 19 \cdot 23 \text{ if } m \in \{67, 68, 69\}. \end{cases}$$

Using Corollary 8, one checks directly that L divides L_m for each m for which it is defined above. Then for such $m \notin \{7, 8, 22, 23, 24, 46, 47, 48\}$, a direct computation shows we have

$$\sum_{n \in M} \frac{1}{n} \leq \sum_{\substack{d | L_m \\ m \leq d \leq 9m}} \frac{1}{d} < 1. \tag{1.3}$$

As (1.3) contradicts the second inequality in (1.2), the proof is complete for all but $m \in \{7, 8, 22, 23, 24, 46, 47, 48\}$. We deal with each of these cases individually.

For $m = 7$, suppose we have a distinct covering with the moduli of all the congruences in the interval $[7, 63]$. We have

$$\sum_{\substack{d | L_7 \\ 7 \leq d \leq 63}} \frac{1}{d} \approx 1.2253968254.$$

Since there are only 2 permissible multiples of 2^4 in the interval $[7, 63]$, namely 2^4 and $2^4 \cdot 3$, by Corollary 9, we can replace the congruences with these moduli by a single congruence modulo $2^3 \cdot 3$ and still have a covering. This brings the sum of the reciprocals down to approximately 1.1837301587.

Denote the resulting covering by $\mathcal{C}'$ and denote the *list* of the moduli of the congruences in $\mathcal{C}'$ by $\mathcal{M}'$.

Next, we reduce the covering $\mathcal{C}'$ modulo 7 and obtain 7 coverings, say $\mathcal{C}'_0$, $\mathcal{C}'_1$, ..., $\mathcal{C}'_6$, whose moduli are $\mathcal{M}'_0$, $\mathcal{M}'_1$, ..., $\mathcal{M}'_6$, respectively. By Lemma 10 the moduli in

$$\mathcal{M}_0 = [8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 24]$$

can be used in all 7 coverings, and each modulus in

$$\mathcal{M}_1 = \{1*, 2*, 3*, 4*, 5*, 6*, 8*, 9*\}$$

can be used in just one of the coverings. Recall that we use * to the right of a modulus to indicate that it can be used in at most one of the 7 coverings $\mathcal{C}'_0$, $\mathcal{C}'_1$, ..., $\mathcal{C}'_7$.

Now,

$$\sum_{d \in M_0} \frac{1}{d} = 0.8 < 1 - \frac{1}{6},$$

which means that each of the seven coverings needs at least one of the 8 moduli in $\mathcal{M}_1$ to get the sum of the reciprocals to be 1 or more.

After relabeling, we can assume that $1*$ is in $\mathcal{M}'_0$, $2*$ is in $\mathcal{M}'_1$, ..., and $5*$ is in $\mathcal{M}'_4$. This leaves us with three moduli, $6*, 8*$, and $9*$, to distribute into the remaining two coverings, but none of these remaining moduli alone are enough to get the sum of the reciprocals to be 1 or more, and thus we have a contradiction. Therefore, the theorem holds for $m = 7$.

For $m = 8$, the exact same proof works, but with slightly modifications. Suppose we have a distinct covering with the moduli of all the congruences in the interval $[8, 72]$. We have

$$\sum_{\substack{d | L_8 \\ 8 \le d \le 72}} \frac{1}{d} \approx 1.1107142857.$$

Again, since there are only 2 permissible multiples of 2^4 in the interval $[8, 72]$, namely 2^4 and $2^4 \cdot 3$, by Corollary 9, we can replace the congruences with these moduli by a

single congruence modulo $2^3 \cdot 3$ and still have a covering. This brings the sum of the reciprocals down to approximately 1.069047619.

Denote the resulting covering by $\mathcal{C}'$ and denote the *list* of the moduli of the congruences in $\mathcal{C}'$ by $\mathcal{M}'$.

Next, we again reduce the covering $\mathcal{C}'$ modulo 7 and obtain 7 coverings, say $\mathcal{C}'_0$, $\mathcal{C}'_1$, ..., $\mathcal{C}'_6$, whose moduli are $\mathcal{M}'_0$, $\mathcal{M}'_1$, ..., $\mathcal{M}'_6$, respectively. By Lemma 10 the moduli in

$$\mathcal{M}_0 = [8, 9, 10, 12, 15, 18, 20, 24, 30, 36, 40, 45, 60, 72, 24]$$

can be used in all 7 coverings, and each modulus in

$$\mathcal{M}_1 = \{2*, 3*, 4*, 5*, 6*, 8*, 9*, 10*\}$$

can be used in just one of the coverings.

Now,

$$\sum_{d \in M_0} \frac{1}{d} \approx 0.813888889 < 1 - \frac{1}{6},$$

which again means that each of the seven coverings needs at least one of the 8 moduli in $\mathcal{M}_1$ to get the sum of the reciprocals to be 1 or more.

After relabeling, we can assume that $2*$ is in $\mathcal{M}'_0$, $3*$ is in $\mathcal{M}'_1$, ..., and $5*$ is in $\mathcal{M}'_3$. This leaves us with four moduli, $6*, 8*, 9*$, and $10*$, to distribute into the remaining three coverings, but none of these remaining moduli alone are enough to get the sum of the reciprocals to be 1 or more, and thus we have a contradiction. Therefore, the theorem holds for $m = 8$.

For $m = 22$, the proof is much simpler. Assume that there exists a distinct covering $\mathcal{C}$ with all moduli in $[22, 198]$. Since every covering contains a subset which is a minimal covering, without loss of generality, we can assume that $\mathcal{C}$ is a minimal covering. Let $\mathcal{M}$ be the set of the moduli of the congruences in $\mathcal{C}$. Also, let L be the least common multiple of the moduli in $\mathcal{M}$.

Note that

$$\sum_{\substack{d|L_{22}\\ 22\le d\le 198}} \frac{1}{d} \approx 1.0539419377.$$

Next, by Corollary 9 we can replace the 13 congruences in $\mathcal{C}$ with moduli divisible by 13 by a single congruence modulo $27720 = \operatorname{lcm}(2, 3, \ldots, 12, 14, 15)$ and still have a covering.

Finally,

$$\left(\sum_{\substack{d|L_{22}\\ 22\le d\le 198}} \frac{1}{d}\right) - \left(\frac{1}{2\cdot 13} + \ldots + \frac{1}{15\cdot 13}\right) + \frac{1}{27720} \approx 0.8815698653 < 1,$$

which implies the theorem holds for $m = 22$.

For $m = 23$, the proof is similar to $m = 22$. Again, denote the minimal distinct covering with moduli in $[23, 207]$ by $\mathcal{C}$. Note that

$$\sum_{\substack{d|L_{23}\\ 23\le d\le 207}} \frac{1}{d} \approx 1.0134873922.$$

Next, by Corollary 9 we can replace the 13 congruences in $\mathcal{C}$ with moduli divisible by 13 by a single congruence modulo $27720 = \operatorname{lcm}(2, 3, \ldots, 12, 14, 15)$ and still have a covering.

Finally,

$$\left(\sum_{\substack{d|L_{23}\\ 23\le d\le 207}} \frac{1}{d}\right) - \left(\frac{1}{2\cdot 13} + \ldots + \frac{1}{15\cdot 13}\right) + \frac{1}{27720} \approx 0.8411153199 < 1,$$

which implies the theorem holds for $m = 23$.

For $m = 24$, the same procedure that worked with $m = 22$ and 23 does not work because we now have 14 congruences with moduli divisible by 13. However, we can use the techniques that worked on $m = 7$ and 8. We suppose we have a minimal distinct covering, denoted by $\mathcal{C}$, with the moduli of all the congruences in the interval $[24, 216]$. Let $\mathcal{M}$ be the set of the moduli of the congruences in $\mathcal{C}$. Also, let L be the least common multiple of the moduli in $\mathcal{M}$.

Since we know $L \mid L_{24}$, we have

$$M \subseteq \{24, 25, 26, 27, 28, 30, 32, 33, 35, 36, 39, 40, 42, 44, 45, 48, 50, 52, 54, 55, 56, 60, 63, 64, 65, 66, 70, 72, 75, 77, 78, 80, 84, 88, 90, 91, 96, 99, 100, 104, 105, 108, 110, 112, 117, 120, 126, 130, 132, 135, 140, 143, 144, 150, 154, 156, 160, 165, 168, 175, 176, 180, 182, 189, 192, 195, 198, 200, 208, 210, 216\},$$

and thus

$$S_m \leq \sum_{\substack{d \mid L_{24} \\ 24 \leq d \leq 216}} \frac{1}{d} \approx 1.0276866189.$$

By Corollary 9 we can replace the two congruences in $\mathcal{C}$ with moduli 2^6 and $2^6 \cdot 3$ by a single congruence modulo $2^5 \cdot 3$ and still have a covering. Our list is now

$$[24, 25, 26, 27, 28, 30, 32, 33, 35, 36, 39, 40, 42, 44, 45, 48, 50, 52, 54, 55, 56, 60, 63, 65, 66, 70, 72, 75, 77, 78, 80, 84, 88, 90, 91, 96, 99, 100, 104, 105, 108, 110, 112, 117, 120, 126, 130, 132, 135, 140, 143, 144, 150, 154, 156, 160, 165, 168, 175, 176, 180, 182, 189, 195, 198, 200, 208, 210, 216, 96].$$

This brings the sum of the reciprocals down to approximately 1.0172699523.

Denote the resulting covering by $\mathcal{C}'$ and denote the list of the moduli of the congruences in $\mathcal{C}'$ by $\mathcal{M}'$.

Next, we reduce the covering $\mathcal{C}'$ modulo 13 and obtain 13 coverings, say $\mathcal{C}'_0, \mathcal{C}'_1, \ldots, \mathcal{C}'_{12}$, whose moduli are $\mathcal{M}'_0, \mathcal{M}'_1, \ldots, \mathcal{M}'_{12}$, respectively. By Lemma 10 the moduli in

$$\mathcal{M}_0 = [24, 25, 27, 28, 30, 32, 33, 35, 36, 40, 42, 44, 45, 48, 50, 54, 55, 56, 60, 63, 66, 70, 72, 75, 77, 80, 84, 88, 90, 96, 99, 100, 105, 108, 110, 112, 120, 126, 132, 135, 140, 144, 150, 154, 160, 165, 168, 175, 176, 180, 189, 198, 200, 210, 216, 96]$$

can be used in all 13 coverings, and each modulus in

$$\mathcal{M}_1 = \{2*, 3*, 4*, 5*, 6*, 7*, 8*, 9*, 10*, 11*, 12*, 14*, 15*, 16*\}$$

can be used in just one of the coverings. Recall that we use $*$ to the right of a modulus to indicate that it can be used in at most one of the 13 coverings $\mathcal{C}'_0$, $\mathcal{C}'_1$, $\ldots$, $\mathcal{C}'_{12}$.

Now,

$$\sum_{d\in M_0} \frac{1}{d} \approx 0.8400541125541119 < 1 - \frac{1}{7},$$

which means that each of the 13 coverings needs at least one of the 14 moduli in $\mathcal{M}_1$ to get the sum of the reciprocals to be 1 or more.

After relabeling, we can assume that $2* \in \mathcal{M}'_0$, $3* \in \mathcal{M}'_1$, $\ldots$, and $6* \in \mathcal{M}'_4$. This leaves us with 9 moduli, $7*, 8*, 9*, 10*, 11*, 12*, 14*, 15*$, and $16*$, to distribute into the remaining 8 coverings, but none of these remaining moduli alone are enough to get the sum of the reciprocals to be 1 or more, and thus we have a contradiction. Therefore, the theorem holds for $m = 24$.

For $m = 46$, by considering all integers in the interval $[46, 414]$ that are divisors of L_{46}, we get

$$\sum_{\substack{d|L_{46}\\ 46\le d\le 414}} \frac{1}{d} \approx 1.0009313914.$$

Now, because there are only 18 multiples of 19 in the interval $[46, 414]$, we can apply Corollary 7 and discard all of these congruences. The sum of the reciprocals of what is left is $0.8907878584611774 < 1$, and so the theorem holds for $m = 46$.

For $m = 47$, the proof is similar to $m = 22$. Again, denote the minimal distinct covering with moduli in $[47, 423]$ by $\mathcal{C}$. Note that

$$\sum_{\substack{d|L_{47}\\ 47\le d\le 423}} \frac{1}{d} \approx 1.0081085344.$$

Next, by Corollary 9 we can replace the 19 congruences in $\mathcal{C}$ with moduli divisible by 19 by a single congruence modulo $6126120 = \operatorname{lcm}(3, 4, \ldots, 18, 20, 21, 22)$ and still have a covering.

Finally,

$$\left(\sum_{\substack{d|L_{47}\\47\le d\le 423}}\frac{1}{d}\right)-\left(\frac{1}{3\cdot 19}+\ldots+\frac{1}{18\cdot 19}\right)+\frac{1}{6126120}\approx 0.8955728202<1,$$

which implies the theorem holds for $m=47$.

For $m=48$, the proof is identical to $m=47$. Again, denote the minimal distinct covering with moduli in $[48,432]$ by $\mathcal{C}$. Note that

$$\sum_{\substack{d|L_{48}\\48\le d\le 432}}\frac{1}{d}\approx 1.0151072928.$$

Next, by Corollary 9 we can replace the 19 congruences in $\mathcal{C}$ with moduli divisible by 19 by a single congruence modulo $6126120=\ \mathrm{lcm}(3,4,\ldots,18,20,21,22)$ and still have a covering.

Finally,

$$\left(\sum_{\substack{d|L_{48}\\48\le d\le 432}}\frac{1}{d}\right)-\left(\frac{1}{3\cdot 19}+\ldots+\frac{1}{18\cdot 19}\right)+\frac{1}{6126120}\approx 0.9025715786<1,$$

which implies the theorem holds for $m=48$, and the proof is complete. □

1.5 Covering systems with minimum least common multiple of the moduli

In this section we solve the problem of minimizing the least common multiple of the moduli of a distinct covering system with a fixed minimum modulus m in the cases $m=3$ and $m=4$.

First, we need a lemma which will help us reduce the number of cases we need to consider. This lemma is Theorem 1 of Simpson and Zeilberger [33] with the extra condition that the minimum modulus does not change.

Lemma 13. *Let $\mathcal{C}$ be a distinct covering with minimum modulus m, and least common multiple of the moduli $L=L_1q^\alpha$, where q is a prime, $\alpha\ge 1$, and $q\nmid L_1m$. Suppose*

p is a prime which does not divide L_1, and $m \leq p < q$. Then, one can construct a distinct covering $\mathcal{C}_1$ with the same minimum modulus m, and such that the least common multiple of the moduli divides $L_1 p^\alpha$.

Proof. This proof relies on the coordinate notation for congruences we introduced. Note, that the jth coordinate corresponds to the jth prime in the prime factorization of L. Up to this point, everywhere the coordinate notation was used, the jth prime divisor of L was simply the jth prime. The proof of this lemma and the example immediately after the lemma will be the only places where coordinate notation is used and the jth prime divisor of L may be different from the jth prime.

Let q be the jth prime in the prime factorization of L. Write all congruences in $\mathcal{C}$ in coordinate notation. We keep in $\mathcal{C}_1$ the congruences in which all base q digits in the jth coordinate are $\leq p-1$ with no change and discard the remaining congruences. In the congruences which survived, we interpret the jth component modulo p. We claim that the congruences in $\mathcal{C}_1$ form a covering with least common multiple of the moduli $L_1 p^\alpha$.

First, consider a residue class r_1 modulo $L_1 p^\alpha$. Write r_1 in coordinate notation. Note that all digits in the jth position do not exceed $p-1$. The residue class r_1 corresponds to a residue class r modulo $L_1 q^\alpha$ where we have kept all digits in all positions the same (but interpreted the digits in jth position modulo q). Since $\mathcal{C}$ is a covering, there is a congruence c in $\mathcal{C}$ which covers the residue class r. The congruence c corresponds to a congruence c_1 in $\mathcal{C}_1$, where both congruences have the same digits in all positions in coordinate notation. Clearly, c_1 covers r_1, so $\mathcal{C}_1$ is a covering. Moreover, $\mathcal{C}$ is a distinct covering, so by construction $\mathcal{C}_1$ is a distinct covering (all we do is replace q by p in the prime factorization of the moduli and discard some congruences).

Now, we need to show that the minimum modulus of $\mathcal{C}_1$ is still m. First, since $q \nmid m$ the congruence modulo m is not discarded. Next, since the new congruences

we created all have moduli which are multiples of p and $p \geq m$ we did not include in $\mathcal{C}_1$ any congruences with moduli less than m. $\square$

For example, consider the covering $\mathcal{C}$ with $L = 80 = 2^4 5$, (1), (01), (001), (0001), $(*|\ 4)$, $(0|\ 3)$, $(00|\ 2)$, $(000|\ 1)$, $(0000|\ 0)$. Proceeding as in the proof of Lemma 13 with $q = 5$ and $p = 3$, we get the covering $\mathcal{C}_1$ with $L = 48 = 2^4 3$, (1), (01), (001), (0001), $(00|\ 2)$, $(000|\ 1)$, $(0000|\ 0)$.

Now, we turn to Theorem 5. Erdős constructed a covering $\mathcal{C}$ with least modulus $m = 3$. Krukenberg [26] also constructed a covering $\mathcal{C}$ with least modulus $m = 3$, $L(\mathcal{C}) = 120$, without using the moduli 40 and 120. Here is a covering with the above properties (11), (101), $(*|\ 2)$, $(0|\ 1)$, $(100|\ 1)$, $(10|\ 0)$, $(*|\ *|\ 4)$, $(0|\ *|\ 3)$, $(*|\ 0|\ 2)$, $(0|\ 0|\ 1)$, $(01|\ *|\ 0)$, $(00|\ 0|\ 0)$. Next, we prove Theorem 5.

Proof of Theorem 5. First, we deal with part (i), the case $m = 3$. We need to show that if n is less than 120 there is no distinct covering having as moduli only divisors of n which are at least 3. Since the only n less than 120 for which $\sum_{d|n, d\geq 3} \frac{1}{d} \geq 1$ are $24, 36, 48, 60, 72, 84, 90, 96$, and 108, we only need to examine the numbers in this list.

We can eliminate some cases using the work of Krukenberg on coverings with least common multiple of the moduli of the form $2^a 3^b$, see Theorem 2. As proved by Krukenberg, there is no covering with $m = 3$, and $L = 24$, or 36, or 48, or 72, or 96, or 108. What is left is to consider the cases when $m = 3$ and $L = 60$, or 84, or 90. By Lemma 13, if there is a covering with $m = 3$ and $L = 84$, then there is a covering with $m = 3$ and $L = 60$.

To finish the proof, we need to show that there is no covering with $m = 3$ and $L = 60$ or $L = 90$.

First, assume that there is a covering $\mathcal{C}$ with $m = 3$ and $L = 60$. Then, the moduli of the congruences are 4; 3, 6, 12; 5, 10, 20; 15, 30, and 60. Reduce the covering modulo 3. We have to construct three coverings with shared moduli: 4, 5,

10, 20, and moduli used by just one covering: $1*$, $2*$, $4*$, $5*$, $10*$, $20*$. Consider the covering, say $\mathcal{C}_1$ which does not include $1*$, and includes at most one of $5*$, $10*$, and $20*$. Its moduli are 4, 5, 10, 20, some of $2*, 4*$, and at most one of $5*, 10*, 20*$. We can discard from $\mathcal{C}_1$ all congruences with moduli which are multiples of 5 (there at most four of them). Thus, $\mathcal{C}_1$ includes both congruences with moduli $2*$ and $4*$. Let $\mathcal{C}_2$ be the covering including the congruence modulo $1*$. Then the moduli of the congruences in $\mathcal{C}_3$ are at most 4, 5, 10, 20, $5*$, $10*$, $20*$. The sum of the reciprocals of these moduli is at most $.95 < 1$, so a covering with $m = 3$ and $L = 60$ does not exist.

Finally, assume that there is a covering $\mathcal{C}$ with $m = 3$ and $L = 90$. Then, the moduli of the congruences are 3, 6; 9, 18; 5, 10; 15, 30; 45, and 90. Reduce the covering modulo 5. We obtain five coverings with shared moduli: 3, 6, 9, 18, and moduli used by just one covering: $1*$, $2*$, $3*$, $6*$, $9*$, $18*$. Consider the two coverings that do not contain any congruences modulo $1*$, $2*$, or $3*$. Since the sum of the reciprocals of $3, 6, 9, 18$ is $2/3$, both coverings need all three moduli $6*$, $9*$, $18*$. Thus, a covering with $m = 3$ and $L = 90$ does not exist completing the proof of part (i) of the theorem.

Now, we turn to part (ii), the case $m = 4$.

Krukenberg [26] constructed a covering $\mathcal{C}$ with $m = 4$ and $L(\mathcal{C}) = 360$. Here is a covering which uses as moduli all divisors of 360 which are at least 4, except 360. It is (11), (101), (0| 2), (100| 2), (01| 1), (*| 02), (0| 01), (100| 01), (10| 00), (*| *| 4), (0| *| 3), (100| *| 3), (00| *| 2), (*| 1| 0), (0| 1| 1), (10| 1| 1), (100| 1| 2), (*| 00| 0), (0| 00| 1), (01| 00| 2).

We need to show that if n is less than 360 there is no covering using only distinct divisors of n which are at least 4. Since the only positive integers n less than 360 for which $\sum_{d|n, d\geq 4} \frac{1}{d} \geq 1$ are $120, 168, 180, 240, 252, 280, 288, 300$, and 336 we only need to examine these values of n.

Since, 120|240, it is sufficient to show that 240 does not work.

Using Lemma 13 we can reduce the cases $n = 168 = 2^3 \cdot 3 \cdot 7$, $n = 252 = 2^2 \cdot 3^2 \cdot 7$, and $n = 336 = 2^4 \cdot 3 \cdot 7$ to $n = 120$, $n = 180$, and $n = 240$ respectively.

As proved by Krukenberg, Theorem 2, $n = 288 = 2^5 3^2$ does not work either.

Let us consider the case $n = 280$. Here and below, we assume as we may, all divisors of n which are at least 4, appear as a modulus of some congruence. The sum of the reciprocals of the divisors of 280 which are at least 4 is $1.0714\ldots$. However, the congruences modulo 4, 5, and 7 cover a portion of the integers with density $1 - \frac{3}{4} \cdot \frac{4}{5} \cdot \frac{6}{7} = \frac{17}{35}$. Since $\frac{1}{4} + \frac{1}{5} + \frac{1}{7} - \frac{17}{35} = .1071\ldots$, there is no covering with $m = 4$ and $L = 280$.

Next, let $n = 300$. The sum of the reciprocals of the divisors of 300 which are at least 4 is 1.06. However, the intersection of the congruences modulo 4, 5, and 15 is at least $\frac{1}{15} = .0666\ldots$. Therefore, there is no covering with $m = 4$ and $L = 280$.

We are left with two remaining cases: $n = 180$ and $n = 240$. We consider each case in a separate lemma.

Lemma 14. *There is no distinct covering with $m = 4$ and $L = 180$.*

Proof. Assume that $\mathcal{C}$ is a covering with moduli 4; 6, 12; 9, 18, 36; 5, 10, 20; 15, 30, 60; 45, 90, and 180. Let S be the set of congruences with moduli 4, 6, 12, 9, 18, 36. Note that the density of the integers covered by congruences in S is at most $\frac{2}{3}$. Indeed, the sum of the reciprocals of the moduli of congruences in S is $\frac{25}{36}$ and the set of integers covered by the congruences modulo 4 and modulo 9 intersect.

Next, reduce $\mathcal{C}$ modulo 5. We need to construct five coverings with common moduli 4, 6, 12, 9, 18, 36 and moduli used by just one covering: $1*$, $2*$, $4*$, $3*$, $6*$, $12*$, $9*$, $18*$, $36*$.

Consider the three coverings containing the congruences with moduli $1*$, $2*$, $3*$. One can see that either the congruence modulo 2 and S do not form a covering or the congruence modulo 3 and S do not form a covering. Otherwise, the set uncovered

by S is inside a residue class modulo 2 and inside a residue class modulo 3, that is, inside a residue class modulo 6. This is not possible since the set uncovered by S has density at least 1/3.

Thus, the three coverings containing the congruences with moduli $1*$, $2*$, $3*$ contain at least one more congruence. We can assume it has modulus $36*$ (all other $*$ moduli are divisors of 36). So, the fourth covering and the fifth covering need to split the moduli $4*$, $6*$, $12*$, $9*$, $18*$. Now, $\frac{1}{4}+\frac{1}{6}+\frac{1}{12}+\frac{1}{9}+\frac{1}{18}=\frac{2}{3}$. Recall that the set uncovered by S has density at least 1/3. Thus, the only possible way to construct the remaining two coverings is if one covering uses moduli $4*$ and $12*$ and the other covering uses $6*$, $9*$, $18*$. Therefore, we need to be able to construct a covering using the moduli in the list $[4,4,6,12,12,9,18,36]$. By Corollary 9 we can replace the congruences with moduli 9, 18, 36 by a single congruence modulo 12. The moduli of the congruences of the resulting covering are in the list $[4,4,6,12,12,12]$. Since the sum of the reciprocals of the elements of the list $[4,4,6,12,12,12]$ is less that one, it is not possible to construct at least one of the five coverings we needed to construct. □

The proof of the next lemma is somewhat complicated. However, we expect that the methods used in the proof of the lemma will be useful when analyzing coverings with least common multiple of the moduli of the form $2^a3^b5^c$.

Lemma 15. *There is no distinct covering with $m=4$ and $L=240$.*

Proof. In the proof of this lemma we will use the notation (n,r_n) to denote the congruence $x\equiv r_n \pmod{n}$.

Assume that there is a covering

$$\mathcal{C}=\{(n,r_n)\mid n\in\{4,8,16,6,12,24,48,5,10,20,40,80,15,30,60,120,240\}\}.$$

We introduce notation for some of the parts of $\mathcal{C}$. Let

$$\mathcal{C}_1=\{(n,r_n)\mid n\in\{4,8,16\}\},\quad \mathcal{C}_3=\{(n,r_n)\mid n\in\{6,12,24,48\}\},$$

$\mathcal{C}_5 = \{(n, r_n) \mid n \in \{10, 20, 40, 80\}\}$, and $\mathcal{C}_{15} = \{(n, r_n) \mid n \in \{15, 30, 60, 120, 240\}\}$.

Also, let R be the set of the 9 integers in $[0, 15]$ representing the 9 residue classes modulo 16 which are not covered by the congruences in $\mathcal{C}_1$. Note that by Lemma 11, without loss of generality, we can assume that the congruences modulo 4, 8, and 16 do not intersect.

Let $R_0 = R \cap \{x \equiv 0 \pmod 2\}$ and $R_1 = R \cap \{x \equiv 1 \pmod 2\}$.

For each $r \in R$ denote by $a_3(r)$ the number of residue classes modulo 48 of the form $x \equiv r \pmod{16},\ x \equiv a \pmod 3$, which are covered by $\mathcal{C}_3$. One way to visualize this is that the residue class ($r \pmod{16}$) splits into three fibers modulo 48. The quantity $a_3(r)$ counts how many of these fibers are covered by $\mathcal{C}_3$.

Similarly, for each $r \in R$ denote by $a_5(r)$ the number of residue classes modulo 80 of the form $x \equiv r \pmod{16},\ x \equiv b \pmod 5$, which are covered by $\mathcal{C}_5$.

Then, the number of residue classes modulo 240 which are not covered by any of the congruences in $\mathcal{C}_1$, $\mathcal{C}_3$, $\mathcal{C}_5$, nor by the congruence $(5, r_5)$ is at least

$$A := \sum_{r \in R} (3 - a_3(r))(4 - a_5(r)). \tag{1.4}$$

Note that the congruences in $\mathcal{C}_{15}$ can cover at most 5 residue classes modulo 240 which are in the residue class ($r \pmod{16}$). Thus, for each $r \in R$ we have $(3 - a_3(r))(4 - a_5(r)) \leq 5$. Clearly, $(3 - a_3(r))(4 - a_5(r)) \neq 5$.

So, for each $r \in R$ we have

$$(3 - a_3(r))(4 - a_5(r)) \leq 4. \tag{1.5}$$

Furthermore, for each $r \in R$,

$$\text{if} \quad a_3(r)a_5(r) \neq 0, \text{ then } a_3(r)a_5(r) \geq 2. \tag{1.6}$$

We give one more observation. Suppose $r_1 \in R$, $r_2 \in R$, and $r_1 \not\equiv r_2 \pmod 2$. Then the number of residue classes modulo 240 which are either $\equiv r_1 \pmod{16}$ or

$\equiv r_2 \pmod{16}$ and can be covered by $\mathcal{C}_{15}$ is at most 6. Indeed, the congruence modulo 15 can cover at most two such classes, and each of $(30, r_{30})$, $(60, r_{60})$, $(120, r_{120})$, and $(240, r_{240})$ can cover at most one. So, in this case

$$(3 - a_3(r_1))(4 - a_5(r_1)) + (3 - a_3(r_2))(4 - a_5(r_2)) \leq 6. \tag{1.7}$$

We can rewrite (1.4) as

$$A = \sum_{r \in R} (12 - 4a_3(r) - 3a_5(r) + a_3(r)a_5(r)) = 108 - 4S_3 - 3S_5 + O, \tag{1.8}$$

where

$$S_3 = \sum_{r \in R} a_3(r), \quad S_5 = \sum_{r \in R} a_5(r) \quad \text{, and} \quad O = \sum_{r \in R} a_3(r)a_5(r).$$

The quantity O measures the amount of overlap between $\mathcal{C}_3$ and $\mathcal{C}_5$. Ideally, we want O to be small. If possible, cover one set of r's by $\mathcal{C}_3$ and a different set of r's by $\mathcal{C}_5$, while S_3 and S_5 are large, that is, cover a lot without much overlap. At least in the case of this lemma, this proves impossible.

Next, we get bounds for S_3 and S_5.

For $n \in \{2, 4, 6, 8, 16\}$ define

$$M_n = \max_{0 \leq j < n} |R \cap \{x \equiv j \pmod{n}\}|.$$

Here M_n is the size of the largest portion of R in a residue class modulo n.

Then, the congruence $(6, r_6)$ can contribute at most M_2 to S_3, the congruence $(12, r_{12})$ can contribute at most M_4, etc.

Thus, $S_3 \leq M_2 + M_4 + M_8 + M_{16}$. Similarly, $S_5 \leq M_2 + M_4 + M_8 + M_{16}$. Define

$$D_3 = (M_2 + M_4 + M_8 + M_{16}) - S_3 \text{ and} \quad D_5 = (M_2 + M_4 + M_8 + M_{16}) - S_5.$$

In a certain sense, D_3 and D_5 measure the difference between the largest amount we could possibly cover, and what we cover in reality with $\mathcal{C}_3$ and $\mathcal{C}_5$, respectively. For example, if R consists of 1 class r such that $r \equiv 0 \pmod{2}$, and 8 classes r_1 such

that $r_1 \equiv 1 \pmod 2$, and if we have a congruence $(6, r_6)$ with $r_6 \equiv 0 \pmod 2$, then $D_3 \geq 7$ (we could have covered 8 residue classes and covered just 1 instead).

Also, the number of residue classes modulo 240 which can be covered by $\mathcal{C}_{15}$ and are not covered by $\mathcal{C}_2$ does not exceed $9 + M_2 + M_4 + M_8 + M_{16}$. Therefore, if $\mathcal{C}$ is a covering, then $A \leq 9 + M_2 + M_4 + M_8 + M_{16}$. Recall that A is the number of residue classes modulo 240 which are not covered by any of the congruences in $\mathcal{C}_1$, $\mathcal{C}_3$, $\mathcal{C}_5$, nor by the congruence $(5, r_5)$. These classes need to be covered by $\mathcal{C}_{15}$.

Define

$$D_{15} = 9 + (M_2 + M_4 + M_8 + M_{16}) - A.$$

Since by assumption $\mathcal{C}$ is a covering, $D_{15} \geq 0$.

Using (1.8), we get

$$9 + 8(M_2 + M_4 + M_8 + M_{16}) \geq 108 + 4D_3 + 3D_5 + D_{15} + O.$$

Since $M_4 \leq 4$, $M_8 \leq 2$, and $M_{16} \leq 1$, we obtain

$$8M_2 \geq 43 + 4D_3 + 3D_5 + D_{15} + O. \tag{1.9}$$

Next, we consider several cases, depending on the structure of $\mathcal{C}_1$. Without loss of generality, we can assume $r_4 = 0$. Since the set of all integers is invariant to translation by an integer, if $\{(n, r_n) | n \in \mathcal{L}\}$, where $\mathcal{L}$ is a list of moduli, is a covering, then for any integer a, $\{(n, r_n + a) | n \in \mathcal{L}\}$ is also a covering.

Case I. $r_8 \equiv r_{16} \equiv 1 \pmod 2$.

In this case, $|R_0| = 4$, $|R_1| = 5$, and $M_2 = 5$.

From (1.9) we get $0 \geq 3 + 4D_3 + 3D_5 + D_{15} + O$. Since $D_3 \geq 0$, $D_5 \geq 0$, $D_{15} \geq 0$, and $O \geq 0$, we get a contradiction. There is no covering in Case I.

Case II. $r_8 \equiv 1 \pmod 2$ and $r_{16} \equiv 0 \pmod 2$.

In this case, $|R_0| = 3$, $|R_1| = 6$, and $M_2 = 6$.

From (1.9) we get $5 \geq 4D_3 + 3D_5 + D_{15} + O$. Thus, $D_3 \leq 1$ and $D_5 \leq 1$. Hence, $r_6 \equiv 1 \pmod 2$ and $r_{10} \equiv 1 \pmod 2$. We obtain that $a_3(r) \geq 1$ and $a_5(r) \geq 1$ for all $r \in R_1$, so $O \geq 6$, a contradiction in this case, too.

Case III. $r_8 \equiv 0 \pmod 2$ and $r_{16} \equiv 1 \pmod 2$.

In this case, $|R_0| = 2$, $|R_1| = 7$, and $M_2 = 7$.

From (1.9) we get $13 \geq 4D_3 + 3D_5 + D_{15} + O$. Therefore $D_3 \leq 3$ and $D_5 \leq 4$. Again, $r_6 \equiv r_{10} \equiv 1 \pmod 2$. So, $a_3(r) \geq 1$ and $a_5(r) \geq 1$ for all $r \in R_1$. By (1.6), $a_3(r)a_5(r) \geq 2$ for all $r \in R_1$. Therefore, $O \geq 14$, so a covering does not exist in this case, too.

Case IV. $r_8 \equiv r_{16} \equiv 0 \pmod 2$.

Here, $|R_0| = 1$, $|R_1| = 8$, and $M_2 = 8$. So, $R_0 = \{r_0\}$ where r_0 is an even integer in $[0, 15]$.

In this case, we can cover a lot with $\mathcal{C}_3$ and $\mathcal{C}_5$ but the overlap between them is too big and again we fall short of constructing a covering.

First, note that $\sum_{r \in R_1} a_3(r) \leq 8 + 4 + 2 + 1 = 15$. Therefore, there exists $r_1 \in R_1$ such that $a_3(r_1) \leq 1$. By (1.5), we get $a_5(r_1) \geq 2$. Thus, $r_{10} \equiv r_{20} \equiv 1 \pmod 2$ (if any of the congruences in $\mathcal{C}_5$ are used to cover R_0, they should be the ones with the largest moduli since $|R_0| = 1$).

Since, $r_{10} \equiv r_{20} \equiv 1 \pmod 2$, we have $a_5(r_0) \leq 2$, and by (1.5) we get $a_3(r_0) \geq 1$. Therefore, $r_{48} \equiv 0 \pmod 2$.

Similarly, as above, $\sum_{r \in R_1} a_5(r) \leq 15$. Therefore, there exists $r_1' \in R_1$ such that $a_5(r_1') \leq 1$. By (1.5), we get $a_3(r_1') \geq 2$. Thus, $r_6 \equiv r_{12} \equiv 1 \pmod 2$. So, $a_3(r_0) \leq 2$. We proved above that $a_3(r_0) \geq 1$, so $a_3(r_0)$ is either 1 or 2.

Assume that $a_3(r_0) = 1$. Then (1.5) implies $a_5(r_0) \geq 2$, so $r_{40} \equiv r_{80} \equiv 0 \pmod 5$. Hence, $a_5(r) \leq 2$ for all $r \in R_1$. This implies $(3 - a_3(r_1))(4 - a_5(r_1)) \geq 4$. Also, $(3 - a_3(r_0))(4 - a_5(r_0)) \geq 4$. Thus,

$$(3 - a_3(r_1))(4 - a_5(r_1)) + (3 - a_3(r_0))(4 - a_5(r_0)) \geq 8,$$

which contradicts (1.7).

So, $a_3(r_0) = 2$, and $r_{24} \equiv r_{48} \equiv 0 \pmod 2$.

Next, let $R_1' = \{r \in R_1 \mid r \not\equiv r_{12} \pmod 4\}$. For all $r \in R_1'$ we have $a_3(r) = 1$.

Also,

$$\sum_{r \in R_1'} a_5(r) \leq 4 + 4 + 2 + 1 = 11,$$

so there exists $r_1^* \in R_1'$ with $a_5(r_1^*) \leq 2$.

Then $(3 - a_3(r_1^*))(4 - a_5(r_1^*)) \geq 4$. By (1.7) we get $((3 - a_3(r_0))(4 - a_5(r_0)) \leq 2$. Thus, $a_5(r_0) = 2$, and $r_{40} \equiv r_{80} \equiv 0 \pmod 2$.

We have allocated all congruences in $\mathcal{C}_3$ and $\mathcal{C}_5$ to R_0 and R_1 (both R_0 and R_1 get two congruences from $\mathcal{C}_3$ and two from $\mathcal{C}_5$). Since $M_2 = 8$, (1.9) becomes

$$21 \geq 4D_3 + 3D_5 + D_{15} + O. \tag{1.10}$$

However, $D_3 \geq 1$, since $(24, r_{24})$ covers just one class modulo 48, and $D_5 \geq 1$ since we did not use $(40, r_{40})$ in the most efficient way either.

Also, $a_3(r)a_5(r) \neq 0$ for all $r \in R$, so by (1.6) $a_3(r)a_5(r) \geq 2$ for all $r \in R$, and $O \geq 18$. Substituting in (1.10) we get $21 \geq 4 + 3 + 18$, a contradiction. □

We just considered the last remaining case, and this concludes the proof of Theorem 5. □

1.6 Open problems and further work

Recall that Krukenberg constructed a distinct covering system with least modulus 5 and largest modulus 108. He also conjectured that one cannot replace 108 by a smaller constant.

Problem 1. Prove or disprove that if the least modulus of a distinct covering system is 5, then its largest modulus is at least 108.

We can show that if the least modulus of a distinct covering system is 5, then its largest modulus is at least 84. However, the result is too weak and the proof too long, to be included in this paper.

Krukenberg also provided a description of the covering systems with least common multiple of the moduli of the form 2^a3^b, see Theorem 2.

Problem 2. Describe the distinct covering systems with least common multiple of the moduli of the form $2^a3^b5^c$ where a, b, and c are positive integers.

Krukenberg [26] already provided such description in the case when $L = 2^a3^b5^c$ and one of the exponents a, b, and c is zero. Using Krukenberg's results and the results of this paper one can find such a description when $a \geq b \geq c \geq 1$ and the minimum modulus $m = 2, 3, 4$ with one exception. Extra work is needed to show that there is no distinct covering system with $m = 4$ and $L = 900$ (our proof of this is too long and technical to be included here). The more interesting case is when $m \geq 5$.

Furthermore, Krukenberg constructed a distinct covering system with $m = 5$ and $L = 1440$.

Problem 3. Prove or disprove that if the least modulus of a distinct covering system is 5, then the least common multiple of its moduli is at least 1440.

Krukenberg also constructed a distinct covering system not using the modulus 3, with all moduli squarefree integers. It is not known whether there exists a distinct covering system with squarefree moduli and least modulus 3.

Problem 4. Prove or disprove that the least modulus of any distinct covering system with squarefree moduli is 2.

Showing that the least modulus of any distinct covering system with squarefree moduli is 2 will lead to a complete solution of the *minimum modulus problem* in the squarefree case.

Problem 5. Find the largest integer c such that there exists a finite set of congruences with distinct moduli with the property that every integer satisfies at least c of the congruences. In other words, what is the largest number of times we can cover the integers by a finite system of congruences with distinct positive moduli?

For a positive integer n let $c(n)$ be the largest number of times we can cover all

integers using congruences with moduli $1, 2, \ldots, n$ respectively. Clearly, $c(1) = 1$. Also, $c(n) \leq c(n+1)$ for all positive integers n (having more congruences allows us to cover more). Furthermore, $c(n+1) \leq c(n)+1$ for all n. Indeed, if a certain integer is covered $c(n)$ times by certain congruences with moduli $1, \ldots, n$, it can be covered at most once more by a congruence with modulus $n+1$.

Recall that by Theorem 1 there is no distinct covering with moduli in the interval $[2, 11]$, and there is a distinct covering with moduli $2, 3, 4, 6, 12$. Therefore, $c(2) = \cdots = c(11) = 1$, and $c(12) = 2$. Moreover, Krukenberg constructed a distinct covering with least modulus 13 and largest modulus 52562109600. Therefore, $c(52562109600) \geq 3$.

Moreover, the sequence $\{c(n)\}_{n=1}^{\infty}$ is bounded. Recall that Balister et al. [1] showed that the least modulus of any distinct covering system does not exceed 616000. If we consider a system of congruences with moduli $1, 2, \ldots, n$ respectively, where $n > 616000$, there will be an integer m which is not covered by any of the congruences with moduli $616001, 616002, \ldots, n$. Even if m is covered by each of the congruences with moduli $1, \ldots, 616000$, then m will be covered 616000 times. Thus, $c(n) \leq 616000$ for all n.

Thus, $c = \lim_{n\to\infty} c(n)$ exists and Problem 5 is to find c.

Problem 5 was considered by Harrington [21] who constructed three distinct covering systems with nonintersecting sets of moduli, thus establishing $c \geq 4$.

We have a heuristic based on several assumptions showing that c is either 4 or 5.

1.7 Construction of a distinct covering with a congruence modulo 180 and the remaining moduli in $[4, 56]$

Here we provide an example of a distinct covering system with a congruence modulo 180 and the remaining moduli in $[4, 56]$. The moduli we use are

$$4, 8, 16; 6, 12, 24, 48; 9, 18, 36; 5, 10, 20, 40; 15, 30; 45, 180; 7, 14, 21, 28, 35, 42, 56,$$

where the semicolons are used to separate the moduli involved in different stages of our argument below.

The congruences modulo $4, 8, 16$ which we use are (11), (101), and (1001). The uncovered set after the first stage consists of a residue class modulo 2, (0), and a residue class modulo 16, (1000).

Splitting modulo 3, the uncovered set is $(0|\ 0, 1, 2)$ and $(1000|\ 0, 1, 2)$.

Next, we use the congruences modulo $12, 24, 48$ to cover (1000). The congruences modulo $12, 24, 48$ given by $(10|\ 0)$, $(100|\ 1)$, and $(1000|\ 2)$ accomplish this.

We use the congruence modulo 6 given by $(0|\ 2)$. After the second stage, the uncovered set is $(0|\ 0, 1)$.

We use the congruences modulo $9, 18, 36$ to attack the residue class $(0|\ 1)$, which is the same as $(0|\ 10, 11, 12)$. We take the congruences modulo $9, 18, 36$ to be $(*|12)$, $(0|\ 11)$, and $(01|\ 10)$. The uncovered set after the third stage is $(0|\ 0)$ and $(00|\ 10)$.

We split the uncovered set modulo 5, to get

$$(0|\ 0|\ 0, 1, 2, 3, 4), \text{ and } (00|\ 10|\ 0, 1, 2, 3, 4).$$

The congruences modulo 5, 10, and 20 are $(*|\ *|\ 4)$, $(0|\ *|\ 3)$, and $(00|\ *|\ 2)$. Now, the uncovered set is $(0|\ 0|\ 0, 1)$, $(01|\ 0|\ 2)$, and $(00|\ 10|\ 0, 1)$. The congruence modulo 40 is $(011|\ *|\ 2)$. The congruences modulo 15 and 30 are $(*|\ 0|\ 1)$ and $(0|\ 0|\ 0)$, and they cover $(0|\ 0|\ 0, 1)$. We are left with the uncovered set $(010|\ 0|\ 2)$ and $(00|\ 10|\ 0, 1)$. We use the congruences modulo 45 and 180, $(*|\ 10|\ 1)$ and $(00|\ 10|\ 0)$ to cover $(00|\ 10|\ 0, 1)$. We are left with the single uncovered residue class $(010|\ 0|\ 2)$ which we cover with the last seven congruences $(*|\ *|\ *|\ 6)$, $(0|\ *|\ *|\ 5)$, $(*|\ 0|\ *|\ 4)$, $(01|\ *|\ *|\ 3)$, $(*|\ *|\ 2|\ 2)$, $(0|\ 0|\ *|\ 1)$, and $(010|\ *|\ *|\ 0)$.

Chapter 2

Bounding the Number of Lattice Points Close to a Helix

2.1 Introduction

The problem of estimating the number of lattice points on or close to a curve has a rich history. In 1926, Jarník [25] proved that the number of integer points on a strictly convex closed curve of length $L > 3$ does not exceed

$$3(2\pi)^{-1/3}L^{2/3} + O\left(L^{1/3}\right)$$

and the exponent and the constant of the leading term are best possible. Assuming higher order smoothness conditions on the curve, a number of authors achieved sharper estimates, in particular Swinnerton-Dyer [35] and Bombieri and Pila [4].

Estimating the number of lattice points *close* to a curve is a more recent topic. For a survey of results on this topic and their applications one may see [18] and [17].

In 1972, Zygmund published a paper on spherical summability of Fourier series in two dimensions where an essential component was the following theorem.

Theorem 16. *(Schinzel) An arc of length $\sqrt[3]{2}R^{1/3}$ on a circle of radius R contains no more than two lattice points.*

The original proof is due to Schinzel but the following short proof was provided by Pelczynski.

Proof. Let $A_0(x_0, y_0)$, $A_1(x_1, y_1)$, and $A_2(x_2, y_2)$ be distinct lattice points on a circle of radius R.

Denote by a, b, and c the lengths of the sides of $\triangle A_0A_1A_2$, and its area by S. Since the circle is a strictly convex curve, we have

$$S = \frac{1}{2}\left|\begin{vmatrix} x_0 & y_0 & 1 \\ x_1 & y_1 & 1 \\ x_2 & y_2 & 1 \end{vmatrix}\right| \geq \frac{1}{2}.$$

.

On the other hand, by a formula attributed to Heron of Alexandria, we have $S = \dfrac{abc}{4R}$.

Thus, $abc \geq 2R$, which implies $(\max\{a, b, c\})^3 \geq 2R$, and the result follows. □

We now give a proof of the formula for the area of a circle in terms of the lengths of the edges and the radius of the circumscribed circle. But first, we provide a proof of the Central Angle Theorem.

Theorem 17 (Central Angle Theorem)**.** *The value of a central angle is twice the value of the inscribed angle that intercepts the same arc.*

Proof. Consider Image 2.1 where a circle is circumscribed on the $\triangle ABC$. Denote the radius of this circle by R, and its center by O.

Let $\measuredangle BAO = x$ and $\measuredangle CAO = y$. Then $\measuredangle ABO = x$ and $\measuredangle ACO = y$. Thus, $\measuredangle AOB = \pi - 2x$ and $\measuredangle AOC = \pi - 2y$. Then $\measuredangle BOE = 2x$ and $\measuredangle COE = 2y$, and therefore $2\measuredangle BAC = \measuredangle BOC$. □

We now state the area formula.

Theorem 18. *The area of a triangle of edge lengths a, b, and c is*

$$\frac{abc}{4R},$$

where R is the radius of the circumscribed circle.

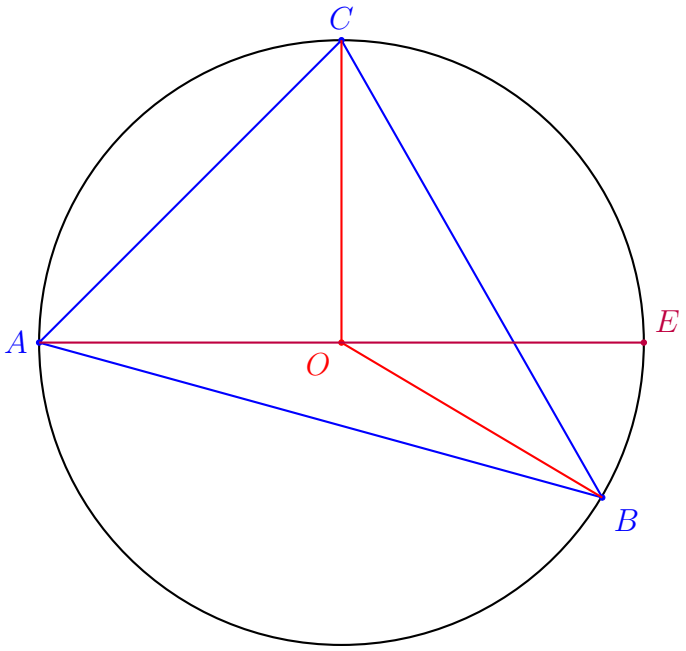

Figure 2.1 The Central Angle Theorem from Geometry

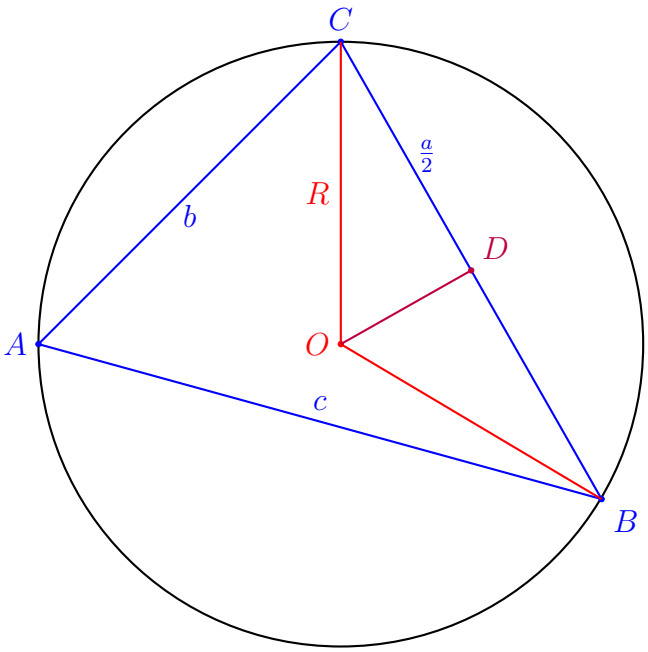

Figure 2.2 An Equation for the Area of a Triangle in Terms of its Edge Lengths and the Radius of the Circumscribed Circle

Proof. Consider Image 2.2 where a circle is circumscribed on the $\triangle ABC$. Denote the radius of this circle by R, and its center by O. Let D be the midpoint on the line-segment BC. Thus $\measuredangle CDO = \measuredangle BDO = \frac{\pi}{2}$. By the Central Angle Theorem, $\measuredangle COD = \measuredangle CAB$.

Thus

$$\text{Area}(\triangle ABC) = \frac{1}{2}bc\sin(\angle CAB) = \frac{1}{2}bc\sin(\angle COD) = \frac{1}{2}bc\left(\frac{a/2}{R}\right) = \frac{abc}{4R}.$$

□

In the paper [23] Howard and Trifonov generalized Schinzel's result to the case of a plane curve with bounded curvature and points close to a plane affine lattice (where a plane affine lattice is the set $\{\mathbf{v}_0 + m\mathbf{v}_1 + n\mathbf{v}_2 : m \in \mathbb{Z}, n \in \mathbb{Z},\}$ where $\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2$ are plane vectors such that $\mathbf{v}_1$ and $\mathbf{v}_2$ are linearly independent).

There are only a few papers on the topic of lattice points close to a three-dimensional curve.

Huang [24] obtains estimates for the number of lattice points close dilations of a curve with parametrization $(x, f_1(x), f_2(x))$, $x \in [a, b]$. Huang's estimates depend on the dilation parameter q, an upper bound δ for the distance between the lattice points and the curve, and a constant depending on the functions f_1 and f_2 which is not explicitly computed.

In Chapter 4 of his PhD dissertation, Letendre [27] obtains estimates for the number of lattice points close dilations of a curve with parametrization $(x, f_1(x), f_2(x))$, $x \in [a, b]$. His results only assume bounds on certain quantities involving derivatives of f_1 and f_2.

We consider the special case when the curve is a helix and obtain a lower bound for the maximal distance between any three distinct points in a general lattice close to a helix.

First we need some general definitions. Let $\mathbf{r}(s)$ be a space curve with arclength parameter s. Let $\mathbf{T} = \frac{d\mathbf{r}}{ds}$ be the unit tangent vector of $\mathbf{r}$. The curvature of $\mathbf{r}(s)$, denoted by κ, is defined as $\kappa = \left|\frac{d\mathbf{T}}{ds}\right|$. The unit normal vector we define as $\mathbf{N} = \frac{1}{\kappa}\frac{d\mathbf{T}}{ds}$, and the binormal vector as $\mathbf{B} = \mathbf{T} \times \mathbf{N}$ where $\times$ denotes the cross product. The torsion, τ, is defined as $-\frac{d\mathbf{B}}{ds} \cdot \mathbf{N}$, where $\cdot$ denotes the scalar product. Lastly, we define a helix as a space curve with constant, non-zero curvature and torsion.

We next define a lattice in three-space as follows.

Definition 19. Let $\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2$, and $\mathbf{v}_3$ be vectors in $\mathbb{R}^3$ with $\mathbf{v}_1$, $\mathbf{v}_2$, and $\mathbf{v}_3$ linearly independent. Then, the *affine lattice generated by* $\boldsymbol{v}_1$, $\boldsymbol{v}_2$, *and* $\boldsymbol{v}_3$ *with origin* $\boldsymbol{v}_0$ is

$$\mathcal{L} = \mathcal{L}(\mathbf{v}_0, \mathbf{v}_1, \mathbf{v}_2, \mathbf{v}_3) = \{\mathbf{v}_0 + m\mathbf{v}_1 + n\mathbf{v}_2 + p\mathbf{v}_3 : m, n, p \in \mathbb{Z}\}.$$

We will show in Section 2.2 that for each lattice $\mathcal{L}$ there exist positive constants $\mathcal{D}_\mathcal{L}$ and $\mathcal{A}_\mathcal{L}$ (depending on $\mathcal{L}$) such that if A_0' and A_1' are two distinct lattice points in $\mathcal{L}$ then

$$|A_0'A_1'| \geq \mathcal{D}_L;$$

furthermore, if A_0', A_1', and A_2' are three non-collinear lattice points in $\mathcal{L}$, then

$$\text{Area}(\triangle A_0'A_1'A_2') \geq \mathcal{A}_\mathcal{L}.$$

Our main result is

Theorem 20. *Let $\mathcal{H}$ be a helix of curvature $\kappa > 0$ and torsion $\tau > 0$, and let*

$$0 \leq \delta \leq \min\left(\frac{\mathcal{D}_\mathcal{L}}{4}, \frac{4\mathcal{D}_\mathcal{L}^2}{11\pi^3}\kappa^2(\kappa^2+\tau^2)^{-\frac{3}{2}}, \frac{2\mathcal{A}_\mathcal{L}}{11\pi}(\kappa^2+\tau^2)^{\frac{1}{2}}\right).$$

Let $\mathcal{L}$ be an affine lattice, and let A_0', A_1', and A_2' be three distinct points in $\mathcal{L}$ which are within δ of the helix $\mathcal{H}$. Then the maximal distance between A_0', A_1', and A_2' is at least

$$\min\left(1.2\mathcal{A}_\mathcal{L}^{\frac{1}{3}}\kappa^{-\frac{1}{3}} - 2\delta, \frac{\pi\tau}{\kappa^2+\tau^2} - 2\delta\right).$$

The above theorem is a generalization of Schinzel's result to the case of a helix.

Corollary 21. *Let $\mathcal{H}$ be a helix of curvature $\kappa > 0$ and torsion $\tau > 0$ with*

$$\tau\kappa^{\frac{1}{3}} \geq 0.4(\kappa^2 + \tau^2).$$

Let A_0, A_1, and A_2 be three distinct lattice points on $\mathcal{H}$. Then, the maximal distance between A_0, A_1, and A_2 is at least $1.1\kappa^{-\frac{1}{3}}$.

We expect that an analogue of our main result will hold for curves such that $0 < c_1K < \kappa(s) < c_2K$ and $0 < c_3T < \tau(s) < c_4T$ where c_1, c_2, c_3, and c_4 are positive constants.

2.2 Some Auxiliary Results

In this section we prove several lemmas which will be needed in the proof of Theorem 20.

Lemma 22. *The area of a triangle in 3-space with non-collinear integer lattice point vertices is at least $\frac{1}{2}$.*

Proof. Let A, B, and C be non-collinear lattice points in $\mathbb{Z}^3$. Then, the area of $\triangle ABC$ equals $\frac{1}{2}\left|\overrightarrow{AB} \times \overrightarrow{AC}\right|$. Since A, B, and C are lattice points, the components of the vectors $\overrightarrow{AB}$, $\overrightarrow{AC}$ are integers. Therefore, the components of the cross product $\overrightarrow{AB} \times \overrightarrow{AC}$ are integers, as well. Thus, $\text{Area}(\triangle ABC) = \frac{1}{2}\sqrt{n}$ for some integer n. Since the points A, B, and C are non-collinear, $\text{Area}(\triangle ABC) \neq 0$, so $n \neq 0$. □

The next two lemmas were proved by Howard and Trifonov [23] in the $\mathbb{R}^2$ case. The lemmas are easily extended to the n-dimensional case.

Lemma 23. *Let A_0, A_1, A_2, and A_2' be points in $\mathbb{R}^n$ where $n \geq 2$. Let $\delta \geq 0$ and $|A_2A_2'| \leq \delta$. Denote by S the area of $\triangle A_0A_1A_2$, and by S_1 the area of $\triangle A_0A_1A_2'$. Then,*

$$|S - S_1| \leq \frac{\delta|A_0A_1|}{2}.$$

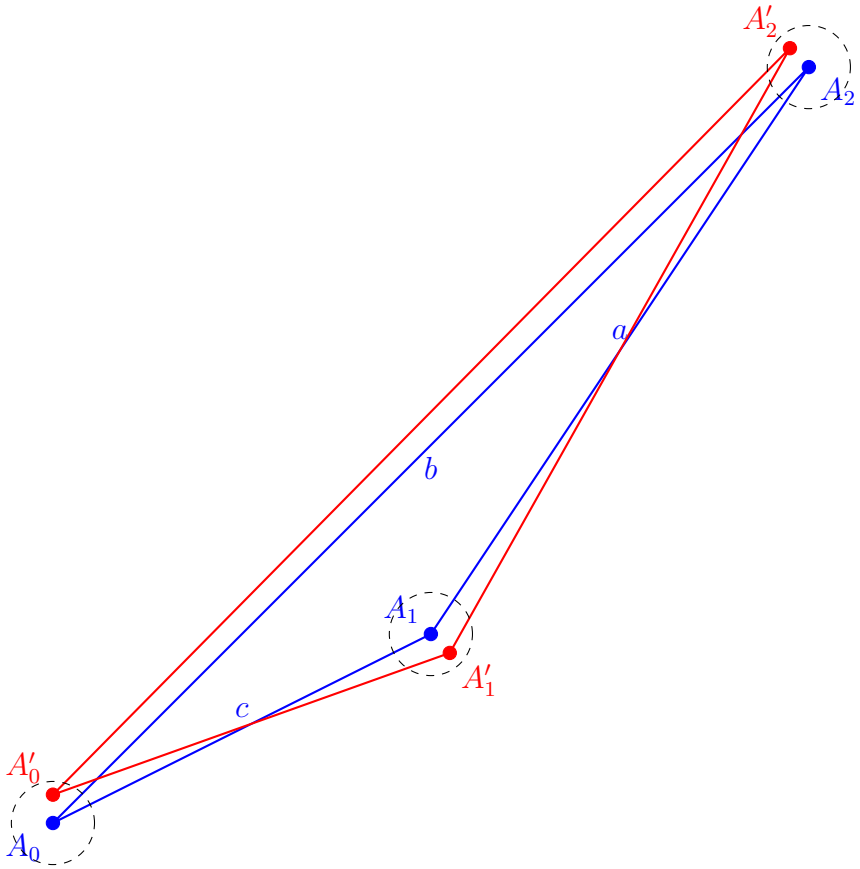

Figure 2.3 Bounding the Difference in Triangle Area When All Three Vertices Are Moved by at Most δ

Proof. Let h be the distance from the point A_2 to the line A_0A_1, and let h_1 be the distance from the point A_2' to the line A_0A_1. Then, $S = \dfrac{|A_0A_1|h}{2}$ and $S_1 = \dfrac{|A_0A_1|h_1}{2}$.

By the triangle inequality,

$$h_1 \leq h + |A_2A_2'| \leq h + \delta \quad \text{and} \quad h \leq h_1 + |A_2A_2'| \leq h_1 + \delta.$$

Therefore, $|h - h_1| \leq \delta$, so

$$|S - S_1| = \frac{|A_0A_1||h - h_1|}{2} \leq \frac{\delta|A_0A_1|}{2}.$$

□

Lemma 24. *Let $\triangle A_0A_1A_2$ and $\triangle A_0'A_1'A_2'$ be triangles in $\mathbb{R}^n$ where $n \geq 2$, with areas S and S_3, respectively. Let $\delta \geq 0$ and assume*

$$|A_0A_0'| \leq \delta,\ |A_1A_1'| \leq \delta,\ \textit{and}\ |A_2A_2'| \leq \delta.$$

Then,

$$|S - S_3| \leq \frac{(|A_0A_1| + |A_0A_2| + |A_1A_2|)\delta}{2} + \frac{3\delta^2}{2}.$$

Proof. Let S_1 be the area of $\triangle A_0A_1A_2'$, and let S_2 be the area of $\triangle A_0A_1'A_2'$. Then

$$\begin{aligned} |S - S_3| &= |S - S_1 + S_1 - S_2 + S_2 - S_3| \\ &\leq |S - S_1| + |S_1 - S_2| + |S_2 - S_3|. \end{aligned}$$

By Lemma 23, $|S - S_1| \leq \dfrac{\delta|A_0A_1|}{2}$. Applying Lemma 23 to the points A_0, A_2', A_1, and A_1', we get $|S_1 - S_2| \leq \dfrac{\delta|A_0A_2'|}{2}$. Finally, applying Lemma 23 to the points A_1', A_2', A_0, and A_0', we get $|S_2 - S_3| \leq \dfrac{\delta|A_1'A_2'|}{2}$.

Therefore,

$$|S - S_3| \leq \frac{\delta(|A_0A_1| + |A_0A_2'| + |A_1'A_2'|)}{2}. \tag{2.1}$$

Note that the the triangle inequality gives us

$$|A_0A_2'| \leq |A_0A_2| + |A_2A_2'| \leq |A_0A_2| + \delta$$

and

$$|A_1'A_2'| \leq |A_1'A_1| + |A_1A_2| + |A_2A_2'| \leq |A_1A_2| + 2\delta.$$

Using the upper bounds for $|A_0A_2'|$ and $|A_1'A_2'|$ in (2.1) gives us the desired bound for $|S - S_3|$. □

We also need the following simple lemma.

Lemma 25. *For all x in the interval $(0, \pi)$, we have $0 < \sin x - x\cos x < \frac{x^3}{3}$. Also, for all x in the interval $(0, \pi/2]$, we have $\sin x \geq \dfrac{2}{\pi}x$.*

Proof. Let $f(x) = \sin x - x\cos x$. Note $f(0) = 0$. Consider $f'(x) = x\sin x$. Clearly, $f'(x) > 0$ on $(0, \pi)$ and we have the first half of the inequality.

Now let $g(x) = \sin x - x\cos x - \frac{x^3}{3}$. Note $g'(x) = x(\sin x - x)$. If $x > 0$, then $\sin x - x < 0$ and thus $g'(x) < 0$ on this interval also. Thus, because $g(0) = 0$ and g is decreasing on $(0, \pi)$, we have the second desired inequality. To prove the last inequality of the lemma, consider the function $h(x) = \dfrac{\sin x}{x}$. We have $h'(x) = \dfrac{x\cos x - \sin x}{x^2}$. We proved above that $\sin x - x\cos x > 0$ for $x \in (0, \pi)$. Thus $h(x)$ is decreasing in $(0, \pi/2]$ and its minimum is $h(\pi/2) = 2/\pi$. □

Here, and throughout the end of this chapter, when A is a point and $\vec{v}$ is a vector, the equation $A = \vec{v}$ will mean $\overrightarrow{OA} = \vec{v}$, where O is the origin of the coordinate system.

A helix is a space curve with constant curvature and torsion. Let A_0, A_1, A_2 be three points on a helix $\mathcal{H}$. In the next lemma we obtain formulas for the distances $|A_0A_1|$, $|A_1A_2|$, $|A_0A_2|$, and for the area of triangle $\triangle A_0A_1A_2$.

Lemma 26. *Let $\mathcal{H}$ be a helix with curvature $\kappa > 0$ and torsion $\tau > 0$. Let A_0, A_1, and A_2 be three distinct points on the helix $\mathcal{H}$ whose arclengths from the origin of the helix are s_0, s_1, s_2 respectively, with $s_0 < s_1 < s_2$. Define $a = \frac{\kappa}{\kappa^2+\tau^2}$, $b = \frac{\tau}{\kappa^2+\tau^2}$, $t_i = \frac{s_i}{\sqrt{a^2+b^2}}$ for $i = 0, 1, 2$, $h_1 = t_1 - t_0$, and $h_2 = t_2 - t_1$. Then*

(i)

$$|A_0A_1|^2 = 4a^2\sin^2\left(\frac{h_1}{2}\right) + b^2h_1^2,$$

$$|A_1A_2|^2 = 4a^2\sin^2\left(\frac{h_2}{2}\right) + b^2h_2^2, \text{ and}$$

$$|A_0A_2|^2 = 4a^2\sin^2\left(\frac{h_1+h_2}{2}\right) + b^2(h_1+h_2)^2;$$

(ii)

$$(Area(\triangle A_0A_1A_2))^2 = (T_1 + T_2 + T_3)/4,$$

where

$$T_1 := 16a^4\sin^2\frac{h_1}{2}\sin^2\frac{h_2}{2}\sin^2\frac{h_1+h_2}{2},$$

$$T_2 := a^2b^2h_1^2h_2^2\left(\frac{\sin\frac{h_2}{2}}{\frac{h_2}{2}} - \frac{\sin\frac{h_1}{2}}{\frac{h_1}{2}}\right)^2, \text{ and}$$
$$T_3 := 16a^2b^2h_1h_2\sin\frac{h_1}{2}\sin\frac{h_2}{2}\sin^2\frac{h_1+h_2}{4}.$$

Proof. First, we consider a helix $\mathcal{H}(a,b)$ with parameterization

$$\vec{r}(t) = \langle a\cos t, a\sin t, bt\rangle. \tag{2.2}$$

It is easy to check that we have $\kappa = \dfrac{a}{a^2+b^2}$, $\tau = \dfrac{b}{a^2+b^2}$, and $\kappa^2+\tau^2 = \dfrac{1}{a^2+b^2}$. From here, we get $a = \dfrac{\kappa}{\kappa^2+\tau^2}$, $b = \dfrac{\tau}{\kappa^2+\tau^2}$. Also, for the arclength parameter s we have $s = t\sqrt{a^2+b^2}$.

The points A_0, A_1, and A_2 on the helix can be written with this parameterization as

$$A_0 = (a\cos t_0, a\sin t_0, bt_0),$$
$$A_1 = (a\cos t_1, a\sin t_1, bt_1), \text{ and}$$
$$A_2 = (a\cos t_2, a\sin t_2, bt_2),$$

with $t_0 < t_1 < t_2$.

Therefore, the vectors based at A_1 can be expressed as

$$\overrightarrow{A_1A_0} = \langle a(\cos t_0 - \cos t_1), a(\sin t_0 - \sin t_1), b(t_0-t_1)\rangle, \text{ and}$$
$$\overrightarrow{A_1A_2} = \langle a(\cos t_2 - \cos t_1), a(\sin t_2 - \sin t_1), b(t_2-t_1)\rangle.$$

And therefore the square of the length of $\overrightarrow{A_1A_0}$ can be written as

$$\begin{aligned}\left|\overrightarrow{A_1A_0}\right|^2 &= a^2(\cos t_0 - \cos t_1)^2 + a^2(\sin t_0 - \sin t_1)^2 + b^2(t_1-t_0)^2\\ &= a^2(2 - 2\cos t_0\cos t_1 - 2\sin t_0\sin t_1) + b^2(t_1-t_0)^2\\ &= a^2(2-2\cos(t_1-t_0)) + b^2(t_1-t_0)^2\\ &= a^2(2-2\cos h_1) + b^2h_1^2\\ &= 4a^2\sin^2\left(\frac{h_1}{2}\right) + b^2h_1^2.\end{aligned}$$

One can obtain the formulas for $|A_1A_2|$ and $|A_0A_2|$ similarly.

For the area of $\triangle A_0A_1A_2$ we use

$$\begin{aligned}
\cos\theta &= \frac{\overrightarrow{A_1A_0}\cdot\overrightarrow{A_1A_2}}{\left|\overrightarrow{A_1A_0}\right|\left|\overrightarrow{A_1A_2}\right|} \\
1-\sin^2\theta &= \frac{\left(\overrightarrow{A_1A_0}\cdot\overrightarrow{A_1A_2}\right)^2}{\left|\overrightarrow{A_1A_0}\right|^2\left|\overrightarrow{A_1A_2}\right|^2} \\
\left|\overrightarrow{A_1A_0}\right|^2\left|\overrightarrow{A_1A_2}\right|^2-\left(\overrightarrow{A_1A_0}\cdot\overrightarrow{A_1A_2}\right)^2 &= \left|\overrightarrow{A_1A_0}\right|^2\left|\overrightarrow{A_1A_2}\right|^2\sin^2\theta \\
&= 4\mathrm{Area}(\triangle A_0A_1A_2)^2,
\end{aligned}$$

where θ is the angle between $\overrightarrow{A_1A_0}$ and $\overrightarrow{A_1A_2}$.

Next we calculate the dot product:

$$\begin{aligned}
\overrightarrow{A_1A_0}\cdot\overrightarrow{A_1A_2} &= a^2(\cos t_0-\cos t_1)(\cos t_2-\cos t_1) \\
&\quad + a^2(\sin t_0-\sin t_1)(\sin t_2-\sin t_1)+b^2(t_0-t_1)(t_2-t_1) \\
&= a^2(\cos t_0\cos t_2-\cos t_1\cos t_2-\cos t_0\cos t_1+\cos^2 t_1) \\
&\quad + a^2(\sin t_0\sin t_2-\sin t_1\sin t_2-\sin t_0\sin t_1+\sin^2 t_1) \\
&\quad + b^2(t_0-t_1)(t_2-t_1) \\
&= a^2(\cos(h_2+h_1)-\cos h_2-\cos h_1+1)-b^2h_1h_2 \\
&= a^2((1-\cos h_2)(1-\cos h_1)-\sin h_2\sin h_1)-b^2h_1h_2 \\
&= 4a^2\sin\frac{h_1}{2}\sin\frac{h_2}{2}\left(\sin\frac{h_1}{2}\sin\frac{h_2}{2}-\cos\frac{h_1}{2}\cos\frac{h_2}{2}\right)-b^2h_1h_2 \\
&= -4a^2\sin\frac{h_1}{2}\sin\frac{h_2}{2}\cos\left(\frac{h_1+h_2}{2}\right)-b^2h_1h_2.
\end{aligned}$$

Combining this last calculation with the one just before it, we have

$$
\begin{aligned}
4\text{Area}(\triangle A_0A_1A_2)^2 &= \left(4a^2\sin^2\frac{h_1}{2} + b^2h_1^2\right)\left(4a^2\sin^2\frac{h_2}{2} + b^2h_2^2\right) \\
&\quad - \left(4a^2\sin\frac{h_1}{2}\sin\frac{h_2}{2}\cos\left(\frac{h_1+h_2}{2}\right) + b^2h_1h_2\right)^2 \\
&= 16a^4\sin^2\frac{h_1}{2}\sin^2\frac{h_2}{2}\sin^2\frac{h_1+h_2}{2} \\
&\quad + 4a^2b^2\left(h_1^2\sin^2\frac{h_2}{2} + h_2^2\sin^2\frac{h_1}{2}\right) \\
&\quad - 8a^2b^2h_1h_2\sin\frac{h_1}{2}\sin\frac{h_2}{2}\cos\frac{h_1+h_2}{2} \\
&= 16a^4\sin^2\frac{h_1}{2}\sin^2\frac{h_2}{2}\sin^2\frac{h_1+h_2}{2} \\
&\quad + 4a^2b^2\left(h_1\sin\frac{h_2}{2} - h_2\sin\frac{h_1}{2}\right)^2 \\
&\quad + 8a^2b^2h_1h_2\sin\frac{h_1}{2}\sin\frac{h_2}{2}\left(1-\cos\frac{h_1+h_2}{2}\right) \\
&= 16a^4\sin^2\frac{h_1}{2}\sin^2\frac{h_2}{2}\sin^2\frac{h_1+h_2}{2} \\
&\quad + a^2b^2h_1^2h_2^2\left(\frac{\sin\frac{h_2}{2}}{\frac{h_2}{2}} - \frac{\sin\frac{h_1}{2}}{\frac{h_1}{2}}\right)^2 \\
&\quad + 16a^2b^2h_1h_2\sin\frac{h_1}{2}\sin\frac{h_2}{2}\sin^2\frac{h_1+h_2}{4}
\end{aligned}
$$

which proves the lemma in the case of a helix $\mathcal{H}(a,b)$ with parametrization 2.2.

Now, consider a helix $\mathcal{H}'$ in general position, with curvature $\kappa > 0$ and torsion $\tau > 0$. Let A_0, A_1, and A_2 be three distinct points on the helix $\mathcal{H}'$ whose arclengths from the origin of the helix are s_0, s_1, s_2 respectively, with $0 < s_0 < s_1 < s_2$.

Here we use the uniqueness part of the Fundamental Theorem of the local theory of curves (for example, see do Carmo [5] p.19). It states that if $\alpha, \alpha' : I \to \mathbb{R}$ are regular parametrized curves with natural parameter s, which have the same curvature $\kappa(s)$ and the same torsion $\tau(s)$ for all s, then α' differs from α by a rigid motion, that is there exist an orthogonal linear map ρ of $\mathbb{R}^3$, with positive determinant, and a vector c such that $\alpha' = \rho \circ \alpha + c$.

Since the helix $\mathcal{H}'$ and the helix $\mathcal{H}(a,b)$ have the same curvature κ and the same torsion τ, there exists a rigid motion which maps the helix $\mathcal{H}'$ onto the helix $\mathcal{H}(a,b)$; and it maps the points A_0, A_1, A_2 to some points A_0', A_1', A_2' respectively, which are on $\mathcal{H}(a,b)$ and have corresponding values of the natural parameter s_0, s_1, s_2.

Note that the rigid motions do not change the distance between two points, and preserve the area of a triangle. Therefore, $|A_0A_1| = |A_0'A_1'|$, $|A_1A_2| = |A_1'A_2'|$, $|A_0A_2| = |A_0'A_2'|$, $\text{Area}(\triangle A_0A_1A_2) = \text{Area}(\triangle A_0'A_1'A_2')$. Moreover, a, b, h_1, and h_2 are uniquely determined by s_0, s_1, s_2, κ and τ. Therefore, the lemma holds in the case of a helix $\mathcal{H}'$ in general position. □

It is easy to estimate the terms T_1 and T_3. To estimate T_2 we use the following lemma.

Lemma 27. *Let h_1 and h_2 be real numbers, both in the interval $(0, 2\pi)$. Then,*

$$\left(\frac{\sin\frac{h_2}{2}}{\frac{h_2}{2}} - \frac{\sin\frac{h_1}{2}}{\frac{h_1}{2}}\right)^2 \leq \frac{\max(h_1,h_2)^2}{144}(h_1-h_2)^2.$$

Proof. Applying the mean value theorem to the function $\dfrac{\sin x}{x}$, we have that there exists ζ between $\frac{h_1}{2}$ and $\frac{h_2}{2}$ such that

$$\left(\frac{\sin\frac{h_2}{2}}{\frac{h_2}{2}} - \frac{\sin\frac{h_1}{2}}{\frac{h_1}{2}}\right)^2 = \left(\frac{h_1}{2} - \frac{h_2}{2}\right)^2 \left(\frac{\zeta\cos\zeta - \sin\zeta}{\zeta^2}\right)^2.$$

By Lemma 25, we get that $0 < \dfrac{\sin x - x\cos x}{x^2} < \dfrac{x}{3}$ for every $x \in (0,\pi)$. Therefore,

$$\left(\frac{\sin\frac{h_2}{2}}{\frac{h_2}{2}} - \frac{\sin\frac{h_1}{2}}{\frac{h_1}{2}}\right)^2 < \left(\frac{h_1}{2} - \frac{h_2}{2}\right)^2 \left(\frac{\zeta}{3}\right)^2 \leq \frac{\max(h_1,h_2)^2}{144}(h_1-h_2)^2.$$

□

In the next two lemmas we prove the existence of the positive constants $\mathcal{D}_{\mathcal{L}}$ and $\mathcal{A}_{\mathcal{L}}$ mentioned in the introduction.

Lemma 28. *Let v_1, v_2, and v_3 be linearly independent vectors in $\mathbb{R}^3$. Then there exists a constant $c > 0$ (depending on v_1, v_2, and v_3) such that*

$$||m_1v_1 + m_2v_2 + m_3v_3|| \geq c$$

for any integers m_1, m_2, and m_3 with $(m_1, m_2, m_3) \neq (0, 0, 0)$.

Proof. We have $||m_1v_1 + m_2v_2 + m_3v_3||^2 = (m_1v_1 + m_2v_2 + m_3v_3) \cdot (m_1v_1 + m_2v_2 + m_3v_3) = \sum_{i=1}^{3}\sum_{j=1}^{3}(v_i \cdot v_j)m_im_j := Q(m_1, m_2, m_3)$.

The quadratic form $Q(m_1, m_2, m_3)$ is positive definite, since v_1, v_2, and v_3 are linearly independent. Denote by $M(Q)$ the matrix of the quadratic form $Q(m_1, m_2, m_3)$. Since $M(Q)$ is symmetric and $Q(m_1, m_2, m_3)$ is positive definite, the eigenvalues of $Q(M)$ are real positive numbers, say $0 < \lambda_1 \leq \lambda_2 \leq \lambda_3$. Moreover, by the Spectral Theorem for real symmetric matrices, there exists an orthonormal basis of vectors w_1, w_2, w_3 for $\mathbb{R}^3$, where w_1, w_2, and w_3 are eigenvectors corresponding to the eigenvalues λ_1, λ_2, and λ_3. This implies that the minimum of $Q(m_1, m_2, m_3)$ on the unit sphere is λ_1. Therefore, the lemma holds with $c = \sqrt{\lambda_1}$. □

Lemma 29. *Consider a lattice $\mathcal{L} = \mathcal{L}(v_0, v_1, v_2, v_3) = \{v_0+mv_1+nv_2+pv_3 : m, n, p \in \mathbb{Z}\}$. There exist positive constants $\mathcal{D}_\mathcal{L}$ and $\mathcal{A}_\mathcal{L}$ (depending on $\mathcal{L}$) such that*
(i) if A_0 and A_1 are any two distinct lattice points in $\mathcal{L}$, then $|A_0A_1| \geq \mathcal{D}_\mathcal{L}$;
and
(ii) if A_0, A_1, and A_2 are any three non-collinear lattice points in $\mathcal{L}$, then

$$Area(\triangle A_0A_1A_2) \geq \mathcal{A}_\mathcal{L}.$$

Proof. If A_0 and A_1 are two distinct lattice points in $\mathcal{L}$, then $\overrightarrow{A_0A_1} = m'v_1+n'v_2+p'v_3$ with m', n', p' integers such that $(m', n', p') \neq (0, 0, 0)$. Now, (i) follows from Lemma 28.

Next, let A_0, A_1, and A_2 be three non-collinear lattice points in $\mathcal{L}$. We have that $\text{Area}(\triangle A_0A_1A_2) = ||\overrightarrow{A_0A_1} \times \overrightarrow{A_0A_2}||/2$.

Since A_0, A_1, and A_2 are non-collinear, then Area$(\triangle A_0A_1A_2) \neq 0$. Therefore, $\overrightarrow{A_0A_1} \times \overrightarrow{A_0A_2} \neq \overrightarrow{0}$.

Furthermore, since $\overrightarrow{A_0A_1} = m'v_1 + n'v_2 + p'v_3$ and $\overrightarrow{A_0A_2} = m''v_1 + n''v_2 + p''v_3$ for some integers m', m'', n', n'', p', and p'', then

$$\overrightarrow{A_0A_1} \times \overrightarrow{A_0A_2} = q(v_1 \times v_2) + r(v_2 \times v_3) + s(v_1 \times v_3),$$

with $q = m'n'' - m'n''$, $r = n'p'' - n''p'$, and $s = m'p'' - m''p'$.

Since, $\overrightarrow{A_0A_1} \times \overrightarrow{A_0A_2} \neq \overrightarrow{0}$ we have $(q, r, s) \neq (0, 0, 0)$.

Moreover, the vectors $v_1 \times v_2$, $v_2 \times v_3$, and $v_1 \times v_3$ are linearly independent.

Indeed, if $c_1(v_1 \times v_2) + c_2(v_2 \times v_3) + c_3(v_1 \times v_3) = 0$, then after taking the dot product of the last equation with v_3, we get $c_1((v_1 \times v_2) \cdot v_3) = 0$. However, the triple product $(v_1 \times v_2) \cdot v_3 \neq 0$, since the vectors v_1, v_2, and v_3 are linearly independent. We show similarly that $c_2 = 0$ and $c_3 = 0$.

Thus, the vectors $v_1 \times v_2$, $v_2 \times v_3$, and $v_1 \times v_3$ are linearly independent.

Now (ii) follows from Lemma 28. □

2.3 Main Result

First, we consider the case when the lattice points are *on* the helix.

Theorem 30. *Let $\mathcal{H}$ be a helix with curvature $\kappa > 0$ and torsion $\tau > 0$. Let $\mathcal{L} = \mathcal{L}(v_0, v_1, v_2, v_3)$ be an affine lattice in $\mathbb{R}^3$, and let A_0, A_1, and A_2 be three distinct points in $\mathcal{L}$ which are also on the helix $\mathcal{H}$ and whose arclengths from the origin of the helix are s_0, s_1, s_2 respectively, with $s_0 < s_1 < s_2$. Then $|A_0A_2| \geq \min\left(\frac{\pi\tau}{\kappa^2+\tau^2}, 1.5\mathcal{A}_{\mathcal{L}}^{\frac{1}{3}}\kappa^{-\frac{1}{3}}\right)$ and the length of the arc $\overset{\frown}{A_0A_2}$ is at least $\min\left(\frac{\pi}{\sqrt{\kappa^2+\tau^2}}, 2.4\mathcal{A}_{\mathcal{L}}^{\frac{1}{3}}\kappa^{-\frac{1}{3}}\right)$.*

Proof. Define $a = \dfrac{\kappa}{\kappa^2+\tau^2}$ and $b = \dfrac{\tau}{\kappa^2+\tau^2}$. Recall that $s = \sqrt{a^2+b^2}t$. For $i = 0, 1,$ and 2, let $t_i = \dfrac{s_i}{\sqrt{a^2+b^2}}$. Then $0 < t_0 < t_1 < t_2$ and $A_i = \vec{r}(t_i)$ for $i = 0, 1, 2$. Let $h_1 = t_1 - t_0$ and $h_2 = t_2 - t_1$.

We consider two cases.

Case I: $h_1 + h_2 \geq \pi$.

Then the arclength of the arc $\overset{\frown}{A_0A_2}$ is

$$s_2 - s_0 = (h_1 + h_2)\sqrt{a^2 + b^2} \geq \pi\sqrt{a^2 + b^2} = \frac{\pi}{\sqrt{\kappa^2 + \tau^2}}.$$

Also, by Lemma 26 (i)

$$|A_0A_2| \geq b(h_1 + h_2) \geq \pi b = \frac{\pi\tau}{\kappa^2 + \tau^2}.$$

Note that one cannot expect to get a nontrivial lower bound on $|A_0A_2|$ depending only on κ. For example, consider the case when a is a large integer, $b = \frac{1}{2\pi}$, $t_0 = 0$, $t_1 = 2\pi$, and $t_2 = 4\pi$.

Case II: $h_1 + h_2 < \pi$.

Denote by S the area of $\triangle A_0A_1A_2$. From Lemma 26 (ii) we have $4S^2 = T_1+T_2+T_3$, where

$T_1 = 16a^4 \sin^2 \frac{h_1}{2} \sin^2 \frac{h_2}{2} \sin^2 \frac{h_1+h_2}{2}$,
$T_2 = a^2b^2h_1^2h_2^2 \left(\frac{\sin \frac{h_2}{2}}{\frac{h_2}{2}} - \frac{\sin \frac{h_1}{2}}{\frac{h_1}{2}} \right)^2$, and
$T_3 = 16a^2b^2h_1h_2 \sin \frac{h_1}{2} \sin \frac{h_2}{2} \sin^2 \frac{h_1+h_2}{4}$.

Since $0 < h_1 + h_2 < \pi$, we have $T_1 > 0$, $T_2 \geq 0$, and $T_3 > 0$. Therefore, $S > 0$, so the points A_0, A_1, and A_2 are non-collinear. Now, by Lemma 29 we have $S \geq \mathcal{A}_{\mathcal{L}} > 0$. We obtain

$$4\mathcal{A}_{\mathcal{L}}^2 \leq T_1 + T_2 + T_3. \tag{2.3}$$

Next we get bounds for T_1, T_2, and T_3.

Since $0 < h_1 + h_2$ and $\sin x < x$ when $x > 0$ we obtain

$$T_1 < \frac{a^4h_1^2h^2(h_1 + h_2)^2}{4} \leq \frac{a^4(h_1 + h_2)^6}{64}. \tag{2.4}$$

(Here and below, we use the inequality $ab \leq (a + b)^2/4$.)

Next, by Lemma 27 we have

$$T_2 \leq a^2b^2h_1^2h_2^2 \frac{\max(h_1, h_2)^2}{144}(h_1 - h_2)^2 < a^2b^2 \frac{(h_1 + h_2)^8}{2304}.$$

Since, $h_1 + h_2 < \pi$, we obtain,

$$T_2 < a^2 b^2 \frac{\pi^2 (h_1 + h_2)^6}{2304}. \tag{2.5}$$

Again, using $\sin x < x$ for $x > 0$, we obtain

$$T_3 < a^2 b^2 h_1^2 h_2^2 \frac{(h_1 + h_2)^2}{4} \leq a^2 b^2 \frac{(h_1 + h_2)^6}{64}. \tag{2.6}$$

Combining equation (2.3) with the bounds (2.4), (2.5), and (2.6), we obtain

$$4\mathcal{A}_{\mathcal{L}}^2 \leq (h_1 + h_2)^6 a^2 \left(\frac{a^2}{64} + b^2 \left(\frac{1}{64} + \frac{\pi^2}{2304} \right) \right).$$

Now $\frac{1}{64} + \frac{\pi^2}{2304} < 0.02$. Therefore,

$$200\mathcal{A}_{\mathcal{L}}^2 < (h_1 + h_2)^6 a^2 (a^2 + b^2). \tag{2.7}$$

Also, $200^{1/6} > 2.4$, so

$$h_1 + h_2 > 2.4 \mathcal{A}_{\mathcal{L}}^{\frac{1}{3}} a^{-\frac{1}{3}} (a^2 + b^2)^{-\frac{1}{6}}, \tag{2.8}$$

in Case II.

Recall that $s_2 - s_0 = (h_1 + h_2)\sqrt{a^2 + b^2}$, $a = \dfrac{\kappa}{\kappa^2 + \tau^2}$, and $a^2 + b^2 = \dfrac{1}{\kappa^2 + \tau^2}$.

We get,

$$s_2 - s_0 > 2.4 \mathcal{A}_{\mathcal{L}}^{\frac{1}{3}} \kappa^{-\frac{1}{3}}, \tag{2.9}$$

completing the stated lower bound for the arclength of $\overset{\frown}{A_0 A_2}$.

Next, we obtain a lower bound for $|A_0 A_2|$.

In this case, using Lemma 25 we obtain $\sin\left(\frac{h_1+h_2}{2}\right) \geq \frac{1}{\pi}(h_1 + h_2)$. By Lemma 26 (i), $|A_0 A_2|^2 = 4a^2 \sin^2\left(\frac{h_1+h_2}{2}\right) + b^2 (h_1 + h_2)^2$. Therefore,

$$|A_0 A_2| \geq \frac{2}{\pi}(h_1 + h_2)(a^2 + b^2)^{\frac{1}{2}} = \frac{2}{\pi}(s_2 - s_0),$$

in Case 2. Using (2.9) we get $|A_0 A_2| \geq \dfrac{4.8}{\pi} \mathcal{A}_{\mathcal{L}}^{\frac{1}{3}} \kappa^{-\frac{1}{3}}$.

Since $\frac{4.8}{\pi} > 1.5$, we obtain the stated bound for $|A_0 A_2|$.

We have established the theorem in the case of a helix $\mathcal{H}(a, b)$ with parameterization $\vec{r}(t) = \langle a \cos t, a \sin t, bt \rangle$. □

Next we prove Corollary 21.

Proof. First, by Lemma 22 in the case of the standard lattice in $\mathbb{R}^3$, $\mathcal{A}_{\mathcal{L}} = \frac{1}{2}$. Therefore, the condition $\tau\kappa^{\frac{1}{3}} \geq 0.4(\kappa^2 + \tau^2)$ implies $\dfrac{\pi\tau}{\kappa^2+\tau^2} > 1.5\mathcal{A}_{\mathcal{L}}^{\frac{1}{3}}\kappa^{-\frac{1}{3}}$ in the case of standard lattice $\mathcal{L}$. The corollary follows by noting that $\frac{1.5}{\sqrt[3]{2}} > 1.1$. □

Finally, we prove Theorem 20.

Proof. Let

$$0 < \delta \leq \min\left(\frac{\mathcal{D}_{\mathcal{L}}}{4}, \frac{4\mathcal{D}_{\mathcal{L}}^2}{11\pi^3}a^2(a^2+b^2)^{-\frac{1}{2}}, \frac{2\mathcal{A}_{\mathcal{L}}(a^2+b^2)^{-\frac{1}{2}}}{11\pi}\right).$$

Let A_0', A_1', and A_2' be three distinct lattice points within δ of the helix $\mathcal{H}$. Therefore, there exist points A_0, A_1, and A_2 on the helix, such that

$$|A_0A_0'| \leq \delta, \quad |A_1A_1'| \leq \delta, \quad \text{and } |A_2A_2'| \leq \delta.$$

Since A_0', A_1', and A_2' are in $\mathcal{L}$, by Lemma 29 we have $|A_0'A_1'| \geq \mathcal{D}_{\mathcal{L}}$, $|A_0'A_2'| \geq \mathcal{D}_{\mathcal{L}}$, and $|A_1'A_2'| \geq \mathcal{D}_{\mathcal{L}}$. Since $\delta \leq \mathcal{D}_{\mathcal{L}}/4$, by the triangle inequality, we get

$$|A_0A_2| \geq |A_0'A_2'| - |A_0A_0'| - |A_2A_2'| \geq \mathcal{D}_{\mathcal{L}} - 2\delta \geq \mathcal{D}_{\mathcal{L}}/2.$$

Similarly, $|A_0A_1| \geq \mathcal{D}_{\mathcal{L}}/2$ and $|A_1A_2| \geq \mathcal{D}_{\mathcal{L}}/2$. Thus, the points A_0, A_1, and A_2 are distinct. Let the values of the natural parameter corresponding to A_0, A_1, and A_2 be s_0, s_1, and s_2, respectively. Without loss of generality we can assume $s_0 < s_1 < s_2$ (otherwise we relabel A_0', A_1', and A_2'). As before, let $t_i = s_i(a^2+b^2)^{-\frac{1}{2}}$ for $i = 0, 1, 2$, $h_1 = t_1 - t_0 > 0$ and $h_2 = t_2 - t_1 > 0$.

We consider two cases.

Case I: $h_1 + h_2 \geq \pi$.

In this case, in exactly the same way as in the proof of Theorem 30, we obtain

$$|A_0A_2| \geq \frac{\pi\tau}{\kappa^2+\tau^2}.$$

Now, by the triangle inequality, we get

$$|A_0'A_2'| \geq |A_0A_2| - |A_0A_0'| - |A_2A_2'| \geq |A_0A_2| - 2\delta,$$

so

$$|A_0'A_2'| \geq \frac{\pi\tau}{\kappa^2+\tau^2} - 2\delta.$$

Case II: $h_1 + h_2 < \pi$.

Here, first we show that A_0', A_1' and A_2' are not on a straight line.

Recall that $|A_0A_1| \geq \mathcal{D}_{\mathcal{L}}/2$. Therefore, $s_1 - s_0 \geq |A_0A_1| \geq \mathcal{D}_{\mathcal{L}}/2$. Next, since $s_1 - s_0 = h_1(a^2+b^2)^{\frac{1}{2}}$, we get $h_1 \geq \frac{\mathcal{D}_{\mathcal{L}}}{2}(a^2+b^2)^{-\frac{1}{2}}$. Similarly, $s_2 - s_1 \geq \mathcal{D}_{\mathcal{L}}/2$ and $h_2 \geq \frac{\mathcal{D}_{\mathcal{L}}}{2}(a^2+b^2)^{-\frac{1}{2}}$.

Denote the area of $\triangle A_0A_1A_2$ by S.

By Lemma 26 (ii), we have $4S^2 = T_1 + T_2 + T_3$, where

$$T_1 = 16a^4 \sin^2\frac{h_1}{2}\sin^2\frac{h_2}{2}\sin^2\frac{h_1+h_2}{2},$$

$T_2 \geq 0$, and $T_3 > 0$.

Since $h_1 + h_2 < \pi$, by Lemma 25

$$T_1 \geq \frac{16}{\pi^6}a^4h_1^2h_2^2(h_1+h_2)^2.$$

Therefore, $4S^2 > \frac{16}{\pi^6}a^4h_1^2h_2^2(h_1+h_2)^2$. We get,

$$S > \frac{2}{\pi^3}a^2h_1h_2(h_1+h_2). \tag{2.10}$$

Denote the area of $\triangle A_0'A_1'A_2'$ by S_3.

Assume that the points A_0', A_1' and A_2' *are* on a straight line. Then, $S_3 = 0$.

Applying Lemma 24 to $\triangle A_0A_1A_2$ and $\triangle A_0'A_1'A_2'$ we obtain

$$|S - S_3| \leq \frac{\delta(|A_0A_1| + |A_1A_2| + |A_0A_2|)}{2} + \frac{3\delta^2}{2}. \tag{2.11}$$

Now, $|A_0A_1| < s_1 - s_0$, $|A_1A_2| < s_2 - s_1$, and $|A_0A_2| < s_2 - s_0$, so we obtain

$$S < \delta(s_2 - s_0) + \frac{3\delta^2}{2}.$$

Since, $s_2 - s_0 \geq |A_0A_1| + |A_1A_2| \geq \mathcal{D}_{\mathcal{L}}$ and $\delta \leq \mathcal{D}_{\mathcal{L}}/4$, we have $\delta \leq (s_2 - s_0)/4$, so

$$S < \frac{11}{8}\delta(s_2 - s_0) = \frac{11}{8}\delta(h_1 + h_2)(a^2 + b^2)^{-\frac{1}{2}}. \tag{2.12}$$

Combining (2.12) and (2.10) we obtain

$$\frac{2}{\pi^3}a^2h_1h_2(h_1 + h_2) < S < \frac{11}{8}\delta(h_1 + h_2)(a^2 + b^2)^{-\frac{1}{2}}.$$

Therefore,

$$\frac{16}{11\pi^3}a^2h_1h_2(a^2 + b^2)^{\frac{1}{2}} < \delta.$$

Now, $h_1 = t_1 - t_0 = (s_1 - s_0)(a^2 + b^2)^{-\frac{1}{2}} > |A_0A_1|(a^2 + b^2)^{-\frac{1}{2}} \geq \frac{\mathcal{D}_{\mathcal{L}}}{2}(a^2 + b^2)^{-\frac{1}{2}}$. Similarly, $h_2 > \frac{\mathcal{D}_{\mathcal{L}}}{2}(a^2 + b^2)^{-\frac{1}{2}}$. Therefore,

$$\delta > \frac{4\mathcal{D}_{\mathcal{L}}^2}{11\pi^3}a^2(a^2 + b^2)^{-\frac{1}{2}},$$

which contradicts the upper bound for δ, so our assumption is false. Hence, the points A_0', A_1' and A_2' *are not* on a straight line. By Lemma 29, S_3, the area of $\triangle A_0'A_1'A_2'$, is at least $\mathcal{A}_{\mathcal{L}}$.

Next, we get a lower bound for the area of $\triangle A_0A_1A_2$. Using (2.11) we obtain

$$S \geq \mathcal{A}_{\mathcal{L}} - \frac{\delta(|A_0A_1| + |A_1A_2| + |A_0A_2|)}{2} - \frac{3\delta^2}{2}.$$

Now, $|A_0A_1| + |A_1A_2| + |A_0A_2| < 2(s_2 - s_0)$ and we showed above that $\delta \leq (s_2 - s_0)/4$. Therefore,

$$S > \mathcal{A}_{\mathcal{L}} - \frac{11\delta(s_2 - s_0)}{8}.$$

We have $s_2 - s_0 = 2(h_1 + h_2)(a^2 + b^2)^{\frac{1}{2}} \leq 2\pi(a^2 + b^2)^{\frac{1}{2}}$.

We obtain,

$$S > \mathcal{A}_{\mathcal{L}} - \frac{11\delta\pi(a^2 + b^2)^{\frac{1}{2}}}{4}.$$

Now, by the upper bound on δ, we have

$$\frac{11\delta\pi(a^2 + b^2)^{\frac{1}{2}}}{4} \leq \frac{\mathcal{A}_{\mathcal{L}}}{2}.$$

Therefore,

$$S > \frac{\mathcal{A}_{\mathcal{L}}}{2}. \tag{2.13}$$

Now, we get a lower bound for $h_1 + h_2$ the same way we did in the case of lattice points *on the helix*, in Case II of the proof of Theorem 30. The upper bounds of T_1, T_2, and T_3 are the same as before, and the estimates (2.4), (2.5), and (2.6) still hold.

The only difference is that the lower bound for the area of $\triangle A_0A_1A_2$ now is greater than $\mathcal{A}_{\mathcal{L}}/2$ rather than at least $\mathcal{A}_{\mathcal{L}}$.

The analogue of equation (2.7) is

$$50\mathcal{A}_{\mathcal{L}}^2 < (h_1 + h_2)^6 a^2(a^2 + b^2), \tag{2.14}$$

(with the difference that now the left-hand-side of (2.14) is 1/4 of the left-hand-side of (2.7)).

Also, $50^{1/6} > 1.9$, so

$$h_1 + h_2 > 1.9\mathcal{A}_{\mathcal{L}}^{\frac{1}{3}} a^{-\frac{1}{3}}(a^2 + b^2)^{-\frac{1}{6}}. \tag{2.15}$$

Using Lemma 25 we obtain $\sin\left(\frac{h_1+h_2}{2}\right) \geq \frac{1}{\pi}(h_1 + h_2)$. By Lemma 26 (i) $|A_0A_2|^2 = 4a^2 \sin^2\left(\frac{h_1+h_2}{2}\right) + b^2(h_1 + h_2)^2$. Therefore,

$$|A_0A_2| \geq \frac{2}{\pi}(h_1 + h_2)(a^2 + b^2)^{\frac{1}{2}}.$$

Using (2.15) and $\kappa = \dfrac{a}{a^2 + b^2}$ we get

$$|A_0A_2| > \frac{3.8}{\pi}\mathcal{A}_{\mathcal{L}}^{\frac{1}{3}}\kappa^{-\frac{1}{3}}.$$

Since $\frac{3.8}{\pi} > 1.2$, and $|A_0'A_2'| \geq |A_0A_2| - 2\delta$ we obtain the stated bound for $|A_0'A_2'|$.

□

Chapter 3

Representing Integers as the Sum of a Squarefree and Small Prime

3.1 Introduction

A positive integer is squarefree if it is not divisible by the square of a prime number. In 1931 Estermann [14] obtained an asymptotic formula for the number of representations of a positive integer as the sum of a squarefree number and a prime. As a consequence, he showed that every sufficiently large integer is the sum of a squarefree number and a prime.

In 2017 Dudek [8] showed that every integer greater than two is a sum of a squarefree number and a prime.

In 1935, Erdős [11] showed that every sufficiently large integer $\not\equiv 1 \pmod 4$ can be represented as a sum of a square of a prime and a squarefree integer. The condition $n \not\equiv 1 \pmod 4$ is needed since if p is an odd prime, then $p^2 \equiv 1 \pmod 4$. Therefore if p is an odd prime and $n \equiv 1 \pmod 4$, then $4 \mid (n - p^2)$, and $n - p^2$ is not squarefree. The result of Erdős was completed by Dudek and Platt [9] who proved in 2016 that every integer $n \geq 10$ such that $n \not\equiv 1 \pmod 4$ can be represented as the sum of a square of a prime and a squarefree integer.

Thus, one can get a complete answer to the question of for which positive integers n there exists a prime $p < \sqrt{n}$ such that $n - p^2$ is squarefree.

A related question is for which positive integers n, there exists a prime $p < \sqrt{n}$ such that $n - p$ is squarefree. We answer the latter question completely.

Theorem 31. *Every positive integer n can be represented in the form $n = s + p$ where s is a squarefree number and p is a prime with $p \leq \sqrt{n}$, except when $n \in \{1, 2, 3, 6, 11, 30, 155, 247\}$.*

Since $2^2 \mid 6 - 2$; $3^2 \mid 11 - 2$, $2^3 \mid 11 - 3$; $2^2 \mid 30 - 2$, $3^3 \mid 30 - 3$, $5^2 \mid 30 - 5$; $3^2 \mid 155 - 2$, $2^3 \mid 155 - 3$, $5^2 \mid 155 - 5$, $2^2 \mid 155 - 7$, $2^2 \mid 155 - 11$; and $7^2 \mid 247 - 2$, $2^2 \mid 247 - 3$, $11^2 \mid 247 - 5$, $2^2 \mid 247 - 7$, $2^2 \mid 247 - 11$, and $3^2 \mid 247 - 13$ we see that indeed the integers $n \in \{1, 2, 3, 6, 11, 30, 155, 247\}$ cannot be represented as a sum of a sqarefree number and a prime not exceeding $\sqrt{n}$.

A natural question is can $\sqrt{n}$ in Theorem 31 be replaced by n^θ for $\theta < 1/2$.

In 2015, Filaseta, Graham, and Trifonov wrote a paper [17] which considered the distribution of various arithmetic sequences. In particular, replacing p by $-p$ in Theorem 5.1 of [17] one obtains the following theorem.

Theorem 32 (Filaseta, Graham, and Trifonov)**.** *There exist effectively computable constants C_0 and n_0 such that for each integer $n \geq n_0$ at least one-fifth of the primes $p \leq C_0 n^{1/5} \log^2 n$ are such that $n - p$ is squarefree.*

The authors of the paper [17] did not compute the values of C_0 and n_0. However it is certain that it will be impossible to check which integers $n \leq n_0$ do not satisfy Theorem 32 by direct computation.

An easy corollary of the above theorem is that for each $\theta > 1/5$ there exists an effectively computable constant n_θ such that each integer $n \geq n_\theta$ can be represented as a sum of a squarefree number and a prime not exceeding n^θ. At present it appears that to get below the exponent $1/5$ one will need to improve the gap result about squarefree numbers.

The proof of our main result follows the method of proof of Theorem 32. However, to obtain the result for all but eight positive integers we substantially sharpened

the estimates in each step and supplemented the proof with a nontrivial amount of computations.

Next, we outline the proof of Theorem 31. First, we verify the theorem for all $n \leq 10^9$. This computation allows us to obtain the first few terms of the following sequence.

Let b_k be the least positive integer $n > p_l$ such that none of the integers $n - p_1, \ldots, n - p_k$ are squarefree. Here and throughout the paper p_l denotes the l-th prime number.

We have $b_1 = 6$, $b_2 = 11$, $b_3 = 30$, $b_4 = b_5 = 155$, $b_6 = 247$, $b_7 = 5753$, $b_8 = b_9 = b_{10} = b_{11} = 90263$, $b_{12} = 1481287$, $b_{13} = b_{14} = b_{15} = 7409327$. Also, $b_{16} > 10^9$.

Clearly, $b_n < \prod_{l=1}^{n} p_l^2$ for $n > 1$, since by the Chinese Remainder Theorem, the system of congruences $n \equiv p_l \pmod{p_l^2}$ has a positive solution not exceeding $\prod_{l=1}^{n} p_l^2$.

One can do much better. For example, if we want to find $n > 53 = p_{16}$ such that $n - p_l$ is not squarefree for $l = 1, \ldots, 16$, one can pick $n \equiv 3 \pmod 4$. Then $4|n-p$ for $p \in \{3, 7, 11, 19, 23, 31, 43, 47\}$. Also, if $n \equiv 8 \pmod 9$, then $9|n - p$ for $p \in \{17, 53\}$. After that, we pick $n \equiv 2 \pmod{5^2}$, $n \equiv 5 \pmod{7^2}$, $n \equiv 13 \pmod{11^2}$, $n \equiv 29 \pmod{13^2}$, $n \equiv 37 \pmod{17^2}$, and $n \equiv 41 \pmod{19^2}$. Solving the last system of congruences, we obtain that its least positive solution is 23708451225527, thus $b_{16} \leq 23708451225527$.

From now on we assume $n > 10^9$. We show that for such n, there exists a prime $p \leq \sqrt{n}$, such that $n - p$ is squarefree.

There are $\pi(\sqrt{n})$ primes which do not exceed $\sqrt{n}$. We will show that there are less than $\pi(\sqrt{n})$ primes $p \leq \sqrt{n}$ such that $n - p$ is not squarefree. Establishing the last statement will imply that for some prime $p \leq \sqrt{n}$, $n - p = s$ where s is squarefree completing the proof of the theorem.

If for some prime $p \leq \sqrt{n}$, $n - p$ is not squarefree, then $q^2|n - p$ for some prime

q, that is

$$p \equiv n \pmod{q^2}. \tag{3.1}$$

Note that congruence (3.1) can hold only for $q < \sqrt{n}$, since $0 < n - p < n$. Furthermore, if $q|n$ the congruence (3.1) has at most one solution, when $p = q$. Also, then the number of solutions of (3.1) is $\pi(\sqrt{n}; q^2, n)$.

Above we have used the standard notation $\pi(a; b, c)$ to denote the number of primes not exceeding a which are in the arithmetic sequence $x \equiv c \pmod{b}$.

We estimate the number of primes p such that congruence (3.1) holds for some prime q in different ways depending on the size of q. For $q \in \{2, 3, 5, 7\}$ we use the paper [3] of Bennett et. al. on explicit bounds for primes in arithmetic sequences. For $q \in [11, n^{1/8}]$, we use a version of the Brun-Titchmarsh Theorem due to Montgomery and Vaughan [28]. For $q \in [n^{1/8}, \sqrt{n}/(c \log n)]$ we use elementary bounds, and for $n \in [\sqrt{n}/(c \log n), \sqrt{n})$ we use an estimate based on first differences of values of a function. Combining the above estimates we were able to show that the theorem holds for $n > 59^8$. Next, considering $n \in [p_k^8, p_{k+1}^8]$ for $k = 6, \ldots, 16$ we were able to get even sharper bounds for certain sums over primes which appear in our estimates and establish the theorem in the last 11 intervals. Since $p_6 = 13$ and $13^8 < 10^9$ this completes the proof.

3.2 Proof of the Main Result

We now prove the main result that all positive integers not equal to

$$1, 2, 3, 6, 11, 30, 155, \text{ or } 247$$

can be written as the sum of a squarefree positive integer and a prime less than the square root of the number.

Proof. First, by direct computation we confirmed the theorem for $n \leq 10^9$. To save memory we check the result in intervals of the form $I_k := [k \cdot 10^7, (k + 1) \cdot 10^7]$.

Computing the indicator function of squarefree integers in I_k is relatively fast since for each prime p the number of multiples of p^2 in I_k is at most $10^7/p^2 + 1$ and one only needs to check multiples of p^2 with $p \leq \sqrt{(k+1) \cdot 10^7}$. Checking the theorem in I_k is also fast because for most n, $n-2$ is squarefree and for each $n \leq 10^9$ it took no more than 17 checks to find a prime p such that $n-p$ is squarefree. Using python on a laptop with an AMD Ryzen 5 3500U processor and 8MB of memory, checking the theorem on each I_k with $k \in [1, 99]$ took less than a minute, so the whole computation was complete in under two hours.

From now on, we assume $n > 10^9$.

We will use the notation $\sum'$ to indicate a sum over prime numbers only. For example, $\sum_{q \leq x}' 1$ is the number of prime numbers up to x, that is $\pi(x)$.

We estimate the number of primes $p < \sqrt{n}$ satisfying congruence (3.1) in different ways depending on the size of q.

Case 1. $q \in \{2, 3, 5, 7\}$.

Let Q_1 be the number of primes less that $\sqrt{n}$ which satisfy congruence (3.1) for some $q \in \{2, 3, 5, 7\}$.

Here we use the following theorem which is one of the statements in Corollary 1.7 from the paper [3].

Theorem 33. *(M. Bennett, G. Martin, K. O'Bryant, and A. Rechnitzer)*

Let a and q be integers with $1 \leq q \leq 10^5$ and $\gcd(a, q) = 1$. If $x \geq 10^6$, then

$$\left| \pi(x; q, a) - \frac{\mathrm{Li}(x)}{\varphi(q)} \right| < 0.027 \frac{x}{\log^2 x}.$$

Above, by $\mathrm{Li}(x)$ the authors mean the function defined by $\mathrm{Li}(x) = \int_2^x \frac{dt}{\log t}$. Also, everywhere in this paper $\log x$ means $\log_e x = \ln x$.

To be able to use the above theorem, we assume $n \geq 10^{12}$ and we will deal with the case $10^9 < n < 10^{12}$ later on.

Using inclusion-exclusion for $q = 2$ and $q = 3$, and that congruence (3.1) has $\pi(\sqrt{n}; q^2, n)$ solutions for fixed q, we obtain,

$$Q_1 \leq \pi(\sqrt{n}; 4, n) + \pi(\sqrt{n}; 9, n) - \pi(\sqrt{n}; 36, n) + \pi(\sqrt{n}; 25, n) + \pi(\sqrt{n}; 49, n). \quad (3.2)$$

When $\gcd(n, 210) = 1$, Theorem 33 applies, and we obtain

$$Q_1 \leq \mathrm{Li}(\sqrt{n}) \left(\frac{1}{2} + \frac{1}{6} - \frac{1}{12} + \frac{1}{20} + \frac{1}{42} \right) + 0.54 \frac{\sqrt{n}}{\log^2 n}. \quad (3.3)$$

The following is Lemma 5.9 of the paper [3].

Lemma 34. *For $x \geq 1865$,*

$$\mathrm{Li}(x) < \frac{x}{\log x} \left(1 + \frac{3}{2 \log x} \right) \quad . \quad (3.4)$$

Using the above lemma and (3.3) we get

$$Q_1 < \frac{46\sqrt{n}}{35 \log n} \left(1 + \frac{3}{\log n} \right) + 0.54 \frac{\sqrt{n}}{\log^2 n} \;=\; \frac{46\sqrt{n}}{35 \log n} + \frac{1569\sqrt{n}}{350 \log^2 n}. \quad (3.5)$$

If $7|n$, $\pi(\sqrt{n}; 49, n) \leq 1$ and we need to replace to upper bound for $\pi(\sqrt{n}; 49, n) \leq 1$ used in (3.5) which is $\dfrac{\sqrt{n}}{21 \log n} \left(1 + \dfrac{3}{\log n} \right) + 0.108 \dfrac{\sqrt{n}}{\log^2 n}$ by 1.

However, the function $f(n) = \dfrac{\sqrt{n}}{\log n}$ is increasing for $n > e^2$ and $f(10^{12}) = 36192.2\ldots$, so

$$\frac{\sqrt{n}}{21 \log n} \left(1 + \frac{3}{\log n} \right) + 0.108 \frac{\sqrt{n}}{\log^2 n} > 36192/21 > 1,$$

for $n \geq 10^{12}$, so equation (3.5) holds when $\gcd(n, 30) = 1$ (regardless of whether $7 \mid n$ or $7 \nmid n$).

We argue similarly when $5 \mid n$ to conclude that equation (3.5) holds when n and 6 are relatively prime and $n \geq 10^{12}$.

When $3 \mid n$ we need to replace to upper bound for $\pi(\sqrt{n}; 9, n) - \pi(\sqrt{n}; 36, n) \leq 1$ used in (3.5) which is $\dfrac{\sqrt{n}}{12 \log n} \left(1 + \dfrac{3}{\log n} \right) + 0.216 \dfrac{\sqrt{n}}{\log^2 n}$ by 1, which is not a problem for $n \geq 10^{12}$. Thus, equation (3.5) holds when $\gcd(n, 2) = 1$ and $n \geq 10^{12}$.

We argue similarly when $2|n$ to show that equation (3.5) holds for all positive integers $n \geq 10^{12}$.

Case 2. $11 \leq q \leq n^{1/8}$

Since $n \geq 10^{12}$ we have $n^{1/8} > 11$.

Let Q_2 be the number of primes $p \leq \sqrt{n}$ such that congruence (3.1) holds for some $q \in [11, n^{1/8}]$. Thus,

$$Q_2 \leq \sum_{11 \leq q \leq n^{1/8}}{}' \pi(\sqrt{n}; q^2, n). \tag{3.6}$$

In Case 2 the following theorem from the paper [28] which is a version of Brun-Titchmarsh's inequality will be helpful.

Theorem 35. *(H. L. Montgomery and R. C. Vaughan) Let $m > 0$ and l be integers with $(m, l) = 1$, and let $x > m$ be a real number. Then*

$$\pi(x; m, l) \leq \frac{2x}{\varphi(m) \log(x/m)}.$$

We apply Theorem 35 with $x = \sqrt{n}$, $m = q^2$, and $l = n$. When $q \nmid n$ and $q^2 < \sqrt{n}$ the conditions of the theorem hold. So, suppose that $q \leq n^{1/8}$ and $q \nmid n$. Then,

$$\pi(\sqrt{n}; q^2, n) \leq \frac{2\sqrt{n}}{(q-1)q \log(\sqrt{n}/q^2)}. \tag{3.7}$$

When $q \mid n$, then $\pi(\sqrt{n}; q^2, n) \leq 1$. However, for $q \geq 2$, $\log(\sqrt{n}/q^2) \leq (\log n)/2$. Also, $q(q-1) < n^{1/4}$. So,

$$\frac{2\sqrt{n}}{(q-1)q \log(\sqrt{n}/q^2)} > \frac{2n^{1/4}}{\log n}.$$

The function $f_1(n) = \dfrac{n^{1/4}}{\log n}$ is increasing for $n > e^4$ and $f_1(10^9) = 8.58\ldots$, so equation (3.7) holds when $q \mid n$, as well.

Note that

$$\frac{1}{\log(\sqrt{n}/q^2)} = \frac{2}{\log n - 4 \log q} = \frac{2}{\log n} \left(\frac{1}{1 - \frac{4 \log q}{\log n}} \right).$$

Next, use that

$$\frac{1}{1-r} \leq 1 + 2r$$

for $r \leq 1/2$ with $r = \dfrac{4\log q}{\log n}$ to obtain,

$$\frac{1}{\log(\sqrt{n}/q^2)} \leq \frac{2}{\log n} + \frac{16\log q}{\log^2 n}.$$

Combining the above inequality with equation (3.7) we get

$$\pi(\sqrt{n}; q^2, n) \leq \frac{4\sqrt{n}}{(q-1)q\log n} + \frac{32\sqrt{n}\log q}{(q-1)q\log^2 n}.$$

Adding the above inequality for primes q in $[11, n^{1/8}]$ we obtain

$$\sum_{11\leq q\leq n^{1/8}}{}' \pi(\sqrt{n}; q^2, n) \leq c_1(11, n^{1/8})\frac{4\sqrt{n}}{\log n} + c_2(11, n^{1/8})\frac{32\sqrt{n}}{\log^2 n}, \tag{3.8}$$

where we define

$$c_1(A, B) = \sum_{A\leq q\leq B}{}' \frac{1}{q(q-1)}, \quad c_2(A, B) = \sum_{A\leq q\leq B}{}' \frac{\log q}{q(q-1)}.$$

Note that

$$c_1(A, B) < C_1(A) := \sum_{A\leq q}{}' \frac{1}{q(q-1)},$$

and

$$c_2(A, B) < C_2(A) := \sum_{A\leq q}{}' \frac{\log q}{q(q-1)}.$$

So, in the case when we have no upper bound on n we will use the estimate

$$Q_2 \leq \sum_{11\leq q\leq n^{1/8}}{}' \pi(\sqrt{n}; q^2, n) \leq \frac{4C_1(11)\sqrt{n}}{\log n} + \frac{32C_2(11)\sqrt{n}}{\log^2 n}. \tag{3.9}$$

Case 3. $n^{1/8} < q \leq n^{1/4}$

Let Q_3 be the number of primes $p \leq \sqrt{n}$ such that congruence (3.1) holds for some $q \in (n^{1/8}, n^{1/4}]$. Thus,

$$Q_3 \leq \sum_{n^{1/8}<q\leq n^{1/4}}{}' \pi(\sqrt{n}; q^2, n). \tag{3.10}$$

Here we use the following lemma.

Lemma 36. *Let $x > 1$, let a be an integer, and let $q > 1$ be a prime p, or a power of a prime, p^k with $p > 3$. Then,*

$$\pi(x; q, a) \leq \frac{x}{3q} + 2. \tag{3.11}$$

Proof. Since $\pi(x; q, a)$ does not change if we shift a by an integer multiple of q, we can assume $0 \leq a \leq q - 1$. Moreover, if $\gcd(a, q) > 1$, then $\pi(x; q, a) \leq 1$ and the lemma holds.

So, we can assume $\gcd(a, q) = 1$.

Let S be the set of positive integers not exceeding x which are congruent to a modulo q. Note that $\pi(x; q, a)$ is the number of elements of S which are prime.

Denote the size of S by k, that is $k := |S|$. Then, $k = \lfloor \frac{x-a}{q} \rfloor + 1$. We consider six cases depending on what is the remainder when k is divided by 6.

Case 1. $k = 6l$.

Here we divide the elements of S into l sextuples of consecutive elements,

$$(a, \ldots, a + 5q), \ldots, (a + (6l - 6)q, \ldots, a + (6l - 1)q).$$

Since $\gcd(a, q) = 1$ in each sextuple we have a complete set of residues modulo 6. Therefore, in each sextuple we have exactly two elements which are relatively prime to 6. So, in each sextuple (except possible the first one) there are at most two primes. The first sextuple may contain three primes (if $a = 2$ or $a = 3$) but not four. So, if $k = 6l$, $\pi(x; q, a) \leq 2l + 1$.

Case 2. $k = 6l + 1$

Here we put all elements of S, except the first one into l sextuples of consecutive elements. None of the sextuples contain 2 or 3, so if $k = 6l + 1$, $\pi(x; q, a) \leq 2l + 1$.

Case 3. $k = 6l + 2$

Here we put all elements of S, except the first two into l sextuples of consecutive elements. Again, none of the sextuples contain more than two primes, so if $k = 6l+2$, $\pi(x; q, a) \leq 2l + 2$.

Case 4. $k = 6l + 3$

Here we put all elements of S, except the first three into l sextuples of consecutive elements. Again, none of the sextuples contain more than two primes. Moreover, the first three elements of S which are $a, a+q, a+2q$ are not all prime since either $a+q$ or $a+2q$ is even and both are greater than 2. Therefore, if $k = 6l+3$, $\pi(x; q, a) \leq 2l+2$.

Case 5. $k = 6l + 4$

Here we put all elements of S, except the first four into l sextuples of consecutive elements.Again, none of the sextuples contain more than two primes. Moreover, the first four elements of S cannot be all prime, since as in the previous case either $a + q$ or $a + 2q$ is composite. Therefore, if $k = 6l + 4$, $\pi(x; q, a) \leq 2l + 3$.

Case 6. $k = 6l + 5$

Here we put all elements of S, except the first five into l sextuples of consecutive elements. Here we claim that among the first five elements of S, $a, a + q, a + 2q, a + 3q, a + 4q$ there are at most three primes. Indeed, if a is even, then $a + 2q$ and $a + 4q$ are composite (both even and greater than 2). If a is odd, then $a + q$ and $a + 3q$ are composite (even and greater than 2). So, if $k = 6l + 4$, $\pi(x; qa) \leq 2l + 3$.

Thus, in all six cases

$$\pi(x; q, a) \leq \frac{k}{3} + \frac{5}{3}.$$

Recalling that $k = \lfloor \frac{x-a}{q} \rfloor + 1$ completes the proof of the lemma. □

Using the above lemma we obtain

$$Q_3 \leq \sum_{n^{1/8} < q \leq n^{1/4}}{}' \pi(\sqrt{n}; q^2, n) \leq \sum_{n^{1/8} < q \leq n^{1/4}}{}' \left(\frac{\sqrt{n}}{3q^2} + 2 \right) \tag{3.12}$$

Define

$$c_3(A, B) := \sum_{A < q \leq B}{}' \frac{1}{q^2}.$$

Then,

$$Q_3 \leq \frac{c_3\left(n^{1/8}, n^{1/4}\right)\sqrt{n}}{3} + 2\pi(n^{1/4}) - 2\pi(n^{1/8}) \tag{3.13}$$

To estimate $c_3(A, B)$ we use the following lemma.

Lemma 37. *Suppose $A > 2$ and*

$$\frac{c_4 t}{\log t} \leq \pi(t) \leq \frac{c_5 t}{\log t} \tag{3.14}$$

for some constants $c_5 > c_4 > 0$ and all $t \geq A$. Then,

$$\sum_{q<A}{}' \frac{1}{q^2} < \frac{2c_5 - c_4}{A \log A}. \tag{3.15}$$

Proof. Using a Riemann-Stieltjes integral we have

$$S(A) := \sum_{A<q}{}' \frac{1}{q^2} = \int_A^\infty \frac{d(\pi(t))}{t^2}.$$

Next, integrating by parts we get

$$S(A) = \left.\frac{\pi(t)}{t^2}\right|_A^\infty + 2\int_A^\infty \frac{\pi(t)}{t^3} dt.$$

Using that $\pi(t) \leq \dfrac{c_5 t}{\log t}$ for $t \geq A$ we obtain,

$$S(A) \leq -\frac{\pi(A)}{A^2} + 2c_5 \int_A^\infty \frac{1}{t^2 \log t} dt.$$

Since, $\log t$ is increasing function for $t > 2$,

$$\int_A^\infty \frac{1}{t^2 \log t} dt < \frac{1}{\log A} \int_A^\infty \frac{1}{t^2} dt = \frac{1}{A \log A}.$$

Finally, using that $\dfrac{c_4 A}{\log A} \leq \pi(A)$ we obtain the lemma. □

Next, we use the bounds of Rosser and Schoenfeld [32] for $\pi(t)$.

Theorem 38. *(J. Rosser and L. Schoenfeld) We have*

$$\pi(x) > \frac{x}{\log x}\left(1 + \frac{1}{2\log x}\right) \quad \textit{for } x \geq 59, \tag{3.16}$$

and

$$\pi(x) < \frac{x}{\log x}\left(1 + \frac{3}{2\log x}\right) \quad \textit{for } x > 1. \tag{3.17}$$

Using Theorem 38 we get that if $A \geq 59$, we can take

$$c_5 = 1 + \frac{3}{2\log A}, \text{ and } c_4 = 1 + \frac{1}{2\log A}.$$

Therefore, for $A \geq 59$ and $B > A$,

$$c_3(A, B) < \frac{1}{A\log A} + \frac{5}{2\log^2 A}.$$

Therefore,

$$c_3\left(n^{1/8}, n^{1/4}\right) < \frac{8\log n + 160}{n^{1/8}\log^2 n}, \tag{3.18}$$

for $n > 59^8$.

We obtain

$$Q_3 \leq \frac{\sqrt{n}(8\log n + 160)}{3n^{1/8}\log^2 n} + 2\pi(n^{1/4}) - 2\pi(n^{1/8}) \tag{3.19}$$

Case 4. $n^{1/4} < q \leq \frac{\sqrt{n}}{c\log n}$, where c is a fixed constant in the interval $(0.5, 5]$.

We already noted above that $f_1(n) = \frac{n^{1/4}}{\log n}$ is increasing for $n > e^4$ and $f(10^9) = 8.55\ldots$. Thus, $\frac{\sqrt{n}}{10\log n} > n^{1/4}$ for $n \geq 10^9$.

Let Q_4 be the number of primes $p \leq \sqrt{n}$ such that congruence (3.1) holds for some $q \in (n^{1/4}, \frac{\sqrt{n}}{c\log n}]$. Thus,

$$Q_4 \leq \sum_{n^{1/4} < q \leq \frac{\sqrt{n}}{c\log n}}{}' \pi(\sqrt{n}; q^2, n). \tag{3.20}$$

Note that if $q \geq n^{1/4}$, then $\pi(\sqrt{n}; q^2, n) \leq 1$ since there will be at most one positive integer congruent to n modulo q^2 not exceeding $\sqrt{n}$. Thus,

$$Q_4 \leq \pi\left(\frac{\sqrt{n}}{c\log n}\right) - \pi\left(n^{1/4}\right). \tag{3.21}$$

Denote $m = \frac{\sqrt{n}}{c\log n}$. We proved above that $m > n^{1/4}$ for $n > 10^{12}$, so $\log m > \log n/4$ for such n. By Theorem 38 we have

$$\pi(m) < \frac{4\sqrt{n}}{c\log^2 n}\left(1 + \frac{6}{\log n}\right),$$

and

$$\pi\left(n^{1/4}\right) < \frac{4n^{1/4}}{\log n}\left(1+\frac{6}{\log n}\right).$$

Combining the above two inequalities with equations (3.13) and (3.21) we obtain

$$Q_3+Q_4 < \frac{\sqrt{n}(8\log n+160)}{3n^{1/8}\log^2 n} + \frac{4\sqrt{n}}{c\log^2 n}\left(1+\frac{6}{\log n}\right) + \frac{4n^{1/4}}{\log n}\left(1+\frac{6}{\log n}\right). \quad (3.22)$$

Case 5. $\sqrt{n}/(c\log n) < q < \sqrt{n}$

Let Q_5 be the number of primes $p \le \sqrt{n}$ such that congruence (3.1) holds for some $q \in (\frac{\sqrt{n}}{c\log n}, \sqrt{n}]$. Thus,

$$Q_5 \le \sum_{\frac{\sqrt{n}}{c\log n}<q<\sqrt{n}}{}' \pi(\sqrt{n}; q^2, n). \quad (3.23)$$

To estimate Q_5 we use the following.

Suppose q_1 and q_2 are distinct primes in $(\sqrt{n}/(c\log n), \sqrt{n})$ such that there exist distinct primes p_1, p_2 both not exceeding $\sqrt{n}$ such that $q_1^2 \mid n-p_1$ and $q_2^2 \mid n-p_2$. Thus, there exist positive integers k_1 and k_2 such that $n-p_1 = k_1q_1^2$ and $n-p_2 = k_2q_2^2$.

We claim that $k_1 \neq k_2$. Assume the opposite, that $k_1 = k_2$

Then, $(n-p_1)-(n-p_2) = k_1(q_1^2-q_2^2)$, that is

$$p_2 - p_1 = k_1(q_1+q_2)(q_1-q_2). \quad (3.24)$$

Note that $k_1q_1 = k_1q_1^2/q_1 = (n-p_1)/q_1 > (n-\sqrt{n})/\sqrt{n} = \sqrt{n}-1$.

Therefore, $k_1(q_1+q_2)|q_1-q_2| > k_1q_1 > \sqrt{n}-1 > |p_1-p_2|$, contradicting (3.24). So, $k_1 \neq k_2$.

We conclude that the contribution from $q \in (\sqrt{n}/(c\log n), \sqrt{n})$ does not exceed the number of distinct integers k such that $n-p = kq^2$. Note that for each such k we have $k = (n-p)/q^2 < (c\log n)^2$, since $q > \sqrt{n}/(c\log n)$. Thus,

$$Q_5 \le (c\log n)^2. \quad (3.25)$$

Now, combining (3.5), (3.9), (3.22), and (3.25) we get

$$Q_1+Q_2+Q_3+Q_4+Q_5<\frac{46\sqrt{n}}{35\log n}+\frac{1569\sqrt{n}}{350\log^2 n}+\frac{4C_1(11)\sqrt{n}}{\log n}+\frac{32C_2(11)\sqrt{n}}{\log^2 n}+$$

$$+\frac{\sqrt{n}(8\log n+160)}{3n^{1/8}\log^2 n}+\frac{4\sqrt{n}}{c\log^2 n}\left(1+\frac{6}{\log n}\right)+\frac{4n^{1/4}}{\log n}\left(1+\frac{6}{\log n}\right)+(c\log n)^2,$$

for $n>59^8$.

Since to prove the theorem it is sufficient to show $Q_1+Q_2+Q_3+Q_4+Q_5<\pi\left(\sqrt{n}\right)$ and by Theorem 38 for $n>59^2$,

$$\pi\left(\sqrt{n}\right)>\frac{2\sqrt{n}}{\log n}\left(1+\frac{1}{\log n}\right),$$

it is sufficient to establish

$$\frac{2\sqrt{n}}{\log n}\left(1+\frac{1}{\log n}\right)>f_2(n), \tag{3.26}$$

where

$$f_2(n):=\frac{46\sqrt{n}}{35\log n}+\frac{1569\sqrt{n}}{350\log^2 n}+\frac{4C_1(11)\sqrt{n}}{\log n}+\frac{32C_2(11)\sqrt{n}}{\log^2 n}+$$

$$+\frac{\sqrt{n}(8\log n+160)}{3n^{1/8}\log^2 n}+\frac{4\sqrt{n}}{c\log^2 n}\left(1+\frac{6}{\log n}\right)+\frac{4n^{1/4}}{\log n}\left(1+\frac{6}{\log n}\right)+(c\log n)^2.$$

Dividing the inequality (3.26) by $\frac{\sqrt{n}}{\log n}$ and simplifying we get that the inequality is equivalent to

$$\frac{24}{35}>\frac{869}{350\log n}+4C_1(11)+\frac{32C_2(11)}{\log n}+\frac{8\log n+160}{3n^{1/8}\log n}+ \tag{3.27}$$

$$+\frac{4}{c\log n}\left(1+\frac{6}{\log n}\right)+4n^{-1/4}\left(1+\frac{6}{\log n}\right)+\frac{c^2\log^3 n}{\sqrt{n}}.$$

Note the functions

$$\frac{1}{\log n},\ \frac{1}{\log^2 n},\ \frac{1}{n^{1/8}},\ \frac{1}{n^{1/8}},\ \frac{1}{n^{1/8}\log n},\ \text{and}\ \frac{1}{n^{1/4}\log n}$$

are all decreasing for $n>1$. Moreover, the function $\frac{\log^3 n}{\sqrt{n}}$ is decreasing for $n>e^6$. Therefore, if inequality (3.27) holds for some $n_0>59^8$, then it holds for all $n\geq n_0$.

Since the inequalities (3.26) and (3.27) are equivalent, then if inequality (3.26) holds for some $n_0 > 59^8$, then it holds for all $n \geq n_0$.

Estimating the tail of the series defining $C_1(11)$ and $C_2(11)$ in the same way we estimated the series $\sum'_{A<q<B} \frac{1}{q^2}$ we get the estimates $C_1(11) < 0.033$ and $C_2(11) < 0.1$.

Taking $c = 4$ and $n = 59^8 + 1$, we get that the left-hand-side of inequality (3.26) exceeds the right-hand-side by more than $95945 > 0$. Thus, the theorem holds for $n > 59^8$.

From now on, we assume $n \leq 59^8$. For such n we cannot use Theorem 38 to get lower bound for $\pi\left(n^{1/8}\right)$. However, we can estimate $c_3(A, B)$ as follows. We have

$$c_3(A, B) < c_3(A) = \sum_q{}' \frac{1}{q^2} - \sum_{q \leq A}{}' \frac{1}{q^2}.$$

Denote

$$g(A) := \sum_{q \leq A}{}' \frac{1}{q^2}.$$

The function g is piecewise continuous and nondecreasing.

Also, it has been known since Euler [15] p.480 (or possibly earlier) that

$$\sum_q{}' \frac{1}{q^2} := c_0 = 0.452247420041065\ldots \tag{3.28}$$

Replacing the estimate for $c_3\left(n^{1/8}, n^{1/4}\right)$ in equation (3.22) we get

$$Q_3 + Q_4 < \frac{\sqrt{n}\left(c_0 - g\left(n^{1/8}\right)\right)}{3} + \frac{4\sqrt{n}}{c\log^2 n}\left(1 + \frac{6}{\log n}\right) + \frac{4n^{1/4}}{\log n}\left(1 + \frac{6}{\log n}\right). \tag{3.29}$$

To prove the theorem now we need to establish

$$\frac{2\sqrt{n}}{\log n}\left(1 + \frac{1}{\log n}\right) > f_3(n), \tag{3.30}$$

where

$$f_3(n) := \frac{46\sqrt{n}}{35\log n} + \frac{1569\sqrt{n}}{350\log^2 n} + \frac{4C_1(11)\sqrt{n}}{\log n} + \frac{32C_2(11)\sqrt{n}}{\log^2 n} +$$
$$+ \frac{\sqrt{n}\left(c_0 - g\left(n^{1/8}\right)\right)}{3} + \frac{4\sqrt{n}}{c\log^2 n}\left(1 + \frac{6}{\log n}\right) + \frac{4n^{1/4}}{\log n}\left(1 + \frac{6}{\log n}\right) + (c\log n)^2.$$

Unfortunately, if we divide $f_3(n)$ by $\frac{\sqrt{n}}{\log n}$ it is not clear that the resulting function is decreasing due to the term $\frac{\sqrt{n}\left(c_0-g\left(n^{1/8}\right)\right)}{3}$, so we proceed as follows.

Let p_k be the kth prime number. Next we will be considering the cases when $n \in (p_k^8, p_{k+1}^8]$ where $31 \leq p_k \leq 53$ (when $p_k = 31$ we will consider $n \in [10^{12}, 37^8]$). For such n we have $g(n^{1/8}) \geq g(p_k)$. Moreover, since $\log n$ is increasing function, $\frac{8 \log p_{k+1}}{\log n} \geq 1$ for $n \in (p_k^8, p_{k+1}^8]$. Also, since now we have upper bound for n, when estimating Q_2 we will use equation (3.8), that is we will use $c_1(11, p_{k+1})$ instead of $C_1(11)$, and $c_2(11, p_{k+1})$ instead of $C_2(11)$.

We replace $f_3(n)$ by the (potentially) slightly larger function

$$f_4(n,k) := \frac{46\sqrt{n}}{35\log n} + \frac{1569\sqrt{n}}{350\log^2 n} + \frac{4c_1(11,p_{k+1})\sqrt{n}}{\log n} + \frac{32c_2(11,p_{k+1})\sqrt{n}}{\log^2 n} +$$

$$+\frac{\sqrt{n}\left(c_0 - g\left(p_k\right)\right)\left(8\log p_{k+1}\right)}{3\log n} + \frac{4\sqrt{n}}{c\log^2 n}\left(1+\frac{6}{\log n}\right) + \frac{4n^{1/4}}{\log n}\left(1+\frac{6}{\log n}\right) + (c\log n)^2.$$

The function $f_4(n,k)$ may be larger than $f_3(n)$ but has the property that it is decreasing on the interval $(p_k^8, p_{k+1}^8]$ after division by $\frac{\sqrt{n}}{\log n}$.

Thus, if

$$\frac{2\sqrt{n_0}}{\log n_0}\left(1+\frac{1}{\log n_0}\right) > f_4(n_0,k) \tag{3.31}$$

for some $p_{k+1}^8 \geq n_0 \geq \max(p_k^8, 10^{12})$, then the theorem holds for all $n \in [n_0, p_{k+1}^8]$.

In the table below we record the results of our computations in several intervals. The symbol Δ will denote the difference between the left-hand-side of inequality (3.31) and its right-hand-side evaluated at the left end of each interval indicated in each row.

The left end of the interval in the last row in the table above is 10^{12} rather than 31^8 since $31^8 < 10^{12}$ and we cannot use Theorem 33 to estimate $\pi(\sqrt{n}; q^2, n)$ when $\sqrt{n} < 10^6$.

When $n \leq 10^{12}$ we use another result of Bennett et. al., Corollary 1.6 of [3].

Table 3.1 Results of Computations of Several Intervals

k	interval	$c_1(11, p_{k+1})$	$c_2(11, p_{k+1})$	c	$c_0 - g(p_k)$	Δ
16	$[53^8, 59^8]$	0.02941652	0.08277361	4	0.00352137	74613.3
15	$[47^8, 53^8]$	0.02912429	0.08158205	3.3	0.00387736	46560.4
14	$[43^8, 47^8]$	0.02876145	0.08014145	2.9	0.00433005	32612.4
13	$[41^8, 43^8]$	0.02829891	0.07836062	2.7	0.00487089	26933.3
12	$[37^8, 41^8]$	0.02774520	0.07627800	2.3	0.00546577	17911.1
11	$[10^{12}, 37^8]$	0.02713545	0.07401364	2	0.00619623	9029.5

Theorem 39. *Let $1 \le q \le 1200$ be an integer, and a be an integer coprime to q. For all $x \ge 50q^2$ we have*

$$\frac{x}{\varphi(q)\log x} < \pi(x; q, a) < \frac{x}{\varphi(q)\log x}\left(1 + \frac{5}{2\log x}\right).$$

We apply the above theorem with $n \ge 10^9$, and $q \in \{2^2, 3^2, 5^2, 7^2\}$. Since $\sqrt{10^9} > 31622 > 50 \cdot 7^2 = 2450$, Theorem 39 applies when $\gcd(n, 210) = 1$ and argue similarly to Case 1 when $\gcd(n, 210) > 1$. Substituting into equation (3.2) we obtain

$$Q_1 < \frac{46\sqrt{n}}{35\log n} + \frac{32\sqrt{n}}{7\log^2 n}. \tag{3.32}$$

We get a somewhat worse estimate. The constant in the second term is $32/7 = 4.57\ldots$ rather than $1569/350 = 4.48\ldots$.

So, for $n \ge 10^9$ now we need to show

$$\frac{2\sqrt{n}}{\log n}\left(1 + \frac{1}{\log n}\right) > f_5(n, k), \tag{3.33}$$

where

$$f_5(n,k) := \frac{46\sqrt{n}}{35\log n} + \frac{32\sqrt{n}}{7\log^2 n} + \frac{4c_1(11, p_{k+1})\sqrt{n}}{\log n} + \frac{32c_2(11, p_{k+1})\sqrt{n}}{\log^2 n} +$$

$$+ \frac{\sqrt{n}\,(c_0 - g\,(p_k))\,(8\log p_{k+1})}{3\log n} + \frac{4\sqrt{n}}{c\log^2 n}\left(1 + \frac{6}{\log n}\right) + \frac{4n^{1/4}}{\log n}\left(1 + \frac{6}{\log n}\right) + (c\log n)^2.$$

We proceed exactly as before, the only difference between $f_4(n,k)$ and $f_5(n,k)$ is that the constant 1569/350 in the second term of $f_4(n,k)$ is replaced by 32/7 to obtain $f_5(n,k)$.

The table below replaces f_4 by f_5 and gives the data for the remaining intervals.

Table 3.2 Results of Computations of Several More Intervals

k	interval	$c_1(11,p_{k+1})$	$c_2(11,p_{k+1})$	c	$c_0-g(p_k)$	Δ
11	$[31^8,10^{12}]$	0.02713545	0.07401364	2	0.00619623	5606.9
10	$[29^8,31^8]$	0.02638469	0.0713027	2	0.00723681	3669.5
9	$[23^8,29^8]$	0.02530942	0.06761027	1.6	0.00842587	910.8
8	$[19^8,23^8]$	0.02407789	0.0634633	1.3	0.01031623	179.8
7	$[17^8,19^8]$	0.02210161	0.05726672	1.1	0.0130863	62.1
6	$[13^8,17^8]$	0.01917763	0.04865725	.6	0.0165465	35.3

Thus, the theorem is holds for $n \geq 13^8 = 815730721$. Since we established the theorem by direct computation for $n \leq 10^9$, this completes the proof. □

Bibliography

[1] Paul Balister et al. "On the Erdős covering problem: the density of the uncovered set". In: *Invent. Math.* 228.1 (2022), pp. 377–414.

[2] Paul Balister et al. "The Erdős-Selfridge problem with square-free moduli". In: *Algebra Number Theory* 15.3 (2021), pp. 609–626.

[3] Michael A. Bennett et al. "Explicit bounds for primes in arithmetic progressions". In: *Illinois J. Math.* 62.1-4 (2018), pp. 427–532.

[4] E. Bombieri and J. Pila. "The number of integral points on arcs and ovals". In: *Duke Math. J.* 59.2 (1989), pp. 337–357.

[5] Manfredo do Carmo. *Differential Geometry of Curves and Surfaces*. Prentice-Hall, Englewood Cliffs, New Jersey, 1976, p. 128.

[6] S. L. G. Choi. "Covering the set of integers by congruence classes of distinct moduli". In: *Math. Comp.* 25 (1971), pp. 885–895.

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

[8] Adrian W. Dudek. "On the sum of a prime and a square-free number". In: *Ramanujan J.* 42.1 (2017), pp. 233–240.

[9] Adrian W. Dudek and David J. Platt. "On the sum of the square of a prime and a square-free number". In: *LMS J. Comput. Math.* 19.1 (2016), pp. 16–24.

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

[11] P. Erdös. "The representation of an integer as the sum of the square of a prime and of a square-free integer". In: *J. London Math. Soc.* 10.4 (1935), pp. 243–245.

[12] P. Erdős and R. L. Graham. *Old and new problems and results in combinatorial number theory*. Vol. 28. Monographies de L'Enseignement Mathéma-

tique [Monographs of L'Enseignement Mathématique]. Université de Genève, L'Enseignement Mathématique, Geneva, 1980, p. 128.

[13] Paul Erdős. "Résultats et problèmes en théorie des nombres". In: *Séminaire Delange-Pisot-Poitou (14e année: 1972/73), Théorie des nombres, Fasc. 2*. Secrétariat Mathématique, Paris, 1973, Exp. No. 24, 7.

[14] T. Estermann. "On the Representations of a Number as the Sum of a Prime and a Quadratfrei Number". In: *J. London Math. Soc.* 6.3 (1931), pp. 219–221.

[15] L Euler. *Introductio in analysin infinitorum*. Academiae imperialis scientiarum Petropolitanae, 1748.

[16] M. Filaseta, K. Ford, and S. Konyagin. "On an irreducibility theorem of A. Schinzel associated with coverings of the integers". In: *Illinois J. Math.* 44.3 (2000), pp. 633–643.

[17] M. Filaseta, S. Graham, and O. Trifonov. "Starting with gaps between k-free numbers". In: *Int. J. Number Theory* 11.5 (2015), pp. 1411–1435.

[18] Michael Filaseta and Ognian Trifonov. "The distribution of fractional parts with applications to gap results in number theory". In: *Proc. London Math. Soc. (3)* 73.2 (1996), pp. 241–278.

[19] Michael Filaseta et al. "Sieving by large integers and covering systems of congruences". In: *J. Amer. Math. Soc.* 20.2 (2007), pp. 495–517.

[20] Donald Jason Gibson. "A covering system with least modulus 25". In: *Math. Comp.* 78.266 (2009), pp. 1127–1146.

[21] Joshua Harrington. "Two questions concerning covering systems". In: *Int. J. Number Theory* 11.6 (2015), pp. 1739–1750.

[22] Bob Hough. "Solution of the minimum modulus problem for covering systems". In: *Ann. of Math. (2)* 181.1 (2015), pp. 361–382.

[23] R. Howard and O. Trifonov. "Bounding the number of lattice points close to a curve by curvature and arclength". In: *Funct. Approx. Comment. Math.* (). (to appear).

[24] Jing-Jing Huang. "Integral points close to a space curve". In: *Math. Ann.* 374.3-4 (2019), pp. 1987–2003.

[25] Vojtěch Jarnıék. "Über bedingt konvergente Reihen". In: *Math. Z.* 24.1 (1926), pp. 715–732.

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

[27] P. Letendre. *Topics in analytic number theory*. Thesis (Ph.D.)–Universite Laval. 2018.

[28] H. L. Montgomery and R. C. Vaughan. "The large sieve". In: *Mathematika* 20 (1973), pp. 119–134.

[29] Ryozo Morikawa. "On a method to construct covering sets". In: *Bull. Fac. Liberal Arts Nagasaki Univ.* 22.1 (1981), pp. 1–11.

[30] Pace P. Nielsen. "A covering system whose smallest modulus is 40". In: *J. Number Theory* 129.3 (2009), pp. 640–666.

[31] Tyler Owens. *A Covering System with Minimum Modulus 42*. Thesis (Masters). Brigham Young University, Provo, UT, 2014.

[32] J. Barkley Rosser and Lowell Schoenfeld. "Approximate formulas for some functions of prime numbers". In: *Illinois J. Math.* 6 (1962), pp. 64–94.

[33] R. J. Simpson and Doron Zeilberger. "Necessary conditions for distinct covering systems with square-free moduli". In: *Acta Arith.* 59.1 (1991), pp. 59–70.

[34] J. D. Swift. "Sets of covering congruences". In: *Bull. Amer. Math. Soc.* 60.4 (1954), p. 390.

[35] H. P. F. Swinnerton-Dyer. "The number of lattice points on a convex curve". In: *J. Number Theory* 6 (1974), pp. 128–135.