Three applications of sieve methods in analytic number theory

by

Lee Thomas Troupe

(Under the direction of Paul Pollack)

Abstract

We establish three results in the area of analytic number theory. These results concern the normal order of an arithmetic function, statistical information on reductions of elliptic curves with complex multiplication, and bounded gaps between primes in the setting of polynomials over a finite field. Along the way, we develop necessary background material and place our results in historical context.

Index words: sieve methods, prime numbers, arithmetic functions, elliptic curves, normal order

Three applications of sieve methods in analytic number theory

by

Lee Troupe

B.A., University of Tennessee, 2010

A Dissertation Submitted to the Graduate Faculty
of The University of Georgia in Partial Fulfillment
of the
Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2016

Three applications of sieve methods in analytic number theory

by

Lee Troupe

Approved:

Major Professor: Paul Pollack

Committee: Alina Carmen Cojocaru
Neil Lyall
Akos Magyar

Electronic Version Approved:

Suzanne Barbour, Ph.D.
Dean of the Graduate School
The University of Georgia
May 2016

Acknowledgments

This thesis would not exist without the guidance and encouragement of my advisor, Paul Pollack. It has been a true privilege to learn from him, and I am grateful for his kindness, his patience and his cleverness. I am proud to be Paul's first student, and certainly I will not be the last.

I have been fortunate enough to meet a number of incredible people at the University of Georgia, and their fingerprints are all over this document. A great many of the faculty have had a profound influence on my mathematical career. In particular, I would like to thank Pete Clark, for teaching me a great many things about both algebraic number theory and life as a mathematician; and Neil Lyall, for showing me that analysis isn't so bad and for being a great mentor and friend over the past six years. Of course, it has also been a joy to work alongside my fellow graduate students. I thank you for your camaraderie, and I intend to stay in touch.

Finally, to my parents: You always told me that I could be anything I wanted, and I chose to be this. Thank you for loving and supporting me anyway! And to Erin: You are my constant, and I can't imagine having done this without you. I love you very much, I'm tremendously excited about what the future holds for us, and I expect a similar mention in this section of your thesis.

Notation

We collect here some notation and terminology that is common throughout this document. Let f and g be (real-valued) functions of a real variable x. We say $f(x) = O(g(x))$ if $|f(x)| < C|g(x)|$ for all x, where $C > 0$ is an absolute constant. An equivalent notation is $f(x) \ll g(x)$. The notation $f(x) = o(g(x))$ means that, for *any* $c > 0$, $|f(x)| < c|g(x)|$ for sufficiently large x; in other words, $f(x) = o(g(x))$ if $\lim_{x\to\infty} f(x)/g(x) = 0$. We say that $f(x)$ and $g(x)$ are asymptotically equal, and we write $f(x) \sim g(x)$, if

$$\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1.$$

Throughout, the letter p will denote a rational prime. In Chapters 2 and 3, the letter q will also denote a rational prime; in Chapter 4, q will be a power of a prime. The function $\log_k(x)$ is the kth iterate of the function $\log_1(x) := \max\{\log(x), 1\}$, where $\log(x)$ is the natural logarithm. An exception to this notation occurs in Chapter 4, where certain calculations involve the base-q logarithm, denoted $\log_q$.

At the end of Sections 3.2 and 4.1, we introduce more notation particular to those chapters. Other notation will be introduced as needed.

Contents

Acknowledgements **iv**

Notation **v**

1 Introduction **1**

1.1 Sieve theory 1

1.2 Arithmetic functions and normal order 10

1.3 Primes in arithmetic progressions 16

1.4 Statement of main results 19

2 The number of prime factors of $s(n)$ **21**

2.1 Introduction 21

2.2 Preliminaries 23

2.3 An average result for $\omega(s(n))$ 28

2.4 Proof of Theorem 2.1.3 32

2.5 From $\omega(s(n))$ to $\Omega(s(n))$ 35

3 Orders of reductions of elliptic curves **41**

3.1 Introduction 41

3.2 Analytic questions concerning $\#E(\mathbb{F}_p)$ 43

3.3 Useful propositions 45

3.4 An upper bound 49
3.5 A lower bound 59
3.6 Generalizing to other CM elliptic curves 69

4 Bounded gaps between primes **72**

4.1 Preliminaries 72
4.2 The necessary tools 76
4.3 Maynard-Tao over $\mathbb{F}_q(t)$ 81
4.4 Proof of Proposition 4.3.3 86
4.5 An example: Primitive polynomials over $\mathbb{F}_2$ 96

Bibliography **103**

Chapter 1

Introduction

1.1 Sieve theory

1.1.1 The sieve of Eratosthenes-Legendre.

By a *sieve problem*, we mean the task of estimating the size of a set that has been sifted in some way. Examples of sifted sets include those whose members possess no small prime factors, or a prescribed number of prime factors. Such sets have been studied for thousands of years; in ancient Greece, Eratosthenes of Cyrene noticed that, to obtain a list of all primes up to some point x, one only needs to know the primes up to $\sqrt{x}$. More specifically, if one crosses off all multiples of primes $p \leq \sqrt{x}$ from a list of the positive integers up to x, the uncrossed numbers will be exactly the primes between $\sqrt{x}$ and x (and the number 1). Quantitatively, if we define $\pi(x, z)$ to be the count of numbers up to x possessing no prime factors less or equal to z, and $\pi(x)$ to be the count of primes up to x, then the sieve of Eratosthenes shows that

$$\pi(x) \leq \pi(x, z) + O(z),$$

with equality when $z = \sqrt{x}$. How large is $\pi(x, z)$? An exact formula for the size of $\pi(x, z)$ is due to Legendre. There are $\lfloor x \rfloor$ positive integers $\leq x$; $\lfloor x/p \rfloor$ of those are divisible by a prime $p \leq z$. Thus,

$$\pi(x, z) \geq \lfloor x \rfloor - \sum_{p \leq z} \Big\lfloor \frac{x}{p} \Big\rfloor,$$

with the greater-than sign coming from the fact that the sum overcounts integers divisible by more than one prime. We can "add back" such numbers via expressions of the form $\lfloor x/p_1 p_2 \rfloor$; again, the corresponding sum overcounts those integers divisible by more than two primes. Carrying this process to its conclusion, we obtain

$$\pi(x, z) = \lfloor x \rfloor - \sum_{p \leq z} \Big\lfloor \frac{x}{p} \Big\rfloor + \sum_{p_1 < p_2 \leq z} \Big\lfloor \frac{x}{p_1 p_2} \Big\rfloor - \sum_{p_1 < p_2 < p_3 \leq z} \Big\lfloor \frac{x}{p_1 p_2 p_3} \Big\rfloor + \cdots + (-1)^{\pi(z)} \sum_{p_1 < \cdots < p_{\pi(z)}} \Big\lfloor \frac{x}{p_1 p_2 \cdots p_{\pi(z)}} \Big\rfloor. \quad (1.1)$$

(In summary, this is an application of the principle of inclusion-exclusion, cf. [Pol09, Theorem 6.1].) The formula above is exact, but unwieldy. By dropping the greatest-integer signs, we obtain an error of size at most 1 for each divisor of $P = \prod_{p \leq z} p$. The resulting expression can be written as a product, and this version of the formula is known as the sieve of Eratosthenes-Legendre.

Theorem 1.1.1. *We have*

$$\pi(x, z) = x \prod_{p \leq z} \Big(1 - \frac{1}{p}\Big) + O\Big(2^{\pi(z)}\Big).$$

Choosing $z = \log x$ and appealing to known results to estimate the product, the above theorem gives

$$\pi(x, \log x) \sim e^{-\gamma} \frac{x}{\log \log x},$$

where γ is the Euler-Mascheroni constant. Thus, since $\pi(x) \leq \pi(x, \log x) + O(\log x)$, the sieve of Eratosthenes-Legendre is enough to show that the primes have asymptotic density zero; however, by 19th century work of Chebyshev, it does not give the correct order of magnitude for $\pi(x)$.

1.1.2 Sieve notation.

Let us replace the ad hoc notation above with what is standard in the field. Let $\mathcal{A}$ be a sequence of integers, and let $\mathcal{P}$ denote a finite set of prime numbers. Write $P := \prod_{p \in \mathcal{P}} p$. Define

$$S(\mathcal{A}, \mathcal{P}) = \#\{a \in \mathcal{A} : \gcd(a, P) = 1\}.$$

We write A_d for the number of terms of $\mathcal{A}$ divisible by d. Let X denote an approximation to the size of $\mathcal{A}$, and let $\alpha(d)$ be a multiplicative function such that, for all d,

$$A_d = X\alpha(d) + r(d), \tag{1.2}$$

where $r(d)$ is defined so that (1.2) is true given X and α. With this notation, the ideas leading to Theorem 1.1.1 produce the formula

$$S(\mathcal{A}, \mathcal{P}) = X \prod_{p \in \mathcal{P}} (1 - \alpha(p)) + \sum_{d | P} \mu(d) r(d),$$

where, in the application of counting primes, $\mathcal{A} = \{n \leq x\}$, $\mathcal{P} = \{p \leq z\}$, $X = x$ and $\alpha(p) = 1/p$, forcing $|r(d)| < 1$. Note that (1.2) is a generalization of Theorem 1.1.1 and can be used in other applications; however, the small range of z for which the error term is manageable limits its utility.

1.1.3 Brun's pure sieve.

In the discussion preceding (1.1), we remarked that truncating the alternating sum after subtraction yields a lower bound for $\pi(x, z)$, while truncating after addition yields an upper bound. Exploring this simple idea led Brun [Bru15] to discover his namesake "pure" sieve.

Theorem 1.1.2. *With the notation described in Section 1.1.2, we have, for every even integer $m \geq 0$,*

$$\sum_{\substack{d|P \\ \omega(d)\leq m-1}} \mu(d)A_d \leq S(\mathcal{A}, \mathcal{P}) \leq \sum_{\substack{d|P \\ \omega(d)\leq m}} \mu(d)A_d.$$

Writing $A_d = X\alpha(d) + r(d)$ and manipulating the result, we obtain a version of Brun's sieve suitable for applications.

Theorem 1.1.3. *For every even integer $m \geq 0$,*

$$S(\mathcal{A}, \mathcal{P}) = X \prod_{p\in\mathcal{P}}(1 - \alpha(p)) + O\Big(\sum_{\substack{d|P \\ \omega(d)\leq m}} |r(d)|\Big) + O\Big(X \sum_{\substack{d|P \\ \omega(d)\geq m}} \alpha(d)\Big).$$

Theorem 1.1.3 can be used to show, among other things, an upper bound for the number of twin primes $\leq x$ that is nearly of the correct order of magnitude (and is close enough to show that the sum of the reciprocals of the twin primes converges). We refer the reader to [Pol09, Chapter 6] for more details.

There are rings of integers besides $\mathbb{Z}$, and one can formulate sieves in these contexts. In particular, we will make extensive use in Chapter 3 of Brun's sieve in the Gaussian integers $\mathbb{Z}[i]$. We conclude this section with a version of Brun's sieve for the ring of integers of a number field.

Theorem 1.1.4. *Let K be a number field with ring of integers $\mathbb{Z}_K$. Let $\mathcal{A}$ be a finite sequence of elements of $\mathbb{Z}_K$, and let $\mathcal{P}$ be a finite set of prime ideals. Define*

$$S(\mathcal{A},\mathcal{P}) := \#\{a \in \mathcal{A} : \gcd(a,\mathfrak{P}) = 1\}, \text{ where } \mathfrak{P} := \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}.$$

For an ideal $\mathfrak{u} \subset \mathbb{Z}_K$, write $A_\mathfrak{u} := \#\{a \in \mathcal{A} : a \equiv 0 \pmod{\mathfrak{u}}\}$. Let X denote an approximation to the size of $\mathcal{A}$. Suppose δ is a multiplicative function taking values in $[0,1]$, and define a function $r(\mathfrak{u})$ such that

$$A_\mathfrak{u} = X\delta(\mathfrak{u}) + r(\mathfrak{u}) \tag{1.3}$$

for each $\mathfrak{u}$ dividing $\mathfrak{P}$. Then, for every even $m \in \mathbb{Z}^+$,

$$S(\mathcal{A},\mathcal{P}) = X\prod_{\mathfrak{p}\in\mathcal{P}}(1-\delta(\mathfrak{p})) + O\Big(\sum_{\mathfrak{u}|\mathfrak{P},\,\omega(\mathfrak{u})\le m} |r(\mathfrak{u})|\Big) + O\Big(X\sum_{\mathfrak{u}|\mathfrak{P},\,\omega(\mathfrak{u})\ge m} \delta(\mathfrak{u})\Big).$$

All implied constants are absolute. Here, the notation $\omega(\mathfrak{u})$ means the number of distinct prime ideals appearing in the factorization of $\mathfrak{u}$ into prime ideals.

Proof. By Theorem 1.1.2 and (1.3),

$$\begin{aligned} S(\mathcal{A},\mathcal{P}) &= \sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\le m}} \mu(\mathfrak{u})A_\mathfrak{u} + O\Big(\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})= m}} A_\mathfrak{u}\Big) \\ &= \sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\le m}} \mu(\mathfrak{u})(X\delta(\mathfrak{u}) + r(\mathfrak{u})) + O\Big(\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})= m}} A_\mathfrak{u}\Big) \\ &= X\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\le m}} \mu(\mathfrak{u})\delta(\mathfrak{u}) + O\Big(\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\le m}} |r(\mathfrak{u})|\Big) + O\Big(\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})= m}} A_\mathfrak{u}\Big). \end{aligned}$$

This last error term is, again by (1.3),

$$\ll X \sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})=m}} \delta(\mathfrak{u}) + \sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})=m}} |r(\mathfrak{u})|.$$

We thus obtain

$$S(\mathcal{A},\mathcal{P}) = X \sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\le m}} \mu(\mathfrak{u})\delta(\mathfrak{u}) + O\Big(\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\le m}} |r(\mathfrak{u})|\Big) + O\Big(X \sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})=m}} \delta(\mathfrak{u})\Big)$$

We can extend the sum in the main term to all $\mathfrak{u} \mid \mathfrak{P}$ and write

$$\begin{aligned} S(\mathcal{A},\mathcal{P}) &= X \sum_{\mathfrak{u}|\mathfrak{P}} \mu(\mathfrak{u})\delta(\mathfrak{u}) + O\Big(\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\le m}} |r(\mathfrak{u})|\Big) + O\Big(X \sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\ge m}} \delta(\mathfrak{u})\Big) \\ &= X \prod_{\mathfrak{p}\in\mathcal{P}} (1-\delta(\mathfrak{p})) + O\Big(\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\le m}} |r(\mathfrak{u})|\Big) + O\Big(X \sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\ge m}} \delta(\mathfrak{u})\Big), \end{aligned}$$

as desired. □

1.1.4 The method of Maynard and Tao.

A k-tuple of integers $\mathcal{H} = \{h_1, \dots, h_k\}$ is called *admissible* if there is no prime p such that the collection $\{h_1 \pmod p, \dots, h_k \pmod p\}$ forms a complete set of residue classes modulo p. In 1923, Hardy and Littlewood [HL23] formulated a conjecture concerning admissible k-tuples that has motivated a tremendous amount of research in the intervening years.

Conjecture 1.1.5. *Let $\mathcal{H} = \{h_1, \dots, h_k\}$ be admissible. Then there are infinitely many integers n such that*

$$n + \mathcal{H} = \{n + h_1, \dots, n + h_k\}$$

consists entirely of primes. More precisely, the number of such $n \leq x$ is asymptotically equal to

$$\mathfrak{S}(\mathcal{H})\frac{x}{\log^k x},$$

as $x \to \infty$, where $\mathfrak{S}(\mathcal{H})$ is a nonzero constant depending on $\mathcal{H}$.

The constant $\mathfrak{S}(\mathcal{H})$ is called the *singular series* for $\mathcal{H}$; it does not play a role in the results of this manuscript. See the survey by Soundararajan [Sou07] for basic information about the singular series and how it arises in this conjecture. Note that admissible sets of integers are precisely those sets for which the prime k-tuples conjecture could possibly hold, since if the members of $\mathcal{H}$ form a complete set of residues when reduced modulo p, any shift $n + \mathcal{H}$, reduced modulo p, will contain $0 \pmod p$. Though it remains open, efforts to prove this conjecture and related questions have produced a number of important results, some of which we mention here.

Conjecture 1.1.5 can be weakened in two natural ways. Given an admissible k-tuple $\mathcal{H}$, one can ask for infinitely many $n \in \mathbb{N}$ such that $n + \mathcal{H}$ contains m primes, for $1 < m < k$; or that $n + \mathcal{H}$ consists entirely of almost primes, i.e. numbers with $O_k(1)$ prime factors. The best known result of this latter type was obtained in the case $k = 2$ by Chen [Che73], who showed that there are infinitely primes p such that $p + 2$ has at most two prime factors. A qualitatively similar result is known for arbitrary k: If $\mathcal{H}$ is an admissible k-tuple, then infinitely many shifts $n + \mathcal{H}$ consist entirely of numbers with $O_k(1)$ prime factors (see [DH97, Theorem 11.1]).

A solution to the problem of finding many primes in shifts of admissible k-tuples proved more elusive. One can weaken the problem further as follows: The prime number theorem implies that

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} \leq 1.$$

Any improvement on this upper bound would imply that, infinitely often, gaps between consecutive primes are smaller than predicted by the prime number theorem. Thus, the following theorem due to Erdős [Erd40] can be considered the first result in the study of small gaps between primes.

Theorem 1.1.6. *We have*

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} < 1.$$

Over the years, several authors brought this upper bound progressively lower. Results of Maier [Mai88] reduced the lim inf to $\leq 0.24...$, and this was the best known until 2009, when Goldston, Pintz and Yıldırım [GPY09] brought the lim inf as low as possible.

Theorem 1.1.7. *We have*

$$\liminf_{n\to\infty} \frac{p_{n+1} - p_n}{\log p_n} = 0.$$

What's more: Goldston, Pintz and Yıldırım's method *just* fails to establish bounded gaps between primes, in the sense that any improvement on the exponent on x in the range of summation over moduli q in the Bombieri-Vinogradov theorem (cf. Theorem 1.3.3) would give bounded gaps. Refer to the excellent survey of Soundararajan [Sou07] for a deeper look at this important work.

In 2013, Yitang Zhang stunned the mathematical world by demonstrating that, for every sufficiently long tuple $\mathcal{H}$, there are infinitely many natural numbers n for which $n + \mathcal{H}$ contains at least two primes, thereby establishing the existence of infinitely many bounded gaps between consecutive primes [Zha14]. Zhang's breakthrough was soon followed by work of Maynard [May15] and Tao, who independently established that infinitely many shifts of admissible k-tuples contain m primes, for any $m \geq 2$, provided k is large enough with respect to m. As a consequence, we have not only bounded gaps between primes, but also that $\liminf_{n\to\infty} p_{n+m} - p_n < \infty$ (here p_n denotes the nth prime number).

Let us briefly describe the Maynard-Tao method, which is a refinement of the method of Goldston, Pintz and Yıldırım. Fix an integer $k \geq 2$, and let $\mathcal{H} = \{h_1, \ldots, h_k\}$ be an admissible k-tuple. With $\mathcal{P}$ denoting the set of primes, let

$$W = \prod_{\substack{p \in \mathbb{P} \\ p < \log\log\log(N)}} p,$$

where N is a large positive integer. Define sums S_1 and S_2 as follows:

$$S_1 = \sum_{\substack{n \in [N, 2N] \\ n \equiv \beta \pmod{W}}} \overline{\omega}(n)$$

and

$$S_2 = \sum_{\substack{n \in [N, 2N] \\ n \equiv \beta \pmod{W}}} \left(\sum_{i=1}^{k} \chi_{\mathcal{P}}(n + h_i) \right) \overline{\omega}(n),$$

where β is chosen so that $(\beta + h_i, W) = 1$ for all $1 \leq i \leq k$ (such a β exists by the admissibility of $\mathcal{H}$), and

$$\overline{\omega}(n) = \left(\sum_{\substack{d_1, \ldots, d_k \\ d_i | (n + h_i) \forall i}} \lambda_{d_1 \ldots, d_k} \right)^2$$

for suitably chosen weights $\lambda_{d_1 \ldots, d_k}$. Suppose $S_2 > (m-1)S_1$, for some integer $m \geq 2$ and some choice of weights; then there exists $n_0 \in [N, 2N]$ such that at least m of the $n_0 + h_1, \ldots, n_0 + h_k$ are prime. Taking $N \to \infty$, we obtain a sequence of such n_0, thereby obtaining infinitely many gaps between primes of size at most $\max_{1 \leq i, j \leq k : i \neq j} |h_i - h_j|$.

Thanks to work of several authors [CHL$^+$15], a direct analogue of this theorem exists for primes in $\mathbb{F}_q[t]$. This is discussed further in Chapter 4.

1.2 Arithmetic functions and normal order

In their classic textbook *An Introduction to the Theory of Numbers* [HW00], G.H. Hardy and E.M. Wright define an *arithmetic function* to be a function f on the natural numbers such that, for $n \in \mathbb{N}$, $f(n)$ "expresses some arithmetical property of n." For instance, consider Euler's totient function, $\varphi(n)$, which gives the number of invertible residue classes modulo n. One might hope to gain arithmetic information about the natural numbers by studying the values of an arithmetic function.

It is natural to try to understand the range of an arithmetic function from a statistical point of view. For example: If n is a very large "randomly chosen" natural number, it is difficult to factor as a product of primes, and therefore it is equally difficult to compute $\omega(n)$, say. However, one can ask if there is a "nice" function $g(n)$ such that, typically, $g(n)$ is roughly the size of $\omega(n)$. More precisely:

Definition 1.2.1. Given an arithmetic function $f(n)$, we say that $f(n)$ has *normal order* $g(n)$ if, for any $\epsilon > 0$,

$$\lim_{x\to\infty} \frac{1}{x} \# \left\{ n \leq x : \left| \frac{f(n)}{g(n)} - 1 \right| < \epsilon \right\} = 1,$$

where $g(n)$ is nonnegative and nondecreasing.

Of particular importance to us are the functions traditionally denoted $\omega(n)$ and $\Omega(n)$, which give the number of prime divisors of n (resp. with multiplicity). In other words,

$$\omega(n) = \sum_{p|n} 1 \quad \text{and} \quad \Omega(n) = \sum_{p^k \| n} k.$$

Among the earliest normal order results is a famous theorem of Hardy and Ramanujan [HR17] concerning $\omega(n)$ and of $\Omega(n)$. We state it below and give a proof due to Turán [Tur34], but first, we dispense with some preliminary facts.

Definition 1.2.2. A subset $A \subset \mathbb{N}$ has *asymptotic density* δ if

$$\lim_{x\to\infty} \frac{\#A \cap [1,x]}{x} = \delta.$$

For example, the set of multiples of three has asymptotic density $1/3$.

In the proof of the Hardy-Ramanujan theorem, we will need to estimate sums of reciprocals of primes. The first part of the following theorem of Mertens [Mer74] allows us to do just that. We will make use of the second part in the sequel.

Theorem 1.2.3. *1. As $x \to \infty$,*

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

where B is an absolute constant.

2. As $x \to \infty$,

$$\prod_{p\le x} \Big(1 - \frac{1}{p}\Big) = \frac{e^{-\gamma} + o(1)}{\log x}.$$

We are now in a position to state and prove the Hardy-Ramanujan theorem.

Theorem 1.2.4. *For any $\epsilon > 0$,*

$$|\omega(n) - \log\log n| < (\log\log n)^{\frac{1}{2}+\epsilon}$$

for all n not belonging to a certain set of asymptotic density zero. In particular, the normal order of $\omega(n)$ is $\log\log n$. The same statement is true with $\omega(n)$ replaced by $\Omega(n)$.

Proof. Let $\epsilon > 0$. First note that, when $x^{1/e} \le n \le x$, we have

$$\log\log x - 1 \le \log\log n \le \log\log x.$$

Thus, since the number of $n \le x^{1/e}$ is $O(x^{1/e}) = o(x)$, it suffices to show that the number of $n \le x$ satisfying

$$|\omega(n) - \log\log x| \ge (\log\log x)^{\frac{1}{2}+\epsilon} \tag{1.4}$$

is $o(x)$ (that is, has asymptotic density 0), as $x \to \infty$.

The theorem follows from the claim that

$$\sum_{n\le x} \Big(\omega(n) - \log\log x\Big)^2 = O(x \log\log x). \tag{1.5}$$

Indeed, suppose contrary to the theorem that the number of $n \le x$ satisfying (1.4) is greater than ηx, for some $\eta > 0$. We then obtain

$$\sum_{n\le x} \Big(\omega(n) - \log\log x\Big)^2 \le \eta x (\log\log x)^{1+2\epsilon}$$

for x sufficiently large depending on ϵ and η, contradicting (1.5).

Notice that

$$\sum_{n\le x} \Big(\omega(n) - \log\log x\Big)^2 = \sum_{n\le x} \omega(n)^2 - 2\log\log x \sum_{n\le x} \omega(n) + \lfloor x \rfloor (\log\log x)^2. \tag{1.6}$$

We will show that

$$\sum_{n\le x} \omega(n) = x\log\log x + O(x) \tag{1.7}$$

and

$$\sum_{n\le x} \omega(n)^2 = x(\log\log x)^2 + O(x\log\log x). \tag{1.8}$$

Inserting these estimates into (1.6), we obtain

$$\sum_{n\leq x}\Big(\omega(n)-\log\log x\Big)^2 = x(\log\log x)^2 - 2\log\log x(x\log\log x + O(x)) \\ + (x+O(1))(\log\log x)^2.$$

Gathering terms, we have

$$\sum_{n\leq x}\Big(\omega(n)-\log\log x\Big)^2 = x(\log\log x)^2 - 2x(\log\log x)^2 + x(\log\log x)^2 + O(x\log\log x) \\ = O(x\log\log x),$$

proving that 1.5 holds. We turn our attention to establishing (1.7) and (1.8).

Observe that

$$\sum_{n\leq x}\omega(n) = \sum_{n\leq x}\sum_{p|n}1 = \sum_{p\leq x}\sum_{\substack{n\leq x\\ p|n}}1 = \sum_{p\leq x}\Big\lfloor\frac{x}{p}\Big\rfloor.$$

Now, $\lfloor x/p\rfloor = x/p + O(1)$. Hence

$$\sum_{p\leq x}\Big\lfloor\frac{x}{p}\Big\rfloor = x\sum_{p\leq x}\frac{1}{p} + O(\pi(x)).$$

By Theorem 1.2.3, $\sum_{p\leq x}1/p = \log\log x + O(1)$. Putting everything together, we have shown that

$$\sum_{n\leq x}\omega(n) = x\log\log x + O(x),$$

as desired.

Turning our attention now to (1.8), we first note that there are $\omega(n)(\omega(n)-1)$ ordered pairs of distinct primes p, q dividing n. In other words,

$$\omega(n)(\omega(n)-1) = \sum_{\substack{pq|n \\ p\neq q}} 1 = \sum_{pq|n} 1 - \sum_{p^2|n} 1.$$

Summing on n, we have

$$\sum_{n\leq x} \omega(n)^2 - \sum_{n\leq x} \omega(n) = \sum_{n\leq x} \Big(\sum_{pq|n} 1 - \sum_{p^2|n} 1 \Big) = \sum_{pq\leq x} \Big\lfloor \frac{x}{pq} \Big\rfloor - \sum_{p^2\leq x} \Big\lfloor \frac{x}{p^2} \Big\rfloor.$$

Now,

$$\sum_{p^2\leq x} \Big\lfloor \frac{x}{p^2} \Big\rfloor \leq x \sum_{p} \frac{1}{p^2} = O(x).$$

Thus, by (1.7),

$$\sum_{n\leq x} \omega(n)^2 = \sum_{pq\leq x} \Big\lfloor \frac{x}{pq} \Big\rfloor + O(x \log\log x).$$

Removing the floor function in the sum above introduces an error of size $O(x)$, which can be absorbed into the existing $O(x \log\log x)$ term. Notice that

$$\Big(\sum_{p\leq \sqrt{x}} \frac{1}{p} \Big)^2 \leq \sum_{pq\leq x} \frac{1}{pq} \leq \Big(\sum_{p\leq x} \frac{1}{p} \Big)^2.$$

Again by Theorem 1.2.3, we see that the outer expressions are both $(\log\log x + O(1))^2 = (\log\log x)^2 + O(\log\log x)$, and thus,

$$\sum_{n\leq x} \omega(n)^2 = x(\log\log x)^2 + O(x \log\log x),$$

as desired. This completes the proof of Theorem 1.2.4. □

Thinking probabilistically, one might want to say, in light of the Hardy-Ramanujan theorem, that $\omega(n)$ has mean value and variance $\log\log n$. Indeed, consider the quantity

$$\frac{\omega(n) - \log\log n}{\sqrt{\log\log n}}.$$

In a 1940 paper, Erdős and Kac [EK40] studied this quantity and established a foundational theorem of probabilistic number theory.

Theorem 1.2.5. *The quantity*

$$\frac{\omega(n) - \log\log n}{\sqrt{\log\log n}}$$

has normal probability distribution; that is,

$$\lim_{x\to\infty} \frac{1}{x}\#\{n \leq x : a \leq \frac{\omega(n) - \log\log n}{\sqrt{\log\log n}} \leq b\} = \frac{1}{\sqrt{2\pi}} \int_a^b e^{-t^2/2}\, dt.$$

A 2007 paper of Granville and Soundararajan [GS07] features a proof of the above result via the method of moments. In particular, one deduces from their proof that $\omega(n)$ has mean and variance $\log\log n$. In light of these results, one may ask how often $\omega(n)$ takes on extreme values, e.g. values greater than $\gamma \log\log n$, for some fixed $\gamma > 1$. A more precise version of the following result appears in [EN79]; its proof is due to Delange.

Theorem 1.2.6. *Fix $\gamma > 1$. As $x \to \infty$,*

$$\#\{n \leq x : \omega(n) > \gamma \log\log x\} = \frac{x}{(\log x)^{1+\gamma\log\gamma-\gamma+o(1)}}.$$

The same statement is true for the quantity $\#\{n \leq x : \omega(n) < \gamma \log\log x\}$ when $0 < \gamma < 1$.

One naturally wants to establish analogues of the above results for other arithmetic functions. In Chapter 2, we prove an analogue of the Hardy-Ramanujan theorem for the

function $\omega(s(n))$, where $s(n)$ denotes the sum-of-proper-divisors function:

$$s(n) = \sum_{\substack{d|n \\ d \neq n}} d.$$

In Chapter 3, we study the quantity $\omega(\#E(\mathbb{F}_p))$, where $E/\mathbb{Q}$ is an elliptic curve with complex multiplication and p is a prime number. Work of Cojocaru [Coj05] and Liu [Liu06] shows that analogues of the Hardy-Ramanujan theorem and the Erdős-Kac theorem hold for $\omega(\#E(\mathbb{F}_p))$. Using Brun's sieve in the Gaussian integers, we investigate how often $\omega(\#E(\mathbb{F}_p))$ takes on extreme values as p varies, establishing a result analogous to Theorem 1.2.6.

1.3 Primes in arithmetic progressions

In the proof of the main result of Chapter 2, we will need asymptotic estimates for the count of primes in fairly short arithmetic progressions. We briefly review some landmark results in the study of primes in arithmetic progressions.

A simple modification of Euclid's proof of the infinitude of the primes yields that there are infinitely many primes congruent to 1 modulo 4. One naturally wonders if there are infinitely many primes congruent to a modulo q, where a and q are arbitrary integers. Clearly, a and q must be coprime; at most one member of the arithmetic progression $a + kq$, $k \geq 1$, can be prime if $\gcd(a, q) > 1$. Dirichlet's theorem [Dir37] is the statement that coprimality is the only restriction one needs on a and q: For any pair of integers a and q with $(a, q) = 1$, there are infinitely many primes p with $p \equiv a \pmod{q}$.

More is true. A modification of the proof of the prime number theorem, due to de la Vallée-Poussin [dlVP96], yields the fact that the primes are evenly distributed among coprime residue classes modulo q, where $q \geq 1$ is a fixed integer. In other words, letting $\pi(X; q, a)$

denote the number of primes $p \leq X$ with $p \equiv a \pmod{q}$, we have

$$\pi(X; q, a) \sim \frac{\pi(X)}{\varphi(q)},$$

as $X \to \infty$.

The Siegel-Walfisz theorem, proved by Walfisz [Wal36] who built on work of Siegel [Sie35], gives a good estimate for the number of primes in an arithmetic progression, provided the modulus q is not too large in comparison to x.

Theorem 1.3.1. *For any positive number N, there is a constant c_N such that*

$$\pi(X; q, a) = \frac{\pi(X)}{\varphi(q)} + O\big(X \exp\{-c_N \sqrt{\log X}\}\big)$$

for all $(a, q) = 1$ where $q \leq (\log X)^N$.

The Siegel-Walfisz theorem says that, uniformly for q up to a certain size, primes are evenly distributed among coprime residue classes modulo q. A natural question might be: What is the least prime in such a residue class? Let $p(q, a)$ denote the smallest prime congruent to a modulo q. It is conjectured that

$$p(q, a) \ll q^{1+\epsilon},$$

for any $\epsilon > 0$. A celebrated result of Linnik [Lin44] establishes an upper bound for $p(q, a)$ which is polynomial in q.

Theorem 1.3.2. *There exist absolute constants $c \geq 1$ and $L \geq 2$ such that*

$$p(q, a) \leq c q^L.$$

The constants c and L appearing in Linnik's theorem are effective; the best-known value of $L = 5$ is due to Xylouris [Xyl11].

What about the distribution of primes modulo larger values of q? The Generalized Riemann Hypothesis implies that

$$\pi(X; q, a) = \frac{\pi(X)}{\varphi(q)} + O(X^{1/2}(\log X)),$$

for all q, a with $\gcd(q, a) = 1$. Thus, the following important result of Bombieri and Vinogradov [Bom65, Theorem 4] says that the Generalized Riemann Hypothesis is true, on average over moduli $q \leq x^{1/2-\epsilon}$ for any $\epsilon > 0$.

Theorem 1.3.3. *We have*

$$\sum_{q \leq x^{1/2}(\log x)^{-B}} \max_{(a,q)=1} \left| \pi(x; q, a) - \frac{\pi(x)}{\varphi(q)} \right| \ll \frac{x}{(\log x)^A}$$

for any $A > 0$, where B is a constant depending on A.

More is thought to be true; the Elliott-Halberstam conjecture posits that, for any $\epsilon > 0$, the above sum over moduli q can be extended to $q \leq x^{1-\epsilon}$ with no change in the result.

If all one needs is an upper bound, the Brun-Titchmarsh theorem gives one of the conjectured order of magnitude for all moduli $q \leq x^{1-\eta}$, where $\eta > 0$.

Theorem 1.3.4. *For $(a, q) = 1$ and $1 \leq q < x$ we have*

$$\pi(x; q, a) < \frac{2x}{\varphi(q) \log(x/q)}.$$

We conclude this section with the statement and proof of a result we will use in Chapter 2. In the proof of Theorem 2.3.1, we will need asymptotic estimates for the count of primes in fairly short progressions. For our purposes, we must consider moduli q exceeding any fixed power of $\log x$. The following theorem is sufficient, though we must exclude moduli which are multiples of a certain integer.

Theorem 1.3.5. *Let X and T satisfy $X \geq T \geq 2$, and suppose $q \leq T^{2/3}$. Then*

$$\pi(X; q, a) \sim \pi(X)/\varphi(q) \quad \text{as} \quad \frac{\log X}{\log T} \to \infty$$

uniformly for all coprime pairs (a, q), except possibly for those q which are multiples of some integer $q_1(T)$. Here φ is the usual Euler phi function.

Proof. Referring to the proof of Linnik's theorem in [Bom74, p. 55], we have

$$\sum_{\substack{p \leq X \\ p \equiv a \pmod{q}}} \log p = \frac{X}{\varphi(q)} + O\left(\frac{X}{\varphi(q)} \exp(-c_1 A)\right) + O\left(\frac{X \log X}{T}\right) + O\left(\frac{1}{\varphi(q)} X^{1/2} T^5\right),$$

unless q is divisible by a certain exceptional modulus $q_1 = q_1(T)$, and where A is such that $T = X^{1/A}$. Notice that the quantity A tends to infinity. Therefore, the first and last O-terms are $o(X/\varphi(q))$, as is the middle O-term, provided $T > (\log X)^6$; but if $T \leq (\log X)^6$, Theorem 2.2.4 follows from the Siegel-Walfisz theorem. One now obtains the desired asymptotic for $\pi(X; q, a)$ by standard arguments. □

We refer the reader to [IK04] for a thorough treatment of the theorems mentioned in this section.

1.4 Statement of main results

The aim of this thesis is to prove the following three results, developing sufficiently the necessary background and historical context along the way. All three results are unified by the sieve: Fundamentally, they are all sieve problems, and the proofs of the last two results especially are obtained via sieve methods.

The first result concerns the normal order of a composition of arithmetic functions.

Theorem 1.4.1. *For any $\epsilon > 0$ and all numbers $n \leq x$ not belonging to a set of size $o(x)$,*

$$|\omega(s(n)) - \log\log s(n)| < \epsilon \log\log s(n).$$

Here, $s(n)$ is the sum of the proper divisors of n, and $\omega(n)$ denotes the number of distinct prime factors of n.

We then turn our attention to rational points on reductions modulo p of elliptic curves with complex multiplication. This result should be compared with the Erdős-Kac theorem and results of Delange, Erdős and Nicolas concerning extreme values of $\omega(n)$, cf. Section 1.2.

Theorem 1.4.2. *Let $E/\mathbb{Q}$ be an elliptic curve with CM, and let $\#E(\mathbb{F}_p)$ denote the number of $\mathbb{F}_p$-rational points on E reduced modulo p. For $\gamma > 1$ fixed,*

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log\log x\} = \frac{x}{(\log x)^{2+\gamma\log\gamma-\gamma+o(1)}}.$$

The same statement is true for the quantity $\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) < \gamma \log\log x\}$ when $0 < \gamma < 1$. Again, $\omega(n)$ denotes the number of distinct prime factors of n.

Finally, we establish a "bounded gaps between primes" result in the setting of $\mathbb{F}_q[t]$, the ring of polynomials with coefficients in $\mathbb{F}_q$. Our result concerns prime polynomials with a given primitive root, and so we outline some important work concerning Artin's primitive root conjecture.

Theorem 1.4.3. *Let g be a monic polynomial in $\mathbb{F}_q[t]$ such that g is not a vth power for any prime v dividing $q-1$, and let $\mathbb{P}_g$ denote the set of prime polynomials in $\mathbb{F}_q[t]$ for which g is a primitive root. For any $m \geq 2$, there exists an admissible k-tuple $\{h_1, \ldots, h_k\}$ such that there are infinitely many $f \in \mathbb{F}_q[t]$ with at least m of $f + h_1, \ldots, f + h_k$ belonging to $\mathbb{P}_g$.*

Chapter 2

The number of prime factors of $s(n)$

2.1 Introduction

Let $s(n)$ denote the sum of the proper divisors of a positive integer n. The function $s(n)$ has been of interest to number theorists since antiquity; for example, the ancient Greeks wanted to know when $s(n) = n$, calling such integers *perfect*. In modern times, open problems concerning $s(n)$ abound, such as the famous Catalan-Dickson conjecture [Dic13]: For any positive integer n, the aliquot sequence at n (that is, the sequence of iterates of the function s on n) either terminates at 0 or is eventually periodic.

Another conjecture pertaining to $s(n)$ is the following, due to Erdös, Granville, Pomerance and Spiro [EGPS90]:

Conjecture 2.1.1. *If $\mathcal{A}$ is a set of natural numbers of asymptotic density zero, then $s^{-1}(\mathcal{A})$ also has density zero.*

Notice that Conjecture 2.1.1, together with the Hardy-Ramanujan theorem (Theorem 1.2.4), would imply the following:

Theorem 2.1.2. *For any $\epsilon > 0$ and all numbers $n \le x$ not belonging to a set of size $o(x)$,*

$$|\omega(s(n)) - \log\log s(n)| < \epsilon \log\log s(n).$$

Though Conjecture 2.1.1 remains intractable, we are able to prove Theorem 2.1.2 unconditionally in the present chapter.

If a number n is composite, then n has a proper divisor greater than $n^{1/2}$; so for all composite $n \in (x^{1/2}, x]$, we have $x^{1/4} \le n^{1/2} \le s(n) \le x^2$. Hence, for all but $o(x)$ numbers n up to x, $\log\log s(n) = \log\log x + O(1)$. Therefore, it suffices to show that, given $\epsilon > 0$,

$$|\omega(s(n)) - \log\log x| < \epsilon \log\log x \tag{2.1}$$

for all n except those belonging to a set of size $o(x)$.

Our normal order result follows from the following estimate; one should compare this result with (1.5).

Theorem 2.1.3. *As $x \to \infty$,*

$$\sum_{n \le x \,:\, n \notin \mathcal{E}(x)} (\omega(s(n)) - \log\log x)^2 = o(x(\log\log x)^2).$$

where $\mathcal{E}(x) \subset \{1, 2, \dots, \lfloor x \rfloor\}$ is of size $o(x)$.

For large enough x, if there are more than δx numbers up to x for which (2.1) fails, where $\delta > 0$ is any positive number, then at least $\frac{\delta}{2}x$ of them (say) do not belong to $\mathcal{E}(x)$, whence

$$\sum_{n \le x \,:\, n \notin \mathcal{E}(x)} (\omega(s(n)) - \log\log x)^2 \ge \tfrac{\delta}{2}\epsilon^2 x(\log\log x)^2;$$

this contradicts Theorem 2.1.3 for sufficiently large x, and Theorem 2.1.2 follows.

Remark. Just as in the Hardy-Ramanujan theorem, we obtain a true statement by replacing $\omega(s(n))$ with $\Omega(s(n))$ in the theorem above; this is shown in §2.5.

2.2 Preliminaries

First we show that it suffices to consider a truncated version of the sum in question.

Lemma 2.2.1.

$$\sum_{n\le x}\omega(s(n)) = \Big(\sum_{\log_2 x<p\le x^{1/\sqrt{\log_2 x}}}\sum_{\substack{n\le x\\ p|s(n)}} 1\Big) + o(x\log_2 x).$$

Proof. We have

$$\sum_{n\le x}\omega(s(n)) = \sum_{n\le x}\sum_{p:p|s(n)} 1.$$

If $n\le x$ then $s(n)\le x^2$. The number of primes $p\notin(\log_2 x, x^{1/\sqrt{\log_2 x}}]$ dividing a number $m\le x^2$ is $\le 2\sqrt{\log_2 x}+\pi(\log_2 x) = o(\log_2 x)$, and the lemma follows. □

2.2.1 The exceptional set.

Let $P(n)$ and $P_2(n)$ denote the largest and second-largest prime factors of n, respectively; if $n=1$, we set $P(n)=P_2(n)=1$, and if n is prime, we set $P_2(n)=1$. Define $\mathcal{E}(x) := \{n\le x :$ one of A, B, C, D, E, F fails$\}$, where

A. $P(n) > x^{1/\log_3 x}$,

B. $P(n)^2 \nmid n$,

C. $P_2(n) > x^{1/\log_3 x}$,

D. $P_2(n) < xP(n)/2n$,

E. $P_2(n)^2 \nmid n$

F. if a prime q divides $\gcd(n/P(n), \sigma(n/P(n)))$, then $q < \log_2 x$.

Lemma 2.2.2. $\#\mathcal{E}(x) = o(x)$.

Let $\Psi(x, y)$ denote the count of y-smooth numbers up to x; that is, the count of numbers $n \leq x$ such that $p \mid n \implies p \leq y$. The following upper bound estimate of de Bruijn [dB66, Theorem 2] will be useful in proving the above lemma. For a survey of known results and open problems concerning smooth numbers, see, e.g., [Gra08].

Proposition 2.2.3. *Let $x \geq y \geq 2$ satisfy $(\log x)^2 \leq y \leq x$. Whenever $u := \frac{\log x}{\log y} \to \infty$, we have*

$$\Psi(x, y) \leq x/u^{u+o(u)}.$$

Proof of Lemma. Let $\mathcal{E}_j(x) = \{n \leq x : \text{condition } j \text{ fails and all prior conditions hold}\}$, $j \in \{A, B, C, D, E, F\}$. If $n \in \mathcal{E}_A(x) \cup \mathcal{E}_B(x)$, then either $P(n) \leq x^{1/\log_3 x}$ or $P(n) > x^{1/\log_3 x}$ and $P(n)^2 \mid n$. By Proposition 2.2.3, the number of $n \leq x$ for which the former holds is $O(x/(\log_2 x)^4)$, noting that $(\log_2 x)^4 \ll (\log_2 x)^{\log_4 x} = (\log_3 x)^{\log_3 x}$. The number of $n \leq x$ for which the latter holds is $\ll x \sum_{p > x^{1/\log_3 x}} p^{-2} \ll x \exp(-\log x/\log_3 x)$, and this is also $O(x/(\log_2 x)^4)$.

If $n \in \mathcal{E}_C(x)$, we proceed as in [Pol14b, Lemma 2.6]. In this case, either (i) $P(n) \leq x^{1/\log_4 x}$ or (ii) $P(n) > x^{1/\log_4 x}$ and $P_2(n) \leq x^{1/\log_3 x}$. The number of $n \leq x$ for which (i) holds is $O(x/(\log_3 x)^{10})$ by Proposition 2.2.3. For $n \leq x$ such that (ii) holds, write $n = mP$, where $P = P(n) > x^{1/\log_4 x}$ and $P(m) \leq x^{1/\log_3 x}$. Then $x/m \geq P > x^{1/\log_4 x}$, and the number of such P given m is, by the prime number theorem,

$$\ll \frac{x/m}{\log(x/m)} \leq \frac{x \log_4 x}{m \log x}.$$

Now we sum this over m such that $P(m) \le x^{1/\log_3 x}$, obtaining that the number of $n \le x$ for which (ii) holds is

$$\ll \frac{x \log_4 x}{\log x} \sum_{m\,:\,P(m) \le x^{1/\log_3 x}} \frac{1}{m} = \frac{x \log_4 x}{\log x} \prod_{p \le x^{1/\log_3 x}} \left(1 - \frac{1}{p}\right)^{-1}$$
$$\ll \frac{x \log_4 x}{\log x} \left(\frac{\log_3 x}{\log x}\right)^{-1} = \frac{x \log_4 x}{\log_3 x}.$$

Thus $\#\mathcal{E}_C(x) = O(x \log_4 x / \log_3 x)$.

For $\#\mathcal{E}_D(x)$, note first that $xP(n)/2n > P(n)/2$. Thus any n in $\mathcal{E}_D(x)$ has a prime factor in $(P(n)/2, P(n))$, and the number of such integers n with $P(n) > x^{1/\log_3(x)}$ is, by the prime number theorem,

$$\le x \sum_{q > x^{1/\log_3 x}} \sum_{q/2 < q' < q} \frac{1}{qq'} \ll x \sum_{q > x^{1/\log_3 x}} \frac{1}{q \log q} = O\left(\frac{x \log_3 x}{\log x}\right).$$

To bound $\#\mathcal{E}_E(x)$, we consider $n \le x$ with $P_2(n)^2 \mid n$ and $P_2(n) > x^{1/\log_3 x}$. The number of such n is $\ll x \sum_{p > x^{1/\log_3 x}} p^{-2} \ll x \exp(-\log x / \log_3 x)$.

Finally, suppose $q \mid \big(n/P(n), \sigma(n/P(n))\big)$ and $q \ge \log_2 x$. Then $q \mid n$ and $q \mid \sigma(n)$. Write $n = q^e s$, with $q \nmid s$. If $e \ge 2$, then n has a squarefull divisor $\ge (\log_2 x)^2$, and the number of such n is $O(x/\log_2 x)$.

So assume $e = 1$. Since $q \mid \sigma(n)$, we have $q \mid \sigma(s)$. Write $s = p_1^{e_1} \cdots p_k^{e_k}$; then $q \mid \sigma(p_i^{e_i})$ for some i. If $e_i \ge 2$, then we have $2p_i^{e_i} > \sigma(p_i^{e_i}) \ge q$, so s has a squarefull divisor $\ge q/2$. The number of such $s \le x/q$ is $O(x/q^{3/2})$, and summing this over $q \ge \log_2 x$ gives that the number of possible n is $O(x/\sqrt{\log_2 x})$.

If $e_i = 1$, then $p_i \equiv -1 \pmod{q}$. By Brun-Titchmarsh and partial summation, the number of $s \leq x/q$ divisible by such a prime p_i is

$$\frac{x}{q} \sum_{\substack{p \leq x/q \\ p \equiv -1 \,(\mathrm{mod}\ q)}} \frac{1}{p} \ll \frac{x \log_2 x}{q^2},$$

and summing this over $q \geq \log_2 x$ we obtain that the number of possible n in this case is $O(x/\log_3 x)$.

This finishes the proof, noting that all size bounds established are $o(x)$. □

As mentioned in Section 1.3, we need a result on primes in arithmetic progressions with large moduli. We restate the result here for convenience.

Theorem 2.2.4. *Let X and T satisfy $X \geq T \geq 2$, and suppose $q \leq T^{2/3}$. Then*

$$\pi(X; q, a) \sim \pi(X)/\varphi(q) \quad \text{as} \quad \frac{\log X}{\log T} \to \infty$$

uniformly for all coprime pairs (a, q), except possibly for those q which are multiples of some integer $q_1(T)$. Here φ is the usual Euler phi function.

We will also make use of the following fact [Pol14b, Lemma 2.7]:

Proposition 2.2.5. *Let q be a natural number with $q \leq x^{\frac{1}{2\log_3 x}}$. The number of $n \leq x$ not belonging to $\mathcal{E}_A(x) \cup \mathcal{E}_B(x)$ for which q divides $s(n)$ is*

$$\ll \frac{\tau(q)}{\varphi(q)} \cdot x \log_3 x,$$

where $\tau(q)$ denotes the number of divisors of q.

Proof. Since $n \notin \mathcal{E}_A(x) \cup \mathcal{E}_B(x)$, we can write $n = Pm$, with $P := P(n) > x^{1/\log_3 x}$ and $P \nmid m$. From this factorization of n, we may obtain a factorization of $q = q_1 q_2$, where

$q_1 := \gcd(q, s(m))$ and $q_2 := q/q_1$. First, we count the number of $n \le x$ with $q \mid s(n)$ and where n corresponds to a fixed factorization $q = q_1 q_2$, and we finish by summing over all possible factorizations $q_1 q_2$ of q.

Since q divides $s(n) = s(Pm) = Ps(m) + \sigma(m)$ and $q_1 \mid s(m)$, it must be the case that $q_1 \mid \sigma(m)$. Thus $q_1 \mid \sigma(m) - s(m) = m$. Note also that $q_2 = q/\gcd(q, s(m))$ is coprime to $s(m)/\gcd(q, s(m)) = s(m)/q_1$, allowing us to write

$$P\frac{s(m)}{q_1} \equiv -\frac{\sigma(m)}{q_1} \pmod{q_2}.$$

This places P in a uniquely determined residue class modulo q_2. Moreover, $P \le x/m$, implying that $x/m > x^{1/\log_3 x}$. By the Brun-Titchmarsh inequality [HR74, Theorem 3.8], the number of choices for P given m is

$$\ll \frac{x/m}{\varphi(q_2)\log\frac{x}{mq_2}} \ll \frac{x\log_3 x}{m\varphi(q_2)\log x},$$

using here that $\frac{x}{mq_2} \ge x^{1/\log_3 x} q^{-1} \ge x^{1/2\log_3 x}$. Summing this expression on $m \le x^{1-\frac{1}{\log_3 x}}$ with $q_1 \mid m$ shows that the number of possible $n = mP$ is

$$\ll \frac{x\log_3 x}{q_1\varphi(q_2)}.$$

Now,

$$\sum_{q_1 q_2 = q} \frac{1}{q_1\varphi(q_2)} = \frac{1}{q}\sum_{q_2 \mid q} \frac{q_2}{\varphi(q_2)} \le \frac{1}{q}\Big(\tau(q)\frac{q}{\varphi(q)}\Big) = \frac{\tau(q)}{\varphi(q)}.$$

Here we use the fact that $q_2/\varphi(q_2) \le q/\varphi(q)$ for every q_2 dividing q. Putting the above estimates together, we obtain that the number of $n \le x$, $n \notin \mathcal{E}_A(x) \cup \mathcal{E}_B(x)$ with $q \mid s(n)$ $(q \le x^{\frac{1}{2\log_3 x}})$ is $\ll (\tau(q)/\varphi(q)) \cdot x\log_3 x$, as desired. □

2.3 An average result for $\omega(s(n))$

First we prove an average order result for $\omega(s(n))$:

Theorem 2.3.1. *As $x \to \infty$,*

$$\sum_{n \le x \,:\, n \notin \mathcal{E}(x)} \omega(s(n)) \sim x \log\log x.$$

This result will serve as a stepping stone towards Theorem 2.1.3.

By Lemma 2.2.1,

$$\sum_{n \le x \,:\, n \notin \mathcal{E}(x)} \omega(s(n)) = \Big(\sum_{\substack{\log_2 x < p \le x^{1/\sqrt{\log_2 x}} \\ p \ne q_1(T)}} \sum_{\substack{n \le x \,:\, n \notin \mathcal{E}(x) \\ p \mid s(n)}} 1 \Big) + o(x \log_2 x),$$

where $q_1(T)$ is the exceptional modulus coming from Theorem 2.2.4. Eventually we will be counting primes in certain progressions modulo $p \le x^{1/\sqrt{\log_2 x}}$, and so it will suffice to take $T = x^{1.5/\sqrt{\log_2 x}}$. To apply Theorem 2.2.4, we need that p is not a multiple of $q_1(T)$; but since p is prime, this is the same as requiring $p \ne q_1(T)$, and this excludes at most one summand above. Fix a prime $p \in (\log_2 x, x^{1/\sqrt{\log_2 x}}]$, $p \ne q_1(T)$ and consider the inner sum above.

Since $n \notin \mathcal{E}(x)$, we can write $n = mP$, $P := P(n)$, where $P \nmid m$, $P > x^{1/\log_3 x}$, $x^{1/\log_3 x} < P(m) < x/2m$ (this follows from condition D, noting that $m = n/P$), and $p \mid (m, \sigma(m)) \implies p < \log_2 x$. Now

$$\sum_{\substack{n \le x \,:\, n \notin \mathcal{E}(x) \\ p \mid s(n)}} 1 = \sum_{\substack{n \le x \,:\, n \notin \mathcal{E}(x) \\ p \mid s(n) \\ p \mid s(m)}} 1 + \sum_{\substack{n \le x \,:\, n \notin \mathcal{E}(x) \\ p \mid s(n) \\ p \nmid s(m)}} 1.$$

But this first sum is actually empty! If $p \mid s(n) = s(mP) = Ps(m) + \sigma(m)$, and $p \mid s(m)$, then $p \mid \sigma(m)$ and hence $p \mid m$ (since $m = \sigma(m) - s(m)$). Since $n \notin \mathcal{E}(x)$, this forces $p < \log_2 x$, contradicting our choice of the fixed prime p.

If $p \nmid s(m)$, then since $p \mid s(n) = Ps(m) + \sigma(m)$, we have

$$P \equiv -\sigma(m)s(m)^{-1} \pmod{p}.$$

For convenience, we now define the following notation: Write

$$\sum_m{}' := \sum_{\substack{x^{1/\log_3 x} < m \le x^{1-1/\log_3 x} \\ p \nmid s(m) \\ x^{1/\log_3 x} < P(m) < x/2m \\ P(m)^2 \nmid m \\ q \mid (m, \sigma(m)) \Longrightarrow q < \log_2 x}}.$$

Now

$$\sum_{\substack{n \le x \,:\, n \notin \mathcal{E}(x) \\ p \mid s(n) \\ p \nmid s(m)}} 1 = \sum_m{}' \sum_{\substack{P(m) < P \le x/m \\ P \equiv -\sigma(m)s(m)^{-1} \pmod{p}}} 1.$$

The inner sum is equal to

$$\pi(x/m; p, -\sigma(m)s(m)^{-1}) - \pi(P(m); p, -\sigma(m)s(m)^{-1}).$$

We now use Theorem 2.2.4 to rewrite the terms above, with $T = x^{1.5/\sqrt{\log_2 x}}$. Note that $P(m), x/m > x^{1/\log_3 x}$, so $P(m)$ and x/m are both greater than any fixed power of T for large enough x. Since $p \neq q_1(T)$, we have

$$\begin{aligned}\sum_m{}' \Big(&\pi(x/m; p, -\sigma(m)s(m)^{-1}) - \pi(P(m); p, -\sigma(m)s(m)^{-1}) \Big) \\ &= \frac{1}{p-1} \sum_m{}' \Big(\pi(x/m) - \pi(P(m)) \Big) + o\Big(\frac{1}{p-1} \sum_m{}' \big(\pi(x/m) + \pi(P(m)) \big) \Big).\end{aligned}$$

To deal with the o-term, observe that from our conditions on m,

$$\begin{aligned}\pi(x/m) + \pi(P(m)) &\le \pi(x/m) + \pi(x/2m) \\ &\le 2\pi(x/m) \le 10\big(\pi(x/m) - \pi(P(m))\big)\end{aligned}$$

for large enough x, and so the above sum on m is

$$\sim \frac{1}{p-1}\sum_m{}' \Big(\pi(x/m) - \pi(P(m))\Big).$$

A prime P counted by the term $\pi(x/m) - \pi(P(m))$ corresponds to an integer $n = Pm$, with $P^2 \nmid n$ and $p \nmid s(m)$; the conditions imposed on m guarantee that $n \le x$ and $n \notin \mathcal{E}(x)$. It is clear that every $n \le x$ with $n \notin \mathcal{E}(x)$ and $p \nmid s(m)$ will be counted by such a summand. Thus

$$\begin{aligned}\sum_m{}' \pi(x/m) - \pi(P(m)) &= \#\{n \le x : n = mP(n) \notin \mathcal{E}(x), p \nmid s(m)\} \\ &= \#\{n \le x : n \notin \mathcal{E}(x)\} - \#\{n \le x : n = mP(n) \notin \mathcal{E}(x), p \mid s(m)\}.\end{aligned}$$

The following lemma allows us to estimate the subtrahend.

Lemma 2.3.2. *For a fixed prime $\log_2 x < q \le x^{1/\sqrt{\log_2 x}}$, the number of $n \le x$ not belonging to $\mathcal{E}(x)$ (so $n = mP(n)$) such that $q \mid s(m)$ is*

$$\ll \frac{x \log_3 x \log_4 x}{q-1}.$$

Proof. Write $n = mP$, with $P = P(n)$. Since $n \notin \mathcal{E}(x)$, $P(m)^2 \nmid m$ and $P(m) > x^{1/\log_3 x}$. Note that $q \le x^{1/\sqrt{\log_2 x}}$, and $(x/P)^{\frac{1}{2\log_3 x}} > x^{\frac{1}{2(\log_3 x)^2}} > x^{1/\sqrt{\log_2 x}}$ for large enough x. By

Proposition 2.2.5, the number of $m \le x/P$ not in $\mathcal{E}(x)$ for which $q \mid s(m)$ is

$$\ll \frac{1}{q-1} \cdot \frac{x \log_3 x}{P}.$$

Summing over $P \in (x^{1/\log_3 x}, x]$ gives the result. □

By the above lemma, we have

$$\sum_m{}' \Big(\pi(x/m) - \pi(P(m))\Big) = x + O\left(\frac{x \log_3 x \log_4 x}{p-1}\right) + O(\#\mathcal{E}(x)).$$

Putting everything together, we have shown that

$$\sum_{n \le x \,:\, n \notin \mathcal{E}(x)} \omega(s(n)) = \sum_{\substack{\log_2 x < p \le x^{1/\sqrt{\log_2 x}} \\ p \ne q_1(T)}} \left(\frac{x}{p-1} + O\left(\frac{x \log_3 x \log_4 x}{(p-1)^2}\right) + o\left(\frac{x}{p-1}\right)\right).$$

The O-term contributes

$$\ll x \log_3 x \log_4 x \sum_{t > \log_2 x} \frac{1}{t^2} \ll \frac{x \log_3 x \log_4 x}{\log_2 x} = o(x \log_2 x).$$

By Mertens' first theorem,

$$\begin{aligned}\sum_{\substack{\log_2 x < p \le x^{1/\sqrt{\log_2 x}} \\ p \ne q_1(T)}} \frac{1}{p-1} &= \log_2(x^{1/\sqrt{\log_2 x}}) - \log_2(\log_2(x)) + O(1) \\ &= (\log_2 x)(1 + o(1)).\end{aligned}$$

Thus,

$$\sum_{n \le x \,:\, n \notin \mathcal{E}(x)} \omega(s(n)) = x \log_2 x + o(x \log_2 x),$$

as desired.

2.4 Proof of Theorem 2.1.3

Notice that

$$\begin{aligned}\sum_{n\le x:n\notin\mathcal{E}(x)} &(\omega(s(n))-\log_2 x)^2\\ &=\sum_{n\le x:n\notin\mathcal{E}(x)}\omega(s(n))^2-2\log_2 x\sum_{n\le x:n\notin\mathcal{E}(x)}\omega(s(n))+x(\log_2 x)^2(1+o(1))\\ &=\sum_{n\le x:n\notin\mathcal{E}(x)}\omega(s(n))^2-x(\log_2 x)^2(1+o(1))\end{aligned}$$

by Theorem 2.3.1. Hence, the following lemma implies Theorem 2.1.3.

Lemma 2.4.1. *As $x\to\infty$,*

$$\sum_{n\le x\,:\,n\notin\mathcal{E}(x)}\omega(s(n))^2\sim x(\log_2 x)^2.$$

We have

$$\sum_{n\le x\,:\,n\notin\mathcal{E}(x)}\omega(s(n))^2=\sum_{n\le x:n\notin\mathcal{E}(x)}\Big(\sum_{p|s(n)}1\Big)^2=\sum_{n\le x:n\notin\mathcal{E}(x)}\sum_{p,q\,:\,p,q|s(n)}1,$$

where the sum is over pairs of primes p,q. This inner sum is equal to

$$\sum_{\substack{p,q\,:\,p,q|s(n)\\ p\neq q}}1+\sum_{p|s(n)}1,$$

and hence

$$\sum_{n\le x\,:\,n\notin\mathcal{E}(x)}\omega(s(n))^2=\sum_{n\le x:n\notin\mathcal{E}(x)}\sum_{\substack{p,q\,:\,p,q|s(n)\\ p\neq q}}1+o(x(\log_2 x)^2)$$

by Theorem 2.3.1.

We can again truncate the sum in question.

Lemma 2.4.2.

$$\sum_{n\le x:n\notin\mathcal{E}(x)}\omega(s(n))^2=\sum_{n\le x:n\notin\mathcal{E}(x)}\sum_{\substack{\log_2 x<p\le x^{1/\sqrt{\log_2 x}}\\ p\mid s(n)}}\sum_{\substack{\log_2 x<q\le x^{1/\sqrt{\log_2 x}}\\ q\mid s(n)\\ q\neq p}}1+o(x(\log_2 x)^2).$$

Proof. By Lemma 2.2.1, we have $\omega(s(n))=\omega'(s(n))+o(\log_2 x)$, where $\omega'(m)$ denotes the number of prime divisors p of m with $p\in(\log_2 x, x^{1/\sqrt{\log_2 x}}]$. Hence,

$$\sum_{n\le x:n\notin\mathcal{E}(x)}\omega(s(n))^2=\sum_{n\le x:n\notin\mathcal{E}(x)}\omega'(s(n))^2+o\Big(\log_2 x\sum_{n\le x:n\notin\mathcal{E}(x)}\omega'(s(n))\Big)+o(x(\log_2 x)^2).$$

Since $\omega'(s(n))\le\omega(s(n))$, we have $\sum_{n\le x:n\notin\mathcal{E}(x)}\omega'(s(n))\ll x\log_2 x$ by Theorem 2.3.1. The lemma follows. □

2.4.1 Proof of Lemma 2.4.1.

As before, we fix primes $p,q\in(\log_2 x, x^{1/\sqrt{\log_2 x}}]$ and count the number of $n\notin\mathcal{E}(x)$ where $p,q\mid s(n)$. Eventually we will need to use Theorem 2.2.4 to count primes modulo pq, and so we take $T=x^{3/\sqrt{\log_2 x}}$ in the theorem. However, we must ensure that pq is not a multiple of some integer $q_1(T)$. Let $p_1(T)$ denote the largest prime factor of $q_1(T)$. If pq is a multiple of $q_1(T)$, then $p_1(T)$ divides pq, which forces $p_1(T)=p$ or $p_1(T)=q$. Therefore, we will insist that $p,q\neq p_1(T)$, which excludes at most one each of p and q.

Write $n=mP$, $P:=P(n)$, where $P\nmid m$, $P>x^{1/\log_3 x}$, $x^{1/\log_3 x}<P(m)<x/2m$, and a prime $\ell\mid(n,\sigma(n))\implies\ell<\log_2 x$. As before, we can split the above sum in two, with one sum over n such that $p,q\nmid s(m)$ and the other over n such that either p or q divides $s(m)$; and as before, the latter sum will be empty, by the same argument. Thus we are reduced to considering $n\notin\mathcal{E}(x)$ with $p,q\mid s(n)$ and $p,q\nmid s(m)$.

If both p and q divide $s(n)$ but not $s(m)$, then since $s(n) = Ps(m) + \sigma(m)$, we have

$$P \equiv -\sigma(m)s(m)^{-1} \pmod{pq}.$$

Therefore

$$\sum_{\substack{n \le x : n \notin \mathcal{E}(x) \\ p,q \mid s(n) \\ p,q \nmid s(m)}} 1 = \sum_m{}' \sum_{\substack{P(m) < P \le x/m \\ P \equiv -\sigma(m)s(m)^{-1} \pmod{pq}}} 1,$$

where now $\sum_m{}'$ includes the condition $q \nmid s(m)$.

The inner sum is equal to

$$\pi\big(x/m; pq, -\sigma(m)s(m)^{-1}\big) - \pi\big(P(m); pq, -\sigma(m)s(m)^{-1}\big).$$

We once again use Theorem 2.2.4 on the terms above, with $T = x^{3/\sqrt{\log_2 x}}$. The analysis proceeds exactly as before, with the factor of $1/\varphi(p)$ replaced by $1/\varphi(pq)$. We have in the end that the inner sum (over n) is asymptotically equal to

$$\frac{1}{\varphi(pq)}\big(\#\{n \le x : n \notin \mathcal{E}(x)\} - \#\{n \le x : n = mP(n) \notin \mathcal{E}(x), \text{ either } p \text{ or } q \mid s(m)\}\big).$$

Applying Lemma 2.3.2 twice, we have that the number of $n \le x$ not belonging to $\mathcal{E}(x)$ such that either p or q divides $s(m)$ is

$$\ll x \log_3 x \log_4 x \left(\frac{1}{p-1} + \frac{1}{q-1}\right).$$

Putting everything together, we have shown that

$$\sum_{n\le x\,:\,n\notin\mathcal{E}(x)}\omega(s(n))^2 = x\sum_p\sum_q\frac{1}{(p-1)(q-1)} + \sum_p\sum_q O\left(\frac{x\log_3 x\log_4 x}{(p-1)^2(q-1)}+\frac{x\log_3 x\log_4 x}{(p-1)(q-1)^2}\right)+o(x(\log_2 x)^2),$$

where the sums over p and q have the restrictions $p,q\in(\log_2 x, x^{1/\sqrt{\log_2 x}}], q\neq p$, and $p,q\neq p_1(T)$ (from Theorem 2.2.4). Now, since $q\le x^{1/\sqrt{\log_2 x}}$ and $\sum_p 1/p^2$ converges,

$$\sum_p\sum_q\frac{1}{(p-1)^2(q-1)} = O(\log_2 x)$$

by Mertens' first theorem. Hence the O-term contributes

$$\ll x\log_2 x\log_3 x\log_4 x = o(x(\log_2 x)^2),$$

and so

$$\sum_{n\le x\,:\,n\notin\mathcal{E}(x)}\omega(s(n))^2 = x\sum_p\sum_q\frac{1}{(p-1)(q-1)}+o(x(\log_2 x)^2).$$

Another application of Mertens' theorem tells us

$$\sum_{n\le x\,:\,n\notin\mathcal{E}(x)}\omega(s(n))^2 = x(\log_2 x)^2+o(x(\log_2 x)^2),$$

which completes the proof.

2.5 From $\omega(s(n))$ to $\Omega(s(n))$

We conclude by showing that the result proved in the previous section holds with $\omega(s(n))$ replaced by $\Omega(s(n))$.

Lemma 2.5.1.

$$\sum_{n\le x: n\notin\mathcal{E}(x)} \big(\Omega(s(n)) - \omega(s(n))\big)^2 = o(x(\log_2 x)^2).$$

It follows quickly from this lemma that $\sum_{n\le x:n\notin\mathcal{E}(x)} \big(\Omega(s(n)) - \log_2 x\big)^2 = o(x(\log_2 x)^2)$. Adding and subtracting $\omega(s(n))$ inside the square and expanding, we have

$$\begin{aligned}\sum_{n\le x:n\notin\mathcal{E}(x)} \big(\Omega(s(n)) - \log_2 x\big)^2 = &\sum_{n\le x:n\notin\mathcal{E}(x)} \big(\Omega(s(n)) - \omega(s(n))\big)^2 \\ &+ \sum_{n\le x:n\notin\mathcal{E}(x)} \big(\omega(s(n)) - \log_2 x\big)^2 \\ &+ 2\sum_{n\le x:n\notin\mathcal{E}(x)} \big[\big(\Omega(s(n)) - \omega(s(n))\big)\big(\omega(s(n)) - \log_2 x\big)\big].\end{aligned}$$

The first and second sums are $o(x(\log_2 x)^2)$, by the above lemma and Theorem 2.1.3, respectively. An application of the Cauchy-Schwarz inequality shows us that the last term squared is

$$\ll \Big(\sum_{n\le x:n\notin\mathcal{E}(x)} \big(\Omega(s(n)) - \omega(s(n))\big)^2\Big)\Big(\sum_{n\le x:n\notin\mathcal{E}(x)} \big(\omega(s(n)) - \log_2 x\big)^2\Big);$$

using Lemma 2.5.1 and Theorem 2.1.3 once more and taking square roots, we see that this is also $o(x(\log_2 x)^2)$.

Proof of Lemma 2.5.1. We wish to estimate from above the quantity

$$\begin{aligned}\sum_{n\le x:n\notin\mathcal{E}(x)} \big(\Omega(s(n)) - \omega(s(n))\big)^2 &= \sum_{n\le x\,:\,n\notin\mathcal{E}(x)} \Big(\sum_{\substack{p^k\mid s(n)\\ k\ge 2}} 1\Big)^2 \\ &= \sum_{n\le x:n\notin\mathcal{E}(x)} \sum_{\substack{p^k,q^j\mid s(n)\\ k,j\ge 2\\ p\ne q}} 1 + \sum_{n\le x:n\notin\mathcal{E}(x)} \sum_{\substack{p^k,p^j\mid s(n)\\ k,j\ge 2}} 1.\end{aligned}$$

We handle the "$p = q$" sum first. If $p^k \mid s(n)$ and $j \le k$, the condition $p^k, p^j \mid s(n)$ is satisfied $k-1$ times given p, and so the sum is

$$\ll 2 \sum_{n \le x : n \notin \mathcal{E}(x)} \sum_{\substack{p^k \mid s(n) \\ k \ge 2}} k = \sum_{k \ge 2} k \sum_{n \le x : n \notin \mathcal{E}(x)} \sum_{p \,:\, p^k \mid s(n)} 1.$$

A number $m \le x^2$ has at most $\frac{20}{k} \log_3 x$ primes $p > x^{1/10 \log_3 x}$ with $p^k \mid m$. Define $L_1 := \lfloor 30 \log_3 x \rfloor$. If $p > x^{1/10 \log_3 x}$, then $p^{L_1} > x^2$, so certainly for $k > L_1$ the condition $p^k \mid s(n)$ cannot be met. Therefore,

$$\sum_{k \ge 2} k \sum_{n \le x : n \notin \mathcal{E}(x)} \sum_{\substack{p > x^{1/10 \log_3 x} \\ p^k \mid s(n)}} 1 \le 20 x \log_3 x \sum_{k=2}^{L_1} 1 = O(x \log_3 x \cdot L_1),$$

and $x \log_3 x \cdot L_1 \ll x (\log_3 x)^2$.

It remains to consider

$$\begin{aligned} \sum_{n \le x : n \notin \mathcal{E}(x)} \sum_{\substack{p \le x^{1/10 \log_3 x} \\ p^k \mid s(n) \\ k \ge 2}} k &= \sum_{p \le x^{1/10 \log_3 x}} \sum_{\substack{n \le x : n \notin \mathcal{E}(x) \\ p^k \mid s(n) \\ k \ge 2}} k \\ &= \sum_{p \le x^{1/10 \log_3 x}} \sum_{\substack{n \le x : n \notin \mathcal{E}(x) \\ p^k \mid s(n) \\ p^k \le x^{1/2 \log_3 x} \\ k \ge 2}} k + \sum_{p \le x^{1/10 \log_3 x}} \sum_{\substack{n \le x : n \notin \mathcal{E}(x) \\ p^k \mid s(n) \\ p^k > x^{1/2 \log_3 x} \\ k \ge 2}} k. \end{aligned}$$

For the first sum, the condition $p^k \le x^{1/2 \log_3 x}$ allows us to apply Proposition 2.2.5, which gives

$$\sum_{p \le x^{1/10 \log_3 x}} \sum_{\substack{n \le x : n \notin \mathcal{E}(x) \\ p^k \mid s(n) \\ p^k \le x^{1/2 \log_3 x} \\ k \ge 2}} k \ll x \log_3 x \sum_{k=2}^{L_2} \sum_{p \le x^{1/10 \log_3 x}} \frac{k^2}{p^k},$$

with $L_2 = \lfloor 3 \log x \rfloor$. But the sum of k^2/p^k over all $p \geq 2$ and all $k \geq 2$ is $O(1)$, so this is $O(x \log_3 x)$.

For the second sum, define $\ell(p) := \max\{m \in \mathbb{N} : p^m \leq x^{1/2 \log_3 x}\}$. Notice that $\ell(p) < \log x$ trivially and that $p^{\ell(p)} > x^{1/2 \log_3 x}/p$. The second sum is bounded from above by

$$\sum_{\substack{p \leq x^{1/10 \log_3 x} \\ p^k > x^{1/2 \log_3 x} \\ k \geq 2}} \sum_{\substack{n \leq x : n \notin \mathcal{E}(x) \\ p^{\ell(p)} | s(n)}} k \ll x \log_3 x \sum_{k=2}^{L_2} k \sum_{p \leq x^{1/10 \log_3 x}} \frac{\ell(p)}{p^{\ell(p)}},$$

using Proposition 2.2.5 once more. The above inequalities then show that this sum is

$$\ll \frac{x (\log x)^3 \log_3 x}{x^{1/2 \log_3 x}} \cdot x^{1/10 \log_3 x} = o(x).$$

Thus $\sum_{n \leq x : n \notin \mathcal{E}(x)} \big(\Omega(s(n)) - \omega(s(n))\big) \ll x \log_3 x \log_4 x$, which is $o(x \log_2 x)$.

We now turn our attention to $\sum_{n \leq x : n \notin \mathcal{E}(x)} \sum_{p^k, q^j | s(n)} 1$, with $k, j \geq 2$ and $p \neq q$. Arguments similar to those used before show

$$\sum_{n \leq x : n \notin \mathcal{E}(x)} \sum_{\substack{p^k | s(n) \\ k \geq 2}} \sum_{\substack{q^j | s(n) \\ j \geq 2 \\ q \neq p}} 1 = \sum_{n \leq x : n \notin \mathcal{E}(x)} \sum_{\substack{p^k | s(n) \\ k \geq 2}} \sum_{\substack{q \leq x^{1/10 \log_3 x} \\ q^j | s(n) \\ j \geq 2 \\ q \neq p}} 1 + o(x \log_2 x \log_3 x),$$

and p can certainly be restricted in the same way. Rearranging the sum, we have

$$\sum_{n \leq x : n \notin \mathcal{E}(x)} \sum_{\substack{p \leq x^{1/10 \log_3 x} \\ p^k | s(n) \\ k \geq 2}} \sum_{\substack{q \leq x^{1/10 \log_3 x} \\ q^j | s(n) \\ j \geq 2 \\ q \neq p}} 1 = \sum_{p \leq x^{1/10 \log_3 x}} \sum_{\substack{q \leq x^{1/10 \log_3 x} \\ q \neq p}} \sum_{\substack{n \leq x : n \notin \mathcal{E}(x) \\ p^k, q^j | s(n) \\ k, j \geq 2}} 1.$$

We now proceed in essentially the same way as before. Write the inner sum over q as two sums, one over $q^j \leq x^{1/4 \log_3 x}$ and the other over $q^j > x^{1/4 \log_3 x}$. Do the same for the outer

sum over p. When the dust settles, we are left with four sums to handle, one for each possible combination of ranges for p^k and q^j.

First we handle the case $p^k, q^j \le x^{1/4\log_3 x}$. Using Proposition 2.2.5, we obtain

$$\sum_{p\le x^{1/10\log_3 x}} \sum_{\substack{q\le x^{1/10\log_3 x}\\ q\neq p}} \sum_{\substack{n\le x: n\notin\mathcal{E}(x)\\ p^k,q^j\mid s(n)\\ p^k,q^j\le x^{1/4\log_3 x}\\ k,j\ge 2}} 1 \ll x\log_3 x \sum_{k\ge 2}\sum_{j\ge 2} \sum_{p\le x^{1/10\log_3 x}} \sum_{\substack{q\le x^{1/10\log_3 x}\\ q\neq p}} \frac{kj}{p^k q^j}$$

$$\ll x\log_3 x.$$

If $p^k, q^j > x^{1/4\log_3 x}$, we define $\ell(p) = \max\{m : p^m \le x^{1/4\log_3 x}\}$ and, as before, obtain that this sum is

$$\ll x\log_3 x \sum_{k\ge 2}\sum_{j\ge 2} \sum_{p\le x^{1/10\log_3 x}} \sum_{q\le x^{1/10\log_3 x}} \frac{\ell(p)\ell(q)}{p^{\ell(p)}q^{\ell(q)}} \ll \frac{x(\log x)^4\log_3 x}{x^{1/2\log_3 x}}\cdot x^{1/5\log_3 x},$$

which is $o(x)$.

Assume now that $q^j \le x^{1/4\log_3 x} \le p^k$; the final case is completely similar. Then this sum is bounded from above by

$$\sum_{\substack{p\le x^{1/10\log_3 x}\\ p^k > x^{1/4\log_3 x}\\ k\ge 2}} \sum_{\substack{q\le x^{1/10\log_3 x}\\ q^j\le x^{1/4\log_3 x}\\ j\ge 2}} \sum_{\substack{n\notin\mathcal{E}(x)\\ p^{\ell(p)},q^j\mid s(n)}} 1 \ll x\log_3 x \sum_{k=2}^{L_2}\sum_{j\ge 2} \sum_{p\le x^{1/10\log_3 x}} \sum_{\substack{q\le x^{1/10\log_3 x}\\ q\neq p}} \frac{\ell(p)j}{p^{\ell(p)}q^j}$$

$$\ll \frac{x(\log x)^2\log_3 x}{x^{1/3\log_3 x}}. \qquad \square$$

Remark. We know, by the celebrated Erdős - Kac theorem, that (roughly speaking) $\omega(n)$ is normally distributed with mean and variance $\log\log n$. The corresponding theorem for $\omega(\sigma(n))$ follows from methods of Erdős and Pomerance [EP85]: $\omega(\sigma(n))$ is also normally distributed, but with mean $\frac{1}{2}(\log\log n)^2$ and standard deviation $\frac{1}{\sqrt{3}}(\log\log n)^{3/2}$. One hopes

that something similar can be said about $\omega(s(n))$. The results of the present article indicate that $s(n)$ typically has just as many prime factors as n; for this reason, we expect the Erdős - Kac theorem to hold with $\omega(s(n))$ in place of $\omega(n)$.

Chapter 3

Orders of reductions of elliptic curves

3.1 Introduction

Elliptic curves are central objects of study in number theory. In this chapter, we investigate the behavior of a certain class of elliptic curves over finite fields $\mathbb{F}_p$, as p varies. We begin by setting up terminology and notation.

Let K be a field of characteristic other than 2 or 3. An *elliptic curve* E defined over K is the set of solutions to a so-called *Weierstrass equation* of the form

$$y^2 = x^3 + Ax + B, \quad \text{where} \quad 4A^3 + 27B^2 \neq 0,$$

together with a "point at infinity." The set of K-rational points of E together with the point at infinity, denoted $E(K)$, turns out to be a group. The group law on $E(K)$ is classically defined via the "chord-and-tangent process" (cf. [Was08, Section 2.2]).

Let E be an elliptic curve over $\mathbb{C}$. We can regard $E \subset \mathbb{P}^2(\mathbb{C})$ as a Riemann surface, and it turns out that this surface is, topologically, a torus. That E is a Riemann surface with a

group law means that E is a complex Lie group. We refer the reader to [Was08, Chapter 9] for more details.

This leads us to an alternative definition of elliptic curves over $\mathbb{C}$. Let $\Lambda \subset \mathbb{C}$ denote a *lattice* (that is, a discrete, full-rank subgroup of $(\mathbb{C}, +)$). The following theorem, known as "Weierstrass uniformization," provides another characterization of elliptic curves.

Theorem 3.1.1. *Every elliptic curve over $\mathbb{C}$ is isomorphic, as a complex Lie group, to $\mathbb{C}/\Lambda$ for some lattice Λ. Conversely, for any lattice $\Lambda \subset \mathbb{C}$, there is an elliptic curve $E/\mathbb{C}$ such that $\mathbb{C}/\Lambda$ is isomorphic to E as a complex Lie group.*

Given this correspondence between elliptic curves E over $\mathbb{C}$ and lattices $\Lambda \subset \mathbb{C}$, we will write $E = \mathbb{C}/\Lambda$. Weierstrass uniformization provides another way to see that $E(\mathbb{C})$ is a group, since $\mathbb{C}/\Lambda$ is an abelian group (and the same is true of $E(K)$ for a number field K, since such K can be viewed as a subfield of $\mathbb{C}$).

For an elliptic curve $E = \mathbb{C}/\Lambda$, define the *ring of endomorphisms of E* by

$$\mathrm{End}(E) = \{\alpha \in \mathbb{C} : \alpha\Lambda = \Lambda\}.$$

From each $\alpha \in \mathrm{End}(E)$ one obtains a map from E to itself in the obvious way: a point $x \bmod \Lambda$ maps to $\alpha x \bmod \Lambda$. These maps preserve 0, and in fact, these are the only maps that do so. Since Λ is a lattice, clearly $\mathbb{Z} \subset \mathrm{End}(E)$; in fact, we can say much more. The following theorem completely characterizes the ring $\mathrm{End}(E)$. Recall that an *order* in a number field K is a subring of K that is a free abelian group of rank 2.

Theorem 3.1.2. *For each lattice $\Lambda \subset \mathbb{C}$, either $\mathrm{End}(E) = \mathbb{Z}$ or $\mathrm{End}(E)$ is isomorphic to an order in an imaginary quadratic field.*

If $\mathbb{Z} \subsetneq \mathrm{End}(E)$, we say that the elliptic curve E has *complex multiplication*. The main result of this chapter focuses on elliptic curves with complex multiplication.

Let E be an elliptic curve defined over $\mathbb{Q}$ with Weierstrass equation $E : y^2 = x^3 + Ax + B$, with $A, B \in \mathbb{Z}$. We can reduce the coefficients modulo a prime p to obtain a curve defined over the field $\mathbb{F}_q$, where q is a power of p; for our present purposes, we will assume $p \neq 2, 3$. If the quantity $4A^3 + 27B^2$ is nonzero in $\mathbb{F}_p$, we say that E has *good reduction* at p. There are only finitely many primes p which are not of good reduction for a given elliptic curve E as above, and we will generally restrict our attention to primes of good reduction. An elliptic curve $E/\mathbb{F}_q$ is said to be *supersingular* if no element of $E(\overline{\mathbb{F}_q})$ has order p; if this is not the case, then p is said to be a prime of *ordinary* reduction for E. The following proposition [Was08, Proposition 4.31] provides a convenient characterization of supersingular elliptic curves over finite fields.

Proposition 3.1.3. *Let E be an elliptic curve over $\mathbb{F}_q$, where q is a power of the prime number p. Let $a_q = q + 1 - \#E(\mathbb{F}_q)$. Then E is supersingular if and only if $a_q \equiv 0 \pmod{p}$.*

It is a well-known result of Hasse that $|a_q| \leq 2\sqrt{q}$. This bound, together with Proposition 3.1.3, implies that if $E/\mathbb{F}_p$ is supersingular and $p \neq 2, 3$, then $a_p = p + 1$.

3.2 Analytic questions concerning $\#E(\mathbb{F}_p)$

Let $E/\mathbb{Q}$ be an elliptic curve. For primes p of good reduction, one has

$$E(\mathbb{F}_p) \simeq \mathbb{Z}/d_p\mathbb{Z} \oplus \mathbb{Z}/e_p\mathbb{Z}$$

where d_p and e_p are uniquely determined natural numbers such that d_p divides e_p. Thus, $\#E(\mathbb{F}_p) = d_p e_p$. We concern ourselves with the behavior $\omega(\#E(\mathbb{F}_p))$, where $\omega(n)$ denotes the number of distinct prime factors of the number n, as p varies over primes of good reduction. Work has been done already in this arena: If the curve E has CM, Cojocaru [Coj05, Corollary 6] showed that the normal order of $\omega(\#E(\mathbb{F}_p))$ is $\log\log p$, and a year later, Liu [Liu06]

established an elliptic curve analogue of the celebrated Erdős - Kac theorem: For any elliptic curve $E/\mathbb{Q}$ with CM, the quantity

$$\frac{\omega(\#E(\mathbb{F}_p)) - \log\log p}{\sqrt{\log\log p}}$$

has a Gaussian normal distribution. In particular, $\omega(\#E(\mathbb{F}_p))$ has normal order $\log\log p$ and standard deviation $\sqrt{\log\log p}$. (These results hold for elliptic curves without CM, if one assumes GRH.)

Presently, we establish a result analogous to Theorem 1.2.6 for the quantity $\omega(\#E(\mathbb{F}_p))$, where $E/\mathbb{Q}$ is an elliptic curve with CM.

Theorem 3.2.1. *Let $E/\mathbb{Q}$ be an elliptic curve with CM. For $\gamma > 1$ fixed,*

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log\log x\} = \frac{x}{(\log x)^{2+\gamma\log\gamma-\gamma+o(1)}}.$$

The same statement is true for the quantity $\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) < \gamma \log\log x\}$ when $0 < \gamma < 1$.

In what follows, the above theorem will be proved for $E/\mathbb{Q}$ with $E : y^2 = x^3 - x$. Essentially the same method can be used for any elliptic curve with CM; refer to the discussion in §4 of [Pol16]. To establish the theorem, we prove corresponding upper and lower bounds in sections §3 and §4, respectively.

Remark. One can ask similar questions about other arithmetic functions applied to $\#E(\mathbb{F}_p)$. For example, Pollack has shown [Pol16] that, if E has CM, then

$$\sum_{p\leq x}{}' \tau(\#E(\mathbb{F}_p)) \sim c_E \cdot x,$$

where the sum is restricted to primes p of good ordinary reduction for E. Several elements of Pollack's method of proof will appear later in this chapter.

For ease of reference, let us collect some frequently-used notation in this chapter. K will denote an extension of $\mathbb{Q}$ with ring of integers $\mathbb{Z}_K$. For each ideal $\mathfrak{a} \subset \mathbb{Z}_K$, we write $\|\mathfrak{a}\|$ for the norm of $\mathfrak{a}$ (that is, $\|\mathfrak{a}\| = \#\mathbb{Z}_K/\mathfrak{a}$) and $\Phi(\mathfrak{a}) = \#(\mathbb{Z}_K/\mathfrak{a})^\times$. The function ω applied to an ideal $\mathfrak{a} \subset \mathbb{Z}_K$ will denote the number of distinct prime ideals appearing in the factorization of $\mathfrak{a}$ into a product of prime ideals. For $\alpha \in \mathbb{Z}_K$, $\|\alpha\|$ and $\Phi(\alpha)$ denote those functions evaluated at the ideal (α). If α is invertible modulo an ideal $\mathfrak{u} \subset \mathbb{Z}_K$, we write $\gcd(\alpha, \mathfrak{u}) = 1$. The notation $\log_k x$ will be used to denote the kth iterate of the natural logarithm; this is not to be confused with the base-k logarithm.

3.3 Useful propositions

Brun's sieve in the Gaussian integers, Theorem 1.1.4 in Chapter 1, will be one of our primary tools. We recall it here for ease of reference.

Theorem 3.3.1. *Let K be a number field with ring of integers $\mathbb{Z}_K$. Let $\mathcal{A}$ be a finite sequence of elements of $\mathbb{Z}_K$, and let $\mathcal{P}$ be a finite set of prime ideals. Define*

$$S(\mathcal{A}, \mathcal{P}) := \#\{a \in \mathcal{A} : \gcd(a, \mathfrak{P}) = 1\}, \text{ where } \mathfrak{P} := \prod_{\mathfrak{p} \in \mathcal{P}} \mathfrak{p}.$$

For an ideal $\mathfrak{u} \subset \mathbb{Z}_K$, write $A_\mathfrak{u} := \#\{a \in \mathcal{A} : a \equiv 0 \pmod{\mathfrak{u}}\}$. Let X denote an approximation to the size of $\mathcal{A}$. Suppose δ is a multiplicative function taking values in $[0, 1]$, and define a function $r(\mathfrak{u})$ such that

$$A_\mathfrak{u} = X\delta(\mathfrak{u}) + r(\mathfrak{u})$$

for each $\mathfrak{u}$ *dividing* $\mathfrak{P}$*. Then, for every even* $m \in \mathbb{Z}^+$*,*

$$S(\mathcal{A}, \mathcal{P}) = X \prod_{\mathfrak{p} \in \mathcal{P}} (1 - \delta(\mathfrak{p})) + O\Big(\sum_{\mathfrak{u} | \mathfrak{P}, \omega(\mathfrak{u}) \leq m} |r(\mathfrak{u})| \Big) + O\Big(X \sum_{\mathfrak{u} | \mathfrak{P}, \omega(\mathfrak{u}) \geq m} \delta(\mathfrak{u}) \Big).$$

All implied constants are absolute. Here, the notation $\omega(\mathfrak{u})$ *means the number of distinct prime ideals appearing in the factorization of* $\mathfrak{u}$ *into prime ideals.*

In our estimation of O-terms arising from the use of Theorem 3.3.1, we will make frequent use of the following analogue of the Bombieri-Vinogradov theorem, which we state for an arbitrary imaginary quadratic field $K/\mathbb{Q}$ with class number 1. For $\alpha \in \mathbb{Z}_K$ and an ideal $\mathfrak{q} \subset \mathbb{Z}_K$, write

$$\pi(x; \mathfrak{q}, \alpha) = \#\{\mu \in \mathbb{Z}_K : \mu \text{ prime}, \|\mu\| \leq x, \mu \equiv \alpha \pmod{\mathfrak{q}}\}.$$

Proposition 3.3.2. *For every* $A > 0$*, there is a* $B > 0$ *so that*

$$\sum_{\|\mathfrak{q}\| \leq x^{1/2} (\log x)^{-B}} \max_{\alpha : \gcd(\alpha, \mathfrak{u}) = 1} \max_{y \leq x} |\pi(y; \mathfrak{q}, \alpha) - w_K \cdot \frac{\mathrm{Li}(y)}{\Phi(\mathfrak{q})}| \ll \frac{x}{(\log x)^A},$$

where the above sum and maximum are taken over $\mathfrak{q} \subset \mathbb{Z}_K$ *and* $\alpha \in \mathbb{Z}_K$*. Here* w_K *denotes the size of the group of units of* $\mathbb{Z}_K$*.*

The above follows from Huxley's analogue of the Bombieri-Vinogradov theorem for number fields [Hux71]; we will state this result in the case when $K/\mathbb{Q}$ is an imaginary quadratic field of class number 1. First, we recall some necessary definitions. Let $\mathfrak{m} \subset \mathbb{Z}_K$ be a nonzero ideal, and set

$$\mathcal{I}(\mathfrak{m}) = \{\text{fractional ideals } \mathfrak{a} \subset K : \mathrm{ord}_p(\mathfrak{a}) = 0 \text{ for all } \mathfrak{p} \mid \mathfrak{m}\},$$

and

$$\mathcal{P}_{\mathfrak{m}}^{+} = \{(\alpha) : \mathrm{ord}_{\mathfrak{p}}(\alpha - 1) \geq \mathrm{ord}_{\mathfrak{p}}(\mathfrak{m}) \text{ for all } \mathfrak{p} \mid \mathfrak{m}\}.$$

Fractional ideals $\mathfrak{a}, \mathfrak{b} \in \mathcal{I}(\mathfrak{m})$ are said to be *equivalent modulo* $\mathfrak{m}$ if they represent the same class in the quotient $\mathcal{I}(\mathfrak{m})/\mathcal{P}_{\mathfrak{m}}^{+}$, called the *strict ray class group*. The number $h(\mathfrak{m}) = \#\mathcal{I}(\mathfrak{m})/\mathcal{P}_{\mathfrak{m}}^{+}$ is called the *strict ray class number*. The formula

$$h(\mathfrak{m}) = \frac{\Phi(\mathfrak{m})}{[\mathcal{U} : \mathcal{U}_{\mathfrak{m}}]}$$

holds in our case, where $\mathcal{U}$ is the unit group of $\mathbb{Z}_K$ and

$$\mathcal{U}_{\mathfrak{m}} = \{\lambda \in \mathcal{U} : \lambda \equiv 1 \pmod{\mathfrak{m}}\}.$$

For $\mathfrak{a} \in \mathcal{I}(\mathfrak{m})$, write

$$\pi(x; \mathfrak{m}, \mathfrak{a}) = \#\{\mathfrak{p} : \|\mathfrak{p}\| \leq x, \mathfrak{p} \text{ is equivalent to } \mathfrak{a} \text{ modulo } \mathfrak{m}\}.$$

The following theorem is obtained from [Hux71, Theorem 1] by partial summation. Note that it holds for K an arbitrary number field, if the definitions above are modified appropriately for more general K.

Theorem 3.3.3. *For each $A > 0$, there is a $B > 0$ such that*

$$\sum_{\|\mathfrak{m}\| \leq x^{1/2}(\log x)^{-B}} \frac{h(\mathfrak{m})}{\Phi(\mathfrak{m})} \max_{\mathfrak{a}} \max_{y \leq x} \left| \pi(y; \mathfrak{m}, \mathfrak{a}) - \frac{\mathrm{Li}(y)}{h(\mathfrak{m})} \right| \ll \frac{x}{(\log x)^A}.$$

The first maximum is over $\mathfrak{a} \in \mathcal{I}(\mathfrak{m})$, and the implied constant depends on A and K.

Now, suppose K is an imaginary quadratic field of class number 1. Tracing through the definitions, we see that, if $\mathfrak{p}$ is a prime ideal, then $\mathfrak{p}$ is equivalent to (α) modulo (μ) whenever

$\mathfrak{p} = (\pi)$ for some prime $\pi \equiv \alpha \pmod{\mu}$. Moreover, if such a π exists, then we can multiply by an element of $\mathcal{U}_{(\mu)}$ to obtain another. Combining these facts with the above theorem yields Proposition 3.3.2 (cf. [Pol16, Lemma 2.3]).

The following proposition is an analogue of Mertens' theorem (cf. part 2 of Theorem 1.2.3) for imaginary quadratic fields. It follows immediately from Theorem 2 of [Ros99].

Proposition 3.3.4. *Let $K/\mathbb{Q}$ be an imaginary quadratic field and let α_K denote the residue of the associated Dedekind zeta function, $\zeta_K(s)$, at $s = 1$. Then*

$$\prod_{\|\mathfrak{p}\| \leq x} \left(1 - \frac{1}{\|\mathfrak{p}\|}\right)^{-1} \sim e^{\gamma} \alpha_K \log x,$$

where the product is over all prime ideals $\mathfrak{p}$ in $\mathbb{Z}_K$. Here (and only here), γ is the Euler-Mascheroni constant.

Note also that the "additive version" of Mertens' theorem, i.e.,

$$\sum_{\|\mathfrak{p}\| \leq x} \frac{1}{\|\mathfrak{p}\|} = \log_2 x + B_K + O_K\left(\frac{1}{\log x}\right)$$

for some constant B_K, holds in this case as well; it appears as Lemma 2.4 in [Rosen].

Finally, we will make use of the following estimate for elementary symmetric functions [HR83, p. 147, Lemma 13].

Lemma 3.3.5. *Let $y_1, y_2, \ldots, y_M$ be M non-negative real numbers. For each positive integer d not exceeding M, let*

$$\sigma_d = \sum_{1 \leq k_1 < k_2 < \cdots < k_d \leq M} y_{k_1} y_{k_2} \cdots y_{k_d},$$

so that σ_d is the dth elementary symmetric function of the y_k's. Then, for each d, we have

$$\sigma_d \geq \frac{1}{d!} \sigma_1^d \left(1 - \binom{d}{2} \frac{1}{\sigma_1^2} \sum_{k=1}^{M} y_k^2\right).$$

3.4 An upper bound

Theorem 3.4.1. *Let E be the elliptic curve $E : y^2 = x^3 - x$ and fix $\gamma > 1$. Then*

$$\#\{p \le x : \omega(\#E(\mathbb{F}_p)) > \gamma \log_2 x\} \ll_\gamma \frac{x(\log_2 x)^5}{(\log x)^{2+\gamma \log \gamma - \gamma}}.$$

The same statement is true if instead $0 < \gamma < 1$ and the strict inequality is reversed on the left-hand side.

Before proving Theorem 3.4.1, we refer to [JU08, Table 2] for the following useful fact concerning the numbers $\#E(\mathbb{F}_p)$: For primes $p \le x$ with $p \equiv 1 \pmod 4$, we have

$$\#E(\mathbb{F}_p) = p + 1 - (\pi + \overline{\pi}) = (\pi - 1)\overline{(\pi - 1)}, \tag{3.1}$$

where $\pi \in \mathbb{Z}[i]$ is chosen so that $p = \pi\overline{\pi}$ and $\pi \equiv 1 \pmod{(1+i)^3}$. (Such π are sometimes called *primary*.) This determines π completely up to conjugation.

We begin the proof of Theorem 3.4.1 with the following lemma, which will allow us to disregard certain problematic primes p.

Lemma 3.4.2. *Let $x \ge 3$ and let $P(n)$ denote the largest prime factor of n. Let $\mathcal{X}$ denote the set of $n \le x$ for which either of the following properties fail:*

(i) $P(n) > x^{1/6 \log_2 x}$

(ii) $P(n)^2 \nmid n$.

Then, for any $A > 0$, the size of $\mathcal{X}$ is $O(x/(\log x)^A)$.

Proof of Lemma 3.4.2. If $n \in \mathcal{X}$, then either (a) $P(n) \le x^{1/6 \log_2 x}$ or (b) $P(n) > x^{1/6 \log_2 x}$ and $P(n)^2 \mid n$. By Proposition 2.2.3, the number of $n \le x$ for which (a) holds is $O(x/(\log x)^A)$

for any $A > 0$, noting that $(\log x)^A \ll (\log x)^{\log_3 x} = (\log_2 x)^{\log_2 x}$. The number of $n \leq x$ for which (b) holds is

$$\ll x \sum_{p > x^{1/6 \log_2 x}} p^{-2} \ll x \exp(-\log x / 6 \log_2 x),$$

and this is also $O(x/(\log x)^A)$. □

We would like to use Lemma 3.4.2 to say that a negligible amount of the numbers $\#E(\mathbb{F}_p)$, for $p \leq x$, belong to $\mathcal{X}$. The following lemma allows us to do so.

Lemma 3.4.3. *The number of $p \leq x$ with $\#E(\mathbb{F}_p) \in \mathcal{X}$ is $O(x/(\log x)^B)$, for any $B > 0$.*

Proof. Suppose $\#E(\mathbb{F}_p) = b \in \mathcal{X}$. Then, by (3.1), $b = \|\pi - 1\|$, where $\pi \in \mathbb{Z}[i]$ is a Gaussian prime lying above p. Thus, the number of $p \leq x$ with $\#E(\mathbb{F}_p) = b$ is bounded from above by the number of Gaussian integers with norm b, which, by [HW00, Theorem 278], is $4 \sum_{d|b} \chi(d)$, where χ is the nontrivial character modulo 4. Now, using the Cauchy-Schwarz inequality and Lemma 3.4.2,

$$\begin{aligned} 4 \sum_{b \in \mathcal{X}} \sum_{d|b} \chi(d) \leq 4 \sum_{b \in \mathcal{X}} \tau(b) &\leq 4 \Big(\sum_{b \in \mathcal{X}} 1 \Big)^{1/2} \Big(\sum_{b \in \mathcal{X}} \tau(b)^2 \Big)^{1/2} \\ &\ll \Big(\frac{x}{(\log x)^A} \Big)^{1/2} \Big(x \log^3 x \Big)^{1/2} = \frac{x}{(\log x)^{A/2 - 3/2}}. \end{aligned}$$

Since $A > 0$ can be chosen arbitrarily, this completes the proof. □

For k a nonnegative integer, define N_k to be the number of primes $p \leq x$ of good ordinary reduction for E such that $\#E(\mathbb{F}_p)$ possesses properties (i) and (ii) from the above lemma and such that $\omega(\#E(\mathbb{F}_p)) = k$. Then, in the case when $\gamma > 1$,

$$\#\{p \leq x : \omega(\#E(\mathbb{F}_p)) > \gamma \log \log x\} = \sum_{k > \gamma \log_2 x} N_k + O\Big(\frac{x}{(\log x)^A} \Big)$$

for any $A > 0$. Our task is now to bound N_k from above in terms of k. Evaluating the sum on k then produces the desired upper bound.

It is clear that

$$N_k \leq \sum_{\substack{a \leq x^{1-1/6\log_2 x} \\ \omega(a)=k-1}} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod 4 \\ a \mid \#E(\mathbb{F}_p) \\ \#E(\mathbb{F}_p)/a \text{ prime}}} 1. \tag{3.2}$$

To handle the inner sum, we need information on the integer divisors of $\#E(\mathbb{F}_p)$, where $p \leq x$ and $p \equiv 1 \pmod 4$. We employ the analysis of Pollack in his proof of [Pol16, Theorem 1.1], which we restate here for completeness.

By (3.1), we have $a \mid \#E(\mathbb{F}_p)$ if and only if $a \mid (\pi - 1)\overline{(\pi - 1)} = \|\pi - 1\|$. With this in mind, we have

$$\sum_{\substack{a \leq x^{1-1/6\log\log x} \\ \omega(a)=k-1}} \sum_{\substack{p \leq x \\ p \equiv 1 \pmod 4 \\ a \mid \#E(\mathbb{F}_p) \\ \#E(\mathbb{F}_p)/a \text{ prime}}} 1 = \frac{1}{2} \sum_{\substack{a \leq x^{1-1/6\log\log x} \\ \omega(a)=k-1}} \sum_{\substack{\pi : \|\pi\| \leq x \\ \pi \equiv 1 \pmod{(1+i)^3} \\ a \mid \|\pi-1\| \\ \|\pi-1\|/a \text{ prime}}}' 1,$$

where the $'$ on the sum indicates a restriction to primes π lying over rational primes $p \equiv 1 \pmod 4$.

3.4.1 Divisors of shifted Gaussian primes.

The conditions on the primed sum above can be reformulated purely in terms of Gaussian integers.

Definition 3.4.4. For a given integer $a \in \mathbb{N}$, write $a = \prod_q q^{v_q}$, with each q prime. For each $q \mid a$ with $q \equiv 1 \pmod 4$, write $q = \pi_q \overline{\pi}_q$. Define a set S_a which consists of all products α of

the form

$$\alpha = (1+i)^{v_2} \prod_{\substack{q \mid a \\ q \equiv 3 \pmod 4}} q^{\lceil v_q/2 \rceil} \prod_{\substack{q \mid a \\ q \equiv 1 \pmod 4}} \alpha_q,$$

where $\alpha_q \in \{\pi_q^i \overline{\pi}_q^{v_q - i} : i = 0, 1, \ldots, v_q\}$.

Notice that the condition $a \mid \|\pi - 1\|$ is equivalent to $\pi - 1$ being divisible by some element of the set S_a. We can therefore write

$$\sum_{\substack{a \le x^{1-1/6\log\log x} \\ \omega(a) = k-1}} \sum_{\substack{p \le x \\ p \equiv 1 \pmod 4 \\ a \mid \#E(\mathbb{F}_p) \\ \#E(\mathbb{F}_p)/a \text{ prime}}} 1 \le \frac{1}{2} \sum_{\substack{a \le x^{1-1/6\log\log x} \\ \omega(a) = k-1}} \sum_{\alpha \in S_a} \sum_{\substack{\pi : \|\pi\| \le x \\ \pi \equiv 1 \pmod{(1+i)^3} \\ \alpha \mid \pi - 1 \\ \|\pi-1\|/a \text{ prime}}}' 1. \tag{3.3}$$

Now, for any $\alpha \in S_a$, we have

$$\alpha\overline{\alpha} = a \prod_{q \equiv 3 \pmod 4} q^{2\lceil v_q/2 \rceil - v_q}.$$

Observe that

$$\frac{\|\pi - 1\|}{a} = \frac{(\pi - 1)(\overline{\pi - 1})}{\alpha\overline{\alpha}} \prod_{q \equiv 3 \pmod 4} q^{2\lceil v_q/2 \rceil - v_q}.$$

Therefore, if $\frac{\|\pi-1\|}{a}$ is to be prime, the number a must satisfy exactly one of the following properties:

1. The number a is divisible by exactly one prime $q \equiv 3 \pmod 4$ with v_q an odd number, and $\alpha = u(\pi - 1)$ where $u \in \mathbb{Z}[i]$ is a unit; or

2. All primes $q \equiv 3 \pmod 4$ which divide a have v_q even, and $(\pi - 1)/\alpha$ is a prime in $\mathbb{Z}[i]$.

This splits the outer sum in (3.3) into two components.

Lemma 3.4.5. *We have*

$$\sideset{}{^\flat}\sum_{\substack{a\le x^{1-1/6\log\log x}\\ \omega(a)=k-1}}\sum_{\alpha\in S_a}\sideset{}{'}\sum_{\substack{\pi:\|\pi\|\le x\\ \pi\equiv 1 \pmod{(1+i)^3}\\ (\pi-1)/\alpha\in U}} 1 = O\Big(\frac{x}{\log^A x}\Big),$$

where U is the set of units in $\mathbb{Z}[i]$ and the $\flat$ on the outer sum indicates a restriction to integers a such that there is a unique prime power $q^{v_q}\|a$ with $q\equiv 3 \pmod 4$ and v_q odd.

Proof. If $\alpha = u(\pi-1)$ for $u\in U$, then there are at most four choices for π, given α. Thus

$$\sideset{}{^\flat}\sum_{\substack{a\le x^{1-1/6\log\log x}\\ \omega(a)=k-1}}\sum_{\alpha\in S_a}\sideset{}{'}\sum_{\substack{\pi:\|\pi\|\le x\\ \pi\equiv 1 \pmod{(1+i)^3}\\ \alpha=u(\pi-1)}} 1 \le 4 \sideset{}{^\flat}\sum_{\substack{a\le x^{1-1/6\log\log x}\\ \omega(a)=k-1}} |S_a|.$$

We have $|S_a| = \prod_{q\equiv 1 \pmod 4}(v_q+1)$; this is bounded from above by the divisor function on a, which we denote $\tau(a)$. Therefore, the above is

$$\ll \sum_{a\le x^{1-1/6\log\log x}} \tau(a) \ll x^{1-1/6\log_2 x}(\log x),$$

which is $O(x/\log^A x)$ for any $A>0$. □

The second case provides the main contribution to the sum.

Lemma 3.4.6. *Let $a\le x^{1-1/6\log\log x}$ with $\omega(a)=k-1$ such that all primes $q\equiv 3 \pmod 4$ dividing a have v_q even. Let $\alpha\in S_a$. Then*

$$\sideset{}{'}\sum_{\substack{\pi:\|\pi\|\le x\\ \pi\equiv 1 \pmod{(1+i)^3}\\ \alpha\mid\pi-1\\ (\pi-1)/\alpha \text{ prime}}} 1 \ll \frac{x(\log_2 x)^5}{\|\alpha\|(\log x)^2}$$

uniformly over all a as above and $\alpha\in S_a$.

Proof. If $\pi \equiv 1 \pmod{\alpha}$, then $\pi = 1 + \alpha\beta$ for some $\beta \subset \mathbb{Z}[i]$. Thus $\beta = \frac{\pi-1}{\alpha}$, and so $\|\beta\| \leq \frac{2x}{\|\alpha\|}$. Let $\mathcal{A}$ denote the sequence of elements in $\mathbb{Z}[i]$ given by

$$\Big\{\beta(1+\alpha\beta) : \|\beta\| \leq \frac{2x}{\|\alpha\|}\Big\}.$$

Define $\mathcal{P} = \{\mathfrak{p} \subset \mathbb{Z}[i] : \|\mathfrak{p}\| \leq z\}$ where z is a parameter to be chosen later. Then, in the notation of Theorem 3.3.1,

$$\sum_{\substack{\pi\,:\,\|\pi\|\leq x \\ \pi\equiv 1 \pmod{(1+i)^3} \\ \alpha|\pi-1 \\ (\pi-1)/\alpha \text{ prime}}}{}' \quad 1 \leq S(\mathcal{A},\mathcal{P}) + O(z).$$

Here, the $O(z)$ term comes from those $\pi \in \mathbb{Z}[i]$ such that both π and $(\pi-1)/\alpha$ are primes, at least one of which has norm less than z.

For $\mathfrak{u} \subset \mathbb{Z}[i]$, write $A_{\mathfrak{u}} = \#\{a \in \mathcal{A} : a \equiv 0 \pmod{\mathfrak{u}}\}$. An element $\mathfrak{a} \in \mathcal{A}$ is counted by $A_{\mathfrak{u}}$ if and only if a generator of $\mathfrak{u}$ divides a. Thus, by familiar estimates on the number of integer lattice points contained in a circle, $A_{\mathfrak{u}}$ satisfies the equation

$$A_{\mathfrak{u}} = \frac{2\pi x}{\|\alpha\|}\frac{\nu(\mathfrak{u})}{\|\mathfrak{u}\|} + O\Big(\nu(\mathfrak{u})\frac{\sqrt{x}}{(\|\alpha\|\|\mathfrak{u}\|)^{1/2}}\Big),$$

where

$$\nu(\mathfrak{u}) = \#\{\beta \pmod{\mathfrak{u}} : \beta(1+\alpha\beta) \equiv 0 \pmod{\mathfrak{u}}\}.$$

We apply Theorem 3.3.1 with

$$X = \frac{2\pi x}{\|\alpha\|} \quad \text{and} \quad \delta(\mathfrak{u}) = \frac{\nu(\mathfrak{u})}{\|\mathfrak{u}\|}.$$

With these choices, we have

$$r(\mathfrak{u}) = O\Big(\nu(\mathfrak{u})\frac{\sqrt{x}}{(\|\alpha\|\|\mathfrak{u}\|)^{1/2}|}\Big).$$

Then, for any even integer $m \geq 0$,

$$S(\mathcal{A},\mathcal{P}) = \frac{2\pi x}{\|\alpha\|}\prod_{\|\mathfrak{p}\|\leq z}\left(1-\frac{\nu(\mathfrak{p})}{\|\mathfrak{p}\|}\right) + O\Big(\frac{\sqrt{x}}{\|\alpha\|^{1/2}}\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\leq m}}\frac{\nu(\mathfrak{u})}{\|\mathfrak{u}\|^{1/2}}\Big) + O\Big(\frac{x}{\|\alpha\|}\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\geq m}}\delta(\mathfrak{u})\Big), \tag{3.4}$$

where $\mathfrak{P} = \prod_{\mathfrak{p}\in\mathcal{P}}\mathfrak{p}$.

For a prime $\mathfrak{p}$, we have $\nu(\mathfrak{p}) = 2$ if $\alpha \not\equiv 0 \pmod{\mathfrak{p}}$ and $\nu(\mathfrak{p}) = 1$ otherwise. Therefore, the product in the first term is

$$\prod_{\substack{\|\mathfrak{p}\|\leq z\\ \mathfrak{p}\nmid(\alpha)}}\left(1-\frac{2}{\|\mathfrak{p}\|}\right)\prod_{\substack{\|\mathfrak{p}\|\leq z\\ \mathfrak{p}|(\alpha)}}\left(1-\frac{1}{\|\mathfrak{p}\|}\right) \leq \prod_{\|\mathfrak{p}\|\leq z}\left(1-\frac{1}{\|\mathfrak{p}\|}\right)^2\prod_{\substack{\|\mathfrak{p}\|\leq z\\ \mathfrak{p}|(\alpha)}}\left(1-\frac{1}{\|\mathfrak{p}\|}\right)^{-1} \ll \frac{1}{(\log z)^2}\frac{\|\alpha\|}{\Phi(\alpha)},$$

where in the last step we used Proposition 3.3.4.

Choose $z = x^{\frac{1}{200(\log_2 x)^2}}$. Then our first term in (3.4) is

$$\ll \frac{x(\log_2 x)^4}{\Phi(\alpha)(\log x)^2}.$$

Recall that $\|\alpha\| = a$, and $a \leq x^{1-1/6\log_2 x}$. Since $\Phi(\alpha) \gg \|\alpha\|/\log_2 x$ (analogous to the minimal order for the usual Euler function, c.f. [HW00, Theorem 328]), the above is

$$\ll \frac{x(\log_2 x)^5}{\|\alpha\|(\log x)^2}.$$

We now show that this "main" term dominates the two O-terms uniformly for $\alpha \in S_a$ and $a \leq x^{1-1/6\log_2 x}$. For the first O-term, we begin by noting that $\nu(\mathfrak{u})/\|\mathfrak{u}\|^{1/2} \ll 1$. Then, taking $m = 10\lfloor \log_2 x \rfloor$, we have

$$\sum_{\substack{\mathfrak{u}|\mathfrak{P} \\ \omega(\mathfrak{u})\leq m}} \frac{\nu(\mathfrak{u})}{\|\mathfrak{u}\|^{1/2}} \ll \sum_{k=0}^{m} \binom{\pi_K(z)}{k} \leq \sum_{k=0}^{m} \pi_K(z)^k \leq 2\pi_K(z)^m \leq x^{1/20\log_2 x},$$

where $\pi_K(z)$ denotes the number of prime ideals $\mathfrak{p} \subset \mathbb{Z}[i]$ with norm up to z. Therefore, the inequality

$$\frac{x(\log_2 x)^5}{\|\alpha\|(\log x)^2} \gg \frac{x^{1/2+1/20\log_2 x}}{\|\alpha\|^{1/2}}$$

holds for all α with $\|\alpha\| \leq x^{1-1/6\log_2 x}$, as desired.

Next we handle the second O-term. The sum in this term is

$$\sum_{\substack{\mathfrak{u}|\mathfrak{P} \\ \omega(\mathfrak{u})\geq m}} \delta(\mathfrak{u}) \leq \sum_{s\geq m} \frac{1}{s!}\Big(\sum_{\|\mathfrak{p}\|\leq z} \frac{\nu(\mathfrak{p})}{\|\mathfrak{p}\|}\Big)^s.$$

Observe that, by Proposition 3.3.4, we have

$$\sum_{\|\mathfrak{p}\|\leq z} \frac{\nu(\mathfrak{p})}{\|\mathfrak{p}\|} \leq 2\log_2 x + O(1).$$

Thus, by the ratio test, one sees that the sum on s is

$$\ll \frac{1}{m!}(2\log_2 x + O(1))^m.$$

Using Proposition 3.3.4 followed by Stirling's formula, we obtain that the above quantity is

$$\frac{1}{m!}(2\log_2 x + O(1))^m \le \Big(\frac{2e\log_2 x + O(1)}{10\lfloor \log_2 x\rfloor}\Big)^{10\lfloor \log_2 x\rfloor} \ll \Big(\frac{e}{5}\Big)^{9\log_2 x} \le \frac{1}{(\log x)^5}.$$

So the second O-term is

$$\ll \frac{x}{\|\alpha\|(\log x)^5},$$

and this is certainly dominated by the main term. □

From Lemmas 3.4.5 and 3.4.6, we see (3.2) can be rewritten

$$N_k \ll \frac{x(\log_2 x)^5}{(\log x)^2} \sum_{\substack{a\le x^{1-1/6\log_2 x}\\ \omega(a)=k-1}} \frac{|S_a|}{a} + O\Big(\frac{x}{\log^A x}\Big),$$

noting that $\|\alpha\| = a$ for all a under consideration and all $\alpha \in S_a$. We are now in a position to bound N_k from above in terms of k.

Lemma 3.4.7. *We have*

$$\sum_{\substack{a\le x^{1-1/6\log_2 x}\\ \omega(a)=k-1}} \frac{|S_a|}{a} \le \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!}.$$

Proof. We have already seen that the size of S_a is $\prod_{p|a:p\equiv 1 \pmod 4}(v_p+1)$, where v_p is defined by $p^{v_p} \parallel a$. Recall that in the current case, each prime $p \equiv 3 \pmod 4$ dividing a appears to an even power. Therefore, we have

$$\sum_{\substack{a\le x\\ \omega(a)=k-1}} \frac{|S_a|}{a} \le \frac{1}{(k-1)!}\Bigg(\sum_{\substack{p^\ell\le x\\ p\not\equiv 3 \pmod 4}} \frac{|S_{p^\ell}|}{p^\ell} + \sum_{\substack{p^{2k}\le x\\ p\equiv 3 \pmod 4}} \frac{|S_{p^{2k}}|}{p^{2k}} + O(1)\Bigg)^{k-1}. \tag{3.5}$$

Note that $|S_{p^{2k}}| = 1$ for each prime $p \equiv 3 \pmod 4$. Thus we can absorb the sum corresponding to these primes into the $O(1)$ term, giving

$$\sum_{\substack{a \le x \\ \omega(a)=k-1}} \frac{|S_a|}{a} \ll \frac{1}{(k-1)!} \left(\sum_{\substack{p^\ell \le x \\ p \not\equiv 3 \pmod 4}} \frac{|S_{p^\ell}|}{p^\ell} + O(1) \right)^{k-1}. \tag{3.6}$$

Now

$$\begin{aligned} \sum_{\substack{p^\ell \le x \\ p \not\equiv 3 \pmod 4}} \frac{|S_{p^\ell}|}{p^\ell} &= \sum_{\substack{p^\ell \le x \\ p \equiv 1 \pmod 4}} \frac{\ell+1}{p^\ell} + O(1) \\ &= \sum_{\substack{p \le x \\ p \equiv 1 \pmod 4}} \frac{2}{p} + O(1) \\ &= \log_2 x + O(1). \end{aligned}$$

Inserting this expression into (3.6) proves the lemma. □

3.4.2 Finishing the upper bound.

We have shown so far that

$$N_k \ll \frac{x(\log_2 x)^5}{(\log x)^2} \cdot \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!}.$$

We now sum on $k > \gamma \log_2 x$ for fixed $\gamma > 1$ to complete the proof of Theorem 3.4.1. (The statement corresponding to $0 < \gamma < 1$ may be proved in a completely similar way.) Again

using the ratio test and Stirling's formula, we have

$$\sum_{k>\gamma \log_2 x} \frac{(\log_2 x + O(1))^{k-1}}{(k-1)!} \ll \left(\frac{e \log_2 x + O(1)}{\lfloor \gamma \log_2 x \rfloor}\right)^{\lfloor \gamma \log_2 x \rfloor}$$
$$\ll \left(\frac{e}{\gamma}\Big(1 + O\Big(\frac{1}{\log_2 x}\Big)\Big)\right)^{\lfloor \gamma \log_2 x \rfloor} \ll \left(\frac{e}{\gamma}\right)^{\lfloor \gamma \log_2 x \rfloor} \ll_\gamma (\log x)^{\gamma - \gamma \log \gamma}.$$

Thus, we have obtained an upper bound of

$$\ll_\gamma \frac{x(\log_2 x)^5}{(\log x)^{2+\gamma \log \gamma - \gamma}},$$

as desired.

3.5 A lower bound

Theorem 3.5.1. *Consider $E : y^2 = x^3 - x$ and fix $\gamma > 1$. Then*

$$\#\{p \le x : \omega(\#E(\mathbb{F}_p)) > \gamma \log_2 x\} \ge \frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}}.$$

The same statement is true if instead $0 < \gamma < 1$ and the strict inequality is reversed on the left-hand side.

Our strategy in the case $\gamma > 1$ is as follows. As before, we write $\#E(\mathbb{F}_p) = \|\pi - 1\|$, where $\pi \equiv 1 \pmod{(1+i)^3}$ and $p = \pi\overline{\pi}$. Let k be an integer to be specified later and fix an ideal $\mathfrak{s} \in \mathbb{Z}[i]$ with the following properties:

(A) $((1+i)^3) \mid \mathfrak{s}$

(B) $\omega(\mathfrak{s}) = k$

(C) $P^+(\|\mathfrak{s}\|) \le x^{1/100\gamma \log_2 x}$

(D) Each prime ideal $\mathfrak{p} \mid \mathfrak{s}$ (with the exception of $(1+i)$) lies above a rational prime $p \equiv 1 \pmod 4$

(E) Distinct $\mathfrak{p}$ dividing $\mathfrak{s}$ lie above distinct p

(F) $\mathfrak{s}$ squarefree

Here $P^+(n)$ denotes the largest prime factor of n. Note that we have $\omega(\mathfrak{s}) = \omega(\|\mathfrak{s}\|)$. First, we will estimate from below the size of the set $\mathcal{M}_{\mathfrak{s}}$, defined to be the set of those $\pi \in \mathbb{Z}[i]$ with $\|\pi\| \leq x$ satisfying the following properties:

1. π prime (in $\mathbb{Z}[i]$)
2. $\|\pi\|$ prime (in $\mathbb{Z}$)
3. $\pi \equiv 1 \pmod{\mathfrak{s}}$
4. $P^-\left(\frac{\|\pi-1\|}{\|\mathfrak{s}\|}\right) > x^{1/100\gamma \log_2 x}$.

Here $P^-(n)$ denotes the smallest prime factor of n. The conditions on the size of the prime factors of $\|\mathfrak{s}\|$ and $\|\pi-1\|/\|\mathfrak{s}\|$ imply that each π with $\|\pi\| \leq x$ belongs to at most one of the sets $\mathcal{M}_{\mathfrak{s}}$. If k is chosen to be greater than $\gamma \log_2 x$, then carefully summing over $\mathfrak{s}$ satisfying the conditions above yields a lower bound on the count of distinct π corresponding to p with the property that $\omega(\#E(\mathbb{F}_p)) \geq k > \gamma \log_2 x$. The problem of counting elements π and $\overline{\pi}$ with $p = \pi\overline{\pi}$ is remedied by inserting a factor of $\frac{1}{2}$, which is of no concern for us.

More care is required in the case $0 < \gamma < 1$, which is handled in Section 3.5.3.

3.5.1 Preparing for the proof of Theorem 3.5.1.

Suppose the fixed ideal $\mathfrak{s}$ is generated by $\sigma \in \mathbb{Z}[i]$. We will estimate from below the size of $\mathcal{M}_{\mathfrak{s}}$ using Theorem 2.1. Define $\mathcal{A}$ to be the sequence of elements of $\mathbb{Z}[i]$ of the form

$$\left\{\frac{\pi-1}{\sigma} : \|\pi\| \leq x, \pi \text{ prime, and } \pi \equiv 1 \pmod{\sigma}\right\}.$$

Let $\mathcal{P}$ denote the set of prime ideals $\{\mathfrak{p} : \|\mathfrak{p}\| \leq z\}$, where $z := x^{1/50\gamma \log_2 x}$. Let $\mathfrak{P} := \prod_{\mathfrak{p}\in\mathcal{P}} \mathfrak{p}$. If $\frac{\pi-1}{\sigma} \equiv 0 \pmod{\mathfrak{p}}$ implies $\|\mathfrak{p}\| \geq z$, then all primes $p \mid \|\frac{\pi-1}{\sigma}\|$ have $p > x^{1/100\gamma \log_2 x}$. Note also that if a prime $\pi \in \mathbb{Z}[i]$, $\|\pi\| \leq x$ is such that $\|\pi\|$ is not prime, then $\|\pi\| = p^2$ for some rational prime p, and so the count of such π is clearly $O(\sqrt{x})$. Therefore, we have

$$\#\mathcal{M}_{\mathfrak{s}} \geq S(\mathcal{A}, \mathcal{P}) + O(\sqrt{x}).$$

Lemma 3.5.2. *With $\mathcal{M}_{\mathfrak{s}}$ defined as above, we have*

$$\#\mathcal{M}_{\mathfrak{s}} \geq c \cdot \frac{\mathrm{Li}(x)\log_2 x}{\Phi(\mathfrak{s})\log x} + O\Bigg(\sum_{\substack{\mathfrak{u}\mid\mathfrak{P}\\ \omega(\mathfrak{u})\leq m}} |r(\mathfrak{us})|\Bigg) + O\bigg(\frac{1}{\Phi(\mathfrak{s})}\frac{\mathrm{Li}(x)}{(\log x)^{22}}\bigg) + O(\sqrt{x}),$$

where $r(\mathfrak{v}) = |\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{v})} - \pi(x;\mathfrak{v},1)|$ and $c > 0$ is a constant.

Proof. First, note that we expect the size of $\mathcal{A}$ to be approximately $X := 4\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{s})}$. Write $A_{\mathfrak{u}} = \#\{a \in \mathcal{A} : \mathfrak{u} \mid a\}$. Then

$$A_{\mathfrak{u}} = X\delta(\mathfrak{u}) + r(\mathfrak{us}),$$

where $\delta(\mathfrak{u}) = \frac{\Phi(\mathfrak{s})}{\Phi(\mathfrak{us})}$ and $r(\mathfrak{us}) = |4\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{us})} - \pi(x;\mathfrak{us},1)|$. By Theorem 3.3.1, for any even integer $m \geq 0$ we have

$$\begin{aligned} S(\mathcal{A},\mathcal{P}) = 4\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{s})}\prod_{\|\mathfrak{p}\|\leq z}\bigg(1-\frac{\Phi(\mathfrak{s})}{\Phi(\mathfrak{ps})}\bigg) + O\Bigg(\sum_{\substack{\mathfrak{u}\mid\mathfrak{P}\\ \omega(\mathfrak{u})\leq m}} |r(\mathfrak{us})|\Bigg) \\ + O\bigg(\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{s})}\sum_{\substack{\mathfrak{u}\mid\mathfrak{P}\\ \omega(\mathfrak{u})\geq m}} \delta(\mathfrak{u})\bigg). \end{aligned}$$

Using Proposition 3.3.4, we have

$$\begin{aligned}\prod_{\|\mathfrak{p}\|\le z}\Big(1-\frac{\Phi(\mathfrak{s})}{\Phi(\mathfrak{p}\mathfrak{s})}\Big) &= \prod_{\substack{\|\mathfrak{p}\|\le z\\ \mathfrak{p}\nmid\mathfrak{s}}}\Big(1-\frac{1}{\Phi(\mathfrak{p})}\Big)\prod_{\substack{\|\mathfrak{p}\|\le z\\ \mathfrak{p}\mid\mathfrak{s}}}\Big(1-\frac{1}{\|\mathfrak{p}\|}\Big)\\ &= \prod_{\|\mathfrak{p}\|\le z}\Big(1-\frac{1}{\|\mathfrak{p}\|}\Big)\prod_{\substack{\|\mathfrak{p}\|\le z\\ \mathfrak{p}\nmid\mathfrak{s}}}\Big(1-\frac{1}{(\|\mathfrak{p}\|-1)^2}\Big)\\ &\gg \frac{1}{\log z}=\frac{\log_2 x}{\log x}.\end{aligned}$$

Take $m = 14\lfloor\log_2 x\rfloor$. We leave aside the first O-term and concentrate for now on the second. This term is handled in essentially the same way as in the proof of the upper bound: The sum in the this term is bounded from above by

$$\sum_{s\ge m}\frac{1}{s!}\Big(\sum_{\|\mathfrak{p}\|\le z}\delta(\mathfrak{p})\Big)^s.$$

By Proposition 3.3.4, we have

$$\sum_{\|\mathfrak{p}\|\le z}\delta(\mathfrak{p})\le\log_2 x+O(1).$$

Now, one sees once again by the ratio test that the sum on s is

$$\ll\frac{1}{m!}\Big(\sum_{\|\mathfrak{p}\|\le z}\delta(\mathfrak{p})\Big)^m\le\frac{1}{m!}(\log_2 x+O(1))^m.$$

Thus, by the same calculations as in the proof of Theorem 3.4.1, the second O-term is

$$\ll\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{s})(\log x)^{22}},$$

completing the proof of the lemma. □

We now sum this estimate over σ in an appropriate range to deal with the O-terms and establish a lower bound. Here, the cases $\gamma > 1$ and $0 < \gamma < 1$ diverge.

3.5.2 The case $\gamma > 1$.

The argument in this case is somewhat simpler. Recall that $\mathfrak{s}$ is chosen to satisfy properties A through F listed below Theorem 3.5.1; in particular, $\omega(\mathfrak{s}) = k$ for some integer k and $P^+(\|\mathfrak{s}\|) \leq x^{1/100\gamma \log_2 x}$. Choose $k := \lfloor \gamma \log_2 x \rfloor + 2$. Since $\omega(\|\mathfrak{s}\|) = \omega(\mathfrak{s})$, we have that $\|\mathfrak{s}\| \leq x^{k/100\gamma \log_2 x} \leq x^{1/10}$. A lower bound follows by estimating the quantity

$$\mathcal{M} = \sum_{\mathfrak{s}}{}' \#\mathcal{M}_{\mathfrak{s}},$$

where the prime indicates a restriction to those ideals $\mathfrak{s} \subset \mathbb{Z}[i]$ satisfying properties A through F mentioned above.

Lemma 3.5.3. *We have*

$$\mathcal{M} \gg \frac{x \log_2 x (\log_2 x + O(\log_3 x))^k}{k!(\log x)^2}.$$

Proof. Since $\sum_{\|\mathfrak{s}\| \leq x} 1/\Phi(\mathfrak{s}) \ll \log x$, the second O-term in Lemma 3.5.2 is, upon summing on $\mathfrak{s}$, bounded by a constant times $\mathrm{Li}(x)/(\log x)^{21}$. The third error term, $O(\sqrt{x})$, is therefore safely absorbed by this term.

We now handle the sum over $\mathfrak{s}$ of the first O-term. We have $|r(\mathfrak{us})| = |\pi(x; \mathfrak{us}, 1) - 4\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{us})}|$. We can think of the double sum (over $\mathfrak{s}$ and $\mathfrak{u}$) as a single sum over a modulus $\mathfrak{q}$, inserting a factor of $\tau(\mathfrak{q})$ to account for the number of ways of writing $\mathfrak{q}$ as a product of two ideals in $\mathbb{Z}[i]$. (Here, $\tau(\mathfrak{q})$ is the number of ideals in $\mathbb{Z}[i]$ which divide $\mathfrak{q}$.) Recalling our choice of

$m = 14\lfloor \log_2 x \rfloor$, we have

$$\sum_{\|\mathfrak{s}\| \le x^{1/10}} \sum_{\substack{\mathfrak{u} \mid \mathfrak{P} \\ \omega(\mathfrak{u}) \le m}} |r(\mathfrak{u}\mathfrak{s})| \ll \sum_{\|\mathfrak{q}\| < x^{2/5}} \Big| \pi(x; \mathfrak{q}, 1) - \frac{\mathrm{Li}(x)}{\Phi(\mathfrak{q})} \Big| \cdot \tau(\mathfrak{q}).$$

The restriction $\|\mathfrak{q}\| \le x^{2/5}$ comes from $\|\mathfrak{s}\| \le x^{1/10}$ and $\|\mathfrak{u}\| \le x^{m/50\gamma \log_2 x} \le x^{.28}$, recalling $m = 14\lfloor \log_2 x \rfloor$ and $\gamma > 1$. Now, for all $y > 0$ and nonzero $\mathfrak{i} \subset \mathbb{Z}[i]$ we have $\pi(y; \mathfrak{i}, 1) \ll y/\|\mathfrak{i}\|$; indeed, the same inequality is true with $\pi(y; \mathfrak{i}, 1)$ replaced by the count of all Gaussian integers $\equiv 1 \pmod{\mathfrak{i}}$. Thus

$$\Big| \pi(x; \mathfrak{q}, 1) - 4\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{q})} \Big| \ll \frac{x}{\Phi(\mathfrak{q})}.$$

Using this together with the Cauchy-Schwarz inequality and Proposition 3.3.2, we see that, for any $A > 0$,

$$\begin{aligned} \sum_{\|\mathfrak{q}\| < x^{2/5}} |\pi(x; \mathfrak{q}, 1) - 4\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{q})}| \tau(\mathfrak{q}) &\ll \sum_{\|\mathfrak{q}\| < x^{2/5}} |\pi(x; \mathfrak{q}, 1) - 4\frac{\mathrm{Li}(x)}{\Phi(\mathfrak{q})}|^{1/2} \Big(\frac{x}{\Phi(\mathfrak{q})} \Big)^{1/2} \tau(\mathfrak{q}) \\ &\ll \Big(x \sum_{\|\mathfrak{q}\| < x^{2/5}} \frac{\tau(\mathfrak{q})^2}{\Phi(\mathfrak{q})} \Big)^{1/2} \Big(\frac{x}{(\log x)^A} \Big)^{1/2}. \end{aligned}$$

We can estimate this sum using an Euler product:

$$\begin{aligned} \sum_{\|\mathfrak{q}\| < x^{2/5}} \frac{\tau(\mathfrak{q})^2}{\Phi(\mathfrak{q})} &\ll \prod_{\|\mathfrak{p}\| \le x^{2/5}} \Big(1 + \frac{4}{\|\mathfrak{p}\|} \Big) \\ &\le \exp \Big\{ \sum_{\|\mathfrak{p}\| \le x^{2/5}} \frac{4}{\|\mathfrak{p}\|} \Big\} \ll (\log x)^4. \end{aligned}$$

Collecting our estimates, we see that the total error is at most $x/(\log x)^{A/2-2}$, which is acceptable if A is chosen large enough.

For the main term, we need a lower bound for the sum

$$\mathcal{M} = \sum_{\mathfrak{s}}{}' \frac{1}{\Phi(\mathfrak{s})}. \tag{3.7}$$

Let $I = (e^{(\log_2 x)^2/k}, x^{1/10k})$. Define a collection of prime ideals $\mathcal{P}$ such that each $\mathfrak{p} \in \mathcal{P}$ lies above a prime $p \equiv 1 \pmod 4$, each prime $p \equiv 1 \pmod 4$ has exactly one prime ideal lying above it in $\mathcal{P}$, and $\|\mathfrak{p}\| \in I$. We apply Lemma 3.3.5, with the y_i chosen to be of the form $1/\Phi(\mathfrak{p})$ with $\mathfrak{p} \in \mathcal{P}$, obtaining

$$\begin{aligned} &\frac{1}{\Phi((1+i)^3)} \sum_{\mathfrak{s}:\mathfrak{p}\mid(\mathfrak{s}/(1+i)^3) \implies \mathfrak{p}\in\mathcal{P}}{}' \frac{1}{\Phi(\mathfrak{s}/(1+i)^3)} \\ &\qquad \gg \frac{1}{(k-1)!}\left(\sum_{\mathfrak{p}\in\mathcal{P}} \frac{1}{\Phi(\mathfrak{p})}\right)^{k-1}\left(1 - \binom{k-1}{2}\Big(\frac{1}{S_1^2}\Big)\sum_{\mathfrak{p}\in\mathcal{P}}\frac{1}{\Phi(\mathfrak{p})^2}\right), \end{aligned} \tag{3.8}$$

where

$$S_1 = \sum_{\mathfrak{p}\in\mathcal{P}} \frac{1}{\Phi(\mathfrak{p})}.$$

By Theorem 3.3.4, $S_1 = \frac{1}{2}\log_2 x - 2\log_3 x + O(1)$. This introduces a factor of $\frac{1}{2^{k-1}}$ to the right-hand side of (3.8), but this is of no concern: If each of the k prime factors of $\mathfrak{s}$, excluding $(1+i)$, lies above a distinct prime $p \equiv 1 \pmod 4$, then there are 2^{k-1} such ideals $\mathfrak{s}$ of a given norm. Thus, if we extend the sum on the left-hand side of (3.8) to range over all $\mathfrak{s}$ counted in primed sums (cf. the discussion above Lemma 3.5.3), we obtain

$$\begin{aligned} \sum_{\mathfrak{s}}{}' \frac{1}{\Phi(\mathfrak{s})} \geq \frac{2^{k-1}}{(k-1)!}&\left(\frac{1}{2}\log_2 x - 2\log_3 x + O(1)\right)^{k-1} \\ &\times \left(1 - \binom{k-1}{2}\Big(\frac{1}{S_1^2}\Big)\sum_{\mathfrak{p}\in\mathcal{P}}\frac{1}{\Phi(\mathfrak{p})^2}\right). \end{aligned}$$

The quantity $\binom{k-1}{2}$ is bounded from above by $\lceil \gamma \log_2 x \rceil^2$, and the sum on $1/\Phi(\mathfrak{p})^2$ tends to 0 as $x \to \infty$. Therefore,

$$1 - \binom{k-1}{2}\Big(\frac{1}{S_1^2}\Big)\sum_{\mathfrak{p}\in\mathcal{P}} \frac{1}{\Phi(\mathfrak{p})^2} \geq 1 - 4\gamma^2 \sum_{\mathfrak{p}\in\mathcal{P}} \frac{1}{\Phi(\mathfrak{p})^2} \geq \frac{1}{2}$$

for large enough x, and so

$$\frac{x \log_2 x}{(\log x)^2} \sum_{\mathfrak{s}}{}' \frac{1}{\Phi(\mathfrak{s})} \gg \frac{x \log_2 x (\log_2 x + O(\log_3 x))^{k-1}}{(k-1)!(\log x)^2},$$

as desired. □

With $k = \lfloor \gamma \log_2 x \rfloor + 2$ and by the more precise version of Stirling's formula $n! \sim \sqrt{2\pi n}(n/e)^n$, we have

$$\begin{aligned}
\frac{(\log_2 x + O(\log_3 x))^{k-1}}{(k-1)!} &\gg \frac{1}{\sqrt{\log_2 x}} \left(\frac{e \log_2 x + O(\log_3 x)}{\lfloor \gamma \log_2 x \rfloor} \right)^{\lceil \gamma \log_2 x \rceil} \\
&= \frac{1}{\sqrt{\log_2 x}} \left(\frac{e}{\gamma} \Big(1 + O\Big(\frac{\log_3 x}{\log_2 x} \Big) \Big) \right)^{\lceil \gamma \log_2 x \rceil} \\
&= (\log x)^{\gamma - \gamma \log \gamma + o(1)}.
\end{aligned}$$

This yields a main term of the shape

$$\frac{x}{(\log x)^{2+\gamma \log \gamma - \gamma + o(1)}},$$

which completes the proof of Theorem 3.5.1 in the case $\gamma > 1$.

3.5.3 The case $0 < \gamma < 1$.

Above, we used the fact that if $\pi - 1$ is divisible by certain $\mathfrak{s} \subset \mathbb{Z}[i]$ with $\omega(\|\mathfrak{s}\|) = k$, then $\|\pi - 1\|$ will have at least $k > \gamma \log_2 x$ prime factors. The case $0 < \gamma < 1$ is requires more care: We need to ensure that the quantity $\|\pi - 1\|/\|\mathfrak{s}\|$ does not have too many prime factors.

Lemma 3.5.4. *For any $\mathfrak{s} \subset \mathbb{Z}[i]$ satisfying properties A through F listed below Theorem 3.5.1, we have*

$$\#\{\pi \in \mathcal{M}_{\mathfrak{s}} : \omega\bigg(\frac{\|\pi - 1\|}{\|\mathfrak{s}\|}\bigg) > \frac{\log_2 x}{\log_4 x}\} \ll \frac{x}{\|\mathfrak{s}\|(\log x)^A}.$$

Upon discarding those π counted by the above lemma, the remaining π will have the property that $\omega(\|\pi - 1\|) \in [k, k + \log_2 x/\log_4 x]$. Choosing k to be the greatest integer strictly less than $\gamma \log_2 x - \log_2 x/\log_4 x$ ensures that $\|\pi - 1\| < \gamma \log_2 x$.

Proof of Lemma 3.5.4. We begin with the observation that, for any $\mathfrak{s} \subset \mathbb{Z}[i]$ under consideration and $\pi \in \mathcal{M}_{\mathfrak{s}}$, we have $\|\pi - 1\|/\|\mathfrak{s}\| \le 2x/\|\mathfrak{s}\|$. Therefore, we estimate

$$\sum_{\substack{\|\mathfrak{a}\| \le \frac{2x}{\|\mathfrak{s}\|} \\ \omega(\|\mathfrak{a}\|) > \log_2 x/\log_4 x \\ P^-(\|\mathfrak{a}\|) > x^{1/100\gamma \log_2 x}}} 1 \le \frac{2x}{\|\mathfrak{s}\|} \sum_{\substack{\|\mathfrak{a}\| \le \frac{2x}{\|\mathfrak{s}\|} \\ \omega(\|\mathfrak{a}\|) > \log_2 x/\log_4 x \\ P^-(\|\mathfrak{a}\|) > x^{1/100\gamma \log_2 x}}} \frac{1}{\|\mathfrak{a}\|}.$$

Noting that $\omega(\|\mathfrak{a}\|) \le \omega(\mathfrak{a})$ for any $\mathfrak{a} \subset \mathbb{Z}[i]$, by Theorem 3.3.4 and Stirling's formula, we have

$$\begin{aligned}
\sum_{\substack{\|\mathfrak{a}\| \le \frac{2x}{\|\mathfrak{s}\|} \\ \omega(\|\mathfrak{a}\|) > \log_2 x/\log_4 x \\ P^-(\|\mathfrak{a}\|) > x^{1/100 \log_2 x}}} \frac{1}{\|\mathfrak{a}\|} &\le \sum_{\substack{\|\mathfrak{a}\| \le \frac{2x}{\|\mathfrak{s}\|} \\ \omega(\mathfrak{a}) > \log_2 x/\log_4 x \\ P^-(\|\mathfrak{a}\|) > x^{1/100 \log_2 x}}} \frac{1}{\|\mathfrak{a}\|} \\
&\le \sum_{\ell > \log_2 x/\log_4 x} \frac{1}{\ell!} \Big(\sum_{x^{1/100 \log_2 x} \le \|\mathfrak{p}\| \le \frac{2x}{\|\mathfrak{s}\|}} \sum_{m=1}^{\infty} \frac{1}{\|\mathfrak{p}\|^m} \Big)^{\ell} \\
&\ll \sum_{\ell > \log_2 x/\log_4 x} \Big(\frac{e \log_3 x + O(1)}{\ell} \Big)^{\ell}.
\end{aligned}$$

For each $\ell > \log_2 x/\log_4 x$, we have $(e\log_3 x + O(1))/\ell < 1/2$. Thus

$$\sum_{\ell > \log_2 x/\log_4 x} \Big(\frac{e\log_3 x + O(1)}{\ell}\Big)^{\ell} \ll \Big(\frac{e\log_3 x + O(1)}{\lfloor \log_2 x/\log_4 x\rfloor + 1}\Big)^{\lfloor \log_2 x/\log_4 x\rfloor + 1}$$
$$\ll \Big(\frac{1}{(\log_2 x)^{1+o(1)}}\Big)^{\log_2 x/\log_4 x} \ll e^{-2\log_2 x \log_3 x/\log_4 x}.$$

This last expression is smaller than $(\log x)^{-A}$, for any $A > 0$. Therefore, for any fixed $A > 0$,

$$\#\{\pi \in \mathcal{M}_{\mathfrak{s}} : \omega\Big(\frac{\|\pi - 1\|}{\|\mathfrak{s}\|}\Big) > \frac{\log_2 x}{\log_4 x}\} \ll \frac{x}{\|\mathfrak{s}\|(\log x)^A}. \qquad \square$$

Write

$$\mathcal{M}'_{\mathfrak{s}} = \{\pi \in \mathcal{M}_{\mathfrak{s}} : \omega\Big(\frac{\|\pi - 1\|}{\|\mathfrak{s}\|}\Big) \le \frac{\log_2 x}{\log_4 x}\}.$$

Lemmas 3.5.2 and 3.5.4 show that $\#\mathcal{M}'_{\mathfrak{s}}$ satisfies

$$\#\mathcal{M}'_{\mathfrak{s}} \ge c \cdot \frac{x\log_2 x}{\Phi(\mathfrak{s})(\log x)^2} + O\Big(\sum_{\substack{\mathfrak{u}|\mathfrak{P}\\ \omega(\mathfrak{u})\le m}} |r(\mathfrak{u}\mathfrak{s})|\Big)$$
$$+ O\Big(\frac{1}{\Phi(\mathfrak{s})}\frac{\mathrm{Li}(x)}{(\log x)^{22}}\Big) + O\Big(\frac{x}{\|\mathfrak{s}\|(\log x)^A}\Big) + O(\sqrt{x}),$$

for any $A > 0$. Here, all quantities are defined as in the previous section. Just as before, we sum this quantity over $\mathfrak{s} \subset \mathbb{Z}[i]$ satisfying conditions A through F listed below Theorem 3.5.1. Letting $'$ on a sum indicate a restriction to such $\mathfrak{s}$, we have, by the same calculations as before,

$$\mathcal{M}' \gg \frac{x\log_2 x(\log_2 x + O(\log_3 x))^{k-1}}{(k-1)!(\log x)^2},$$

where

$$\mathcal{M}' = \sum_{\mathfrak{s}}{}' \#\mathcal{M}'_{\mathfrak{s}}.$$

Recall that k is chosen to be the largest integer strictly less than $\gamma \log_2 x - \log_2 x/\log_4 x$; then by Stirling's formula,

$$\begin{aligned}\frac{(\log_2 x + O(\log_3 x))^{k-1}}{(k-1)!} &\gg \frac{1}{\sqrt{\log_2 x}}\Big(\frac{e\log_2 x + O(\log_3 x)}{k-1}\Big)^{k-1} \\ &\gg \frac{1}{\sqrt{\log_2 x}}\Big(\frac{e}{\gamma}\Big(1+O\big(\frac{1}{\log_4 x}\big)\Big)\Big)^{\gamma\log_2 x - \log_2 x/\log_4 x - 1} \\ &\gg (\log x)^{\gamma\log\gamma - \gamma + o(1)}.\end{aligned}$$

A final assembly of estimates yields Theorem 3.5.1 in the case $0 < \gamma < 1$.

3.6 Generalizing to other CM elliptic curves

Let $E_1/\mathbb{Q}$ and $E_2/\mathbb{Q}$ be elliptic curves with complex multiplication. An *isogeny* from E_1 to E_2 is a homomorphism $\alpha : E_1(\overline{\mathbb{Q}}) \to E_2(\overline{\mathbb{Q}})$ defined by

$$\alpha(x_1, y_1) = (R_1(x_1, y_1), R_2(x_1, y_1)),$$

where R_1 and R_2 are rational functions. The isogeny is said to be $\mathbb{Q}$-*rational* if the coefficients of the functions R_1 and R_2 belong to $\mathbb{Q}$. By clearing denominators, we can assume that the coefficients of rational functions defining a $\mathbb{Q}$-rational isogeny belong to $\mathbb{Z}$.

Suppose $E/\mathbb{Q}$ has CM by an order in the imaginary quadratic field K. It is known ([CCS13, Proposition 25]) that there is a $\mathbb{Q}$-rational isogeny from a CM elliptic curve $E/\mathbb{Q}$ to an elliptic curve $E'/\mathbb{Q}$, where E' has CM by the maximal order $\mathbb{Z}_K$. By reducing coefficients modulo p, this $\mathbb{Q}$-rational isogeny induces an $\mathbb{F}_p$-rational isogeny for all but finitely many primes p, and this implies that $\#E(\mathbb{F}_p) = \#E'(\mathbb{F}_p)$ for all but finitely many primes p. Thus, for the purpose of our present result, we assume that E has CM by the maximal order $\mathbb{Z}_K$.

Let p be a sufficiently large prime of ordinary reduction for the elliptic curve $E/\mathbb{Q}$. Then $\#E(\mathbb{F}_p) = \|\pi - 1\|$ for some prime $\pi \in \mathbb{Z}_K$ lying above p. In the case $E : y^2 = x^3 - x$ worked out above, we chose $\pi \equiv 1 \pmod{(1+i)^3}$. In general, explicit formulas for $\#E(\mathbb{F}_p)$ (and thus the choice of π) can be determined from the following table, which is a reproduction of Table 2 in [JU08]. The notation is as follows: Let $K = \mathbb{Q}(\sqrt{D})$, and let $E : y^2 = x^3 + g_4 x + g_6$ be an elliptic curve over $\mathbb{Q}$ with CM by the maximal order $\mathbb{Z}_K \subset K$. With this setup, a prime $\pi \in \mathbb{Z}_K$, $\pi = (u + v\sqrt{D})/2$, is primary if $\pi \equiv 1 \pmod{(1+i)^3}$ and $D = -1$, if $\pi \equiv 2 \pmod 3$ and $D = -3$, or if $\Re(\pi) > 0$ for other choices of D. Table 3.1 gives a formula for the number $a_p := p + 1 - \#E(\mathbb{F}_p)$. In the table, $(\cdot)_m$ denotes the mth-power residue symbol, and for $d \neq 8$, $\chi_{\pi,d}(g) = \epsilon(\epsilon g/p)(u/d)u$ where $\epsilon = (-1)^{(d^2-1)/8}$. If $d = 8$, $\chi_{\pi,8}(g) = -(g/p)(-1)^k(-1/U)u$ where $U = u/2$ and $k = \lfloor p/8 \rfloor$.

Table 3.1: Formula for a_p; see [JU08, Table 2]

D	(g_4, g_6)	a_p
$D = -3$	$(0, g)$	$-(\frac{4g}{\overline{\pi}})_6\pi - (\frac{4g}{\pi})_6\overline{\pi}$
$D = -4$	$(-g, 0)$	$(\frac{g}{\overline{\pi}})_4\pi + (\frac{g}{\pi})_4\overline{\pi}$
$D = -8$	$(-5 \cdot 2g^2/3, -14 \cdot 2^2 g^3/27)$	$\chi_{\pi,8}(g)u$
$D = -7$	$(-5 \cdot 7g^2/16, -7^2 g^3/32)$	$\chi_{\pi,7}(g)u$
$D = -11$	$(-2 \cdot 11g^2/3, -7 \cdot 11^2 g^3/108)$	$\chi_{\pi,11}(g)u$
$D = -19$	$(-2 \cdot 19g^2, -19g^3/4)$	$\chi_{\pi,19}(g)u$
$D = -43$	$(-20 \cdot 43g^2, -21 \cdot 43^2 g^3/4)$	$\chi_{\pi,43}(g)u$
$D = -67$	$(-110 \cdot 67g^2, -217 \cdot 67^2 g^3/4)$	$\chi_{\pi,67}(g)u$
$D = -163$	$(-13340 \cdot 163g^2, -185801 \cdot 163^2 g^3/4)$	$\chi_{\pi,163}(g)u$

Let us consider an example. Take $D = -11$; then E satisfies a Weierstrass equation of the form

$$y^2 = x^3 - \frac{2 \cdot 11g^2}{3}x - \frac{7 \cdot 11^2 g^3}{108}$$

for some integer g. Let p be a sufficiently large prime of good ordinary reduction and write $p = \pi\overline{\pi}$, with $\pi = (u + v\sqrt{-11})/2 \in \mathbb{Z}_K$. Notice that $\pi + \overline{\pi} = u$. If $a_p = u$, then

$$\#E(\mathbb{F}_p) = p + 1 - (\pi + \overline{\pi}) = \|\pi - 1\|.$$

According to Table 3.1, $a_p = u$ if

$$\chi_{\pi,11} = \epsilon(\frac{\epsilon g}{p})(\frac{u}{11}) = 1.$$

By definition, $\epsilon = (-1)^{(11^2-1)/8} = -1$, so we require that $(g/p)(u/11) = 1$. By quadratic reciprocity, whether this is true is determined by the residue class of $p \pmod{g}$ and $u \pmod{11}$, and these classes are determined by the residue class of $\pi \pmod{11g}$ in $\mathbb{Z}_K$. These congruence conditions replace the requirement in the argument of the preceding sections that $\pi \equiv 1 \pmod{(1+i)^3}$. For other curves with CM by an order in another imaginary quadratic field, one uses the corresponding data in the table, and the situation is entirely similar.

Chapter 4

Bounded gaps between primes

4.1 Preliminaries

4.1.1 The field $\mathbb{F}_q(t)$.

Let q be a power of a prime number, and consider the field $K := \mathbb{F}_q(t)$ of rational functions with coefficients in the finite $\mathbb{F}_q$. There are a number of parallels between K and $\mathbb{Q}$. Like $\mathbb{Z} \subset \mathbb{Q}$, the ring of integers $\mathbb{F}_q[t]$ of K is a principal ideal domain. For $f \in \mathbb{F}_q[t]$, set $|f| = q^{\deg(f)}$; this is analogous to the absolute value of an integer n, as

$$|n| = |\mathbb{Z}/n\mathbb{Z}| \quad \text{and} \quad |f| = |\mathbb{F}_q[t]/f\mathbb{F}_q[t]|.$$

In particular, the residue class ring corresponding to an ideal $(f) \subset \mathbb{F}_q[t]$ is finite. Both $\mathbb{Z}$ and $\mathbb{F}_q[t]$ have finitely many units (in the latter case, these are $(\mathbb{F}_q)^\times$), and both have infinitely many prime elements, where $f \in \mathbb{F}_q[t]$ is *prime* if f is monic and irreducible.

Owing to these similarities, it is natural to ask whether results which hold in $\mathbb{Z}$ have analogues in $\mathbb{F}_q[t]$. Often, the answer is yes; in particular, the Maynard-Tao machinery (see Section 1.1.4) can be utilized to probe questions concerning bounded gaps between primes

in $\mathbb{F}_q[t]$. The following theorem, a direct analogue of Maynard's theorem for $\mathbb{F}_q[t]$, is due to Castillo, Hall, Lemke Oliver, Pollack, and Thompson [CHL$^+$15].

Theorem 4.1.1. *Let $m \geq 2$. There exists an integer k_0 depending on m but independent of q such that for any admissible k-tuple $\{h_1, \dots, h_k\} \subset \mathbb{F}_q[t]$ with $k \geq k_0$, there are infinitely many $f \in \mathbb{F}_q[t]$ such that at least m of $f + h_1, \dots, f + h_k$ are prime.*

In particular, if $\{h_1, \dots, h_k\} \subset \mathbb{F}_q[t]$ is a long enough admissible tuple, the difference in norm between primes in $\mathbb{F}_q[t]$ is at most $\max_{1 \leq i \neq j \leq k} |h_i - h_j|$, infinitely often.

4.1.2 Artin's primitive root conjecture.

Artin's famous primitive root conjecture states that for any integer $g \neq -1$ and not a square, there are infinitely many primes for which g is a primitive root; that is, there are infinitely many primes p for which g generates $(\mathbb{Z}/p\mathbb{Z})^*$. Though this conjecture remains unproved, substantial progress has been made by several authors. Heath-Brown [HB86], by refining methods of Gupta and Murty [GM84], proved that there are infinitely many primes p possessing one of $\{q, r, s\}$ as a primitive root, where q, r and s are integers satisfying certain technical conditions; for example, q, r and s can be any three distinct primes, establishing that at most two primes are not primitive roots for infinitely many primes.

In 1967, Hooley [Hoo67] established the truth of Artin's conjecture, conditional on the Generalized Riemann Hypothesis. We shall give a brief overview of Hooley's method, following Murty's wonderfully readable survey [Mur88]. Fix an integer a not equal to -1 and not a square. The number a is a primitive root modulo p if and only if, for all primes $q \mid p - 1$, $a^{(p-1)/q} \not\equiv 1 \pmod{p}$. We will say that p "fails the q-test" if

$$p \equiv 1 \pmod{q} \quad \text{and} \quad a^{\frac{p-1}{q}} \equiv 1 \pmod{p}. \tag{4.1}$$

Now, the conditions 4.1 are equivalent to p splitting completely in the field $K_q := \mathbb{Q}(\zeta_q, a^{1/q})$. Let $N_a(x)$ denote the number of primes $p \leq x$ possessing a as a primitive root, and for squarefree k let P_k denote the count of primes that split completely in K_q for some $q \mid k$. The quantity $P_2 + P_3 + P_5 + \ldots$ overcounts those primes that split completely in more than one of the K_q (note that the sum is actually finite, since $P_q = 0$ for $q > x$). We apply the principle of inclusion-exclusion and obtain

$$N_a(x) = \sum_{k=1}^{\infty} \mu(k) P_k,$$

where μ is the Möbius function.

A prime $p \leq x$ is counted by P_k if p splits completely in the compositum L_k of the fields K_q for $q \mid k$. An effective version of the Chebotarev density theorem gives an estimate for P_k; however, the error term in this estimate is too large for k outside of a small range. The Generalized Riemann Hypothesis implies that

$$P_k = \frac{1}{[L_k : \mathbb{Q}]} \frac{x}{\log x} + O(x^{1/2} \log(kx)), \tag{4.2}$$

as $x \to \infty$. Unfortunately, inserting this estimate into the above sum for $N_a(x)$ results in an accumulation of error terms that is still too large.

Set $K = \prod_{p \leq z} p$. Hooley noticed that

$$N_a(x) \leq \sum_{d \mid K} \mu(d) P_d,$$

since primes counted by the right-hand side pass the q test for $q \leq z$, and that

$$N_a(x) \geq \sum_{d \mid K} \mu(d) P_d - M(x; z, x),$$

where $M(x; z, w)$ is the count of primes $p \leq x$ that fail the q-test. Assuming GRH, (4.2) implies that

$$N_a(x) = c_a \frac{x}{\log x} + O\Big(\frac{x}{\log^2 x}\Big) + O(M(x; z, x)).$$

The term $O(M(x; z, x))$ is handled by writing

$$M(x; z, x) = M(x; z, \frac{x^{1/2}}{\log^2 x}) + M(x; \frac{x^{1/2}}{\log^2 x}, x^{1/2} \log x) + M(x; x^{1/2} \log x, x).$$

The first term can be handled using the Chebotarev density theorem with error term coming from GRH; the Brun-Titchmarsh theorem (Theorem 1.3.4) is the primary tool in dealing with the second term; and the last is estimated using a clever, elementary argument. The upshot is that, on GRH, to each integer not -1 and not a square, there corresponds an infinite set of primes. In light of the breakthrough of Maynard-Tao, one can ask: Does this sequence of primes have a bounded gaps property? The following result due to Pollack [Pol14a] answers this question.

Theorem 4.1.2 (conditional on GRH)**.** *Fix an integer $g \neq -1$ and not a square. Let $q_1 < q_2 < \ldots$ denote the sequence of primes for which g is a primitive root. Then for each m,*

$$\liminf_{n \to \infty} (q_{n+m-1} - q_n) \leq C_m,$$

where C_m is finite and depends on m but not on g.

Artin's conjecture can be formulated in the setting of polynomials over a finite field with q elements, where q is a prime power. Let $g \in \mathbb{F}_q[t]$ be monic and not a vth power, for any v dividing $q - 1$; this is analogous to the requirement that g not be a square in the integer case. We say that g is a primitive root for a prime polynomial $p \in \mathbb{F}_q[t]$ if g generates the group $(\mathbb{F}_q[t]/p\mathbb{F}_q[t])^*$. In Bilharz's 1937 Ph.D. thesis [Bil37], he confirms Artin's conjecture that

there are infinitely many such p for a given g satisfying the above requirements, conditional on the Riemann Hypothesis for global function fields, a result proved by Weil in 1948.

Motivated by the results catalogued above, we presently establish an unconditional result which can be viewed as a synthesis of Theorems 4.1.1 and 4.1.2.

Theorem 4.1.3. *Let g be a monic polynomial in $\mathbb{F}_q[t]$ such that g is not a vth power for any prime v dividing $q-1$, and let $\mathbb{P}_g$ denote the set of prime polynomials in $\mathbb{F}_q[t]$ for which g is a primitive root. For any $m \geq 2$, there exists an admissible k-tuple $\{h_1, \dots, h_k\}$ such that there are infinitely many $f \in \mathbb{F}_q[t]$ with at least m of $f+h_1, \dots, f+h_k$ belonging to $\mathbb{P}_g$.*

Remark 4.1.4. A prime polynomial $a \in \mathbb{F}_q[t]$ is called *primitive* if t is a primitive root for a; see [LN97] for an overview of primitive polynomials. Taking $g = t$, we obtain as an immediate corollary the existence of bounded gaps between primitive polynomials.

Notation. The Greek letter Φ will denote the Euler phi function for $\mathbb{F}_q[t]$; that is, $\Phi(f) = \#(\mathbb{F}_q[t]/f\mathbb{F}_q[t])^*$. For $d, e \in \mathbb{Z}$, we write $[d,e] = \operatorname{lcm}(d,e)$. We let $\tau_k(n)$ denote the number of (ordered) factorizations of n into k factors. As usual, we write $\mu(n)$ for the M obius function applied to n; for $f \in \mathbb{F}_q[t]$, $\mu(f) = (-1)^m$ where m is the number of distinct prime polynomials dividing f. Other notation will be defined as necessary.

4.2 The necessary tools

For a monic polynomial a and a prime polynomial P not dividing a in $\mathbb{F}_q[t]$, define the d-th power residue symbol $(a/P)_d$ to be the unique element of $\mathbb{F}_q^*$ such that

$$a^{\frac{|P|-1}{d}} \equiv \left(\frac{a}{P}\right)_d \pmod{P}.$$

Let $b \in \mathbb{F}_q[t]$ be monic, and write $b = P_1^{e_1} \cdots P_s^{e_s}$, where $P_1, \ldots, P_s$ are distinct prime polynomials. Define

$$\left(\frac{a}{b}\right)_d = \prod_{j=1}^{s} \left(\frac{a}{P_j}\right)_d^{e_j}.$$

We will make use of a number of properties of the dth power residue symbol. The following is taken from Propositions 3.1 and 3.4 of [Ros02].

Proposition 4.2.1. *The dth power residue symbol has the following properties.*

(a) $\left(\frac{a_1}{b}\right)_d = \left(\frac{a_2}{b}\right)_d$ *if* $a_1 \equiv a_2 \pmod{b}$.

(b) Let $\zeta \in \mathbb{F}_q^*$ be an element of order dividing d. Then, for any prime $P \in \mathbb{F}_q[t]$ with $P \nmid a$, there exists $a \in \mathbb{F}_q[t]$ such that $\left(\frac{a}{P}\right)_d = \zeta$.

We now state a special case of the general reciprocity law for dth power residue symbols in $\mathbb{F}_q[t]$, Theorem 3.5 in [Ros02]:

Theorem 4.2.2. *Let $a, b \in \mathbb{F}_q[t]$ be monic, nonzero and relatively prime. Then*

$$\left(\frac{a}{b}\right)_d = \left(\frac{b}{a}\right)_d (-1)^{\frac{q-1}{d} \deg(a) \deg(b)}.$$

Another essential tool in our analysis is the Chebotarev density theorem; first, let us set up some notation. Recall that $K = \mathbb{F}_q(t)$, and let P be a prime element in the ring of integers of K. Suppose L/K is a finite Galois extension of function fields. For each unramified prime $\mathfrak{P}$ lying above P, there is an automorphism $(\mathfrak{P}, L/K)$ characterized by

$$(\mathfrak{P}, L/K)\omega \equiv \omega^{q^{\deg P}} \pmod{\mathfrak{P}}$$

for all $\omega \in O_{\mathfrak{P}}$, where $O_{\mathfrak{P}}$ is the set of $\beta \in L$ such that β is integral at $\mathfrak{P}$. These automorphisms are conjugate to one another; that is, if $\mathfrak{P}_1$ and $\mathfrak{P}_2$ are unramified primes lying above $P \in K$,

then there is some $\sigma \in \mathrm{Gal}(L/K)$ such that

$$(\mathfrak{P}_1, L/K) = \sigma(\mathfrak{P}_2, L/K)\sigma^{-1}.$$

We define the *Artin symbol* $\left(\frac{L/K}{P}\right)$ to be the conjugacy class of such automorphisms. We refer the reader to Chapter 9 of [Ros02] for more details of these constructions.

Let $q = p^k$, where p is a rational prime. For a finite field $\mathbb{F}_{q^n}$, define $\mathrm{Frob}_q : \mathbb{F}_{q^n} \to \mathbb{F}_{q^n}$ by $\mathrm{Frob}_q(a) = a^q$. The field $\mathbb{F}_q$ has exactly one extension of degree n, namely $\mathbb{F}_{q^n}$, for all $n \in \mathbb{N}$. The extension $\mathbb{F}_{q^n}/\mathbb{F}_q$ is Galois, and it turns out that the map Frob_q generates $\mathrm{Gal}(\mathbb{F}_{q^n}/\mathbb{F}_q)$.

We are now prepared to state the Chebotarev density theorem. The following is a restatement of Proposition 6.4.8 in [FJ08].

Theorem 4.2.3. *Let L be a finite Galois extension of K, and let $\mathcal{C}$ be a conjugacy class of $\mathrm{Gal}(L/K)$. Let $\mathbb{F}_{q^n}$ be the constant field of L/K. For each $\tau \in \mathcal{C}$, suppose $\mathrm{res}_{\mathbb{F}_{q^n}} \tau = \mathrm{res}_{\mathbb{F}_{q^n}} \mathrm{Frob}_q^k$, where $k \in \mathbb{N}$. The number of unramified primes P of degree k whose Artin symbol $\left(\frac{L/K}{P}\right)$ is $\mathcal{C}$ is given by*

$$\frac{\#\mathcal{C}}{m}\frac{q^k}{k} + O\left(\frac{\#\mathcal{C}}{m}\frac{q^{k/2}}{k}(m + g_L)\right),$$

where $m = [L : K\mathbb{F}_{q^n}]$, g_L is the genus of L/K, and the constant implied by the big-O is absolute.

We mention above that Weil's proof of the Riemann Hypothesis for curves allows the result of the present chapter to be unconditional. In particular, the size of the O-term in Theorem 4.2.3 is a consequence of Weil's work.

4.2.1 Cyclotomic function fields

Fix an algebraic closure $\overline{K}$ of K. One can define an analogue of exponentiation in $\mathbb{F}_q[t]$ as follows. Let A denote the $\mathbb{F}_q$-algebra of $\mathbb{F}_q$-endomorphisms of the additive group of K; in other words,

$$A = \{\varphi : \overline{K} \to \overline{K} : \varphi(a+b) = \varphi(a) + \varphi(b), \varphi(\alpha a) = \alpha\varphi(a) \ \ \forall \alpha \in \mathbb{F}_q, a, b \in \overline{K}\}.$$

Let Frob_q denote the Frobenius automorphism of $\overline{K}/\mathbb{F}_q$ (so $\mathrm{Frob}_q(u) = u^q$ for all $u \in \overline{K}$), and let μ_t denote the multiplication-by-t map. Define a map

$$\xi : \mathbb{F}_q[t] \to A, \quad \xi(f(t)) = f(\mathrm{Frob}_q + \mu_t),$$

so for $f(t) = a_n t^n + \cdots + a_1 t + a_0 \in \mathbb{F}_q[t]$ and $u \in \overline{K}$,

$$\xi(f(t))(u) = f(\mathrm{Frob}_q + \mu_t)(u) = a_n(\mathrm{Frob}_q + \mu_t)^n(u) + \cdots + a_1(\mathrm{Frob}_q + \mu_t)(u) + a_0(u).$$

Let $u \in \overline{K}$ and $M \in \mathbb{F}_q[t]$. Define

$$u^M := M(\mathrm{Frob}_q + \mu_t)(u).$$

In other words, $u^M = \xi(M)(u)$. One readily checks that $u^{M+N} = u^M + u^N$ and $u^{MN} = (u^M)^N$, and we consider this an analogue of exponentiation in this setting.

Define $\Lambda_M := \{u \in \overline{K} : u^M = 0\}$. It turns out that Λ_M is an $\mathbb{F}_q[t]$-submodule of $\overline{K}$; it is called the *Carlitz-Hayes module of* M. For $M \in \mathbb{F}_q[t]$, we call extensions of the form $K(\Lambda_M)/K$ *cyclotomic* extensions, since these extensions have many properties similar to those of cyclotomic extensions of $\mathbb{Q}$. For example, the extension $K(\Lambda_M)/K$ is a geometric (that is, the constant field of $K(\Lambda_M)$ is the same as the constant field of K) Galois extension

of degree $\Phi(M)$, and a prime $P \in K$ is ramified in $K(\Lambda_M)/K$ only if P divides M (just like a prime $p \in \mathbb{N}$ is ramified in $\mathbb{Q}(\zeta_n)/\mathbb{Q}$ only if $p \mid n$). See Chapter 12 of [Sal07] for details of this construction and for further properties of these extensions.

In our application, the extension L/K will be the compositum of a Kummer extension and a cyclotomic extension of K. The next three results will help us estimate g_L, the genus of the extension L/K.

We begin with Castelnuovo's inequality (Theorem 3.11.3 in [Sti09]), which says that if a function field L/k with constant field k is the compositum of two subfields K_1/k and K_2/k, we can estimate the genus of L given the genera of K_1 and K_2 as follows.

Proposition 4.2.4. *Let K_1/k and K_2/k be subfields of L/k satisfying*

- *$L = K_1K_2$ is the compositum of K_1 and K_2, and*
- *$[L : K_i] = n_i$ and K_i/K has genus g_i, $i = 1, 2$.*

Then the genus g_L of L/K is bounded by

$$g_L \leq n_1g_1 + n_2g_2 + (n_1 - 1)(n_2 - 1).$$

We say that an element $a \in K^*$ is *geometric* at a prime number $r \neq q$ if $K(\sqrt[r]{a})$ is a geometric field extension of K. Proposition 10.4 in [Ros02] concerns the genus of such extensions; we state it below.

Proposition 4.2.5. *Suppose r is a prime not equal to the characteristic of $\mathbb{F}_q$ and $K' = K(\sqrt[r]{a})$, $a \in K$ nonzero. Assume that a is geometric at r and that a is not an rth power in K^*. With $g_{K'}$ denoting the genus of K'/K,*

$$2g_{K'} - 2 = -2r + R_a(r - 1),$$

where R_a is the sum of the degrees of the finitely many primes $P \in K$ where the order of P in a is not divisible by r.

The following proposition, a formula for the genus of cyclotomic extensions of K, is taken from [Sal07, Theorem 12.7.2].

Proposition 4.2.6. *Let $M \in \mathbb{F}_q[t]$ be monic of the form $M = \prod_{i=1}^{r} P_i^{\alpha_i}$, where the P_i are distinct prime polynomials. Then*

$$2g_M - 2 = -2\Phi(M) + \sum_{i=1}^{r} d_i s_i \frac{\Phi(M)}{\Phi(P_i^{\alpha_i})} + (q-2)\frac{\Phi(M)}{q-1},$$

where g_M is the genus of $K(\Lambda_M)/K$, $d_i = \deg P_i$, and $s_i = \alpha_i \Phi(P_i^{\alpha_i}) - q^{d_i(\alpha_i - 1)}$.

4.3 Maynard-Tao over $\mathbb{F}_q(t)$

We now briefly recall the Maynard-Tao method as adapted for the function field setting in [CHL+15]. Fix an integer $k \geq 2$, and let $\mathcal{H} = \{h_1, \ldots, h_k\}$ be an admissible k-tuple of elements of $\mathbb{F}_q[t]$ (that is, for each prime $p \in \mathbb{F}_q[t]$, the set $\{h_i \pmod p : 1 \leq i \leq k\}$ is not a complete set of residues modulo p). With $\mathbb{P}$ denoting the set of prime polynomials in $\mathbb{F}_q[t]$, let

$$W = \prod_{\substack{p \in \mathbb{P} \\ |p| < \log\log\log(q^\ell)}} p.$$

Define sums S_1 and S_2 as follows:

$$S_1 = \sum_{\substack{n \in A(\ell) \\ n \equiv \beta \pmod W}} \omega(n)$$

and

$$S_2 = \sum_{\substack{n \in A(\ell) \\ n \equiv \beta \pmod{W}}} \left(\sum_{i=1}^{k} \chi_{\mathbb{P}}(n + h_i) \right) \omega(n),$$

where $A(\ell)$ is the set of all monic polynomials in $\mathbb{F}_q[t]$ of norm q^ℓ (i.e., degree ℓ), $\beta \in \mathbb{F}_q[t]$ is chosen so that $(\beta + h_i, W) = 1$ for all $1 \leq i \leq k$ (such a β exists by the admissibility of $\mathcal{H}$), and

$$\omega(n) = \left(\sum_{\substack{d_1, \ldots, d_k \\ d_i | (n+h_i) \forall i}} \lambda_{d_1 \ldots, d_k} \right)^2$$

for suitably chosen weights $\lambda_{d_1 \ldots, d_k}$. Suppose $S_2 > (m-1)S_1$, for some integer $m \geq 2$ and some choice of weights; then there exists $n_0 \in A(\ell)$ such that at least m of the $n_0 + h_1, \ldots, n_0 + h_k$ are prime. The goal is to find a sequence of such $n_0 \in A(\ell)$ as $\ell \to \infty$. If this can be done, then infinitely often we obtain gaps between primes of size at most $\max_{1 \leq i,j \leq k : i \neq j} |h_i - h_j|$.

For the choice of suitable weights and the subsequent asymptotic formulas for S_1 and S_2, we refer to Proposition 2.3 of [CHL$^+$15], which we restate here for convenience:

Proposition 4.3.1. *Let $0 < \theta < \frac{1}{4}$ be a real number and set $R = |A(\ell)|^\theta = q^{\ell\theta}$. Let F be a piecewise differentiable real-valued function supported on the simplex $\mathcal{R}_k := \{(x_1, \ldots, x_k) \in [0,1]^k : \sum_{i=1}^k x_i \leq 1\}$, and let*

$$F_{\max} := \sup_{(t_1, \ldots, t_k) \in [0,1]^k} |F(t_1, \ldots, t_k)| + \sum_{i=1}^{k} \left| \frac{\partial F}{\partial x_i}(t_1, \ldots, t_k) \right|.$$

Set

$$\lambda_{d_1, \ldots, d_k} := \left(\prod_{i=1}^{k} \mu(d_i) |d_i| \right) \sum_{\substack{r_1, \ldots, r_k \\ d_i | r_i \forall i \\ (r_i, W) = 1 \, \forall i}} \frac{\mu(r_1, \ldots, r_k)^2}{\prod_{i=1}^{k} \Phi(r_i)} F\left(\frac{\log |r_1|}{\log R}, \ldots, \frac{\log |r_k|}{\log R} \right)$$

whenever $|d_1 \cdots d_k| < R$ *and* $(d_1 \cdots d_k, W) = 1$, *and* $\lambda_{d_1,\dots,d_k} = 0$ *otherwise. Then the following asymptotic formulas hold:*

$$S_1 = \frac{(1+o(1))\Phi(W)^k q^\ell (\ell\theta)^k}{|W|^{k+1}} I_k(F)$$

and

$$S_2 = \frac{(1+o(1))\Phi(W)^k |q^\ell| (\ell\theta)^{k+1}}{\big(\log(q^\ell)\big)|W|^{k+1}} \sum_{m=1}^{k} J_k^{(m)}(F),$$

where

$$I_k(F) := \int \cdots \int_{\mathcal{R}_k} F(x_1, \dots, x_k)^2 dx_1 \dots dx_k,$$

and

$$J_k^{(m)}(F) := \int \cdots \int_{[0,1]^{k-1}} \left(\int_0^1 F(x_1, \dots, x_k) dx_m \right)^2 dx_1 \dots dx_{m-1} dx_{m+1} \dots dx_k.$$

By the above proposition, as $\ell \to \infty$, $S_2/S_1 \to \theta \frac{\sum_{m=1}^k J_k^{(m)}(F)}{I_k(F)}$. Set

$$M_k := \sup_F \frac{\sum_{m=1}^k J_k^{(m)}(F)}{I_k(F)},$$

where the supremum is taken over all F satisfying the conditions of the Proposition 4.3.1. Following Proposition 4.13 of [May15], we have $M_k > \log k - 2\log\log k - 2$ for all large enough k. In particular, $M_k \to \infty$, so upon choosing k large enough depending on m (and choosing F and θ appropriately), we obtain the desired result for any admissible k-tuple $\mathcal{H}$.

For the present article, we fix g satisfying the conditions of Theorem 4.1.3 and modify the above argument as necessary; our modifications are somewhat similar to those in [Pol14a]. Given an admissible k-tuple $\mathcal{H} = \{h_1, \dots, h_k\}$, the set $g\mathcal{H} = \{gh_1, \dots, gh_k\}$ is again admissible. We work from now on with admissible k-tuples $\mathcal{H}$ such that every element of $\mathcal{H}$ is

divisible by g. Set

$$W := \operatorname{lcm}\left(g, \prod_{|p|<\log\log\log(q^\ell)} p\right).$$

With $A(\ell)$ defined as above, we will insist that ℓ is prime; this will be advantageous in what follows. We again search among $n \in A(\ell)$ belonging to a certain residue class modulo W, but we must choose this residue class more carefully than in the original Maynard-Tao argument; that is, we choose this residue class so that primes detected by the sieve will have g as a primitive root.

Lemma 4.3.2. *We can choose $\alpha \in \mathbb{F}_q[t]$ such that, for any $1 \le i \le k$ and for any $n \equiv \alpha \pmod{W}$ with $\deg(n)$ odd,*

- *$n + h_i$ is coprime to W, and*
- *$\left(\frac{g}{n+h_i}\right)_{q-1}$ generates $\mathbb{F}_q^*$.*

Proof. Fix a generator $\omega \in \mathbb{F}_q^*$. Suppose $\deg(g)$ is even. Write $g = p_1^{f_1} \cdots p_r^{f_r}$ with p_i irreducible for each i. Since g is not an vth power for any $v \mid q-1$, the numbers $f_1, \ldots, f_r, q-1$ have greatest common divisor equal to one. Hence, we may write

$$1 = b_1 f_1 + \ldots + b_r f_r + b_{r+1}(q-1)$$

for some integers b_i not all zero. Thus

$$\omega = \omega^{b_1 f_1 + \ldots + b_r f_r + b_{r+1}(q-1)} = \omega^{b_1 f_1 + \ldots + b_r f_r}.$$

Now, for each $1 \le i \le r$, ω^{b_i} is an element of $\mathbb{F}_q^*$ of order dividing $q-1$. By Proposition 4.2.1b, for each such i there exists $a_i \in \mathbb{F}_q[t]$ with $(a_i/p_i)_{q-1} = \omega^{b_i}$; and by the Chinese remainder theorem, we can replace each a_i in the system of congruences above by a single element

$a \in \mathbb{F}_q[t]$. So, by definition,

$$\left(\frac{a}{g}\right)_{q-1} = \prod_{i=1}^{r} \left(\frac{a_i}{p_i}\right)_{q-1}^{f_i} = \prod_{i=1}^{r} \omega^{b_i f_i} = \omega.$$

(note that all polynomials here are monic). Choose α so that $\alpha \equiv a \pmod{g}$ and $(\alpha + h_i, W/g) = 1$ for all $h_i \in \mathcal{H}$; such an α can be chosen by the admissibility of $\mathcal{H}$. Then by Proposition 4.2.1a, for all $n \equiv \alpha \pmod{W}$, we have

$$\left(\frac{a}{g}\right)_{q-1} = \left(\frac{\alpha + h_i}{g}\right)_{q-1} = \left(\frac{n + h_i}{g}\right)_{q-1},$$

recalling that all $h_i \in \mathcal{H}$ are divisible by g. According to Theorem 4.2.2,

$$\left(\frac{n + h_i}{g}\right)_{q-1} = (-1)^{\deg(n+h_i)\deg(g)} \left(\frac{g}{n + h_i}\right)_{q-1} = \left(\frac{g}{n + h_i}\right)_{q-1},$$

so that $(\frac{g}{n+h_i})_{q-1}$ generates $\mathbb{F}_q^*$ as desired. If $\deg(g)$ is odd, so that the factor of -1 remains on the right-hand side of the above equation, repeat the argument with $-\omega$ in place of ω. $\square$

Let $\alpha \in \mathbb{F}_q[t]$ be suitably chosen according to Lemma 4.3.2. Recall that k is the size of the fixed tuple $\mathcal{H} \subset \mathbb{F}_q[t]$ and $\mathbb{P}_g$ denotes the set of primes in $\mathbb{F}_q[t]$ possessing g as a primitive root. Define

$$\tilde{S}_1 := S_1$$

and

$$\tilde{S}_2 := \sum_{\substack{n \in A(\ell) \\ n \equiv \alpha \pmod{W}}} \left(\sum_{i=1}^{k} \chi_{\mathbb{P}_g}(n + h_i) \right) \omega(n).$$

(So $\tilde{S}_2$ is just S_2 with $\mathbb{P}$ replaced with $\mathbb{P}_g$.) Our theorem follows immediately from the following proposition.

Proposition 4.3.3. *As ℓ tends to infinity, we have the same asymptotic formulas for $\tilde{S}_1$ and $\tilde{S}_2$ as we do for S_1 and S_2 in Proposition 4.3.1.*

If we can establish Proposition 4.3.3, Maynard's argument to establish the existence of bounded rational prime gaps can be used to obtain Theorem 4.1.3.

4.4 Proof of Proposition 4.3.3

In what follows, any uses of asymptotic notation (e.g. o and O, $\sim$, etc.) are for ℓ tending to infinity.

This proof follows essentially the same strategy as Section 3.3 of [Pol14a]. Since $\tilde{S}_1 = S_1$, we need only concern ourselves with $\tilde{S}_2$. We can write $\tilde{S}_2 = \sum_{m=1}^{k} \tilde{S}_2^{(m)}$, where

$$\tilde{S}_2^{(m)} := \sum_{\substack{n \in A(\ell) \\ n \equiv \alpha \pmod{W}}} \chi_{\mathbb{P}_g}(n + h_m)\omega(n).$$

The proof of Proposition 4.3.1 (which refers to Maynard's analysis) shows that, for any m,

$$S_2^{(m)} \sim \frac{\Phi(W)^k q^\ell (\ell\theta)^{k+1}}{|W|^{k+1} \log q^\ell} \cdot J_k^{(m)}(F).$$

To establish Proposition 4.3.3, it would certainly suffice to prove that the difference between $S_2^{(m)}$ and $\tilde{S}_2^{(m)}$ is asymptotically negligible, i.e., that as $\ell \to \infty$ through prime values,

$$S_2^{(m)} - \tilde{S}_2^{(m)} = o\left(\frac{\Phi(W)^k q^\ell (\log q^\ell)^k}{|W|^{k+1}}\right). \tag{4.3}$$

We now focus on establishing (4.3) for each fixed m. For prime $r \in \mathbb{Z}$ dividing $q^\ell - 1$, let $\mathcal{P}_r$ denote the set of all prime polynomials $p \in A(\ell)$ satisfying

$$g^{\frac{q^\ell - 1}{r}} \equiv 1 \pmod{p}.$$

We have the inequality

$$0 \leq \chi_{\mathbb{P}} - \chi_{\mathbb{P}_g} \leq \sum_{r \mid q^\ell - 1} \chi_{\mathcal{P}_r}$$

for any argument which is not an irreducible polynomial dividing g, and it follows that

$$0 \leq S_2^{(m)} - \tilde{S}_2^{(m)} \leq \sum_{r \mid q^\ell - 1} \sum_{\substack{n \in A(\ell) \\ n \equiv \alpha \pmod{W}}} \chi_{\mathcal{P}_r}(n + h_m)\omega(n). \tag{4.4}$$

We will show that this double sum satisfies the asymptotic estimate in (4.3).

First note that primes r dividing $q-1$ make no contribution to the sum. Indeed, suppose $r \mid q-1$ and $p := n + h_m$ is detected by the sum. Then

$$1 \equiv g^{\frac{q^\ell - 1}{r}} \equiv \left(\frac{g}{p}\right)_r = \left(\frac{g}{p}\right)_{q-1}^{\frac{q-1}{r}}.$$

So $(g/p)_{q-1}$ does not generate $\mathbb{F}_q^*$, and this contradicts the choice of the residue class $\alpha \pmod{W}$.

Upon expanding the weights and reversing the order of summation, the right-hand side of (4.4) becomes

$$\sum_{\substack{r \mid q^\ell - 1 \\ r \nmid q - 1}} \sum_{\substack{d_1, \ldots, d_k \\ e_1, \ldots, e_k}} \lambda_{d_1 \ldots, d_k} \lambda_{e_1 \ldots, e_k} \sum_{\substack{n \in A(\ell) \\ n \equiv \alpha \pmod{W} \\ [d_i, e_i] \mid n + h_i \, \forall i}} \chi_{\mathcal{P}_r}(n + h_m). \tag{4.5}$$

By definition of the λ terms, the $\{d_i\}$ and $\{e_i\}$ that contribute to the sum are precisely those such that $W, [d_1, e_1], \ldots, [d_k, e_k]$ are pairwise coprime. Thus, the inner sum can be written as a sum over a single residue class modulo $M := W \prod_{i=1}^k [d_i, e_i]$. We will also require that $n + h_m$ is coprime to M (otherwise, it will not contribute to the inner sum), which occurs when $d_m = e_m = 1$.

With this in mind, we claim

$$\sum_{\substack{n\in A(\ell)\\ n\equiv\alpha \pmod W\\ [d_i,e_i]|n+h_i\forall i}} \chi_{\mathcal{P}_r}(n+h_m) = \frac{1}{r\Phi(M)}\frac{q^\ell}{\ell} + O(q^{\ell/2}). \tag{4.6}$$

Indeed, suppose $p := n + h_m$ is detected by $\chi_{\mathcal{P}_r}$. Then p belongs to a certain residue class modulo M, and g is an rth power modulo p. Write $K = \mathbb{F}_q(t)$. The former condition forces Frob_p to be a certain element of $\mathrm{Gal}(K(\Lambda_M)/K)$, and the latter condition is equivalent to p splitting completely in the field $K(\zeta_r, \sqrt[r]{g})$, where ζ_r is a primitive rth root of unity. Let $L := K(\zeta_r, \Lambda_M, \sqrt[r]{g})$. If $K(\Lambda_M)/K$ and $K(\zeta_r, \sqrt[r]{g})/K$ are linearly disjoint extensions of K, then the above conditions on p amount to placing Frob_p in a uniquely determined conjugacy class $\mathcal{C}$ of size 1 in $\mathrm{Gal}(L/K)$.

To see that $K(\Lambda_M)/K$ and $K(\zeta_r, \sqrt[r]{g})/K$ are linearly disjoint extensions of K, first note that since ℓ is prime, our conditions on r imply that the order of q modulo r is equal to ℓ. In particular, this means $r > \ell$. Then since g is fixed while ℓ (and thus r) can be taken arbitrarily large, we can say that g is not an rth power in K.

The extension $K(\sqrt[r]{g})/K$ is not Galois, since the roots of the minimal polynomial $t^r - g$ of $\sqrt[r]{g}$ are $\{\zeta_r^s \sqrt[r]{g}\}_{s=1}^r$, where ζ_r is a primitive rth root of unity. If all of these roots are elements of K, then K must contain all rth roots of unity, implying that $r \mid q-1$, contradicting the conditions on the sum over values of r above. Thus $K(\sqrt[r]{g}) \not\subset K(\Lambda_M)$, as $K(\Lambda_M)$ is an abelian extension of K, and hence any subfield, corresponding to a (normal) subgroup of $\mathrm{Gal}(K(\Lambda_M)/K)$, is Galois. By a theorem of Capelli on irreducible binomials,

$$[K(\sqrt[r]{g}, \Lambda_M) : K] = [K(\sqrt[r]{g}, \Lambda_M) : K(\Lambda_M)][K(\Lambda_M) : K] = r\Phi(M).$$

So we see that $K(\sqrt[r]{g})$ and $K(\Lambda_M)$ are linearly disjoint extensions of K.

For what follows, we need that $K(\sqrt[r]{g}, \Lambda_M)/K$ is a geometric extension of K (i.e., that $\mathbb{F}_q$ is the full constant field of $K(\sqrt[r]{g}, \Lambda_M)$). By Corollary 12.3.7 of [Sal07], $K(\Lambda_M)/K$ is a geometric extension of K, so it is enough to show that the extension $K(\sqrt[r]{g}, \Lambda_M)/K(\Lambda_M)$ is also geometric. This follows from Proposition 3.6.6 of [Sti09], provided we have that $t^r - g$ is irreducible in $K\bar{\mathbb{F}}_q(\Lambda_M)$. The previous paragraph shows that g is not an rth power in $K(\Lambda_M)$, so Capelli's theorem tells us $t^r - g$ is irreducible in $K(\Lambda_M)$. Now, $K\bar{\mathbb{F}}_q(\Lambda_M)$ is a constant field extension of $K(\Lambda_M)$, the compositum of $K(\Lambda_M)$ and $\mathbb{F}_{q^b}$, say. Thus, $K\bar{\mathbb{F}}_q(\Lambda_M)/K$ is an abelian extension of K, as it is the compositum of two abelian extensions of K. If $t^r - g$ factors in this extension, then once again by Capelli, $K\bar{\mathbb{F}}_q(\Lambda_M)/K$ must contain an rth root of g; but this is impossible, by the argument of the previous paragraph. This establishes the claim.

Let K' denote the constant field extension $K(\zeta_r)$ of K; then according to Proposition 3.6.1 of [Sti09], we have $[K'(\Lambda_M, \sqrt[r]{g}) : K'] = r\Phi(M)$, and hence

$$[L : K] = [L : K'][K' : K] = [K'(\Lambda_M, \sqrt[r]{g}) : K'][K' : K] = r\Phi(M)\ell,$$

using Proposition 10.2 of [Ros02] to determine $[K' : K] = \mathrm{ord}_q(r) = \ell$ (here $\mathrm{ord}_q(r)$ denotes the multiplicative order of q modulo r). Thus $K(\zeta_r, \sqrt[r]{g})$ and $K(\Lambda_M)$ are linearly disjoint Galois extensions of K with compositum L, as desired.

We are nearly in a position to use Theorem 4.2.3 to estimate the sum in (4.6). If $\tau \in \mathcal{C}$, the map τ fixes $K(\zeta_r, \sqrt[r]{g})/K$, and in particular restricts to the identity map on $\mathbb{F}_{q^\ell}$, the constant field of $K(\zeta_r, \sqrt[r]{g})$. Now for any $a \in \mathbb{F}_{q^\ell}$, we have

$$\mathrm{Frob}_q^\ell(a) = a^{q^\ell} = a(a^{q^\ell - 1}) = a,$$

and so the restriction condition of Theorem 4.2.3 is satisfied. The sum in question is therefore equal to

$$\frac{1}{r\Phi(M)}\frac{q^\ell}{\ell}+O\Big(\frac{1}{r\Phi(M)}\frac{q^{\ell/2}}{\ell}\big(r\Phi(M)+g_L\big)\Big). \tag{4.7}$$

Let g_1 and g_2 denote the genus of $K'(\sqrt[r]{g})/K'$ and $K'(\Lambda_M)/K'$, respectively. By Proposition 4.2.4,

$$g_L \le \Phi(M)g_1 + rg_2 + (\Phi(M)-1)(r-1).$$

Since $K(\sqrt[r]{g})/K$ is a geometric extension, it follows from Proposition 4.2.5 that $g_1 \ll r$, with the implied constant depending on g. For g_2, we refer to Proposition 4.2.6, which states that

$$2g_2-2 = -2\Phi(M)+\sum_{i=1}^{v} d_i s_i \frac{\Phi(M)}{\Phi(P_i^{\alpha_i})} + (q-2)\frac{\Phi(M)}{q-1},$$

where $M=\prod_{i=1}^{v} P_i^{\alpha_i}$ (with the P_i distinct prime polynomials), $d_i=\deg P_i$, and $s_i = \alpha_i\Phi(P_i^{\alpha_i}) - q^{d_i(\alpha_i-1)}$. At any rate, the middle sum is

$$\le \Phi(M)\sum_{i=1}^{v} d_i\alpha_i = \Phi(M)\sum_{i=1}^{v}\alpha_i\deg(P_i) = \Phi(M)\deg(M).$$

The first and third terms are clearly $O(\Phi(M))$, and thus $g_L \ll r\Phi(M)\deg M$. Inserting this estimate into (4.7), we obtain that the number of primes p detected by the sum in (4.6) is

$$\frac{1}{r\Phi(M)}\frac{q^\ell}{\ell}+O\Big(\frac{1}{r\Phi(M)}\frac{q^{\ell/2}}{\ell}\big(r\Phi(M)+r\Phi(M)\deg M\big)\Big). \tag{4.8}$$

Recall that $M = W\prod_{i=1}^{k}[d_i, e_i]$. Owing to the support of the weights λ, we have $|\prod[d_i, e_i]| < R^2$, and hence

$$\begin{aligned}\log|M| &= \log\Big(|W|\prod_{i=1}^{k}|[d_i, e_i]|\Big) = \log|W| + \log(R^2)\\ &\ll \log|W| + \log(q^{2\theta\ell}).\end{aligned} \tag{4.9}$$

We claim that the expression in (4.9) is $\ll \ell$. To see this, note that there are

$$\rho_q(n) := \frac{1}{n}\sum_{d|n}\mu(n/d)q^d$$

prime polynomials of degree n over $\mathbb{F}_q$, by Gauss's formula (see [Ros02, Proposition 2.1]). Recall that $W := \prod_{|P|<Q} P$, with $Q = \log\log\log(q^\ell)$. Now, letting $\log_q$ denote the base-q logarithm,

$$\begin{aligned}\log|W| = \log\Big|\prod_{|P|<Q}P\Big| = \sum_{|P|<Q}\log|P| &\le \sum_{k=1}^{\lfloor\log_q Q\rfloor}\rho_q(k)\log(q^k)\\ &= (\log q)\sum_{k=1}^{\lfloor\log_q Q\rfloor}k\Big(\frac{1}{k}\sum_{d|k}\mu(k/d)q^d\Big)\\ &= (\log q)\sum_{k=1}^{\lfloor\log_q Q\rfloor}\Big(q^k + O(q^{k/2})\Big).\end{aligned}$$

We crudely estimate the sum on the O-term by

$$\sum_{k=1}^{\lfloor\log_q Q\rfloor}q^{k/2} \le \lfloor\log_q Q\rfloor q^{\lfloor\log_q Q\rfloor/2} \le (\log_q Q)Q^{1/2} \ll (\log\log\log(q^\ell))^{0.51}.$$

The sum on q^k gives

$$\sum_{k=1}^{\lfloor \log_q Q \rfloor} q^k = \frac{q^{\lfloor \log_q Q \rfloor + 1} - q}{q-1} \leq q(Q-1) \leq q \log\log\log(q^\ell),$$

and so $\log|W|$ is certainly bounded by a constant times ℓ, as desired. Thus, the error term in (4.8) is $O(q^{\ell/2})$, as claimed in (4.6).

Inserting the above into (4.5), we produce an O-term of size

$$\begin{aligned} &\ll q^{\ell/2}\Big(\sum_{r|q^\ell-1} 1\Big)\Big(\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}} |\lambda_{d_1\dots,d_k}||\lambda_{e_1\dots,e_k}|\Big) \\ &\qquad \ll q^{\ell/2}\log(q^\ell-1)\lambda_{\max}^2\Big(\sum_{s\,:\,|s|<R}\tau_k(s)\Big)^2 \\ &\qquad \ll q^{\ell/2}\cdot \ell \cdot R^2(\log R)^{2k}, \end{aligned}$$

and this is $o(q^\ell)$ since $R = q^{\theta\ell}$ where $0 < \theta < 1/4$. In going from the second line to the third, we use a polynomial analogue of a familiar bound for the divisor function: We have

$$\sum_{s\,:\,|s|<R}\tau_k(s) \leq \sum_{s\,:\,|s|<R}\sum_{\substack{d_1,\dots,d_k\\ \prod d_i = s}} 1 \leq \sum_{s\,:\,|s|<R}\sum_{\substack{d_1,\dots,d_k\\ \prod d_i = s}} \frac{R}{|d_1\cdots d_k|} \leq R\Big(\sum_{d\,:\,|d|<R}\frac{1}{|d|}\Big)^k.$$

For $m \geq 1$, there are q^m monic elements of $\mathbb{F}_q[t]$ of degree equal to m. Thus, if $R = q^{\theta\ell}$,

$$\sum_{d\,:\,|d|<R}\frac{1}{|d|} \ll \theta\ell \ll \log R,$$

and the bound follows.

We now focus on the main term:

$$\Big(\sum_{\substack{r\mid q^\ell-1\\ r\nmid q-1}}\frac{1}{r}\Big)\frac{q^\ell}{\ell\Phi(W)}\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots,e_k}}{}'\frac{\lambda_{d_1\dots,d_k}\lambda_{e_1\dots,e_k}}{\prod_{i=1}^k\Phi([d_i,e_i])}, \tag{4.10}$$

where the $'$ on the sum means that $[d_1,e_1],\dots,[d_k,e_k]$, and W are all pairwise coprime. Recalling the support of the weights λ, this is equivalent to requiring that $(d_i,e_j)=1$ for all $1\le i,j\le k$ with $i\neq j$. We account for this by inserting the quantity $\sum_{s_{i,j}\mid d_i,e_j}\mu(s_{i,j})$, which is 1 precisely when $(d_i,e_j)=1$ and is 0 otherwise. Define a completely multiplicative function g such that $g(p)=|p|-2$ on prime polynomials p; since all nonzero d_i and e_i are squarefree by definition of the weights $\lambda_{d_1,\dots,d_k}$, we have

$$\frac{1}{\Phi([d_i,e_i])}=\frac{1}{\Phi(d_i)\Phi(e_i)}\sum_{u_i\mid d_i,e_i}g(u_i).$$

Therefore, the primed sum above is equal to

$$\sum_{u_1,\dots,u_k}\Big(\prod_{i=1}^k g(u_i)\Big)\sum_{s_{1,2},\dots,s_{k-1,k}}{}''\Big(\prod_{\substack{1\le i,j\le k\\ i\neq j}}\mu(s_{i,j})\Big)\sum_{\substack{d_1,\dots,d_k\\ e_1,\dots e_k\\ u_i\mid d_i,e_i\forall i\\ s_{i,j}\mid d_i,e_j\forall i\neq j\\ d_m=e_m=1}}\frac{\lambda_{d_1\dots,d_k}\lambda_{e_1\dots,e_k}}{\prod_{i=1}^k\Phi(d_i)\Phi(e_i)}, \tag{4.11}$$

where the double-prime indicates that the sum is restricted to those $s_{i,j}$ which contribute to the sum, i.e. those coprime to $u_i,u_j,s_{i,a}$, and $s_{b,j}$ for all $a\neq j$ and $b\neq i$.

Define new variables

$$y^{(m)}_{r_1,\dots,r_k}:=\Big(\prod_{i=1}^k\mu(r_i)g(r_i)\Big)\sum_{\substack{d_1,\dots,d_k\\ r_i\mid d_i\forall i\\ d_m=1}}\frac{\lambda_{d_1,\dots,d_k}}{\prod_{i=1}^k\Phi(d_i)}.$$

Then we can rewrite (4.11) as

$$\sum_{u_1,\dots,u_k} \Big(\prod_{i=1}^{k} g(u_i)\Big) \sum_{s_{1,2},\dots,s_{k-1,k}}{}'' \Big(\prod_{\substack{1\le i,j\le k\\ i\neq j}} \mu(s_{i,j})\Big) \times \Big(\prod_{i=1}^{k} \frac{\mu(a_i)}{g(a_i)}\Big)\Big(\prod_{j=1}^{k} \frac{\mu(b_j)}{g(b_j)}\Big) y^{(m)}_{a_1,\dots,a_k} y^{(m)}_{b_1,\dots,b_k},$$

where $a_i = u_i \prod_{j\neq i} s_{i,j}$ and $b_j = u_j \prod_{i\neq j} s_{i,j}$. (Note that $\deg a_i, \deg b_i > 1$ for all i, so the denominators $g(a_i)$, $g(b_i)$ above are nonzero for all q.) Recombining terms, we see that this is equal to

$$\sum_{u_1,\dots,u_k} \Big(\prod_{i=1}^{k} \frac{\mu(u_i)^2}{g(u_i)}\Big) \sum_{s_{1,2},\dots,s_{k-1,k}}{}'' \Big(\prod_{\substack{1\le i,j\le k\\ i\neq j}} \frac{\mu(s_{i,j})}{g(s_{i,j})^2}\Big) y^{(m)}_{a_1,\dots,a_k} y^{(m)}_{b_1,\dots,b_k}. \tag{4.12}$$

Let $y^{(m)}_{\max} := \max_{r_1,\dots,r_k} |y^{(m)}_{r_1,\dots,r_k}|$ and note that $y^{(m)}_{\max} \ll \frac{\Phi(W)}{|W|}\log R$; this follows from Lemma 2.6 of [CHL$^+$15]. Using again the fact that $r \geq \ell$, we have

$$\sum_{\substack{r \mid q^\ell - 1\\ r \nmid q-1}} \frac{1}{r} \leq \frac{1}{\ell} \#\{\text{primes } p : p \mid q^\ell - 1\} = o(1),$$

using the standard result that the number of distinct prime divisors of a natural number n is $\ll \frac{\log n}{\log\log n}$.

Putting everything together, we see that (4.10) is

$$\begin{aligned}
&\ll \Bigg(\sum_{\substack{r\mid q^\ell-1\\ r\nmid q-1}}\frac{1}{r}\Bigg)\frac{q^\ell}{\ell\Phi(W)}\Bigg(\sum_{\substack{\deg u<\theta\ell\\(u,W)=1}}\frac{\mu(u)^2}{g(u)}\Bigg)^{k-1}\Bigg(\sum_s\frac{\mu(s)^2}{g(s)^2}\Bigg)^{k(k-1)}\big(y_{\max}^{(m)}\big)^2\\
&\ll \Bigg(\sum_{\substack{r\mid q^\ell-1\\ r\nmid q-1}}\frac{1}{r}\Bigg)\frac{q^\ell}{\ell\Phi(W)}\Big(\frac{\Phi(W)}{|W|}\Big)^{k+1}(\log R)^{k+1}\\
&= o\Big(q^\ell\frac{\Phi(W)^k}{|W|^{k+1}}(\log q^\ell)^k\Big),
\end{aligned}$$

as desired. Note that, in going from the first line to the second, we use the bound

$$\sum_{\substack{\deg u<\theta\ell\\(u,W)=1}}\frac{\mu(u)^2}{g(u)}\ll\frac{\Phi(W)}{|W|}\ell. \tag{4.13}$$

To see this, observe that

$$\begin{aligned}
\sum_{\substack{\deg u<\theta\ell\\(u,W)=1}}\frac{\mu(u)^2}{g(u)}&\le\prod_{\substack{\deg p<\theta\ell\\p\nmid W}}\Big(1+\frac{1}{g(p)}\Big)=\prod_{\deg p<\theta\ell}\Big(1+\frac{1}{g(p)}\Big)\prod_{\substack{\deg p<\theta\ell\\p\mid W}}\Big(1+\frac{1}{g(p)}\Big)^{-1}\\
&\ll\prod_{\deg p<\theta\ell}\Big(1+\frac{1}{g(p)}\Big)\prod_{\substack{\deg p<\theta\ell\\p\mid W}}\Big(1-\frac{1}{|p|}\Big)
\end{aligned}$$

since $\big(1+\frac{1}{g(p)}\big)^{-1}=\big(1-\frac{1}{|p|}\big)\big(1+O(\frac{1}{|p|^2})\big)$. (Here the products over p are restricted to prime polynomials.) Now $g(p)=|p|-2$, and so the first product above is $\ll\ell$. For the second product, we have

$$\prod_{\substack{\deg p<\theta\ell\\p\mid W}}\Big(1-\frac{1}{|p|}\Big)\le\frac{\Phi(W)}{|W|}\prod_{\deg p\ge\theta\ell}\Big(1-\frac{1}{|p|}\Big)^{-1}\le\frac{\Phi(W)}{|W|}\prod_{\deg p\ge\theta\ell}\Big(1+\frac{2}{|p|}\Big)\ll\frac{\Phi(W)}{|W|}$$

for large enough ℓ. Putting it all together, we obtain the bound (4.13), and this completes the proof.

4.5 An example: Primitive polynomials over $\mathbb{F}_2$

We conclude by calculating an explicit bound on small gaps between primitive polynomials over $\mathbb{F}_2$. Referring to the remark after Theorem 1.3 in [CHL$^+$15], any admissible 105-tuple $\mathcal{H}$ of polynomials in $\mathbb{F}_2[t]$ admits infinitely many shifts $f + \mathcal{H}$, $f \in \mathbb{F}_2[t]$, containing at least two primes. Let $\mathcal{H}$ be a collection of 105 prime polynomials in $\mathbb{F}_2[t]$ of norm greater than 105 (that is, of degree at least seven). Note that $\mathcal{H}$ is admissible, since $\mathcal{H} \pmod p$ avoids the residue class 0 for prime polynomials p with $|p| \leq 105$, and $\mathcal{H} \pmod p$ has too few elements to cover all residue classes modulo p when $|p| > 105$. By Gauss's formula for the number of irreducible polynomials of a given degree over a finite field, there are 104 irreducible polynomials of degree seven, eight or nine over $\mathbb{F}_2$, so take $\mathcal{H}$ to be a 105-tuple of primes of degree at least seven and at most ten.

To apply our method, we require in general that each element of $\mathcal{H}$ be a multiple of the given primitive root g, and we may modify an admissible tuple $\mathcal{H}$ to obtain an appropriate admissible tuple by replacing each $h \in \mathcal{H}$ by gh. In the present case, with $g = t$ and $\mathcal{H}$ the 105-tuple described above, this operation results in an admissible 105-tuple $\mathcal{H}$ of polynomials of degree at least eight and at most eleven. Thus, with this choice of $\mathcal{H} = \{h_1, h_2, \ldots, h_{105}\}$, one finds that there are infinitely many gaps of norm at most N between primitive polynomials, where

$$N \leq \max_{1 \leq i \neq j \leq 105} |h_i - h_j| \leq 2^{11} = 2048.$$

For other choices of g and q, one can start with the same 105-tuple $\mathcal{H}$ described above. After replacing each $h \in \mathcal{H}$ by gh, the 105-tuple consists of polynomials of degree at least $\deg(g) + 7$

and at most $\deg(g) + 10$. Thus, in general, this construction produces a bound of the form $q^{\deg(g)+10}$.

Bibliography

[Bil37] H. Bilharz, *Primdivisoren mit vorgegebener Primitivwurzel*, Math. Ann. **114** (1937), no. 1, 476–492.

[Bom65] E. Bombieri, *On the large sieve*, Mathematika **12** (1965), 201–225.

[Bom74] ———, *Le grand crible dans la théorie analytique des nombres*, Astérisque **18** (1974), 1 – 87.

[Bru15] V. Brun, *Über das Golbachsche Gesetz und die Anzahl der Primzahlpaare*, Archiv for Mathem. og Naturw. **34** (1915), no. 8, 1 – 19.

[CCS13] P. L. Clark, B. Cook, and J. Stankewicz, *Torsion points on elliptic curves with complex multiplication (with an appendix by Alex Rice)*, Int. J. Number Theory **9** (2013), no. 2, 447–479.

[Che73] J. R. Chen, *On the representation of a larger even integer as the sum of a prime and the product of at most two primes*, Sci. Sinica **16** (1973), 157–176.

[CHL+15] A. Castillo, C. Hall, R.J. Lemke Oliver, P. Pollack, and L. Thompson, *Bounded gaps between primes in number fields and function fields*, Proc. Amer. Math. Soc. (2015).

[Coj05] A. C. Cojocaru, *Reductions of an elliptic curve with almost prime orders*, Acta Arith. **119** (2005), no. 3, 265–289.

[dB66] N. G. de Bruijn, *On the number of positive integers $\leq x$ and free of prime factors $> y$. II*, Indag. Math. **28** (1966), 239 – 247.

[DH97] H. Diamond and H. Halberstam, *Some applications of sieves of dimension exceeding 1*, Sieve methods, exponential sums, and their applications in number theory (Cardiff, 1995), London Math. Soc. Lecture Note Ser., vol. 237, Cambridge Univ. Press, Cambridge, 1997, pp. 101–107.

[Dic13] L. E. Dickson, *Theorems and tables on the sum of the divisors of a number*, Quart. J. Math. **44** (1913), 264 – 296.

[Dir37] P. G. L. Dirichlet, *Beweis des satzes, dass jede unbegrenzte arithmetische progression, deren erstes glied und differenz ganze zahlen ohne gemeinschaftlichen factor sing, unendlich viele primzahlen erhlt*, Abhandlungen der Kniglich Preussischen Akademie der Wissenschaften (1837), 45 – 81.

[dlVP96] C.J. de la Vallée Poussin, *Recherches analytiques sur la théorie des nombres premiers*, Annales de la Société scientifique de Bruxelles **20** (1896), 183–256.

[EGPS90] P. Erdős, A. Granville, C. Pomerance, and C. Spiro, *On the normal behavior of the iterates of some arithmetic functions*, Analytic Number Theory, Proc. Conf. in honor of Paul T. Bateman (B. C. Berndt et al., eds.), Birkhäuser, Boston, 1990, pp. 165 – 204.

[EK40] P. Erdős and M. Kac, *The Gaussian law of errors in the theory of additive number theoretic functions*, American Journal of Mathematics **62** (1940), no. 1/4, 343 – 352.

[EN79] P. Erdős and J-L. Nicolas, *Sur la fonction nombre de facteurs premiers de n*, Séminaire Delange-Pisot-Poitou. Théorie des nombres **20** (1978-1979), no. 2, 1–19.

[EP85] P. Erdős and C. Pomerance, *The normal number of prime factors of $\varphi(n)$*, Rocky Mtn. J. Math. **15** (1985), 343 – 352.

[Erd40] P. Erdős, *The difference of consecutive primes*, Duke Math. J. **6** (1940), 438–441.

[FJ08] M. D. Fried and M. Jarden, *Field arithmetic*, third ed., Ergebnisse der Mathematik und ihrer Grenzgebiete. 3. Folge. A Series of Modern Surveys in Mathematics [Results in Mathematics and Related Areas. 3rd Series. A Series of Modern Surveys in Mathematics], vol. 11, Springer-Verlag, Berlin, 2008, Revised by Jarden.

[GM84] R. Gupta and M. R. Murty, *A remark on Artin's conjecture*, Invent. Math. **78** (1984), no. 1, 127–130.

[GPY09] D. A. Goldston, J. Pintz, and C. Y. Yıldırım, *Primes in tuples. I*, Ann. of Math. (2) **170** (2009), no. 2, 819–862.

[Gra08] A. Granville, *Smooth numbers: computational number theory and beyond*, Algorithmic number theory: lattices, number fields, curves and cryptography, Math. Sci. Res. Inst. Publ., vol. 44, Cambridge Univ. Press, Cambridge, 2008, pp. 267–323.

[GS07] A. Granville and K. Soundararajan, *Sieving and the Erdős-Kac theorem*, Equidistribution in number theory, an introduction, NATO Sci. Ser. II Math. Phys. Chem., vol. 237, Springer, Dordrecht, 2007, pp. 15–27.

[HB86] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2) **37** (1986), no. 145, 27–38.

[HL23] G. H. Hardy and J. E. Littlewood, *Some problems of 'Partitio numerorum'; III: On the expression of a number as a sum of primes*, Acta Math. **44** (1923), no. 1, 1–70.

[Hoo67] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math. **225** (1967), 209–220.

[HR17] G. H. Hardy and S. Ramanujan, *The normal number of prime factors of a number n*, Quart. J. Math. **48** (1917), 76 – 92.

[HR74] H. Halberstam and H.-E. Richert, *Sieve methods*, Academic Press [A subsidiary of Harcourt Brace Jovanovich, Publishers], London-New York, 1974, London Mathematical Society Monographs, No. 4.

[HR83] H. Halberstam and K. F. Roth, *Sequences*, second ed., Springer-Verlag, New York-Berlin, 1983. MR 687978 (83m:10094)

[Hux71] M. N. Huxley, *The large sieve inequality for algebraic number fields. III. Zero-density results*, J. London Math. Soc. (2) **3** (1971), 233–240.

[HW00] G.H. Hardy and E.M. Wright, *An introduction to the theory of numbers*, fifth ed., Oxford University Press, Oxford, 2000.

[IK04] H. Iwaniec and E. Kowalski, *Analytic number theory*, American Mathematical Society Colloquium Publications, vol. 53, American Mathematical Society, Providence, RI, 2004.

[JU08] J. Jiménez Urroz, *Almost prime orders of CM elliptic curves modulo p*, Algorithmic number theory, Lecture Notes in Comput. Sci., vol. 5011, Springer, Berlin, 2008, pp. 74–87. MR 2467838 (2009m:11081)

[Lin44] U. V. Linnik, *On the least prime in an arithmetic progression. I. The basic theorem*, Rec. Math. [Mat. Sbornik] N.S. **15(57)** (1944), 139–178.

[Liu06] Y-R. Liu, *Prime analogues of the Erdős-Kac theorem for elliptic curves*, J. Number Theory **119** (2006), no. 2, 155–170.

[LN97] R. Lidl and H. Niederreiter, *Finite fields*, second ed., Encyclopedia of Mathematics and its Applications, vol. 20, Cambridge University Press, Cambridge, 1997, With a foreword by P. M. Cohn.

[Mai88] H. Maier, *Small differences between prime numbers*, Michigan Math. J. **35** (1988), no. 3, 323–344.

[May15] J. Maynard, *Small gaps between primes*, Ann. of Math. (2) **181** (2015), no. 1, 383–413.

[Mer74] F. Mertens, *Ein Beitrag zur analytischen Zahlentheorie*, J. Reine Angew. Math. **78** (1874), 46–62.

[Mur88] M. R. Murty, *Artin's conjecture for primitive roots*, Math. Intelligencer **10** (1988), no. 4, 59–67.

[Pol09] P. Pollack, *Not always buried deep*, American Mathematical Society, Providence, RI, 2009. MR 2555430 (2010i:11003)

[Pol14a] ———, *Bounded gaps between primes with a given primitive root*, Algebra Number Theory **8** (2014), no. 7, 1769–1786.

[Pol14b] ———, *Some arithmetic properties of the sum of proper divisors and the sum of prime divisors*, Illinois J. Math. **10** (2014), 885–903.

[Pol16] ———, *A Titchmarsh divisor problem for elliptic curves*, Math. Proc. Cambridge Philos. Soc. **160** (2016), no. 1, 167–189.

[Ros99] M. Rosen, *A generalization of Mertens' theorem*, J. Ramanujan Math. Soc. **14** (1999), no. 1, 1–19.

[Ros02] ———, *Number theory in function fields*, Graduate Texts in Mathematics, vol. 210, Springer-Verlag, New York, 2002.

[Sal07] G.D.V. Salvador, *Topics in the theory of algebraic function fields*, Mathematics: Theory & Applications, Birkhäuser, 2007.

[Sie35] C. L. Siegel, *uber die Classenzahl quadratischer Zahlk orper*, Acta Arith. **1** (1935), no. 1, 83 – 86.

[Sou07] K. Soundararajan, *Small gaps between prime numbers: the work of Goldston-Pintz-Yıldırım*, Bull. Amer. Math. Soc. (N.S.) **44** (2007), no. 1, 1–18.

[Sti09] H. Stichtenoth, *Algebraic function fields and codes*, second ed., Graduate Texts in Mathematics, vol. 254, Springer-Verlag, Berlin, 2009.

[Tur34] P. Turàn, *On a theorem of Hardy and Ramanujan*, J. Lond. Math. Soc. **9** (1934), 274 – 276.

[Wal36] A. Walfisz, *Zur additiven Zahlentheorie. II*, Math. Z. **40** (1936), no. 1, 592–607.

[Was08] L. C. Washington, *Elliptic curves*, second ed., Discrete Mathematics and its Applications (Boca Raton), Chapman & Hall/CRC, Boca Raton, FL, 2008, Number theory and cryptography.

[Xyl11] T. Xylouris, *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression*, Bonner Mathematische Schriften [Bonn Mathematical Publications], 404, Universität Bonn, Mathematisches Institut, Bonn, 2011, Dissertation for the degree of Doctor of Mathematics and Natural Sciences at the University of Bonn, Bonn, 2011.

[Zha14] Y. Zhang, *Bounded gaps between primes*, Ann. of Math. (2) **179** (2014), no. 3, 1121–1174.