Results in Analytic and Algebraic Number Theory

A Thesis

presented to

the Faculty of the Graduate School

University of Missouri

In Partial Fulfillment

of the Requirements for the Degree

Master of Arts

---

by

Aaron Yeager

Dr. William Banks, Thesis Supervisor

December 2012

The undersigned, appointed by the Dean of the Graduate School, have examined the thesis entitled

Results in Analytic and Algebraic Number Theory

presented by Aaron Yeager,

a candidate for the degree of Master of Arts and hereby certify that in their opinion it is worthy of acceptance.

Professor William Banks

Professor Youssef Saab

Professor Jan Segert

Professor Konstantin Makarov

ACKNOWLEDGEMENTS

To begin, I would like to thank my friends and family members for their support, guidance, and encouragement; without them I certainly would not be where I am today. I must also give credit to the numerous excellent math teachers, instructors, and professors I have had throughout my collegiate career. I would like to thank Ryan Alvarado and Kevin Brewster for their aid with LaTex commands that made my thesis possible. I would like to thank my co-authors of the papers I written while at the University of Missouri: William Banks, Ahmet M. Güloğlu, Zhenyu Guo, and Roger Baker. I would like to thank Youssef Saab, Konstantin Makarov, and Jan Segert for being on my master's committee. On a final note, I would like to express my gratitude to William Banks for being my advisor and for his assistance on my thesis.

Contents

RESULTS IN ANALYTIC AND ALGEBRAIC NUMBER THEORY

Aaron Yeager

Dr. William Banks, Thesis Supervisor

Preface

This work is a compilation of five papers that contain some related topics and techniques. These papers were written during the last two years at the University of Missouri. The papers are divided as chapters, each having its own introduction and bibliography. Although the topics are connected and similar techniques are used, the chapters are mostly self-contained and can be read independently.

0.1 Chapters I and II

The first two chapters are exposition topics in Analytic and Algebraic Number Theory. I began working on the first chapter while I attended a course in Analytic Number Theory during Fall 2011. The work in the second chapter started when I took a course in Algebraic Number Theory in Spring 2012.

The first chapter gives a brief introduction to sums over finite fields. The chapter also discusses Gauss sums, generalized Gauss sums, exponential sums, and Jacobi sums. If we let $\mathbb{F}$ be a finite field with q elements, it is shown that the modulus of the Gauss sum and the modulus of the Jocobi sum is equal to $\sqrt{q}$. Using these theorems the chapter concludes by showing that if p is a prime such that $p \equiv 1 \pmod 4$, then there are integers a and b such that $p = a^2 + b^2$.

The second chapter proves some useful results concerning the Dedekind zeta function. The chapter starts with some basic properties of this function. An auxiliary function is then defined and shown to have a functional equation. Using these results for the auxiliary function, the Dedekind zeta function is shown to have a factorization in the right half of the complex plane that has the gamma function and sums regarding the incomplete gamma function as some of its factors. Given this factorization and using properties of the gamma function and the incomplete gamma function as well as using techniques from real and complex analysis, the function is proven to be meormorphic on the whole complex plane, shown to have a simple pole, and the residue is exhibited. The function is also shown to have a functional equation that has a factor of the gamma function. The chapter concludes by giving the evaluation of the function at zero and showing that this function is zero on the negative integers.

0.2 Chapters III, IV, and V

The last three chapters were written with co-authors. The chapters are an expansion of a series of new research papers in mathematics with topics from Analytic and Algebraic Number Theory. The papers that resemble chapters III and IV have been accepted by journals and the paper that represents chapter V will be submitted shortly. The papers were written in Spring 2011, Fall 2011, and Spring 2012 respectively.

My advisor is the co-author of the third chapter, which has been accepted by *Colloquium Mathematicum.* In the chapter we give a new result concerning Carmicheal numbers. Specifically, let $\alpha, \beta \in \mathbb{R}$ be fixed with $\alpha > 1$, and suppose that α is irrational and of finite type. We show that there are infinitely many Carmichael numbers composed solely of primes from the non-homogeneous Beatty sequence $\mathscr{B}_{\alpha,\beta} = (\lfloor \alpha n + \beta \rfloor)_{n=1}^{\infty}$. The result is proved by appealing to a construction of infinitely many

Carmicheal numbers given by Alford, Granville, and Pomerance. To use their construction we bound exponential sums over arithmetic progressions by many techniques such as exploiting the type of α, using the Balog and Perelli theorem, and by applying a classical result by Vinogradov on bounds of Fourier coefficients. The chapter concludes with heuristic evidence via Dickson's conjecture to support our conjecture that we obtain same result when α is an irrational number of infinite type.

The fourth chapter was co-authored by my advisor and Ahmet M. Güloğlu and is accepted by the *Canadian Mathematical Bulletin*. The chapter contains a proof of a new result in Algebraic Number Theory that has an application to Carmicheal numbers. We show that for any finite Galois extension K of the rational numbers $\mathbb{Q}$, there are infinitely many Carmichael numbers composed solely of primes for which the associated class of Frobenius automorphisms coincides with any given conjugacy class of $\mathrm{Gal}(K|\mathbb{Q})$. The result has three corollaries: for any algebraic number field K, there are infinitely many Carmichael numbers which are composed solely of primes that split completely in K; for every natural number n, there are infinitely many Carmichael numbers of the form $a^2 + nb^2$ with a, b integers; and there are infinitely many Carmichael numbers composed solely of primes $p \equiv a \pmod{d}$ with a, d coprime. To obtain our main result we begin by examining zeros of the Dedekind zeta function in a region to get the existence of a proper integral ideal. We use this result along with the Chebotarev Density Theorem to yield a lower bound on a counting function that detects primes in our setting. Finally after this bound is proven, we show how the construction of infinitely many Carmichael numbers given by Alford, Granville, and Pomerance can be applied using these primes.

The fifth chapter is to be submitted in the near future. It is co-authored by my advisor, Roger Baker, and Zhenyu Guo. In the chapter we prove a new result regarding Piatetski-Shapiro primes, primes from sequences of the form $(\lfloor n^c \rfloor)_{n\in\mathbb{N}}$ where $c > 1$ and $c \notin \mathbb{N}$, in relation to almost primes. We show that for any fixed $c \in (1, \frac{77}{76})$ there are infinitely many primes of the form $p = \lfloor n^c \rfloor$, where n is a natural number with at most eight prime factors (counted with multiplicity). To achieve this result we begin by using an approximation by Vaaler for bounds on exponential sums with the saw-tooth function. Eventually we have to bound type I and type II exponential sums. One of our main tools in the desired bounds on these sums is the use of exponential pairs. Furthermore, we show how to find the optimal exponential pairs for our setting. Using these techniques and appealing to a weighted sieve we obtain the main result for when $c \in (1, \frac{8635}{8568})$. The chapter concludes with giving a refinement of our argument that shows the same result is true when $c \in (1, \frac{77}{76})$.

Chapter 1

Sums Over Finite Fields

1.1 Introduction

The contents of this chapter are a result of studies from [1] and [2]. The main object of study is a sum that has a character convolved with an exponential function. Some examples of these types of sums are the quadratic Gauss sum

$$G_a(p) = \sum_{\chi \pmod p} \left(\frac{x}{p}\right) e\left(\frac{ax}{p}\right),$$

where $e(\frac{ax}{p}) = e^{2\pi i \frac{ax}{p}}$ and $(\frac{x}{p})$ is the Legendre symbol modulo p, or Kloosterman sums

$$S(a, b; p) = \sum_{\chi \pmod p}^{*} e\left(\frac{ax + b\overline{x}}{p}\right),$$

where the weight $*$ means that the sum can be extended to all x which are not poles for the function in the sum and where $\overline{x}$ is the inverse in $\mathbb{Z}/p\mathbb{Z}$ of the invertible element $x \in (\mathbb{Z}/p\mathbb{Z})^{\times}$. The quadratic Gauss sums are used for many results. Among these results are the Hasse-Davenport relation and quadratic reciprocity. The Kloosterman sums can also be used to show many results. One of the most notable results is that for $a_1, ..., a_4 \geq 1$ positive integers for n large enough, depending on the $a_i's$, there exists at least one integral solution $(x_1, ..., x_4) \in \mathbb{Z}^4$ to the diophantine equation

$$a_1x_1^2 + ... + a_4x_4^2 = n$$

provided there is no congruence obstruction.

The Gauss and Kloosterman sums can be generalized. That is, the Legendre character can be replaced with an arbitrary multiplicative character and the exponential function can be replaced with an arbitrary arithmetic function. Sums of this type are called *Complete Sums*. We will address these sums in the next section.

To begin our study of these sums let p be a prime number and consider the field $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$. Since this field has p elements, the Galois theory is easy to describe. For $n \geq 1$, there exists up to isomorphism a unique field extension of $\mathbb{F}_p$ of degree n, $\mathbb{F}_{p^n}$. Conversely, any finite field $\mathbb{F}$ with q elements is isomorphic to a unique field $\mathbb{F}_{p^d}$, so $q = p^d$, and $\mathbb{F}$ has a unique extension of degree n, namely $\mathbb{F}_{p^{dn}}$.

Let $\mathbb{F} = \mathbb{F}_q$ be a finite field with $q = p^d$ elements. Let $\overline{\mathbb{F}}$ be the algebraic closure of $\mathbb{F}$ and set $\mathbb{F}_n$ to be the unique extension of degree n of $\mathbb{F}$ for $n \geq 1$. Observe we have the cardinality relation $|\mathbb{F}_n| = q^n$. Thus the extension $\mathbb{F}_n/\mathbb{F}$ is Galois. Set $G_n = Gal(\mathbb{F}_n/\mathbb{F})$. Then by the map $\mathbb{Z}/n\mathbb{Z} \to G_n$ by $1 \mapsto \sigma$, where σ is the Frobenius automorphism of $\mathbb{F}_n$ given by $\sigma(x) = x^q$, we have $G_n \cong \mathbb{Z}/n\mathbb{Z}$. Given this we have $\overline{\mathbb{F}} = \bigcup_{n\geq 1} \mathbb{F}_n$. Furthermore, since $\overline{\mathbb{F}}$ is a Galois extension of $\mathbb{F}$, for $x \in \overline{\mathbb{F}}$ we have that

$$x \in \mathbb{F} \Longleftrightarrow \sigma(x) = x \Longleftrightarrow x^q = x.$$

Then in general, for the extension $\mathbb{F}_n$ over $\mathbb{F}$ we have

$$x \in \mathbb{F}_n \Longleftrightarrow \sigma^n(x) = x \Longleftrightarrow x^{q^n} = x.$$

Given this we can conclude that $\mathbb{F}_n$ is the splitting field for $x^{q^n} - x \in \mathbb{F}[x]$.

1.2 Generalized Gauss Sums

The quadratic Gauss Sum can be generalized by using a multiplicative character and an additive character. Specifically, let $\mathbb{F}_q$ be a field with q elements and let χ be a multiplicative character on $\mathbb{F}_q$ and ψ be additive character of $\mathbb{F}_q$. The general Gauss sum over the finite field $\mathbb{F}_q$ is given by

$$\tau(\chi, \psi) = \sum_{x \in \mathbb{F}_q^\times} \chi(x)\psi(x).$$

From this definition, our first theorem regards the size of the modulus of $\tau(\chi, \psi)$.

Theorem 1. *Let χ be non-trivial multiplicative character and ψ be a non-trivial additive character on $\mathbb{F}_q$. Then*

$$|\tau(\chi, \psi)| = \sqrt{q}.$$

Proof. If we consider the modulus squared, expanding the product of the Gauss sum and its conjugate yields

$$\begin{aligned} |\tau(\chi, \psi)|^2 &= \sum_{x,y \in \mathbb{F}_q^\times} \chi(x)\overline{\chi(y)}\psi(x)\overline{\psi(y)} \\ &= \sum_{x,y \in \mathbb{F}_q^\times} \chi(xy^{-1})\psi(x-y). \end{aligned}$$

Now put $u = xy^{-1}$. Then for a fixed y we have

$$|\tau(\chi, \psi)|^2 = \sum_{u \in \mathbb{F}_q^\times} \chi(u) \sum_{y \in \mathbb{F}_q^\times} \psi(y(u-1)),$$

where the inner sum above is purely additive. By the orthogonality relations of the additive characters on $\mathbb{F}_q$, this inner is sum is such that

$$\sum_{\alpha} \alpha(u-1) - 1 = \begin{cases} -1 & \text{if } u \neq 1, \\ q-1 & \text{if u=1,} \end{cases}$$

for all α of the additive characters on $\mathbb{F}_q$. Using this and by the orthogonality relations of the multiplicative character χ, we have

$$\begin{aligned} |\tau(\chi, \psi)|^2 &= -\sum_{u \in \mathbb{F}_q^\times} \chi(u) + q \\ &= q. \end{aligned}$$

Taking the square root of both sides of the above yields the result. $\square$

1.3 Jacobi Sums

As with the generalized Gauss Sums, let $\mathbb{F}_q$ be a field with q elements. Let χ and ϕ be multiplicative characters of $\mathbb{F}_q$. The Jacobi sum associated to the multiplicative characters χ and ϕ of $\mathbb{F}_q$ is defined by

$$J(\chi, \phi) = \sum_{x \in \mathbb{F}_q} \chi(x)\phi(1-x) = \sum_{x+y=1} \chi(x)\phi(y).$$

The values of such a sum occur in relation to local zeta-functions for diagonal forms.

Our next proposition shows how these sums can be expressed as general Gauss sums.

Theorem 2. *Let χ and ϕ be non-trivial multiplicative characters such the product $\chi\phi$ is also a non-trivial on $\mathbb{F}_q$, a field with q elements. Fix a non-trivial additive character ψ of $\mathbb{F}_q$. Then*

$$J(\chi, \phi) = \frac{\tau(\chi, \psi)\tau(\phi, \psi)}{\tau(\chi\phi, \psi)}. \tag{1.1}$$

Furthermore,

$$|J(\chi, \phi)| = \sqrt{q}.$$

Proof. By definition the Jacobi and Gauss sums we have

$$
\begin{aligned}
J(\chi,\phi)\tau(\chi\phi,\psi) &= \sum_{x\in\mathbb{F}_q} \chi(x)\phi(1-x) \sum_{y\in\mathbb{F}_q^\times} \chi\phi(y)\psi(y) \\
&= \sum_{x\in\mathbb{F}_q} \chi(x)\phi(1-x) \sum_{y\in\mathbb{F}_q^\times} \chi(y)\phi(y)\psi(y) \\
&= \sum_{x\in\mathbb{F}_q} \sum_{y\in\mathbb{F}_q^\times} \chi(x)\phi(1-x)\chi(y)\phi(y)\psi(y).
\end{aligned}
$$

By χ and ϕ being nontrivial, the above sum can be restricted to $x \notin \{0,1\}$. Set $u = xy$ and $v = y - xy$. Then by this change of variables we obtain a bijection from $(x,y) \in (\mathbb{F}_q - \{0,1\}) \times \mathbb{F}_q^\times$ to $\{(u,v) \in \mathbb{F}_q^\times \times \mathbb{F}_q^\times : u+v \neq 0\}$. Furthermore by $\chi\phi$ being non-trivial it follows that

$$
\begin{aligned}
J(\chi,\phi)\tau(\chi\phi,\psi) &= \sum_{\substack{u,v\in\mathbb{F}_q^\times \\ u+v\neq 0}} \chi(u)\phi(v)\psi(u+v) \\
&= \tau(\chi,\psi)\tau(\phi,\psi) - \sum_{u\in\mathbb{F}_q^\times} \chi(u)\phi(-u) \\
&= \tau(\chi,\psi)\tau(\phi,\psi).
\end{aligned}
$$

Using theorem 1 we have $|\tau(\chi\phi,\psi)| = \sqrt{q} \neq 0$. Thus by definition of the modulus it follows that $\tau(\chi\phi,\psi) \neq 0$. Hence dividing both sides of the above by $\tau(\chi\phi,\psi)$ yields equation 1.1. To obtain the other result, we use equation 1.1 along with Theorem 1 and simplify to complete the proof. $\square$

Our final result shows how a Jacobi sum can be used to answer a classical problem in Number Theory.

Theorem 3. *Let p be a prime number such that $p \equiv 1 \pmod 4$. Then there exists $a, b \in \mathbb{Z}$ such that*

$$p = a^2 + b^2.$$

Proof. By the theory of characters, since $p \equiv 1 \pmod 4$, there exists a character χ of order 4 on $\mathbb{F}_p^\times$. Consider the Jacobi sum $J(\chi,\phi)$, where ϕ is the usual Legendre character. Then by definition

$$J(\chi, \phi) = \sum_{x+y=1} \chi(x)\phi(y).$$

By ϕ being a Legendre character we have $\phi(y) \in \{-1, 0, 1\}$ and by χ being a character of order 4 on $\mathbb{F}_p^\times$, we have $\chi(x) \in \{-i, -1, 0, 1, i\}$. Give this observation, the Jacobi sum $J(\chi, \phi)$ can be written as $J(\chi, \phi) = a + bi$, for some $a, b \in \mathbb{Z}$. Therefore with this in consideration, using Theorem 2 we obtain

$$\begin{aligned} p =& |J(\chi, \phi)|^2 \\ =& |a + bi|^2 \\ =& (\sqrt{a^2 + b^2})^2 \\ =& a^2 + b^2. \end{aligned}$$

$\square$

Bibliography

[1] H. Iwaniec, E. Kowalski, 'Analytic Number Theory,' Amer. Math., Providence, RI, (2004), 269–291.

[2] H. Iwaniec, 'Exponential sums over finite fields, I: elementary methods,' http://www.math.ethz.ch/ kowalski/exp-sums.pdf (2010), 1–27.

Chapter 2

Dedekind Zeta Functions

2.1 Introduction

The contents of this chapter are results from studies of the references and working through problems 25 (a) and (b) and 26 (a) through (f) of [3]. The lemmas and theorems in the paper are these problems worked out. All proofs are the author's work with few proofs using variations of techniques in chapter 10 of [3]. Let K be an algebraic number field. That is, K is a finite dimensional field extension of the rational field $\mathbb{Q}$. Let $N(\cdot)$ be the norm on the field K . For $s = \sigma + it \in \mathbb{C}$, with $\sigma > 1$, the Dedekind zeta function is defined to be

$$\zeta_K(s) = \sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$$

where the sum is over all integral ideals in the ring $\mathcal{O}_K$ of algebraic integers in K. By [2], the Dedekind zeta function can also be written as

$$\zeta_K(s) = \sum_{1}^{\infty} \frac{a_K(n)}{n^s},$$

where $a_K(n)$ is the number of integral ideals of K with norm exactly n. When $K = \mathbb{Q}$, $\zeta_K(s) = \zeta(s)$. Hence why the sum bears its name. This function is of great importance for many reasons. For instance it can be used to show various density theorems such as the Cebatorev Density theorem. It can also be used to get a generalization of a Dirichlet L-series which leads Dirichlet's Prime Number Theorem. Some natural questions to consider would be: What properties does this function have like the usual ζ function? Does it have an Euler product, a functional equation? Can it be factored to recover the original ζ function? Is it meromorphic, and if so, what are the singularities and residues, and so on? To answer some of these questions we need to start with how the norm acts on ideals in $\mathcal{O}_K$. Given that ideals in the ring $\mathcal{O}_K$ factor uniquely into prime ideals, and since both the norm $N(\cdot)$ and n^{-s} are multiplicative, their product is also multiplicative. Hence we have a Euler product of

$$\zeta_K(s) = \prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1},$$

for $\sigma > 1$.

2.2 The auxiliary function ϑ_Q

Let $Q(x,y) = ax^2 + bxy + cy^2$, where a, b, c are real numbers, and put $d = b^2 - 4ac$. Suppose that Q is positive-definite, which is to say that $a > 0$ and $d < 0$. For $z \in \mathbb{C}$ with $\mathfrak{R}(z) > 0$, put

$$\vartheta_Q(z) = \sum_{m,n \in \mathbb{Z}} e^{-2\pi Q(m,n) z/\sqrt{-d}}.$$

Lemma 1. *The function $\vartheta_Q(z)$ can be written as*

$$\vartheta_Q(z) = \sum_n e^{-\pi z n^2 \sqrt{-d}/(2a)} \sum_m e^{-2\pi a (m + bn/(2a))^2 z/\sqrt{-d}}.$$

Proof. Completing the square in the definition of the quadratic form and combining like terms yields,

$$
\begin{aligned}
Q(m,n) &= am^2 + bmn + cn^2 \\
&= a(m + bn/(2a))^2 - \frac{(bn)^2}{4a} + cn^2 \\
&= a(m + bn/(2a))^2 - \frac{(bn)^2 - cn^2 4a}{4a} \\
&= a(m + bn/(2a))^2 - \frac{n^2 d}{4a}.
\end{aligned}
$$

Thus

$$
\begin{aligned}
\vartheta_Q(z) &= \sum_{m,n\in\mathbb{Z}} e^{-2\pi Q(m,n)z/\sqrt{-d}} \\
&= \sum_{m,n\in\mathbb{Z}} e^{-2\pi(am^2+bmn+cn^2)z/\sqrt{-d}} \\
&= \sum_n \sum_m e^{-2\pi(a(m+\frac{bn}{2a})^2 - \frac{n^2 d}{4a})z/\sqrt{-d}} \\
&= \sum_n e^{-\pi z n^2\sqrt{-d}/(2a)} \sum_m e^{-2\pi a(m+bn/(2a))^2 z/\sqrt{-d}}.
\end{aligned}
$$

□

Lemma 2. *The function $\vartheta_Q(z)$ has a functional equation of $\vartheta_Q(z) = \vartheta_Q(1/z)/z$.*

Proof. Applying Theorem 10.1 of [3], with choices of $\alpha = \frac{bn}{2a}$ and $\tilde{z} = \frac{2az}{\sqrt{-d}}$, to the inner sum in the previous lemma yields

$$
\sum_m e^{-2\pi a(m+bn/(2a))^2 z/\sqrt{-d}} = \Big(\frac{2az}{\sqrt{-d}}\Big)^{\frac{-1}{2}} \sum_k e(kbn/(2a)) e^{-\pi k^2\sqrt{-d}/(2az)}.
$$

Using this and switching the sums shows

$$
\begin{aligned}
\vartheta_Q(z) &= \sum_n e^{-\pi z n^2\sqrt{-d}/(2a)} \sum_m e^{-2\pi a(m+bn/(2a))^2 z/\sqrt{-d}} \\
&= \Big(\frac{2az}{\sqrt{-d}}\Big)^{\frac{-1}{2}} \sum_n e^{-\pi z n^2\sqrt{-d}/(2a)} \sum_k e(kbn/(2a)) e^{-\pi k^2\sqrt{-d}/(2az)} \\
&= \Big(\frac{2az}{\sqrt{-d}}\Big)^{\frac{-1}{2}} \sum_k e^{-\pi k^2\sqrt{-d}/(2az)} \sum_n e^{-\pi z n^2\sqrt{-d}/(2a) + \pi i k b n/a}.
\end{aligned}
$$

By writing the exponent on the last sum above as

$$
-\pi z n^2\sqrt{-d}/(2a) + \pi i k b n/a = -\pi(n - ikb/(z\sqrt{-d}))^2 z\sqrt{-d}/(2a) - \pi(kb)^2/(2az\sqrt{-d})
$$

we see that

$$\sum_n e^{-\pi z n^2\sqrt{-d}/(2a)+\pi ikbn/a} = \sum_n e^{-\pi(kb)^2/(2az\sqrt{-d})} e^{-\pi(n-ikb/(z\sqrt{-d}))^2 z\sqrt{-d}/(2a)}$$
$$= e^{-\pi(kb)^2/(2az\sqrt{-d})} \sum_n e^{-\pi(n-ikb/(z\sqrt{-d}))^2 z\sqrt{-d}/(2a)}.$$

Using Theorem 10.1 of [3] again, this time with $\alpha = \frac{-ikb}{z\sqrt{-d}}$ and $\tilde{z} = \frac{2az}{\sqrt{-d}}$, we obtain that the sum above is

$$e^{-\pi(kb)^2/(2az\sqrt{-d})}(z\sqrt{-d}/2a)^{\frac{-1}{2}} \sum_l e(-likb/(z\sqrt{-d}))e^{-\pi l^2/(z\sqrt{-d}/(2a))}.$$

If we now combine the exponents from the exponential functions and factor them, we see that

$$-\pi(kb)^2/(2az\sqrt{-d})+2\pi lkb/(z\sqrt{-d})-\pi l^2/(z\sqrt{-d}/(2a)) = -2\pi a/(z\sqrt{-d})(l-kb/(2a))^2.$$

Putting this in the sum and combining with the previous sum shows

$$\left(\frac{2az}{\sqrt{-d}}\right)^{\frac{-1}{2}} \left(\frac{z\sqrt{-d}}{2a}\right)^{\frac{-1}{2}} \sum_k e^{-\pi k^2\sqrt{-d}/(2az)} \sum_l e^{-2\pi a(l-bk/(2a)^2/(z\sqrt{-d})}$$
$$= (z)^{-1} \sum_k e^{-\pi k^2\sqrt{-d}/(2az)} \sum_l e^{-2\pi a(l-bk/(2a)^2/(z\sqrt{-d})}.$$

If we let $l = m$ and $k = -n$ we achieve the result. □

2.3 The properties of Dedekind Zeta Functions

Let us now consider the case when K is a complex quadratic field. Let d be the discriminant of K. Then $K = \mathbb{Q}(\sqrt{d})$, where $d < 0$. Let w be the number of units in $\mathcal{O}_k$, and h be the class number of K. Then there are h reduced positive definite binary quadratic forms of discriminant d, say $Q_1, ..., Q_h$. Consider when $(m, n) \neq (0, 0)$. As these run over integral values, $Q_i(m, n)$ runs over the values of $N(\mathfrak{a})$ for ideals $a \in \mathcal{C}_i$, where $\mathcal{C}_i$ is the i^{th} ideal class, each value being taken w times. Hence on each Q_i,

$$\zeta_{Q_i}(s) = w \sum_{a \in \mathcal{C}_i} N(\mathfrak{a})^{-s}.$$

Theorem 4. *For $\Re(z) \geq 0$, let*

$$\vartheta_K(z) = \sum_{i=1}^{h} \vartheta_{Q_i}(z) = h + w \sum_{n=1}^{\infty} r(n) e^{-2\pi n z/\sqrt{-d}}$$

where $r(n) = r_K(n) = \sum_{k|n} \chi_d(k)$ is the number of ideals in $\mathcal{O}_k$ with norm equal to n. Give this we have $\vartheta_K(z) = \vartheta_K(1/z)/z$.

Proof. By definition

$$\begin{aligned} \vartheta_{Q_i}(z) &= \sum_{m,n \in O_K} e^{-2\pi Q_i(m,n) z/\sqrt{-d}} \\ &= 1 + \sum_{\substack{m,n \in \mathcal{O}_K \\ m,n \neq 0}} e^{-2\pi Q_i(m,n) z/\sqrt{-d}}. \end{aligned}$$

If we sum from 1 to h, by the definition of how $Q_i(m,n)$ runs over the its values, we see

$$\vartheta_K(z) = \sum_{i=1}^{h} \vartheta_{Q_i}(z) = h + w \sum_{n=1}^{\infty} r(n) e^{-2\pi n z/\sqrt{-d}}.$$

By Lemma 2 it follows that $\vartheta_{Q_i}(z) = \vartheta_{Q_i}(1/z)/z$. Therefore we have

$$\vartheta_K(z) = \sum_{i=1}^{h} \vartheta_{Q_i}(1/z)/z = \vartheta_K(1/z)/z.$$

□

Theorem 5. *If $\Re(z) \geq 0$, then*

$$\begin{aligned} \zeta_K(s)\Gamma(s)(-d)^{s/2}(2\pi)^{-s} = (-d)^{s/2}(2\pi)^{-s} &\sum_{n=1}^{\infty} r(n) n^{-s} \Gamma(s, 2\pi n z/\sqrt{-d}) \\ &+ (-d)^{(1-s)/2}(2\pi)^{s-1} \sum_{n=1}^{\infty} r(n) n^{s-1} \Gamma(1-s, 2\pi n/(z\sqrt{-d})) \\ &+ \frac{hz^{s-1}}{2w(s-1)} - \frac{hz^s}{2ws}, \end{aligned}$$

where $\Gamma(s,a)$ is the incomplete gamma function

$$\Gamma(s,a) = \int_a^{\infty} e^{-w} w^{s-1} dw.$$

Proof. By Euler's integral formula for $\Gamma(s)$, if $\sigma > 0$, then

$$\Gamma(s) = \int_0^\infty e^{-x} x^{s-1} dx.$$

If we make of change of variables of $x = 2\pi nu/\sqrt{-d}$ we obtain

$$\begin{aligned}\Gamma(s) &= \int_0^\infty e^{-2\pi nu/\sqrt{-d}} (2\pi nu/\sqrt{-d})^{s-1} (2\pi n/\sqrt{-d}) du \\ &= (2\pi n/\sqrt{-d})^s \int_0^\infty e^{-2\pi nu/\sqrt{-d}} u^{s-1} du.\end{aligned}$$

Thus

$$n^{-s}\Gamma(s)(-d)^{-s/2}(2\pi)^{-s} = \int_0^\infty e^{-2\pi nu/\sqrt{-d}} u^{s-1} du.$$

Since $r(n)$ is the number of ideals in $\mathcal{O}_K$ with norm exactly n, for $\sigma > 0$, if we multiply both sides of the equation above by $r(n)$ and then sum over n we achieve,

$$\begin{aligned}\zeta_K(s)\Gamma(s)(-d)^{-s/2}(2\pi)^{-s} &= \sum_{n=1}^\infty r(n) \int_0^\infty e^{-2\pi nu/\sqrt{-d}} u^{s-1} du \\ &= \int_0^\infty \Big(\sum_{n=1}^\infty r(n) e^{-2\pi nu/\sqrt{-d}} \Big) u^{s-1} du.\end{aligned} \tag{2.1}$$

I note that the exchange of the integration and the summation above is permitted by the absolute convergence of the series. Suppose the $\Re(z) > 0$. By Cauchy's theorem, we may replace the path of integration by a ray from 0 that passes through z. We now consider the integral from 0 to z and z to ∞ separably. Call these integrals $\int_1$ and $\int_2$ respectively. By reversing the steps above we have that

$$\int_2 = (-d)^{s/2}(2\pi)^{-s} \sum_{n=1}^\infty r(n) n^{-s} \Gamma(s, 2\pi nz/\sqrt{-d}).$$

Notice that the inner sum in (2.1) is $(\vartheta_K(u) - h)/(2w)$. Thus

$$\int_1 = \frac{1}{2w} \int_0^z \vartheta_K(u) u^{s-1} du - \frac{h}{2w} \int_0^z u^{s-1} du.$$

The later integral above is $\frac{-hz^s}{2ws}$. From theorem 1 we know that $\vartheta_K(z) = \vartheta_K(1/z)/z$. Thus the first integral above is

$$\frac{1}{2w}\int_0^z \vartheta_K(1/u)u^{s-2}du = \frac{1}{2w}\int_0^z \Big(h + 2w\sum_{n=1}^{\infty} r(n)e^{-2\pi n/u\sqrt{-d}}\Big)u^{s-2}du$$
$$= \frac{hz^{s-1}}{2w(s-1)} + \int_0^{\infty}\Big(\sum_{n=1}^{\infty} r(n)e^{-2\pi n/u\sqrt{-d}}\Big)u^{s-2}du.$$

Using a change of variables of $v = 1/u$, we see that the integral above is

$$\int_{1/z}^{\infty}\Big(\sum_{n=1}^{\infty} r(n)e^{-2\pi nv/\sqrt{-d}}\Big)v^{-s}dv.$$

Changing the order of summation and integration and using the change of variables of $x = 2\pi nv/\sqrt{-d}$ we obtain

$$(-d)^{(1-s)/2}(2\pi)^{s-1}\sum_{n=1}^{\infty} r(n)n^{s-1}\Gamma(1-s, 2\pi n/(z\sqrt{-d})).$$

Putting the integrals $\int_1$ and $\int_2$ together we obtain the result. $\square$

Theorem 6. *The function $\zeta_K(s)$ is a meromorphic function whose only singularity is a simple pole at $s = 1$ with residue $h\pi/(w\sqrt{-d})$.*

Proof. Isolating the Dedekind zeta function in the equation in theorem 5 gives that for $\Re(z) \geq 0$,

$$\begin{aligned}\zeta_K(s) = &\frac{1}{\Gamma(s)}\sum_{n=1}^{\infty} r(n)n^{-s}\Gamma(s, 2\pi nz/\sqrt{-d})\\ &+\frac{1}{\Gamma(s)}(-d)^{(1-2s)/2}(2\pi)^{2s-1}\sum_{n=1}^{\infty} r(n)n^{s-1}\Gamma(1-s, 2\pi n/(z\sqrt{-d}))\\ &+\frac{(2\pi)^s hz^{s-1}}{\Gamma(s)d^{s/2}2w(s-1)} - \frac{(2\pi)^s hz^s}{\Gamma(s)d^{s/2}2ws}.\end{aligned} \tag{2.2}$$

By properties of the gamma function and the incomplete gamma function, the two sums above represent entire functions. Hence the right side of the equation above is analytic for all s except $s = 0, 1$. The fact that $\zeta_K(s)$ is also analytic at $s = 0$

follows from theorem 8 below. To see that ζ_K as a simple pole at $s = 1$, observe that $\lim_{s\to 1} |\zeta_K(s)| = \infty$ by the last term above forcing this to happen. Furthermore, by $\lim_{s\to 1} |(s-1)\zeta_K(s)| \neq \infty$, this pole is simple. Therefore ζ_K is meromorphic and the only singularity is a simple pole at $s = 1$. To find the residue at $s = 1$, notice

$$\begin{aligned} Res_{s=1}(\zeta_K(s)) &= \lim_{s\to 1}(s-1)\zeta_K(s) \\ &= \lim_{s\to 1}(s-1)\frac{1}{\Gamma(s)}(-d)^{-s/2}(2\pi)^s\frac{hz^{s-1}}{2w(s-1)} \\ &= \frac{1}{\Gamma(1)}(-d)^{-1/2}(2\pi)\frac{h}{2w} \\ &= h\pi/(w\sqrt{-d}) \end{aligned}$$

where the second equality above follows from all the other terms in the right side of (2.2) going to zero. This completes the proof. □

Theorem 7. *Put $\xi_K(s) = \zeta_K(s)\Gamma(s)(-d)^{s/2}(2\pi)^{-s}$. Then it follows that $\xi_K(s) = \xi_K(1-s)$ for all s except $s = 1$ and $s = 0$.*

Proof. If we replace s by $1-s$ in the equality in Theorem 5 we see that

$$\begin{aligned} \xi_K(1-s) &= \zeta_K(1-s)\Gamma(1-s)(-d)^{(1-s)/2}(2\pi)^{s-1} \\ &= (-d)^{(1-s)s/2}(2\pi)^{s-1}\sum_{n=1}^{\infty} r(n)n^{s-1}\Gamma(1-s, 2\pi nz/\sqrt{-d}) \\ &+ (-d)^{s/2}(2\pi)^{-s}\sum_{n=1}^{\infty} r(n)n^{-s}\Gamma(s, 2\pi n/z\sqrt{-d}) \\ &+ \frac{hz^{-s}}{2w(-s)} + \frac{hz^{1-s}}{2w(1-s)}. \end{aligned}$$

Now doing a change of variables of z mapped to $1/z$ and cleaning up the equation we see that the above is equal to the desired $\xi_K(s)$. □

Theorem 8. *The value of the Dedekind zeta function at zero is equal to $-h/(2w)$.*

Proof. By Theorem 7 we have that

$$\zeta_K(s)\Gamma(s)(-d)^{s/2}(2\pi)^{-s} = \zeta_K(1-s)\Gamma(1-s)(-d)^{(1-s)s/2}(2\pi)^{-(1-s)},$$

for all $s \neq 0, 1$. If we multiply the above equation by $s-1$ and take the limit as s approaches 1, we see that the left hand side above goes to

$$Res(\zeta_K(s), 1)(-d)^{1/2}(2\pi)^{-1} = h/(2w)$$

by the residue calculation in Theorem 3. As s approaches 1 on the right hand side we get

$$\zeta_K(0)Res(\Gamma(s), 0)(-d)^0(2\pi)^0 = -\zeta_K(0).$$

Thus equating these limits and multiplying by -1 on both sides yields the result. □

Theorem 9. *For all positive integers k we have that $\zeta_K(-k) = 0$.*

Proof. Solving for $\zeta_K(s)$ from the functional equation in Theorem 4 yields

$$\zeta_K(s) = \zeta_K(1-s)\frac{\Gamma(1-s)}{\Gamma(s)}(-d)^{1-s}(2\pi)^{2s-1}.$$

By Theorem 6 we know that $\zeta_K(s)$ is meromorphic with only one singularity at $s = 1$. Hence for k any positive integer, $\zeta_K(1-(-k)) = \zeta_K(1+k)$ is well defined. Also by $\Gamma(s)$ being analytic for positive real numbers, again for any k a positive integer, $\Gamma(1-(-k)) = \Gamma(1+k)$ is also well-defined. However since $\Gamma(s)$ has poles at the negative integers, $1/\Gamma(s)$ has simple zeros at the negative integers. Thus for all positive integers k, it follows that

$$\zeta_K(-k) = \zeta_K(1+k)\frac{\Gamma(1+k)}{\Gamma(-k)}(-d)^{1+k}(2\pi)^{-2k-1} = 0.$$

□

Bibliography

[1] H. Iwaniec, E. Kowalski, 'Analytic Number Theory,' Amer. Math., Providence, RI, (2004), 269–291.

[2] G. Janusz, 'Algebraic Number Fields,' Academic Press, New York (1973), 117–130.

[3] H. Montgomery, R. Vaughan, 'Multiplicative Number Theory I. Classical Theory,' Cambridge University Press, New York (2007), 326–344.

[4] J. Neukirch, 'Class Field Theory,' Springer, New York (1980), 117–121.

[5] P. Samuel, 'Algebraic Theory of Numbers,' Dover Publications, New York (1970).

[6] A. Weil, 'Basic Number Theory,' Springer, New York (1974), 120–138.

Chapter 3

Carmichael Numbers composed of Primes from a Beatty Sequence

3.1 Introduction

If N is a prime number, *Fermat's little theorem* asserts that

$$a^N \equiv a \pmod{N} \qquad \text{for all } a \in \mathbb{Z}.$$

Around 1910, Robert Carmichael initiated the study of composite numbers N with the same property, which are now known as *Carmichael numbers*. In 1994 the existence of infinitely many Carmichael numbers was first established by Alford, Granville and Pomerance [1]. In recent years, using variants of the method of [1], several arithmetically defined classes of Carmichael numbers have been shown to contain infinitely many members; see [4, 5, 6, 14].

In the present note we consider the problem of constructing Carmichael numbers that are composed of primes from a Beatty sequence. We recall that for fixed $\alpha, \beta \in \mathbb{R}$ the associated *non-homogeneous Beatty sequence* is the sequence of integers defined by

$$\mathscr{B}_{\alpha,\beta} = \big(\lfloor \alpha n + \beta \rfloor \big)_{n \in \mathbb{Z}}.$$

Beatty sequences appear in many seemingly unrelated mathematical settings, and because of this versatility, the arithmetic properties of Beatty sequences have been extensively explored in the literature; see, for example, [1, 7, 8, 9, 10, 13, 16, 17, 20, 21, 26] and the references contained therein.

Theorem 10. *Let $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, and suppose that α is irrational and of finite type. Then, there are infinitely many Carmichael numbers composed solely of primes from the Beatty sequence $\mathscr{B}_{\alpha,\beta}$.*

A quantitative version of this result is given in §3.4; see Theorem 12. To prove Theorem 18, we show that when α is of finite type (see §3.2.2) the set of primes in a Beatty sequence is sufficiently well-distributed over arithmetic progressions that one can construct Carmichael numbers from such primes using an adaptation of the method of [1]. To do this, we extend various results and techniques of Banks and Shparlinski [7].

Conjecture. *The conclusion of Theorem 10 also holds when α is an irrational number of infinite type.*

For irrational numbers α of infinite type, the approach described above fails. However, assuming the validity of a certain natural extension of Dickson's conjecture (see Conjecture II in §3.5) we establish the above conjecture in the case that $\beta = 1$ (see Theorem 14 in §3.5). This method can be adapted to conditionally establish many other cases of the conjecture.

3.2 Preliminaries

3.2.1 General notation

The notation $[\![t]\!]$ is used to denote the distance from the real number t to the nearest integer; that is,

$$[\![t]\!] = \min_{n\in\mathbb{Z}} |t-n| \qquad (t \in \mathbb{R}).$$

We denote by $\lfloor t\rfloor$ and $\{t\}$ the greatest integer $\leqslant t$ and the fractional part of t, respectively. We also put $e(t) = e^{2\pi i t}$ for all $t \in \mathbb{R}$. As usual, we use $\Lambda(\cdot)$ and $\varphi(\cdot)$ to denote the von Mangoldt and Euler functions, respectively.

Throughout the paper, the implied constants in symbols O, $\ll$ and $\gg$ may depend on the parameters α, β and ε but are absolute otherwise. We recall that for functions F and G the notations $F \ll G$, $G \gg F$ and $F = O(G)$ are all equivalent to the statement that the inequality $|F| \leqslant C\,|G|$ holds for some constant $C > 0$.

3.2.2 Discrepancy and type

Recall that the *discrepancy* $D(M)$ of a sequence of (not necessarily distinct) real numbers $a_1, a_2, \ldots, a_M \in [0,1)$ is defined by

$$D(M) = \sup_{\mathcal{I}\subseteq[0,1)} \left| \frac{V(\mathcal{I},M)}{M} - |\mathcal{I}| \right|, \tag{3.1}$$

where the supremum is taken over all intervals $\mathcal{I}$ contained in $[0,1)$, $V(\mathcal{I},M)$ denotes the number of positive integers $m \leqslant M$ such that $a_m \in \mathcal{I}$, and $|\mathcal{I}|$ denotes the length of the interval $\mathcal{I}$.

The *type* $\tau = \tau(\gamma)$ of an irrational number γ is defined via the relation

$$\tau = \sup\left\{t \in \mathbb{R} : \liminf_{n\to\infty}\ n^t\,[\![\gamma n]\!] = 0\right\}.$$

By Dirichlet's approximation theorem, one has $\tau \geqslant 1$ for every irrational number γ. The theorems of Khinchin [15] and of Roth [23, 24] assert that $\tau = 1$ for almost all real numbers (in the sense of the Lebesgue measure) and all irrational algebraic numbers γ, respectively; see also [11, 25].

For every irrational number γ, the sequence of fractional parts $(\{n\gamma\})_{n=1}^{\infty}$ is uniformly distributed in $[0,1)$ (see, e.g., [18, Example 2.1, Chapter 1]). In the case that γ is of finite type, the following more precise statement holds (see [18, Theorem 3.2, Chapter 2]).

Lemma 3. *Let γ be a fixed irrational number of finite type τ. Then, for every $\delta \in \mathbb{R}$ the discrepancy $D_{\gamma,\delta}(M)$ of the sequence $(\{\gamma m + \delta\})_{m=1}^{M}$ satisfies the bound*

$$D_{\gamma,\delta}(M) \leqslant M^{-1/\tau + o(1)} \qquad (M \to \infty),$$

where the function implied by $o(\cdot)$ depends only on γ.

3.2.3 Numbers in a Beatty sequence

The following lemma provides a convenient characterization of the numbers which occur in a Beatty sequence $\mathscr{B}_{\alpha,\beta}$.

Lemma 4. *Let $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, and put $\gamma = \alpha^{-1}$, $\delta = \alpha^{-1}(1-\beta)$. Then, $n \in \mathscr{B}_{\alpha,\beta}$ if and only if $\psi(\gamma n + \delta) = 1$, where $\psi = \psi_\alpha$ is the periodic function defined by*

$$\psi(t) = \begin{cases} 1 & \text{if } 0 < \{t\} \leqslant \alpha^{-1}, \\ 0 & \text{otherwise.} \end{cases} \tag{3.2}$$

3.2.4 Sums with the von Mangoldt function

The next statement is a simplified and weakened version of a theorem of Balog and Perelli [3] (see also [19]).

Lemma 5. *For an arbitrary real number θ and coprime integers c and d with $0 \leqslant c < d$, if $\left|\theta - a/q\right| \leqslant 1/x$ and $\gcd(a,q) = 1$, then*

$$\sum_{\substack{n \leqslant x \\ n \equiv c \,(\mathrm{mod}\ d)}} \Lambda(n) e(\theta n) \ll \left(q^{-1/2}x + q^{1/2}x^{1/2} + x^{4/5}\right)(\log x)^3.$$

As an application of Lemma 5 we derive the following statement, which is an explicit version of [7, Theorem 4.2].

Lemma 6. *Let γ be an irrational number of finite type τ, and fix $A \in (0,1)$ and $\varepsilon > 0$. For any coprime integers c and d with $0 \leqslant c < d$ and any nonzero integer k such that $|k| \leqslant x^A$, the bound*

$$\sum_{\substack{n \leqslant x \\ n \equiv c \,(\mathrm{mod}\ d)}} \Lambda(n) e(k\gamma n) \ll x^{\frac{A+2+1/\tau}{2+2/\tau}+\varepsilon} + x^{4/5}(\log x)^3$$

holds, where the implied constant depends only on the parameters α, β, A and ε.

Proof. It suffices to prove this for $\varepsilon \in (0, \frac{1}{3})$. Put

$$B = \frac{A+1}{1+1/\tau}, \qquad C = \frac{\tau(1+\varepsilon)}{1-\varepsilon\tau}, \qquad D = \frac{A+1}{1+1/\tau} + 2\varepsilon.$$

Note that $B \in (0,1)$ (since $\tau \geqslant 1$ for an irrational γ), $C \in (\tau, 2\tau)$, and

$$D = B + 2\varepsilon > B(1+\varepsilon) = \frac{A+1}{1+1/C},$$

which implies that

$$-A + C/D > 1 - D. \tag{3.3}$$

Since $C \in (\tau, 2\tau)$ and γ is of type τ, we have

$$[\![\gamma m]\!] \geqslant c_0 |m|^{-C} \qquad (m \in \mathbb{Z},\ m \neq 0) \tag{3.4}$$

for some number $c_0 > 0$ that depends only on τ and ε.

Let a/q be the convergent in the continued fraction expansion of $k\gamma$ which has the largest denominator q not exceeding $c_0^{-1}x^D$; then,

$$\left|k\gamma - \frac{a}{q}\right| \leqslant \frac{1}{qc_0^{-1}x^D} = \frac{c_0}{qx^D}\,. \tag{3.5}$$

Multiplying by q and using (3.4) we have

$$c_0x^{-D} \geqslant |qk\gamma - a| \geqslant [\![qk\gamma]\!] \geqslant c_0|qk|^{-C}.$$

Since $|k| \leqslant x^A$ it follows that $q \geqslant x^{-A+D/C}$. By (3.3) we have $q \geqslant c_0x^{1-D}$ for all sufficiently large x, hence by (3.5) we see that $|k\gamma - a/q| \leqslant 1/x$. Applying Lemma 5 with $\theta = k\gamma$, and taking into account our choice of D and the inequalities $c_0x^{1-D} \leqslant q \leqslant c_0^{-1}x^D$, we derive the stated bound. □

3.3 Beatty primes in arithmetic progressions

For the remainder of the paper, let $\alpha, \beta \in \mathbb{R}$ be fixed with $\alpha > 1$, and assume that α is irrational. The following statement provides an explicit version of [7, Theorem 5.4].

Theorem 11. *If α is of finite type $\tau = \tau(\alpha)$, then for any fixed $\varepsilon > 0$ we have*

$$\sum_{\substack{n\leqslant x,\ n\in\mathscr{B}_{\alpha,\beta}\\ n\equiv c\,(\mathrm{mod}\ d)}} \Lambda(n) = \frac{1}{\alpha}\sum_{\substack{n\leqslant x\\ n\equiv c\,(\mathrm{mod}\ d)}} \Lambda(n) + O\big(x^{1-1/(4\tau+2)+\varepsilon}\big), \tag{3.6}$$

where the implied constant depends only on the parameters α, β and ε.

Proof. Let $F(x; d, a)$ denote the left side of (3.6), and let $\psi = \psi_\alpha$ be defined by (3.2). In view of Lemma 4 we have

$$F(x; d, a) = \sum_{\substack{n\leqslant x\\ n\equiv c\,(\mathrm{mod}\ d)}} \Lambda(n)\psi(\gamma n + \delta),$$

where $\gamma = \alpha^{-1}$ and $\delta = \alpha^{-1}(1-\beta)$. Note that α and γ are of the same type, that is, $\tau(\alpha) = \tau(\gamma)$.

By a classical result of Vinogradov (see [27, Chapter I, Lemma 12]), for any Δ such that $0 < \Delta < \frac{1}{8}$ and $\Delta \leqslant \frac{1}{2}\min\{\gamma, 1-\gamma\}$, there is a real-valued function Ψ with the following properties:

(i) Ψ is periodic with period one;

(ii) $0 \leqslant \Psi(t) \leqslant 1$ for all $t \in \mathbb{R}$;

(iii) $\Psi(t) = \psi(t)$ if $\Delta \leqslant \{t\} \leqslant \gamma - \Delta$ or if $\gamma + \Delta \leqslant \{t\} \leqslant 1 - \Delta$;

(iv) $\Psi(t) = \sum_{k\in\mathbb{Z}} g(k)e(kt)$ for all $t \in \mathbb{R}$, where $g(0) = \gamma$, and the other Fourier coefficients satisfy the uniform bound

$$g(k) \ll \min\left\{|k|^{-1}, |k|^{-2}\Delta^{-1}\right\} \qquad (k \neq 0). \tag{3.7}$$

Using properties (i)–(iii) it follows that

$$F(x; d, a) = \sum_{\substack{n\leqslant x\\ n\equiv c \,(\mathrm{mod}\ d)}} \Lambda(n)\Psi(\gamma n + \delta) + O\big(V(\mathcal{I}, x)\log x\big), \tag{3.8}$$

where $V(\mathcal{I}, x)$ is the number of positive integers $n \leqslant x$ such that

$$\{\gamma n + \delta\} \in \mathcal{I} = [0, \Delta) \cup (\gamma - \Delta, \gamma + \Delta) \cup (1 - \Delta, 1).$$

Since $|\mathcal{I}| = 4\Delta$, it follows from the definition (3.1) and Lemma 3 that

$$V(\mathcal{I}, x) \ll \Delta x + x^{1-1/\tau+o(1)} \qquad (x \to \infty). \tag{3.9}$$

Now let $K \geqslant \Delta^{-1}$ be a large real number, and let Ψ_K be the trigonometric polynomial defined by

$$\Psi_K(t) = \sum_{|k|\leqslant K} g(k)e(kt). \tag{3.10}$$

Using (3.7) it is clear that the estimate

$$\Psi(t) = \Psi_K(t) + O(K^{-1}\Delta^{-1}) \tag{3.11}$$

holds uniformly for all $t \in \mathbb{R}$. Combining (3.11) with (3.8) and taking into account (3.9), we derive that

$$F(x; d, a) = \sum_{\substack{n \leqslant x \\ n \equiv c \,(\mathrm{mod}\ d)}} \Lambda(n)\Psi_K(\gamma n + \delta) + O\big(\Delta x \log x + x^{1-1/\tau+\varepsilon} + K^{-1}\Delta^{-1}x\big).$$

For fixed $A \in (0, 1)$ (to be specified below) we now set

$$\Delta = x^{-A/2} \qquad \text{and} \qquad K = x^A.$$

By the definition (3.10) it follows that

$$F(x; d, a) = \sum_{|k| \leqslant x^A} g(k)e(k\delta) \sum_{\substack{n \leqslant x \\ n \equiv c \,(\mathrm{mod}\ d)}} \Lambda(n)e(k\gamma n) + O\big(x^{1-1/\tau+\varepsilon} + x^{1-A/2+\varepsilon}\big).$$

Using Lemma 6 together with (3.7) we see that

$$\begin{aligned} \sum_{\substack{|k| \leqslant x^A \\ k \neq 0}} g(k)e(k\delta) \sum_{\substack{n \leqslant x \\ n \equiv c \,(\mathrm{mod}\ d)}} \Lambda(n)e(k\gamma n) &\ll \sum_{\substack{|k| \leqslant x^A \\ k \neq 0}} |k|^{-1} \Bigg| \sum_{\substack{n \leqslant x \\ n \equiv c \,(\mathrm{mod}\ d)}} \Lambda(n)e(k\gamma n) \Bigg| \\ &\ll x^{\frac{A+2+1/\tau}{2+2/\tau}+\varepsilon} + x^{4/5}(\log x)^4. \end{aligned}$$

Since $g(0) = \gamma$ we therefore have

$$F(x; d, a) = \gamma \sum_{\substack{n \leqslant x \\ n \equiv c \,(\mathrm{mod}\ d)}} \Lambda(n) + O\left(x^{\frac{A+2+1/\tau}{2+2/\tau}+\varepsilon} + x^{4/5+\varepsilon} + x^{1-1/\tau+\varepsilon} + x^{1-A/2+\varepsilon}\right).$$

Taking $A = 1/(2\tau + 1)$ we obtain the desired estimate (3.6). □

3.4 Construction of Carmichael numbers

In this section, we outline our proof of Theorem 18. We shall be brief since our construction of Carmichael numbers composed of primes from Beatty sequence $\mathscr{B}_{\alpha,\beta}$

closely parallels (and relies on) the construction of “ordinary” Carmichael numbers given in [1]. Here, we discuss only those modifications that are needed to establish Theorem 18.

Let $\mathscr{P}$ denote the set of all prime numbers, and set $\mathscr{P}_{\alpha,\beta} = \mathscr{P} \cap \mathscr{B}_{\alpha,\beta}$. The underlying idea behind our proof of Theorem 18 is to show that $\mathscr{P}_{\alpha,\beta}$ is sufficiently well-distributed over arithmetic progressions so that, following the method of [1], the primes used to form Carmichael numbers can all be drawn from $\mathscr{P}_{\alpha,\beta}$ rather than $\mathscr{P}$. Unfortunately, this idea appears only to succeed in the case that α is of finite type, which we now assume for the remainder of this section.

Let $\tau = \tau(\alpha) < \infty$ be the type of α. Using the standard estimate

$$\sum_{n \leqslant x} \Lambda(n) = \sum_{p \leqslant x} \log p + O(x^{1/2})$$

together with Theorem 11, it follows that

$$\left| \sum_{\substack{p \leqslant x,\ p \in \mathscr{B}_{\alpha,\beta} \\ p \equiv c \,(\mathrm{mod}\ d)}} \log p - \frac{1}{\alpha} \sum_{\substack{p \leqslant x \\ p \equiv c \,(\mathrm{mod}\ d)}} \log p \right| \leqslant x^{1-1/(4\tau+2)+\varepsilon} \qquad (x \geqslant x_1(\alpha,\beta,\varepsilon)).$$

For any modulus $d \leqslant (4\alpha)^{-1} x^{1/(4\tau+2)-\varepsilon}$ the right side of this inequality does not exceed $x/(4\alpha\varphi(d))$; therefore, applying [1, Theorem 2.1] and taking into account the above inequality, we derive the following statement, which plays a role in our construction analogous to that played by [1, Theorem 2.1].

Lemma 7. *For every $B \in \left(0, \frac{1}{4\tau+2}\right)$ there exist numbers $\eta_B > 0$, $x_2(B)$ and D_B such that for all $x \geqslant x_2(B)$ there is a set $\mathcal{D}_B(x)$ consisting of at most D_B integers such that*

$$\left| \sum_{\substack{p \leqslant x,\ p \in \mathscr{B}_{\alpha,\beta} \\ p \equiv c \,(\mathrm{mod}\ d)}} \log p - \frac{x}{\alpha\varphi(d)} \right| \leqslant \frac{x}{2\alpha\,\varphi(d)}$$

whenever d is not divisible by any element of $\mathcal{D}_B(x)$, $1 \leqslant d \leqslant x^B$, and c is coprime to d. Furthermore, every number in $\mathcal{D}_B(x)$ exceeds $\log x$, and all, but at most one, exceeds x^{η_B}.

We remark that, in the statement of Lemma 7, η_B, $x_2(B)$, D_B and $\mathcal{D}_B(x)$ all depend on the parameters α and β, but we have suppressed this from the notation for the sake of clarity. Similarly, $x_3(B)$ depends on α and β in the statement of Lemma 8 below.

As an application of Lemma 7 we deduce the following statement, which extends [1, Theorem 3.1] to the setting of primes in a Beatty sequence.

Lemma 8. *Suppose that $B \in \big(0, \frac{1}{4\tau+2}\big)$. There exists a number $x_3(B)$ such that if $x \geqslant x_3(B)$ and L is a squarefree integer not divisible by any prime exceeding $x^{(1-B)/2}$ and for which $\sum_{\text{prime } q \mid L} 1/q \leqslant (1-B)/(32\alpha)$, then there is a positive integer $k \leqslant x^{1-B}$ with $\gcd(k, L) = 1$ such that*

$$\begin{aligned}\#\big\{d \mid L : dk+1 \leqslant x \text{ and } p = dk+1 \text{ is a prime in } \mathscr{B}_{\alpha,\beta}\big\}\\ \geqslant \frac{2^{-D_B-2}}{\alpha \log x}\,\#\big\{d \mid L : 1 \leqslant d \leqslant x^B\big\}.\end{aligned}$$

Sketch of Proof. Let $\pi(x; d, a)$ [*resp.* $\pi_{\alpha,\beta}(x; d, a)$] be the number of primes [*resp.* primes in $\mathscr{P}_{\alpha,\beta}$] up to x that belong to the arithmetic progression a mod d. Using Lemma 7 we can replace the lower bound [1, Equation (3.2)] with the bound

$$\pi_{\alpha,\beta}(dx^{1-B}; d, 1) \geqslant \frac{1}{2\alpha}\frac{dx^{1-B}}{\varphi(d)\log x}\,.$$

Also, since $\pi_{\alpha,\beta}(x; d, a)$ never exceeds $\pi(x; d, a)$, the upper bound that follows [1, Equation (3.2)] can be replaced with the bound

$$\pi_{\alpha,\beta}(dx^{1-B}; dq, 1) \leqslant \frac{8}{q(1-B)}\frac{dx^{1-B}}{\varphi(d)\log x}\,.$$

Taking into account the inequality $\sum_{\text{prime } q \mid L} 1/q \leqslant (1-B)/(32\alpha)$, the proof is completed using arguments given in the proof of [1, Theorem 3.1]. □

Let $\pi(x)$ be the number of primes $p \leqslant x$, and let $\pi(x,y)$ be the number of those for which $p-1$ is free of prime factors exceeding y. As in [1], we denote by $\mathcal{E}$ the set of numbers E in the range $0 < E < 1$ for which there exist numbers $x_4(E), \gamma(E) > 0$ such that

$$\pi(x, x^{1-E}) \geqslant \gamma(E)\pi(x)$$

for all $x \geqslant x_4(E)$. With only a very slight modification to the proof of [1, Theorem 4.1], using Lemma 8 in place of [1, Theorem 3.1], we derive the following quantitative version of Theorem 18.

Theorem 12. *For each $E \in \mathcal{E}$, $B \in \left(0, \frac{1}{4\tau+2}\right)$ and $\varepsilon > 0$, there is a number $x_4 = x_4(\alpha, \beta, E, B, \varepsilon)$ such that for any $x \geqslant x_4$, there are at least $x^{EB-\varepsilon}$ Carmichael numbers up to x composed solely of primes from $\mathscr{P}_{\alpha,\beta}$.*

3.5 Dickson's conjecture and Beatty primes

As before, we fix $\alpha, \beta \in \mathbb{R}$ with $\alpha > 1$, and assume that α is irrational. In this section, *we do not assume that α is of finite type.*

Let $\{f_1, \ldots, f_k\}$ be a set of linear polynomials of the type $f_j(X) = a_jX + b_j$ with $a_j, b_j \in \mathbb{Z}$ and $a_j \geqslant 1$. In 1904, Leonard Dickson [12] made the following well known and widely believed conjecture.

Conjecture I. *Suppose that there is no integer $n > 1$ with the property that $n \mid f_1(m) \cdots f_k(m)$ for all $m \in \mathbb{Z}$. Then, there exist infinitely many $m \in \mathbb{N}$ such that all of the numbers $f_1(m), \ldots, f_k(m)$ are prime.*

Let $\mathcal{S}$ be the set of natural numbers m for which $f_1(m), \ldots, f_k(m)$ are all prime numbers. If $\mathcal{S}$ is an infinite set, then it seems reasonable to expect that for every irrational number γ the sequence of fractional parts $(\{m\gamma\})_{m \in \mathcal{S}}$ is uniformly distributed in $[0, 1)$; in particular, for any interval $\mathcal{I}$ contained in $[0, 1)$ we expect that

$$\lim_{M \to \infty} \frac{\#\{m \leqslant M : m \in \mathcal{S} \text{ and } \{m\gamma\} \in \mathcal{I}\}}{\#\{m \leqslant M : m \in \mathcal{S}\}} = |\mathcal{I}|. \tag{3.12}$$

This is easy to prove when $k = 1$ (see [22]), and this is the only case in which the truth of Conjecture I has been established (Dirichlet's theorem). For other cases, numerical evidence in support of (3.12) can be acquired when the set $\{f_1, \ldots, f_k\}$ and the interval $\mathcal{I}$ have been specified explicitly. For our purposes here, however, we require only a weak hypothesis implied by (3.12).

Conjecture II. *If $\mathcal{S}$ is an infinite set, then for every irrational number γ and every interval $\mathcal{I}$ in $[0, 1)$ with $|\mathcal{I}| > 0$, there are infinitely many numbers $m \in \mathcal{S}$ for which $\{m\gamma\} \in \mathcal{I}$.*

Combining both conjectures, we obtain the following conditional result.

Theorem 13. *Assume both Conjectures I and II are true, and suppose that*

(*i*) *there is no integer $n > 1$ such that $n \mid f_1(m) \cdots f_k(m)$ for all $m \in \mathbb{Z}$;*

(*ii*) *there is an integer m such that all of the numbers $f_1(m), \ldots, f_k(m)$ lie in the Beatty sequence $\mathscr{B}_{\alpha,\beta}$.*

Then, for infinitely many $m \in \mathbb{N}$, all of the numbers $f_1(m), \ldots, f_k(m)$ are prime numbers that occur in $\mathscr{B}_{\alpha,\beta}$.

Proof. For any real numbers c, d with $c < d$, we denote by $(c, d] + \mathbb{Z}$ the sumset of the interval $(c, d]$ and $\mathbb{Z}$; that is,

$$(c, d] + \mathbb{Z} = \big\{x + m : x \in (c, d] \text{ and } m \in \mathbb{Z}\big\}.$$

Let Ω be the collection of all such sumsets $(c, d] + \mathbb{Z}$ together with the empty set $\varnothing$, and let Ω° be the collection of all finite unions of sets in Ω. Note that Ω is closed under finite intersections, and Ω° is closed under finite intersections and finite unions.

As before, we let $\mathcal{S}$ denote the set of $m \in \mathbb{N}$ such that $f_1(m), \ldots, f_k(m)$ are all prime numbers. Under Conjecture I and using (i) we see that $\mathcal{S}$ is an infinite set. Hence, under Conjecture II it follows that for any irrational number γ, the set $\mathcal{S}\gamma = \{m\gamma : m \in \mathcal{S}\}$ has an infinite intersection with every set $(c, d]+\mathbb{Z}$, and therefore $\mathcal{S}\gamma$ has an infinite intersection with every nonempty set in Ω°.

For each $j = 1, \ldots, k$ it follows from Lemma 4 that

$$\begin{aligned} f_j(m) \in \mathscr{B}_{\alpha,\beta} \quad &\Longleftrightarrow \quad \gamma(a_j m + b_j) + \delta \in (0, \gamma] + \mathbb{Z} \\ &\Longleftrightarrow \quad \gamma m \in \bigcup_{i=1}^{a_j} \Big((c_{i,j}, d_{i,j}] + \mathbb{Z}\Big), \end{aligned}$$

where

$$c_{i,j} = \frac{i - \gamma b_j - \delta}{a_j} \qquad \text{and} \qquad d_{i,j} = c_{i,j} + \frac{\gamma}{a_j} \qquad (i = 1, \ldots, a_j).$$

Hence, if we put

$$\mathcal{T} = \bigcap_{j=1}^{k} \Bigl(\bigcup_{i=1}^{a_j} \bigl((c_{i,j}, d_{i,j}] + \mathbb{Z} \bigr) \Bigr),$$

then $m\gamma \in \mathcal{T}$ if and only if all of the numbers $f_1(m), \ldots, f_k(m)$ lie in the Beatty sequence $\mathscr{B}_{\alpha,\beta}$. Clearly, $\mathcal{T}$ belongs to Ω°, and $\mathcal{T} \neq \varnothing$ by (ii). By the previous argument, we conclude that $\mathcal{S}\gamma$ has an infinite intersection with $\mathcal{T}$, and the result follows. □

Theorem 14. *Assume both Conjectures I and II are true and $\beta = 1$. Then, there are infinitely many Carmichael numbers composed solely of primes from the Beatty sequence $\mathscr{B}_{\alpha,\beta}$.*

Proof. The linear polynomials

$$f_1(X) = 6X + 1, \qquad f_2(X) = 12X + 1 \qquad \text{and} \qquad f_3(X) = 18X + 1$$

satisfy condition (i) of Theorem 13, hence it suffices to show that condition (ii) also holds when $\beta = 1$. Indeed, when this is the case, Theorem 13 implies (under Conjectures I and II) that there are infinitely many triples (p, q, r) of primes in $\mathscr{B}_{\alpha,\beta}$ with $p = 6m + 1$, $q = 12m + 1$ and $r = 18m + 1$ for some $m \in \mathbb{N}$, and for any such triple the number $N = pqr$ is a Carmichael number of the required form.

When $\beta = 1$ we see that $\delta = \gamma(1 - \beta) = 0$. Hence, in the notation of the proof of Theorem 13 we have

$$a_1 = 6, \qquad a_2 = 12, \qquad a_3 = 18, \qquad b_1 = b_2 = b_3 = 1,$$

and therefore,

$$c_{6,1} = 1 - \frac{\gamma}{6}, \quad c_{12,2} = 1 - \frac{\gamma}{12}, \quad c_{18,3} = 1 - \frac{\gamma}{18}, \quad d_{6,1} = d_{12,2} = d_{18,3} = 1.$$

We deduce that $\mathcal{T}$ contains the set $(1 - \frac{\gamma}{18}, 1] + \mathbb{Z}$, which shows that condition (ii) of Theorem 13 is satisfied. $\square$

Bibliography

[1] A. Abercrombie, 'Beatty sequences and multiplicative number theory,' *Acta Arith.* **70** (1995), 195–207.

[2] W. Alford, A. Granville, and C. Pomerance, 'There are infinitely many Carmichael numbers,' *Ann. of Math. (2)* **139** (1994), 703–722.

[3] A. Balog and A. Perelli, 'Exponential sums over primes in an arithmetic progression,' *Proc. Amer. Math. Soc.* **93** (1985), 578–582.

[4] W. Banks, 'Carmichael numbers with a square totient,' *Canad. Math. Bull.* **52** (1) (2009), no. 1, 3–8.

[5] W. Banks, 'Carmichael numbers with a totient of the form $a^2 + nb^2$,' to appear in *Monat. Math.*

[6] W. Banks and C. Pomerance, 'On Carmichael numbers in arithmetic progressions,' *J. Aust. Math. Soc.* **88** (2010), 313–321.

[7] W. Banks and I. Shparlinski, 'Prime numbers with Beatty sequences,' *Colloq. Math.* **115** (2009), no. 2, 147–157.

[8] W. Banks and I. Shparlinski, 'Non-residues and primitive roots in Beatty sequences,' *Bull. Austral. Math. Soc.* **73** (2006), 433–443.

[9] W. Banks and I. Shparlinski, 'Short character sums with Beatty sequences,' *Math. Res. Lett.* **13** (2006), 539–547.

[10] A. Begunts, 'An analogue of the Dirichlet divisor problem,' *Moscow Univ. Math. Bull.* **59** (2004), no. 6, 37–41.

[11] Y. Bugeaud, *Approximation by algebraic numbers.* Cambridge Tracts in Mathematics, **160**. Cambridge University Press, Cambridge, 2004.

[12] L. E. Dickson, 'A new extension of Dirichlet's theorem on prime numbers,' *Messenger of mathematics* **33** (1904), 155-161.

[13] A. Fraenkel and R. Holzman, 'Gap problems for integer part and fractional part sequences,' *J. Number Theory* **50** (1995), 66–86.

[14] J. Grantham, 'There are infinitely many Perrin pseudoprimes,' *J. Number Theory* **130** (2010), no. 5, 1117–1128.

[15] A. Khinchin, 'Zur metrischen Theorie der diophantischen Approximationen,' *Math. Z.* **24** (1926), no. 4, 706–714.

[16] T. Komatsu, 'A certain power series associated with a Beatty sequence,' *Acta Arith.* **76** (1996), 109–129.

[17] T. Komatsu, 'The fractional part of $n\vartheta + \varphi$ and Beatty sequences,' *J. Théor. Nombres Bordeaux* **7** (1995), 387–406.

[18] L. Kuipers and H. Niederreiter, *Uniform distribution of sequences.* Pure and Applied Mathematics. Wiley-Interscience, New York-London-Sydney, 1974.

[19] A. Lavrik, 'Analytic method of estimates of trigonometric sums by the primes of an arithmetic progression,' (Russian) *Dokl. Akad. Nauk SSSR* **248** (1979), no. 5, 1059–1063.

[20] G. Lü and W. Zhai, 'The divisor problem for the Beatty sequences,' *Acta Math. Sinica* **47** (2004), 1213–1216 (in Chinese).

[21] K. O'Bryant, 'A generating function technique for Beatty sequences and other step sequences,' *J. Number Theory* **94** (2002), 299–319.

[22] P. Ribenboim, *The new book of prime number records.* Springer-Verlag, New York, 1996.

[23] K. Roth, 'Rational approximations to algebraic numbers,' *Mathematika* **2** (1955), 1–20.

[24] K. Roth, 'Corrigendum to "Rational approximations to algebraic numbers",' *Mathematika* **2** (1955), 168.

[25] W. Schmidt, *Diophantine approximation.* Lecture Notes in Mathematics, **785**. Springer, Berlin, 1980.

[26] R. Tijdeman, 'Exact covers of balanced sequences and Fraenkel's conjecture,' *Algebraic number theory and Diophantine analysis (Graz, 1998)*, 467–483, de Gruyter, Berlin, 2000.

[27] I. Vinogradov, *The method of trigonometrical sums in the theory of numbers.* Dover Publications, Inc., Mineola, NY, 2004.

Chapter 4

Carmichael meets Chebotarev

4.1 Introduction

The aim of the present work is to prove the following extension of the result mentioned in the previous chapter, the existence of infinitely many Carmichael numbers from Alford, Grandville, and Pomerence.

Theorem 15. *Let $K/\mathbb{Q}$ be a finite Galois extension. Then, there are infinitely many Carmichael numbers composed solely of primes for which the associated class of Frobenius automorphisms equals a given conjugacy class of* $\mathrm{Gal}(K|\mathbb{Q})$.

Let $K/\mathbb{Q}$ be any number field and $\widetilde{K}$ its Galois closure. Taking the conjugacy class of the identity automorphism of $\widetilde{K}$ in Theorem 18 it follows that there exist infinitely many Carmichael numbers composed solely of primes that split completely in $\widetilde{K}$. Since such primes will necessarily split completely in K, we immediately obtain the following result.

Corollary 1. *For any fixed algebraic number field K, there are infinitely many Carmichael numbers which are composed solely of primes that split completely in K.*

Since prime numbers and Carmichael numbers are linked by the common property given by Fermat's Little Theorem, it is natural to ask whether certain questions about primes can be settled for Carmichael numbers; see [2, 3]. For example, it is well known that for every natural number n, there are infinitely many primes of the form a^2+nb^2 with $a, b \in \mathbb{Z}$ (see the book [4] by Cox), so it is natural to ask whether the same result holds for the set of Carmichael numbers. As a result of Corollary 1, we give an affirmative answer to this question.

Corollary 2. *For any fixed natural number n, there are infinitely many Carmichael numbers of the form $a^2 + nb^2$ with $a, b \in \mathbb{Z}$.*

Indeed, let $\mathcal{S}_n = \{a^2+nb^2 \ : \ a, b \in \mathbb{Z}\}$, and let K_n be the ring class field associated to the order $\mathbb{Z}[\sqrt{-n}\,]$ in the imaginary quadratic field $\mathbb{Q}(\sqrt{-n}\,)$. According to [4, Theorem 9.4], if p is an odd prime not dividing n, then p splits completely in K_n if and only if $p \in \mathcal{S}_n$. Applying Corollary 1 with $K = K_n$, we see that there are infinitely Carmichael numbers N composed solely of primes $p \in \mathcal{S}_n$. Since $\mathcal{S}_n$ is closed under multiplication, every such N also lies in $\mathcal{S}_n$, and the corollary follows.

In a different direction taking $K = \mathbb{Q}(\mu_d)$, where μ_d is a primitive dth root of unity, we obtain:

Corollary 3. *There are infinitely many Carmichael numbers composed solely of primes $p \equiv a \pmod{d}$ with a, d coprime.*

4.2 Preliminaries

Let $K/\mathbb{Q}$ be a finite Galois extension of degree $n_K = [K : \mathbb{Q}]$ and absolute discriminant $\mathscr{D}_K$. We put

$$\mathbb{N}_K = \big\{d \in \mathbb{N} \ : \ \gcd(d, \mathscr{D}_K) = 1\big\}. \tag{4.1}$$

For any Galois extension M/N and any unramified prime ideal $\mathfrak{p}$ of N, $(\mathfrak{p}, M|N)$ will denote the conjugacy class of Frobenius automorphisms of $\mathrm{Gal}(M/N)$ corresponding to the prime ideals of M above $\mathfrak{p}$.

Given a conjugacy class C in $\mathrm{Gal}(K/\mathbb{Q})$, let

$$\mathscr{P}_C = \{p \in \mathbb{N}_K \ : \ (p, K|\mathbb{Q}) = C\}.$$

For $d \in \mathbb{N}$ and M a number field, put $M_d = M(\mu_d)$, where μ_d is a primitive dth root of unity. According to [12, Proposition 2.7], the discriminant of $\mathbb{Q}_d$ is

$$\mathscr{D}_{\mathbb{Q}_d} = (-1)^{\phi(d)/2} \frac{d^{\phi(d)}}{\prod_{p\,|\,d} p^{\phi(d)/(p-1)}}\,, \tag{4.2}$$

where $\phi(\cdot)$ is the Euler function.

Lemma 9. *For each $d \in \mathbb{N}_K$, K_d is a Galois extension of $\mathbb{Q}$ of degree $n_K\phi(d)$ with discriminant*

$$\mathscr{D}_{K_d} = \mathscr{D}_K^{\phi(d)} \mathscr{D}_{\mathbb{Q}_d}^{n_K}.$$

Furthermore, Gal($K_d/\mathbb{Q}$) $\simeq Gal(K/\mathbb{Q}) \times Gal(\mathbb{Q}_d/\mathbb{Q})$, where the isomorphism is given by the restriction map $\sigma \to (\sigma_{|K}, \sigma_{|\mathbb{Q}_d})$.

Proof. In view of (4.1) and (4.2), the discriminants $\mathscr{D}_K$ and $\mathscr{D}_{\mathbb{Q}_d}$ are coprime for every $d \in \mathbb{N}_K$. It follows from [10, Ch.3, Corollary 2.10] that $K \cap \mathbb{Q}_d = \mathbb{Q}$. The result now follows from [10, Ch. 1, Proposition 2.11] and [5, 14.4, Corollary 22]. $\square$

The constants $c_0, c_1, c_2, \ldots$ that appear in our proofs are assumed to be positive and depend only on the field K. All constants implied by the symbols O, $\ll$ and $\gg$ are absolute; we write O_K, $\ll_K$ and $\gg_K$ to indicate that the implied constant depends on K.

4.3 Zeros of Dedekind zeta functions

For each $d \in \mathbb{N}_K$, let $\zeta_d(s)$ be the Dedekind zeta function $\zeta_{K_d}(s)$ associated with the field K_d considered in §4.2.

Lemma 10. *There are constants $c_1, c_2 > 0$ depending only on K with the property that for all $T \geqslant 1$ and $U \geqslant 2$ there exists a proper integral ideal $\mathfrak{f} = \mathfrak{f}(K, U, T)$ of K such that for any $d \in \mathbb{N}_K$ with $d \leqslant U$, $\mathfrak{f} \mid d\mathcal{O}_K$, where $\mathcal{O}_K$ is the ring of integers of K, whenever $\zeta_d(s)$ has a zero $\beta + i\gamma$ in the region*

$$\Omega(T,U) = \left\{ \beta + i\gamma \ : \ \beta \geqslant 1 - \frac{c_1}{\log(c_2 TU)}, \ |\gamma| \leqslant T \right\}. \tag{4.3}$$

Proof. We use the notation of [13, §1]. For each $d \in \mathbb{N}_K$ with $d \leqslant U$, and any Dirichlet character χ modulo $(d) = d\mathcal{O}_K$ of conductor $\mathfrak{f}_\chi$, we see that

$$d_\chi := |\mathscr{D}_K| \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{f}_\chi) \underset{K}{\ll} d^{n_K} \leqslant U^{n_K}.$$

Hence, it follows that $d_\chi \leqslant (c_2 U)^{n_K}$ for some constant $c_2 = c_2(K)$. Applying [13, Theorem 1.9] with $Q = (c_2 U)^{n_K}$ and

$$\mathscr{L} = \log(QT^{n_K}) = n_K \log(c_2 TU),$$

we see that for some constant $c_1 = c_1(K)$, any Hecke L-function $L(s,\chi)$ with $d_\chi \leqslant Q$ has at most one zero in the region $\Omega(T,U)$. Moreover, the remark following [13, Theorem 1.9] asserts that there is at most one function $L(s,\chi_*)$ vanishing in $\Omega(T,U)$ among all $L(s,\chi)$ associated with *primitive* characters χ with $d_\chi \leqslant Q$. If such a zero exists, then it is a real number β_* (which can be bounded in terms of Q). For such a zero we have

$$\beta_* \geqslant 1 - \frac{c_1}{\log(c_2 TU)} \geqslant 1 - \frac{c_1}{\log c_2}\,.$$

Replacing c_1 by a smaller constant (which also depends only on K), we can assume that $\zeta_K(\beta_*) \neq 0$, i.e., χ_* is not the trivial character.

By [10, Ch.7, Corollary 10.5]

$$\zeta_d(s) = \zeta_K(s) \prod_{\chi \neq 1} L(s, \chi, K_d|K)$$

is the product of Artin L-functions, where χ runs over the irreducible characters of $\mathrm{Gal}(K_d/K)$. Let K_χ be the fixed field of the kernel of χ. Then, χ is injective as a character of $\mathrm{Gal}(K_\chi/K)$. Hence, by [10, Ch.7, Theorem 10.6] there exists a *primitive* Dirichlet character $\widetilde{\chi}$ modulo the conductor $\mathfrak{f}_\chi$ of the extension K_χ/K such that

$$L(s, \chi, K_d|K) = L(s, \widetilde{\chi}).$$

Furthermore, since $K \subseteq K_\chi \subseteq K_d$, we see by [7, 5.1.5] and the last paragraph of [7, §6] that the conductor $\mathfrak{f}_\chi$ divides (d); thus, $d_{\widetilde{\chi}} \leqslant Q$.

Using the remarks above we conclude that $\zeta_d(s)$ vanishes in $\Omega(T, U)$ if and only if $L(s, \chi_*)$ is a factor of $\zeta_d(s)$ and $L(\beta_*, \chi_*) = 0$. In this case, we know that $\mathfrak{f}_{\chi_*} \mid (d)$ and $\mathfrak{f}_{\chi_*} \neq 1$; thus, we can take $\mathfrak{f} = \mathfrak{f}_{\chi_*}$. □

Lemma 11. *There are constants $c_3, c_4, c_5 > 0$ depending only on K with the property that for all $d \in \mathbb{N}_K$, $T \geqslant c_3 d$, and $\sigma \geqslant 1 - 1/c_5$, the number $N_d(\sigma, T)$ of zeros $\beta + i\gamma$ of $\zeta_d(s)$ with $\beta \geqslant \sigma$ and $|\gamma| \leqslant T$ satisfies the bound*

$$N_d(\sigma, T) \leqslant c_4 (Td)^{c_5(1-\sigma)}.$$

Proof. We continue to use notation of [13, §1]. As in the proof of Lemma 10, for each $d \in \mathbb{N}_K$ let H (in the notation of [13, §1]) denote the trivial subgroup of the ideal class group $I((d))/P_{(d)}$ modulo (d), and note that the quantities h_H and $d(H)$ defined by [13, Equation (1.1b)] satisfy the bound

$$\max\{h_H, d(H)\} \leqslant (cd)^{n_K}$$

for some constant $c = c(K)$ in view of [13, Lemma 1.16]. The result now follows by applying [13, Corollary 4.4] with $Q = (cd)^{n_K}$ and $T \geqslant c_3 d$, where $c_3 = c_3(K)$ is any constant that is large enough so that the conditions $T \gg 1$ and $T \geqslant n_K^2 h_H^{1/n_K}$ of [13, Corollary 4.4] are met (for the latter condition, any number $c_3 \geqslant cn_K^2$ suffices by the inequality above). $\square$

4.4 Chebotarev Density Theorem

Our goal in this section is to provide a lower bound for the counting function of the set

$$\mathscr{P}_{C_d} = \big\{p \in \mathscr{P}_C : \ p \equiv 1 \pmod d\big\}$$

using an effective version of the Chebotarev density theorem given by [8].

By [10, Ch.1, Corollary 10.4] we see that $p \equiv 1 \pmod d$ if and only if p splits completely in $\mathbb{Q}_d$ if and only if $(p, \mathbb{Q}_d|\mathbb{Q}) = \{\mathbf{1}_d\}$ for $p \in \mathbb{N}_K$, where $\mathbf{1}_d$ denotes the identity element of $\mathrm{Gal}(\mathbb{Q}_d|\mathbb{Q})$. It follows by the isomorphism in Lemma 9 that there exists a conjugacy class C_d in $\mathrm{Gal}(K_d/\mathbb{Q})$ (one that corresponds to $C \times \{\mathbf{1}_d\}$) with the property that

$$p \in \mathscr{P}_{C_d} \quad \Longleftrightarrow \quad (p, K_d|\mathbb{Q}) = C_d \quad (p \in \mathbb{N}_K).$$

Accordingly, we study the function

$$\pi_C(x; d, 1) = \#\{p \leqslant x \ : \ p \in \mathbb{N}_K, \, (p, K_d|\mathbb{Q}) = C_d\}$$

and its weighted version

$$\psi_C(x;d,1) = \sum_{\substack{p,\,m:\ p^m \leqslant x \\ (p^m, K_d|\mathbb{Q}) = C_d}} \log p,$$

where the sum is taken over primes in $\mathbb{N}_K$. Our main result is the following:

Theorem 16. *There are constants $x_1, B > 0$ depending only on K with the property that for all $x \geqslant x_1$ and every $d \in \mathbb{N}_K$ with $d \leqslant x^B$,*

$$\pi_C(y;d,1) \geqslant \frac{|C|}{2n_K\phi(d)} \frac{y}{\log y} \qquad (x^{4/5} \leqslant y \leqslant x) \tag{4.4}$$

whenever $\zeta_d(s)$ has no zeros in the region

$$\Omega_B(x) = \left\{ \beta + i\gamma \ : \ \beta \geqslant 1 - \frac{c_1}{\log(c_2 x^{4B})}\,, \ |\gamma| \leqslant x^{3B} \right\}. \tag{4.5}$$

Proof. Let $B = B(K)$ be a constant in the interval $(0, \frac{1}{100})$ to be further determined below. For convenience, we set

$$\theta_B(y) = \frac{c_1 \log y}{\log(c_2 y^{5B})}\,. \tag{4.6}$$

For $x^{4/5} \leqslant y \leqslant x$, we have

$$1 - \frac{\theta_B(y)}{\log y} \geqslant 1 - \frac{c_1}{\log(c_2 x^{4B})} \qquad \text{and} \qquad y^{3B} \leqslant x^{3B},$$

hence the region

$$\widetilde{\Omega}_B(y) = \left\{ \beta + i\gamma \ : \ \beta \geqslant 1 - \frac{\theta_B(y)}{\log y}\,, \ |\gamma| \leqslant y^{3B} \right\}$$

is contained in $\Omega_B(x)$; therefore, $\zeta_d(s)$ has no zeros in $\widetilde{\Omega}_B(y)$ whenever it has no zeros in $\Omega_B(x)$.

Let g be a fixed element of C_d with $d \in \mathbb{N}_K$ and $d \leqslant x^B$, $H = \langle g \rangle$ the cyclic subgroup of G generated by g, E the fixed field of H, and $\widehat{H}$ the dual of H, i.e., the set of irreducible characters $\chi : H \to \mathbb{C}^\times$.

Applying [8, Theorem 7.1] with the choices $G = \mathrm{Gal}(K_d|\mathbb{Q})$ and $T = y^{3B}$, and taking into account the bounds

$$\begin{aligned} |G| &= n_{K_d} = \phi(d) n_K \underset{K}{\ll} d \leqslant y^{2B} \\ \log |\mathscr{D}_{K_d}| &\ll \phi(d) \left(\log |\mathscr{D}_K| + n_K \log d \right) \underset{K}{\ll} y^{2B} \log y, \end{aligned} \tag{4.7}$$

which hold by Lemma 9 for all $d \leqslant x^B \leqslant y^{5B/4}$, we derive that

$$\psi_C(y; d, 1) - \frac{|C|}{|G|}\, y + \frac{|C|}{|G|}\, Z_B(y) \underset{K}{\ll} \frac{|C|}{|G|} y^{1-B} \log y \tag{4.8}$$

where we have used $|C_d| = |C|$, and

$$Z_B(y) = \sum_{\chi \in \widehat{H}} \overline{\chi}(g) \Bigg(\sum_{\substack{\rho \\ |\gamma| \leqslant T}} \frac{y^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho| < \frac{1}{2}}} \frac{1}{\rho} \Bigg).$$

Here, the inner sums are taken over the nontrivial zeros $\rho = \beta + i\gamma$ of the Artin L-functions $L(s, \chi, K_d|E)$ so that

$$\zeta_d(s) = \prod_{\chi \in \widehat{H}} L(s, \chi, K_d|E).$$

Assuming $\zeta_d(s)$ has no zeros in the region $\Omega_B(x)$, it follows by the functional equation of $\zeta_d(s)$ that every zero $\rho = \beta + i\gamma$ of $\zeta_d(s)$, and thus also of each $L(s, \chi, K_d|E)$, lies outside of the region

$$\left\{ \beta + i\gamma \ : \ 0 \leqslant \beta \leqslant \frac{\theta_B(y)}{\log y}\ ,\ |\gamma| \leqslant y^{3B} \right\},$$

and thus $|\rho| > \theta_B(y)/\log y \underset{K}{\gg} 1/\log y$ for every such zero. We conclude that

$$\sum_{\substack{\rho:\ \beta < \frac{1}{2} \\ |\gamma| \leqslant 1}} \frac{y^\rho}{\rho} - \sum_{\substack{\rho \\ |\rho| < \frac{1}{2}}} \frac{1}{\rho} \ll y^{1/2} \sum_{\substack{\rho \\ |\gamma| \leqslant 1}} \frac{1}{|\rho|} \underset{K}{\ll} n_\chi(0)\, y^{1/2} \log y,$$

where $n_\chi(t)$ is the number of zeros $\beta + i\gamma$ of $L(s, \chi, K_d|E)$ such that $0 < \beta < 1$ and $|\gamma - t| \leqslant 1$. By [8, Lemma 5.4],

$$n_\chi(t) \ll \log d_\chi + \frac{n_K \phi(d)}{|H|} \log(|t| + 2), \tag{4.9}$$

where $d_\chi = |\mathscr{D}_E|\mathrm{N}_{E/\mathbb{Q}}(\mathfrak{f}_\chi)$. Summing over all characters $\chi \in \widehat{H}$ and using (4.9) we see that

$$\begin{aligned}\sum_{\chi\in\widehat{H}}\overline{\chi}(g)\Bigg(\sum_{\substack{\rho:\ \beta<\frac12\\ |\gamma|\leqslant 1}}\frac{y^\rho}{\rho}-\sum_{\substack{\rho\\ |\rho|<\frac12}}\frac{1}{\rho}\Bigg) &\ll_K y^{1/2}\log y\sum_{\chi\in\widehat{H}}\left(\log d_\chi+\frac{d}{|H|}\right)\\ &= y^{1/2}\log y\left(\log|\mathscr{D}_{K_d}|+y^{2B}\right)\ll_K y^{1/2+2B}\log^2 y,\end{aligned}\tag{4.10}$$

where the equality $|\mathscr{D}_{K_d}| = \prod_\chi d_\chi$ follows from [10, Ch.3, Lemma 2.10] and the Conductor-Discriminant formula [10, Ch.7, Proposition 11.9]. Moreover,

$$\sum_{\substack{\rho:\ \beta<\frac12\\ 1<|\gamma|\leqslant y^{3B}}}\frac{y^\rho}{\rho}\ll y^{1/2}\sum_{\substack{\rho\\ 1\leqslant|\gamma|\leqslant y^{3B}}}\frac{1}{|\rho|}\leqslant y^{1/2}\sum_{j=1}^{\lfloor y^{3B}\rfloor}\sum_{\substack{\rho\\ j\leqslant|\gamma|\leqslant j+1}}\frac{1}{|\rho|};$$

thus, summing over the characters we obtain

$$\begin{aligned}\sum_{\chi\in\widehat{H}}\overline{\chi}(g)\sum_{\substack{\rho:\ \beta<\frac12\\ 1<|\gamma|\leqslant y^{3B}}}\frac{y^\rho}{\rho} &\ll y^{1/2}\sum_{j=1}^{\lfloor y^{3B}\rfloor}\frac{1}{j}\sum_{\chi\in\widehat{H}}\Big(\log d_\chi+\frac{n_K\phi(d)}{|H|}\log(j+1)\Big)\\ &\ll_K y^{1/2+2B}\log^2 y.\end{aligned}\tag{4.11}$$

In view of (4.10) and (4.11) we have

$$Z_B(y)=\sum_{\chi\in\widehat{H}}\overline{\chi}(C)\sum_{\substack{\rho:\ \beta\geqslant\frac12\\ |\gamma|\leqslant y^{3B}}}\frac{y^\rho}{\rho}+O_K\big(y^{1/2+2B}\log^2 y\big).\tag{4.12}$$

To estimate the sum in (4.12), we use ideas (and notation) from the proof of [1, Theorem 2.1]. For each zero $\rho=\beta+i\gamma$ in the sum, we have $|y^\rho| = y^\beta$ and $|\rho| \geqslant \frac14+|\gamma| \gg 1+|\gamma|$. Fix $\chi\in\widehat{H}$ and write $\sum_\sigma^\alpha$ for any sum over all zeros $\beta+i\gamma$ of $L(s,\chi,K_d/E)$ with $\sigma\leqslant\beta<\alpha$ and $|\gamma|\leqslant y^{3B}$. Put $\tau = 1-\theta_B(y)/\log y$, and note that

$$\sum_\tau^1\frac{y^\rho}{\rho}=0$$

since $\zeta_d(s)$ has no zeros in $\widetilde{\Omega}_B(y)$. Hence, using the upper bound $y^\beta\leqslant y^{1-1/c_5}$ when $\beta\leqslant 1-1/c_5$ and the identity $y^\beta = y^{1-1/c_5}+\log y\int_{1-1/c_5}^\beta y^\sigma\,d\sigma$ when β lies in the range $1-1/c_5 \leqslant \beta \leqslant \tau$, it follows that

$$
\begin{aligned}
\sum_{\substack{\rho \\ \beta\geqslant\frac{1}{2},\ |\gamma|\leqslant y^{3B}}} \frac{y^\rho}{\rho} &= \sum_{1/2}^{1-1/c_5} \frac{y^\rho}{\rho} + \sum_{1-1/c_5}^{\tau} \frac{y^\rho}{\rho} \ll \sum_{1/2}^{1-1/c_5} \frac{y^\beta}{1+|\gamma|} + \sum_{1-1/c_5}^{\tau} \frac{y^\beta}{1+|\gamma|} \\
&\ll y^{1-1/c_5} \sum_{1/2}^{\tau} \frac{1}{1+|\gamma|} + \log y \sum_{1-1/c_5}^{\tau} \frac{1}{1+|\gamma|} \int_{1-1/c_5}^{\beta} y^\sigma \, d\sigma \qquad (4.13) \\
&\ll y^{1-1/c_5} \sum_{\substack{\rho \\ |\gamma|\leqslant y^{3B}}} \frac{1}{1+|\gamma|} + \log y \int_{1-1/c_5}^{\tau} y^\sigma \left(\sum_{\sigma}^{\tau} \frac{1}{1+|\gamma|} \right) d\sigma.
\end{aligned}
$$

Summing over all characters and using (4.9) the first term above can be bounded as before:

$$
\begin{aligned}
\sum_{\chi\in\widehat{H}} \overline{\chi}(g) \sum_{\substack{\rho \\ |\gamma|\leqslant y^{3B}}} \frac{1}{1+|\gamma|} &\leqslant \sum_{\chi\in\widehat{H}} \sum_{j=0}^{\lfloor y^{3B}\rfloor} \sum_{\substack{\rho \\ j\leqslant|\gamma|\leqslant j+1}} \frac{1}{1+|\gamma|} \\
&\ll_K \sum_{j=0}^{\lfloor y^{3B}\rfloor} \frac{d\log d + d\log(1+j)}{j+1} \ll y^{2B}\log^2 y.
\end{aligned} \qquad (4.14)
$$

Let $N_\chi(\sigma,T)$ be the number of zeros $\beta+i\gamma$ of $L(s,\chi,K_d|E)$ with $\beta\geqslant\sigma$ and $|\gamma|\leqslant T$. Then, it follows by partial summation that for $\sigma\geqslant 1-1/c_5$,

$$
\sum_{\sigma}^{\tau} \frac{1}{1+|\gamma|} \leqslant N_\chi(\sigma, c_3 d) + \frac{N_\chi(\sigma, y^{3B})}{y^{3B}} + \int_{c_3 d}^{y^{3B}} \frac{N_\chi(\sigma,t)}{t^2}\, dt.
$$

Summing over all characters χ once again we obtain

$$
\sum_{\chi\in\widehat{H}} \overline{\chi}(g) \sum_{\sigma}^{\tau} \frac{1}{1+|\gamma|} \ll N_d(\sigma, c_3 d) + \frac{N_d(\sigma, y^{3B})}{y^{3B}} + \int_{c_3 d}^{y^{3B}} \frac{N_d(\sigma,t)}{t^2}\, dt. \qquad (4.15)
$$

By Lemma 11, we have for all $\sigma\geqslant 1-1/c_5$ and $d\leqslant x^B\leqslant y^{2B}$,

$$
\begin{aligned}
\sum_{\chi\in\widehat{H}} \overline{\chi}(g) \sum_{\sigma}^{\tau} \frac{1}{1+|\gamma|} &\ll c_4 (c_3 d^2)^{c_5(1-\sigma)} + \frac{c_4 (y^{3B} d)^{c_5(1-\sigma)}}{y^{3B}} + \int_{c_3 d}^{y^{3B}} \frac{c_4 (td)^{c_5(1-\sigma)}}{t^2}\, dt \\
&\ll_K y^{4c_5 B(1-\sigma)} + y^{2c_5 B(1-\sigma)} \int_1^{y^{3B}} \frac{t^{c_5(1-\sigma)}}{t^2}\, dt.
\end{aligned}
$$

Using the bound

$$
\int_1^{y^{3B}} \frac{t^{c_5(1-\sigma)}}{t^2}\, dt \ll_K \begin{cases} \log y & \text{if } 1-1/c_5\leqslant\sigma\leqslant 1-1/(2c_5) \\ 1 & \text{if } \sigma\geqslant 1-1/(2c_5), \end{cases}
$$

and assuming that $B < 1/(4c_5)$, we derive that

$$\begin{aligned}
&\int_{1-1/c_5}^{\tau} y^\sigma \left(\sum_{\chi\in\widehat{H}} \overline{\chi}(g) \sum_{\sigma}^{\tau} \frac{1}{1+|\gamma|} \right) d\sigma \\
&\quad \underset{K}{\ll} \int_{1-1/c_5}^{\tau} y^\sigma \cdot y^{4c_5B(1-\sigma)}\, d\sigma + \int_{1-1/c_5}^{1-1/(2c_5)} y^\sigma \cdot y^{2c_5B(1-\sigma)} \log y \, d\sigma \\
&\quad = y^{4c_5B} \int_{1-1/c_5}^{\tau} y^{\sigma(1-4c_5B)}\, d\sigma + y^{2c_5B} \log y \int_{1-1/c_5}^{1-1/(2c_5)} y^{\sigma(1-2c_5B)}\, d\sigma \\
&\quad \ll y^{4c_5B} \frac{y^{\tau(1-4c_5B)}}{(1-4c_5B)\log y} + y^{2c_5B} \frac{y^{(1-1/(2c_5))(1-2c_5B)}}{(1-2c_5B)} \\
&\quad = \frac{y\, \exp(-(1-4c_5B)\theta_B(y))}{(1-4c_5B)\log y} + \frac{y^{1+B-1/(2c_5)}}{(1-2c_5B)}
\end{aligned}$$

where we have used the definition of τ in the last step. Combining this bound with (4.12), (4.13) and (4.14), and assuming further that $B \leqslant 1/(5c_5)$, we find that

$$Z_B(y) \underset{K}{\ll} y\, \exp(-\tfrac{1}{5}\theta_B(y)).$$

Finally, using (4.8) we see that

$$\left| \psi_C(y; d, 1) - \frac{|C|}{|G|}\, y \right| \leqslant \frac{|C|}{|G|}\, cy \left(\exp(-\tfrac{1}{5}\theta_B(y)) + y^{-B} \log^2 y \right) \tag{4.16}$$

for some sufficiently large constant $c = c(K)$.

To finish the proof, we now put

$$B = \min \left\{ \frac{1}{100}, \frac{1}{5c_5}, \frac{c_1}{30\log(6c)} \right\}.$$

Note that B depends only on K, the bound (4.16) holds, and we have

$$c\, \exp\left(-\frac{c_1}{30\, B} \right) \leqslant \frac{1}{6}\, .$$

On the other hand, from the definition (4.6) one sees that $\theta_B(y) \geqslant c_1/(6B)$ holds for any $y \geqslant y_1$, where $y_1 = \exp((\log c_2)/B)$. Therefore,

$$c\, \exp(-\tfrac{1}{5}\theta_B(y)) \leqslant \frac{1}{6} \qquad (y \geqslant y_1). \tag{4.17}$$

Increasing the value of y_1 if necessary, we also have

$$c\,y^{-B}\log^2 y \leqslant \frac{1}{6} \qquad (y \geqslant y_1). \tag{4.18}$$

Put $x_1 = y_1^{5/4}$ so that the condition $y \geqslant y_1$ is satisfied whenever $x^{4/5} \leqslant y \leqslant x$ and $x \geqslant x_1$. Combining the bounds (4.16), (4.17) and (4.18) we obtain

$$\psi_C(y;d,1) \geqslant \frac{2|C|}{3|G|}\,y \qquad (x^{4/5} \leqslant y \leqslant x) \tag{4.19}$$

for all $x \geqslant x_1$. Partial summation yields

$$\pi_C(y;d,1) \geqslant \frac{2|C|}{3|G|}\,\frac{y}{\log y} - \frac{4\sqrt{y}}{\log y} \geqslant \frac{|C|}{2|G|}\,\frac{y}{\log y} \qquad (x^{4/5} \leqslant y \leqslant x), \tag{4.20}$$

where the last inequality holds when $\sqrt{y} \geqslant 24|G|/|C|$, which is guaranteed by our choice of B and d with $d \leqslant x^B$. We finish the proof by noting that $|G| = n_K\phi(d)$. $\square$

4.5 Construction of Carmichael numbers

In view of Theorem 16, our construction of Carmichael numbers with the property stated in Theorem 18 follows closely that given in [1]. We shall be brief, since most of the details are the same. Our principal tool is the following variant of [1, Theorem 3.1]:

Lemma 12. *Let the constants x_1, B have the property stated in Theorem 16, and suppose that $x \geqslant x_1$. If L is any squarefree number in $\mathbb{N}_K$ that is not divisible by any prime exceeding $x^{(1-B)/2}$, and*

$$\sum_{\text{prime } q \,|\, L} \frac{1}{q} \leqslant \frac{1}{60 n_K}\,,$$

then there is a positive number $k \leqslant x^{1-B}$ with $\gcd(k,L)=1$ such that

$$\#\big\{d \mid L \ :\ dk+1 \in \mathscr{P}_C,\ dk+1 \leqslant x\big\} \geqslant \frac{1}{6n_K \log x}\cdot \#\big\{d \mid L \ :\ d \leqslant x^B\big\}.$$

Proof. We use ideas (and notation) from the proof of [1, Theorem 3.1].

Observe that the region $\Omega_B(x)$ defined by (4.5) is the same as the region $\Omega(T, U)$ defined by (4.3) when we put $T = x^{3B}$ and $U = x^B$.

Fix a prime p_0 with the property that $p_0 \mid \mathrm{N}_{K/\mathbb{Q}}(\mathfrak{f})$, where $\mathfrak{f} = \mathfrak{f}(K, x^B, x^{3B})$ is given by Lemma 10. If L is divisible by p_0 let $L' = L/p_0$; otherwise, let $L' = L$. Note that

$$\#\{d \mid L' \,:\, d \leqslant y\} \geqslant \frac{1}{2} \cdot \#\{d \mid L \,:\, d \leqslant y\} \qquad (y \geqslant 1) \tag{4.21}$$

(see [1, p. 716]). Since $p_0 \nmid L'$, for every divisor d of L' with $d \leqslant x^B$, Lemma 10 shows that $\zeta_d(s)$ has no zeros in $\Omega_B(x)$; therefore, using the lower bound (4.4) from Theorem 16 we have

$$\pi_C(dx^{1-B}; d, 1) \geqslant \frac{|C|}{2n_K} \frac{dx^{1-B}}{\phi(d) \log x}.$$

On the other hand, since any prime divisor q of L does not exceed $x^{(1-B)/2}$, we have from [9, Theorem 2]:

$$\pi_C(dx^{1-B}; dq, 1) \leqslant \pi(dx^{1-B}; dq, 1) \leqslant \frac{10}{q} \frac{dx^{1-B}}{\phi(d) \log x}.$$

Therefore, the number of primes $p \in \mathscr{P}_{C_d}$ with $p \leqslant dx^{1-B}$ and such that $\gcd((p-1)/d, L) = 1$ is at least

$$\begin{aligned} &\pi_C(dx^{1-B}; d, 1) - \sum_{\text{prime } q \mid L} \pi_C(dx^{1-B}; dq, 1) \\ &\qquad \geqslant \left(\frac{1}{2n_K} - 10 \sum_{\text{prime } q \mid L} \frac{1}{q} \right) \frac{dx^{1-B}}{\phi(d) \log x} \geqslant \frac{x^{1-B}}{3n_K \log x}. \end{aligned}$$

Using this bound together with (4.21) (instead of [1, Equation (3.1)]), the proof can be concluded in the same manner as that of [1, Theorem 3.1]; the remaining details are omitted. □

We are now in a position to establish a quantitative version of Theorem 18.

Theorem 17. *There are constants $x_0, c_0 > 0$ depending only on K such that for all $x \geqslant x_0$, there are at least x^{c_0} Carmichael numbers up to x that are composed solely of primes which split completely in K.*

Proof. To prove this, we only need to modify the proof of [1, Theorem 4.1] slightly, as follows.

Let $\mathcal{E}$ be the set of numbers $E \in (0,1)$ for which there exists a constant $x_2 > 0$ depending only on E such that

$$\pi(x, x^{1-E}) \underset{E}{\gg} \pi(x) \qquad (x \geqslant x_2), \tag{4.22}$$

where $\pi(x,y)$ denotes the number of primes $p \leqslant x$ such that $p-1$ is free of prime factors exceeding y.

Fix $E = 3/5$, which lies in the set $\mathcal{E}$ (see, e.g., [6]), and let x_2 be a number for which the bound (4.22) holds. Let x_1, B be numbers with the property stated in Theorem 16, and put $x_3 = \max\{x_1, x_2\}$. Note that our choice of x_3 depends only on K.

Let $y \geqslant 2$ be a parameter and Q the set of primes $q \in \mathbb{N}_K$ with

$$y^{5/2}/\log y < q \leqslant y^{5/2}$$

for which $q-1$ is free of prime factors exceeding y. By (4.22)

$$|Q| \geqslant \pi(y^{5/2}, y) - \pi(y^{5/2}/\log y) - \sum_{q \mid \mathscr{D}_K} 1 \gg y^{5/2}/\log y \tag{4.23}$$

for all sufficiently large y. Let L be the product of primes in Q; then

$$\log L = \sum_{q \in Q} \log q \leqslant \sum_{q \leqslant y^{5/2}} \log q = \vartheta(y^{5/2}) \leqslant 1.1 y^{5/2}$$

for all $y > 0$, where we have used [11] for the last inequality. Furthermore,

$$\lambda(L) = \prod_{p^a || \lambda(L)} p^a \leqslant \prod_{p \leqslant y} p^{\lfloor \frac{\log y^{5/2}}{\log p} \rfloor} \leqslant y^{5\pi(y)/2} \leqslant e^{\pi \cdot y} \tag{4.24}$$

where the last inequality follows again by [11]. We also have

$$n(G_L) \leqslant \lambda(L)(1 + \log L) \leqslant e^{\pi y}(1 + 1.1y^{5/2}) \leqslant e^{5y}, \tag{4.25}$$

where $G_L = (\mathbb{Z}/L\mathbb{Z})^*$.

Let $x = e^{y^{1+\delta}}$ where $\delta = 5\varepsilon/(8B)$. Since

$$\sum_{\text{prime } q \,|L} \frac{1}{q} \leqslant \sum_{y^{5/2}/\log y < q \leqslant y^{5/2}} \frac{1}{q} \leqslant 4\frac{\log\log y}{5\log y} \leqslant \frac{1}{60 n_K}$$

for sufficiently large y, it follows from Lemma 12 that there exists an integer k coprime to L, for which the set $\mathcal{P}$ of primes $p \leqslant x$ with $p \in \mathscr{P}_C$ and $p = dk + 1$ for some divisor d of L, satisfies

$$|\mathcal{P}| \geqslant \frac{1}{6n_K \log x} \cdot \#\big\{d \mid L \;:\; 1 \leqslant d \leqslant x^B\big\}. \tag{4.26}$$

The product of any

$$u := \left[\frac{\log(x^B)}{\log y^{5/2}}\right]$$

distinct prime factors of L, is a divisor d of L with $d \leqslant x^B$. We deduce from (4.23) that

$$\begin{aligned} \#\{d|L : 1 \leqslant d \leqslant x^B\} &\geqslant \binom{\omega(L)}{u} \geqslant \left(\frac{\omega(L)}{u}\right)^u \\ &\geqslant \left(\frac{cy^{5/2}}{2B\log x}\right)^u. \end{aligned} \tag{4.27}$$

Thus, by (4.26) and the identity $(5/2 - 1 - \delta)2B/5 = 3B/5 - \varepsilon/4$,

$$|\mathcal{P}| \geqslant \frac{1}{6n_K \log x} \left(\frac{c}{2B} y^{5/2-1-\delta}\right)^{\lfloor \frac{2B\log x}{5\log y} \rfloor} \geqslant x^{3B/5-\varepsilon/3}$$

for all sufficiently large values of y. Now take $\mathcal{P}' = \mathcal{P} \backslash Q$. Since $|Q| \leqslant y^{5/2}$, it follows by the above inequality that

$$|\mathcal{P}'| \geqslant x^{3B/5-\varepsilon/2} \tag{4.28}$$

for all sufficiently large values of y.

We may view $\mathcal{P}'$ as a subset of the group $(\mathbb{Z}/L\mathbb{Z})^\star$ by considering the residue class of each $p \in \mathcal{P}'$ modulo L. If S is a subset of $\mathcal{P}'$ that contains more than one element and if

$$\Pi(S) := \prod_{p \in S} p \equiv 1 \pmod{L},$$

then $\Pi(S)$ is a Carmichael number. Indeed, every member of $\mathcal{P}'$ is 1 mod k so that $\Pi(S) \equiv 1 \pmod{k}$, and thus $\Pi(S) \equiv 1 \pmod{kL}$, since $(k, L) = 1$. However, if $p \in \mathcal{P}'$ then $p \in \mathcal{P}$ so that $p - 1$ divides kL. Thus $\Pi(S)$ satisfies Korselt's criterion.

Let $t = e^{y^{1+\delta/2}}$. Then, by [1, Proposition 1.2], we see that the number of Carmichael numbers of the form $\Pi(S)$, where $S \subseteq \mathcal{P}'$ and $|S| \leqslant t$, is at least

$$\binom{|\mathcal{P}'|}{\lfloor t \rfloor} \binom{|\mathcal{P}'|}{n(G_L)}^{-1} \geqslant \left(\frac{|\mathcal{P}'|}{\lfloor t \rfloor}\right)^{\lfloor t \rfloor} |\mathcal{P}'|^{-n(G_L)} \geqslant x^{t(3B/5-\varepsilon)}$$

for all sufficiently large values of y, using (4.25) and (4.28). But each such Carmichael number $\Pi(S)$ so formed is such that $\Pi(S) \leqslant x^t$. Thus for $X = x^t$ we have $C(X) \geqslant X^{3B/5-\varepsilon}$ for all sufficiently large y. But $X = \exp(y^{1+\delta} \exp(y^{1+\delta/2}))$, so that $C(X) \geqslant X^{3B/5-\varepsilon}$ for all sufficiently large values of X. Since y can be uniquely determined from X, we complete the proof by taking $c_0 = EB/2$. $\square$

Bibliography

[1] W. Alford, A. Granville, and C. Pomerance, 'There are infinitely many Carmichael numbers', *Ann. of Math. (2)* **139** (1994), 703–722.

[2] W. Banks, 'Carmichael numbers with a square totient', *Canad. Math. Bull.* **52** (1) (2009), no. 1, 3–8.

[3] W. Banks and C. Pomerance, 'On Carmichael numbers in arithmetic progressions', to appear in *J. Austral. Math. Soc.*

[4] D.A. Cox, *Primes of the form $x^2 + ny^2$. Fermat, class field theory, and complex multiplication.* John Wiley & Sons, Inc., New York, 1989.

[5] D.S. Dummit and R. M. Foote, *Abstract Algebra.* Third edition. John Wiley & Sons, Inc., Hoboken, NJ, 2004. xii+932 pp. ISBN: 0-471-43334-9

[6] J.B. Friedlander, 'Shifted primes without large prime factors', in *Number theory and applications* (ed. R. A. Mollin), (Kluwer, NATO ASI, 1989), 393–401.

[7] G. J., Janusz, *Algebraic number fields*, Pure and Applied Mathematics, Vol. 55., Academic Press [A Subsidiary of Harcourt Brace Jovanovich, Publishers], New York-London, 1973. x+220 pp.

[8] J. C. Lagarias and A. M. Odlyzko, 'Effective versions of the Chebotarev density theorem', in *Algebraic number fields: L-functions and Galois properties* (Proc. Sympos., Univ. Durham, Durham, 1975), 409–464.

[9] H. L. Montgomery and R.C. Vaughan, 'The large sieve', *Mathematika* **20** (1973), 119–134.

[10] J. Neukirch, *Algebraic number theory*. Grundlehren der Mathematischen Wissenschaften, **322**. Springer-Verlag, Berlin, 1999.

[11] J. B. Rosser and L. Schoenfeld, 'Approximate formulas for some functions of prime numbers', *Illinois J. Math.* **6** (1962), 64–94.

[12] L. C. Washington, *Introduction to cyclotomic fields*. Second edition. Graduate Texts in Mathematics, **83**. Springer-Verlag, New York, 1997.

[13] A. Weiss, 'The least prime ideal', *J. Reine Angew. Math.* **338** (1983), 56–94.

Chapter 5

Piatetski-Shapiro Primes from Almost Primes

5.1 Introduction

The *Piatetski-Shapiro sequences* are those sequences of the form

$$(\lfloor n^c \rfloor)_{n\in\mathbb{N}} \qquad (c>1,\ c\notin\mathbb{N}),$$

where $\lfloor t \rfloor$ denotes the integer part of any $t\in\mathbb{R}$. Such sequences are named in honor of Piatetski-Shapiro, who showed in [6] that for any number $c\in(1,\frac{12}{11})$ the set

$$\mathscr{P}^{(c)} := \big\{ p \text{ prime} : p = \lfloor n^c \rfloor \text{ for some } n\in\mathbb{N} \big\}$$

is infinite. The admissible range for c in this result has been extended many times over the years and is currently known for all $c\in(1,\frac{243}{205})$ thanks to Rivat and Wu [8].

For any natural number r, let $\mathbb{N}_r$ denote the set of r-*almost primes*, i.e., the set of natural numbers having at most r prime factors, counted with multiplicity. In this chapter, we introduce and study sets of Piatetski-Shapiro primes of the form

$$\mathscr{P}_r^{(c)} := \big\{ p \text{ prime} : p = \lfloor n^c \rfloor \text{ for some } n\in\mathbb{N}_r \big\}.$$

Our main result is the following:

Theorem 18. *For any fixed* $c \in (1, \frac{77}{76})$ *the set* $\mathscr{P}_8^{(c)}$ *is infinite. More precisely,*

$$\big|\{n \leqslant x : n \in \mathbb{N}_8 \text{ and } \lfloor n^c \rfloor \text{ is prime}\}\big| \gg \frac{x}{(\log x)^2}\,,$$

where the implied constants in the symbol $\gg$ *depend only on* c.

5.2 Notation

Throughout the chapter, we set $\gamma := 1/c$ for a given real number $c > 1$.

The letter p always denotes a prime number.

We use Λ to denote the von Mangoldt function.

Any implied constants in the symbols O, $\ll$, $\asymp$, $\sim$ may depend on c and on the small parameters ε, δ but are absolute otherwise. We use notation of the form $m \sim M$ as an abbreviation for $M < m \leqslant 2M$.

As is customary, we put

$$\mathbf{e}(t) := e^{2\pi i t} \qquad \text{and} \qquad \{t\} := t - \lfloor t \rfloor \qquad (t \in \mathbb{R}).$$

Throughout the chapter, we make considerable use of the sawtooth function defined by

$$\psi(t) := t - \lfloor t \rfloor - \tfrac{1}{2} = \{t\} - \tfrac{1}{2} \qquad (t \in \mathbb{R}) \tag{5.1}$$

as well as the well known approximation of Vaaler [10]: for any $H \geqslant 1$ there exist numbers a_h and b_h such that

$$\Big|\psi(t) - \sum_{0<|h|\leqslant H} a_h\,\mathbf{e}(th)\Big| \leqslant \sum_{|h|\leqslant H} b_h\,\mathbf{e}(th), \qquad a_h \ll \frac{1}{|h|}\,, \qquad b_h \ll \frac{1}{H}\,. \tag{5.2}$$

5.3 Proof of Theorem 18

5.3.1 Initial approach

We analyze exponential sums that are relevant for finding primes in $\mathscr{P}_r^{(c)}$ with the number r as small as possible. The set that we sieve is

$$\mathscr{A} := \big\{n \leqslant x : \lfloor n^c \rfloor \text{ is prime}\big\}.$$

For any $d \leqslant D$, where D is a fixed power of x to be specified later, we must estimate accurately the cardinality of

$$\mathscr{A}_d := \big\{n \in \mathscr{A} : d \mid n\big\}.$$

Since $md \in \mathscr{A}$ if and only if

$$p \leqslant (md)^c < p+1 \qquad \text{and} \qquad md \leqslant x,$$

to within $O(1)$ the cardinality of $\mathscr{A}_d$ is equal to the number of primes $p \leqslant x^c$ for which the interval $\big[p^\gamma d^{-1}, (p+1)^\gamma d^{-1}\big)$ contains a natural number; thus,

$$\begin{aligned}|\mathscr{A}_d| &= \Big|\big\{p \leqslant x^c : -(p+1)^\gamma d^{-1} < -m \leqslant -p^\gamma d^{-1} \text{ for some } m \in \mathbb{N}\big\}\Big| + O(1)\\ &= \sum_{p \leqslant x^c} \big(\big\lfloor -p^\gamma d^{-1} \big\rfloor - \big\lfloor -(p+1)^\gamma d^{-1} \big\rfloor \big) + O(1)\\ &= Xd^{-1} + \sum_{p \leqslant x^c} \big(\psi(-(p+1)^\gamma d^{-1}) - \psi(-p^\gamma d^{-1})\big) + O(1),\end{aligned}$$

where ψ is given by (5.1), and

$$X := \sum_{p \leqslant x^c} ((p+1)^\gamma - p^\gamma) = \sum_{p \leqslant x^c} \gamma p^{\gamma-1} + O(1) \sim \frac{x}{c \log x} \qquad (x \to \infty).$$

It is unnecessary to evaluate X more precisely than this; however, for any sufficiently small $\varepsilon > 0$ we need to show that

$$\sum_{d \leqslant D} \big| |\mathscr{A}_d| - Xd^{-1} \big| \leqslant Xx^{-\varepsilon/3} \asymp \frac{x^{1-\varepsilon/3}}{\log x} \qquad (x \to \infty). \tag{5.3}$$

Splitting the range of d into dyadic subintervals and using partial summation in a standard way, it suffices to prove that the bound

$$\sum_{d\sim D_1}\Bigg|\sum_{N<n\leqslant N_1}\Lambda(n)\big(\psi(-(n+1)^\gamma d^{-1})-\psi(-n^\gamma d^{-1})\big)\Bigg|\ll x^{1-\varepsilon/2} \tag{5.4}$$

holds uniformly for $D_1\leqslant D$, $N\leqslant x^c$, $N_1\sim N$. In turn, (5.4) is an immediate consequence of the uniform bound

$$\sum_{N<n\leqslant N_1}\Lambda(n)\big(\psi(-(n+1)^\gamma d^{-1})-\psi(-n^\gamma d^{-1})\big)\ll x^{1-\varepsilon/2}d^{-1} \tag{5.5}$$

for $d\leqslant D$, $N\leqslant x^c$, $N_1\sim N$. Our aim is to establish (5.5) with D as large as possible, and in this subsection we show that (5.5) holds when

$$D\leqslant x^{1-136c/157} \tag{5.6}$$

and $\varepsilon>0$ is sufficiently small. Suppose this has been done, and observe that

$$1-\frac{136c}{157}>\frac{8}{63}\qquad\text{whenever}\quad c<\frac{8635}{8568}\,.$$

Then, for any fixed $c\in(1,\frac{8635}{8568})$ and $\alpha\in(\frac{8}{63},1-\frac{136c}{157})$, the inequality (5.3) with $D:=x^\alpha$ implies the bound

$$\sum_{d\leqslant D}\big||\mathscr{A}_d|-Xd^{-1}\big|\ll\frac{X}{(\log X)^2}\,,$$

thus we can apply the weighted sieve in the form [4, Ch. 5, Prop. 1] with the choices

$$R:=8,\qquad \delta_R:=0.124820\cdots\qquad\text{and}\qquad g:=\frac{63}{8}\,.$$

Note that $g<R-\delta_R$, and (if x is large enough) the inequality $a<D^g$ holds for all $a\in\mathscr{A}$ since $\alpha g>1$; thus, the conditions of [4, Ch. 5, Prop. 1] are met, and we conclude that $\mathscr{A}$ contains at least $\gg X/\log X$ numbers with at most eight prime factors. This yields the statement of the theorem for all c in the interval $(1,\frac{8635}{8568})$.

We now turn to the proof of (5.5) for all D satisfying (5.6). Let S denote the sum on the left side of (5.5). From Vaaler's approximation (5.2) we derive the inequality

$$|S| \leqslant |S_1| + S_2 + S_3 + 2b_0 \sum_{N<n\leqslant N_1} \Lambda(n), \tag{5.7}$$

where

$$\begin{aligned} S_1 &:= \sum_{N<n\leqslant N_1} \Lambda(n) \sum_{0<|h|\leqslant H} a_h \big(\mathbf{e}(-h(n+1)^\gamma d^{-1}) - \mathbf{e}(-hn^\gamma d^{-1})\big), \\ S_2 &:= \sum_{N<n\leqslant N_1} \Lambda(n) \sum_{0<|h|\leqslant H} b_h\, \mathbf{e}(-h(n+1)^\gamma d^{-1}), \\ S_3 &:= \sum_{N<n\leqslant N_1} \Lambda(n) \sum_{0<|h|\leqslant H} b_h\, \mathbf{e}(-hn^\gamma d^{-1}). \end{aligned}$$

To ensure that the last term on the right side of (5.7) satisfies the bound

$$2b_0 \sum_{N<n\leqslant N_1} \Lambda(n) \ll x^{1-\varepsilon/2} d^{-1},$$

we choose

$$H := x^{-1+\varepsilon} N d. \tag{5.8}$$

Next, we use a partial summation argument from the book of Graham and Kolesnik [3]. Writing

$$S_1 = \sum_{0<|h|\leqslant H} a_h \sum_{N<n\leqslant N_1} \Lambda(n) \overline{\phi_h(n) \mathbf{e}(hn^\gamma d^{-1})}$$

with

$$\phi_h(t) := \mathbf{e}(h(t+1)^\gamma d^{-1} - ht^\gamma d^{-1}) - 1,$$

we would like to show that

$$\sum_{0<|h|\leqslant H} h^{-1} \Bigg| \sum_{N<n\leqslant N_1} \Lambda(n) \phi_h(n)\, \mathbf{e}(hn^\gamma d^{-1}) \Bigg| \ll x^{1-\varepsilon} d^{-1} \qquad (d \leqslant D). \tag{5.9}$$

Taking into account the bounds

$$\phi_h(t) \ll hN^{\gamma-1} d^{-1} \qquad \text{and} \qquad \phi_h'(t) \ll hN^{\gamma-2} d^{-1} \qquad (N \leqslant t \leqslant N_1),$$

the left side of (5.9) is, on integrating by parts, bounded by

$$\begin{aligned}
&\ll \sum_{h\leqslant H} h^{-1}\left|\phi_n(N_1)\sum_{N<n\leqslant N_1}\Lambda(n)\,\mathbf{e}(hn^\gamma d^{-1})\right| \\
&\qquad + \sum_{h\leqslant H} h^{-1}\int_N^{N_1}\left|\phi_h'(t)\sum_{N<n\leqslant t}\Lambda(n)\,\mathbf{e}(hn^\gamma d^{-1})\right|dt \\
&\ll N^{\gamma-1}d^{-1}\sum_{h\leqslant H}\left|\sum_{N<n\leqslant N_2}\Lambda(n)\,\mathbf{e}(hn^\gamma d^{-1})\right|
\end{aligned}$$

for some number $N_2\in(N,N_1]$. Therefore, it suffices to show that the bound

$$\sum_{h\leqslant H}\left|\sum_{N<n\leqslant N_2}\Lambda(n)\,\mathbf{e}(hn^\gamma d^{-1})\right| \ll x^{1-\varepsilon}N^{1-\gamma} \tag{5.10}$$

holds uniformly for $d\leqslant D$, $N\leqslant x^c$, $N_2\sim N$.

To establish (5.10) we use the decomposition of Heath-Brown [5]; it suffices to show that our type I and type II sums satisfy the uniform bounds

$$S_I := \sum_{H_1\leqslant h\leqslant H_2}\left|\sum_{\ell\sim L}a_\ell\sum_{\substack{m\sim M\\ \ell m\in\mathcal{J}}}\mathbf{e}(h\ell^\gamma m^\gamma d^{-1})\right| \ll x^{1-2\varepsilon}N^{1-\gamma}, \tag{5.11}$$

$$S_{II} := \sum_{H_1\leqslant h\leqslant H_2}\left|\sum_{\ell\sim L}a_\ell\sum_{\substack{m\sim M\\ \ell m\in\mathcal{J}}}b_m\mathbf{e}(h\ell^\gamma m^\gamma d^{-1})\right| \ll x^{1-2\varepsilon}N^{1-\gamma}, \tag{5.12}$$

in some specific ranges. Here, $\mathcal{J}$ is an interval in $(N,N_1]$, $H_1\leqslant H$, $H_2\sim H_1$, $LM\asymp N$, and the numbers $a_\ell,b_m\in\mathbb{C}$ satisfy $|a_\ell|\leqslant 1$, $|b_m|\leqslant 1$. In view of [5, pp. 1367–1368] we need to show that (5.12) holds uniformly for all L in the range

$$u\ll L\ll N^{1/3}\qquad\text{for some}\quad u\leqslant x^{-\varepsilon}N^{1/5}, \tag{5.13}$$

and for such u we need to show that (5.11) holds uniformly for all M satisfying

$$M\gg N^{1/2}u^{-1/2}.$$

Put $F:=H_1N^\gamma d^{-1}$. For the type II sum, we apply Baker [1, Thm. 2], which yields the bound

$$S_{II}\ll\big(T_{II,1}+T_{II,2}\big)H_1Nx^\varepsilon$$

with

$$T_{II,1} := (H_1L)^{-1/2} \qquad \text{and} \qquad T_{II,2} := \left(\frac{F}{H_1L}\right)^{k/(2+2k)} M^{-(1+k-\ell)/(2+2k)}$$

for any exponent pair (k,ℓ) provided that $F \geqslant H_1L$. For the type I sum, by Robert and Sargos [9, Thm. 3] we have the bound

$$S_I \ll \big(T_{I,1} + T_{I,2} + T_{I,3}\big) H_1 N x^{\varepsilon}$$

with

$$T_{I,1} := \left(\frac{F}{H_1LM^2}\right)^{1/4}, \qquad T_{I,2} := M^{-1/2} \qquad \text{and} \qquad T_{I,3} := F^{-1}.$$

Hence, to establish (5.11) and (5.12) it suffices to verify that

$$\max\big\{T_{I,1}, T_{I,2}, T_{I,3}, T_{II,1}, T_{II,2}\big\} \ll x^{1-3\varepsilon} H_1^{-1} N^{-\gamma}. \tag{5.14}$$

From the definition of F we see that the bound

$$T_{I,3} = F^{-1} \ll x^{1-3\varepsilon} H_1^{-1} N^{-\gamma} \tag{5.15}$$

is equivalent to $d \ll x^{1-3\varepsilon}$ and thus follows from the inequality $D \leqslant x^{1-3\varepsilon}$ which is implied by (5.6) when ε is small enough.

To guarantee that

$$T_{II,1} = (H_1L)^{-1/2} \ll x^{1-3\varepsilon} H_1^{-1} N^{-\gamma} \tag{5.16}$$

holds for all $L \geqslant u$ we simply define

$$u := x^{-2+6\varepsilon} H_1 N^{2\gamma}.$$

We need to check that the condition $u \leqslant x^{-\varepsilon} N^{1/5}$ of (5.13) is met. For this, taking into account (5.8), it suffices to have

$$D \leqslant x^{3-8\varepsilon} N^{-4/5-2\gamma}.$$

The worst case occurs when $N = x^c$, leading to the constraint $D \leqslant x^{1-4c/5-8\varepsilon}$, which follows from (5.6) if ε is sufficiently small.

Next, if M satisfies the lower bound

$$M \gg N^{1/2} u^{-1/2} = x^{1-3\varepsilon} H_1^{-1/2} N^{1/2-\gamma},$$

then the upper bound

$$M^{-1/2} \ll x^{-1/2+2\varepsilon} H_1^{1/4} N^{-1/4+\gamma/2} \tag{5.17}$$

holds; therefore, the bound

$$T_{I,2} = M^{-1/2} \ll x^{1-3\varepsilon} H_1^{-1} N^{-\gamma} \tag{5.18}$$

holds provided that

$$H_1 \ll x^{6/5-4\varepsilon} N^{1/5-6\gamma/5}.$$

Using (5.8) again, we see that (5.18) follows from the inequality

$$D \leqslant x^{11/5-5\varepsilon} N^{-4/5-6\gamma/5}.$$

Taking $N := x^c$ leads to the restriction $D \leqslant x^{1-4c/5-5\varepsilon}$, and this is implied by (5.6) when ε is small enough.

Next, using the definition of F and the relation $LM \asymp N$ one sees that the bound

$$T_{I,1} = \left(\frac{F}{H_1 L M^2}\right)^{1/4} \ll x^{1-3\varepsilon} H_1^{-1} N^{-\gamma} \tag{5.19}$$

holds whenever

$$H_1 M^{-1/4} d^{-1/4} \ll x^{1-3\varepsilon} N^{1/4-5\gamma/4}.$$

Taking into account (5.8) and (5.17) this bound follows from the condition

$$D \ll x^{19/7-7\varepsilon} N^{-6/7-12\gamma/7}.$$

With $N := x^c$ we derive the constraint $D \leqslant x^{1-6c/7-7\varepsilon}$, which is a consequence of (5.6) if ε is sufficiently small.

Our next goal is to establish the bound

$$T_{II,2} = \left(\frac{N^\gamma}{Ld}\right)^{k/(2+2k)} M^{-(1+k-\ell)/(2+2k)} \ll x^{1-3\varepsilon} H_1^{-1} N^{-\gamma}. \tag{5.20}$$

To begin, we check that the condition $F \geqslant H_1 L$ is met, or equivalently, that $d \leqslant N^\gamma L^{-1}$. Since $L \ll N^{1/3}$ for the type II sum, it is enough to have

$$D \leqslant N^{\gamma-1/3-\varepsilon}. \tag{5.21}$$

If ε is sufficiently small, then (5.21) follows essentially from (5.6). Indeed, since $c > 1$ and $\gamma := 1/c$, the inequality

$$(1 - 136c/157)(2/3 + 2\gamma) < 2(\gamma - 1/3)$$

is easily verified; hence, for small enough ε (depending only on c) we have by (5.6):

$$D^{2/3+2\gamma-\varepsilon} \leqslant \left(x^{1-136c/157}\right)^{2/3+2\gamma-\varepsilon} \leqslant \left(x^{2-3\varepsilon}\right)^{\gamma-1/3-\varepsilon},$$

which implies that

$$D^{1+\gamma} \leqslant \left(\frac{x^{2-3\varepsilon}}{D}\right)^{\gamma-1/3-\varepsilon}.$$

On the other hand, we can certainly assume that $HN \geqslant x^{1-2\varepsilon} N^{1-\gamma}$, for otherwise (5.11) and (5.12) are trivial; therefore

$$N^{1+\gamma} \geqslant x^{2-3\varepsilon} d^{-1},$$

and we have

$$D^{1+\gamma} \leqslant \left(\frac{x^{2-3\varepsilon}}{D}\right)^{\gamma-1/3-\varepsilon} \leqslant \left(\frac{x^{2-3\varepsilon}}{d}\right)^{\gamma-1/3-\varepsilon} \leqslant \left(N^{1+\gamma}\right)^{\gamma-1/3-\epsilon},$$

which yields (5.21).

Using the relation $LM \asymp N$, the upper bound $M \ll N^{2/3}$ (which follows from $L \ll N^{1/3}$) and the definition (5.8), we see that the bound (5.20) holds if

$$d^{\nu-k} \ll x^{2\nu-4\nu\varepsilon} N^{-\nu-\gamma\nu-\gamma k+k+2(1-\ell)/3},$$

where we have put $\nu := 2k+2$. The exponent of N is negative since

$$k + 2(1-\ell)/3 < k + 1/3 < \nu/2;$$

therefore, the worst case occurs when $N = x^c$, and it suffices to have

$$D \leqslant x^{1-c\mu/3-2\varepsilon}, \tag{5.22}$$

where

$$\mu := \frac{\nu - k - 2(1-\ell)/3}{\nu - k} = \frac{3k + 2\ell + 4}{k+2}.$$

With the choice $(k, \ell) := (\frac{57}{126}, \frac{64}{126})$ (which is $BA^5(\frac{1}{2}, \frac{1}{2})$ in the notation of Graham [2]) we have

$$\frac{\mu}{3} = \frac{803}{927} < \frac{136}{157},$$

and therefore (5.22) follows from (5.6) if ε is small enough. This proves (5.20).

Combining the bounds (5.15), (5.16), (5.18), (5.19) and (5.20), we obtain (5.14), and this completes the proof of Theorem 18 for $c \in (1, \frac{8635}{8568})$.

5.3.2 Refinement

Here, we extend the ideas of §5.3.1 to show that for any $\delta > 0$, the bound (5.5) holds for all sufficiently small $\varepsilon > 0$ (depending on δ) under the less stringent condition that

$$D \leqslant x^{1-\frac{380c}{441}-\delta}. \tag{5.23}$$

After this has been done, taking into account that

$$1 - \frac{380c}{441} > \frac{8}{63} \qquad \text{whenever} \quad c < \frac{77}{76}\,,$$

the proof of Theorem 18 for the full range $c \in (1, \frac{77}{76})$ is completed using the sieve argument presented after (5.6).

Following Rivat and Sargos [7, Lem. 2] it suffices to show that

(i) The type II bound (5.12) holds for L in the range $u_0 \ll L \ll u_0^2$ for some $u_0 \in [N^{1/10}, N^{1/6}]$;

(ii) For such u_0, the type I bound (5.11) holds whenever $M \gg N^{1/2} u_0^{-1/2}$;

(iii) For such u_0 and any numbers $a_m, c_h \in \mathbb{C}$ with $|a_m| \leqslant 1$, $|c_h| \leqslant 1$, the type I' bound

$$S_{I'} := \sum_{h \sim H} c_h \sum_{m \sim M} a_m \sum_{\ell \sim L} e(h\ell^\gamma m^\gamma d^{-1}) \ll x^{1-2\varepsilon} N^{1-\gamma}$$

holds whenever $u_0^2 \ll L \ll N^{1/3}$.

Taking $u := x^{-2+6\varepsilon} H_1 N^{2\gamma}$ as in §5.3.1, we put

$$u_0 := \max\{N^{1/10}, u\}.$$

The condition $u_0 \leqslant N^{1/6}$ follows from the inequality $x^{-2+6\varepsilon} H N^{2\gamma} \leqslant N^{1/6}$, which in view of (5.8) is implied by

$$D \leqslant x^{3-7\varepsilon} N^{-5/6-2\gamma}.$$

Taking $N := x^c$ leads to $D \leqslant x^{1-5c/6-7\varepsilon}$, which follows from (5.23). Since $\frac{380}{441} > \frac{5}{6}$ and $u \ll L \ll N^{1/3}$ holds whenever $u_0 \ll L \ll u_0^2$, the condition (i) is a consequence of our work in §5.3.1.

Condition (ii) also follows from §5.3.1 in the case that $u \geqslant N^{1/10}$. When $u < N^{1/10}$ it suffices to show that

$$\max\left\{T_{I,1}, T_{I,2}, T_{I,3}\right\} \ll x^{1-3\varepsilon} H_1^{-1} N^{-\gamma} \tag{5.24}$$

when $M \gg N^{9/20}$. Taking into account (5.8) we see that the bound

$$T_{I,2} = M^{-1/2} \ll x^{1-3\varepsilon} H_1^{-1} N^{-\gamma} \tag{5.25}$$

holds provided that

$$D \leqslant x^{2-4\varepsilon} N^{-31/40-\gamma}.$$

The worst case $N = x^c$ leads to $D \leqslant x^{1-31c/40-4\varepsilon}$, and since $\frac{380}{441} > \frac{31}{40}$ this is implied by (5.23) when ε is small enough. We also know that (5.19) holds whenever

$$H_1 M^{-1/4} d^{-1/4} \ll x^{1-3\varepsilon} N^{1/4-5\gamma/4}.$$

Taking into account (5.8) this bound follows from the inequality

$$D \leqslant x^{8/3-3\varepsilon} N^{-51/60-5\gamma/3}.$$

With $N := x^c$ we derive the constraint $D \leqslant x^{1-51c/60-3\varepsilon}$, and as $\frac{380}{441} > \frac{51}{60}$ this a consequence of (5.23) if ε is small enough. Combining (5.15), (5.19) and (5.25) we obtain (5.24) as required.

It remains to verify condition (iii). Rather than adapting Rivat and Sargos [7], we quote an abstraction of their method due to Wu [11]. Taking $k := 5$ in [11, Thm. 2] we have (in Wu's notation) a bound of the form

$$(\log x)^{-1} S_{I'} \ll (X^{32} H^{114} M^{147} N^{137})^{1/174} + \cdots .$$

However, in place of (X, H, M, N) we use the quadruple $(H_1 N^{\gamma} d^{-1}, M, H_1, L)$. The triple of exponents (α, β, γ) becomes $(\gamma, 1, \gamma)$ in our case, and it is straightforward to check that the various hypotheses of [11, Thm. 2] are satisfied. Applying the theorem and taking into account that $H_1 \leqslant x^{-1+\varepsilon}Nd$, it follows that

$$S_{I'} \ll \big(T_{I',1} + T_{I',2} + T_{I',3} + T_{I',4} + T_{I',5} + T_{I',6} + T_{I',7}\big)x^{\varepsilon},$$

where

$$T_{I',1} := \big(H_1^{179}N^{114+32\gamma}L^{23}d^{-32}\big)^{1/174}, \qquad T_{I',5} := H_1^{1/2}NL^{-1/2},$$

$$T_{I',2} := H_1^{3/4}N^{1/2+\gamma/4}L^{1/2}d^{-1/4}, \qquad T_{I',6} := H_1N^{1/2}L^{1/2},$$

$$T_{I',3} := H_1^{5/4}N^{1/2+\gamma/4}d^{-1/4}, \qquad T_{I',7} := H_1^{1/2}N^{1-\gamma/2}d^{1/2}.$$

$$T_{I',4} := H_1NL^{-1},$$

It suffices to show that

$$\max\big\{T_{I',1}, T_{I',2}, T_{I',3}, T_{I',4}, T_{I',5}, T_{I',6}, T_{I',7}\big\} \ll x^{1-3\varepsilon}N^{1-\gamma} \tag{5.26}$$

given that

$$N \leqslant x^c, \qquad H_1 \leqslant x^{-1+\varepsilon}Nd \qquad \text{and} \qquad N^{1/5} \ll L \ll N^{1/3}. \tag{5.27}$$

First, we note that the bound

$$T_{I',1} = \big(H_1^{179}N^{114+32\gamma}L^{23}d^{-32}\big)^{1/174} \ll x^{1-3\varepsilon}N^{1-\gamma} \tag{5.28}$$

is equivalent to

$$H_1^{179}N^{-60+206\gamma}L^{23}d^{-32} \ll x^{174-522\varepsilon}.$$

Using the first two inequalities and the upper bound on L in (5.27), it suffices to have

$$D^{147} \leqslant x^{147-380c/3-701\varepsilon},$$

which is (5.23). Similarly, the bounds

$$T_{I',2} = H_1^{3/4} N^{1/2+\gamma/4} L^{1/2} d^{-1/4} \ll x^{1-3\varepsilon} N^{1-\gamma}, \tag{5.29}$$

$$T_{I',6} = H_1 N^{1/2} L^{1/2} \ll x^{1-3\varepsilon} N^{1-\gamma}, \tag{5.30}$$

follow from the inequalities

$$D \leqslant x^{1-5c/6-15\varepsilon/2} \qquad \text{and} \qquad D \leqslant x^{1-2c/3-4\varepsilon},$$

respectively, and these are easy consequences of (5.23) since $\frac{380}{441} > \frac{5}{6} > \frac{2}{3}$. On the other hand, using the first two inequalities and the lower bound on L in (5.27), we see that both bounds

$$T_{I',4} = H_1 N L^{-1} \ll x^{1-3\varepsilon} N^{1-\gamma}, \tag{5.31}$$

$$T_{I',5} = H_1^{1/2} N L^{-1/2} \ll x^{1-3\varepsilon} N^{1-\gamma}, \tag{5.32}$$

follow from the inequality

$$D \leqslant x^{1-4c/5-7\varepsilon},$$

which is implied by (5.23) since $\frac{380}{441} > \frac{4}{5}$. Next, using the first two inequalities in (5.27) and disregarding the bounds on L, it is easy to check that

$$T_{I',3} = H_1^{5/4} N^{1/2+\gamma/4} d^{-1/4} \ll x^{1-3\varepsilon} N^{1-\gamma} \tag{5.33}$$

follows from

$$D \ll x^{1-3c/4-17\varepsilon/4},$$

which is implied by (5.23) since $\frac{380}{441} > \frac{3}{4}$. Similarly,

$$T_{I',7} = H_1^{1/2} N^{1-\gamma/2} d^{1/2} \ll x^{1-3\varepsilon} N^{1-\gamma} \tag{5.34}$$

is a consequence of the inequality

$$D \ll x^{1-c/2-7\varepsilon/2},$$

which follows from (5.23) since $\frac{380}{441} > \frac{1}{2}$.

Combining the bounds (5.28), (5.29), (5.30), (5.31), (5.32), (5.33) and (5.34), we obtain (5.26), and Theorem 18 is proved.

Bibliography

[1] R. C. Baker, 'The square-free divisor problem,' *Quart. J. Math. Oxford* **45** (1994), 269–277.

[2] S. W. Graham, 'An algorithm for computing optimal exponent pairs,' *J. London Math. Soc. (2)* **33** (1986), no. 2, 203–218.

[3] S. W. Graham and G. Kolesnik, *Van der Corput's method of exponential sums.* London Mathematical Society Lecture Note Series, **126**. Cambridge University Press, Cambridge, 1991.

[4] G. Greaves, *Sieves in Number Theory.* Results in Mathematics and Related Areas (3), **43**. Springer-Verlag, Berlin, 2001.

[5] D. R. Heath-Brown, 'Prime numbers in short intervals and a generalized Vaughan identity,' *Canad. J. Math.* **34** (1982), no. 6, 1365–1377.

[6] I. I. Piatetski-Shapiro, 'On the distribution of prime numbers in the sequence of the form $\lfloor f(n) \rfloor$,' *Mat. Sb.* **33** (1953), 559–566.

[7] J. Rivat and P. Sargos, 'Nombres premiers de la forme $\lfloor n^c \rfloor$,' *Canad. J. Math.* **53** (2001), no. 2, 414–433.

[8] J. Rivat and J. Wu, 'Prime numbers of the form $\lfloor n^c \rfloor$,' *Glasg. Math. J.* **43** (2001), no. 2, 237–254.

[9] O. Robert and P. Sargos, 'Three-dimensional exponential sums with monomials,' *J. Reine Angew. Math.* **591** (2006), 1–20.

[10] J. D. Vaaler, 'Some extremal problems in Fourier analysis,' *Bull. Amer. Math. Soc.* **12** (1985), 183–216.

[11] J. Wu, 'On the primitive circle problem,' *Monatsh. Math.* **135** (2002), no. 1, 69–81.

VITA

Aaron Yeager was born on December 28, 1976 in Springfield, Missouri. In 1995 he graduated from Kickapoo High School. In 2002, after a few years spent pursuing a career in professional skateboarding, he began college at Los Angeles City College. He graduated with an AS in mathematics from LACC in 2005. From 2005 to 2006 Aaron attended Cal State Los Angeles. In 2006 Aaron returned home to be with family and attend Missouri State University. He graduated from MSU with a BS in mathematics in 2008. Aaron began his graduate work at the University of Missouri in 2008. In fall 2012, Aaron received his MA in mathematics from the University of Missouri-Columbia.