Three Topics in Analytic Number Theory

by

Kübra Benli

(Under the Direction of Paul Pollack)

Abstract

This thesis discusses three topics in Number Theory, where the results are obtained by using analytic methods. First, we discuss results on the distribution of the small prime power residues modulo a prime. We give an elementary approach by using reciprocity laws first, and then we discuss how to improve and generalize these results using character sum estimates and sieve results. Secondly, we discuss a quantitative improvement on the number of weakly prime numbers, the primes that change to a composite number after altering a single digit. Finally, we discuss an asymptotic formula for the number of pure fields of fixed prime degree and bounded discriminant.

Index words: sieve methods, prime numbers, character sums, pure fields, partial covering of congruences

Three Topics in Analytic Number Theory

by

Kübra Benlİ

B.S., Boğaziçi University, Turkey, 2012

M.S., Boğaziçi University, Turkey, 2015

A Dissertation Submitted to the Graduate Faculty

of The University of Georgia in Partial Fulfillment

of the

Requirements for the Degree

Doctor of Philosophy

Athens, Georgia

2020

Three Topics in Analytic Number Theory

by

Kübra Benlİ

Approved:

Major Professor:	Paul Pollack
Committee:	Neil Lyall
	Akos Magyar
	Giorgis Petridis

Electronic Version Approved:

Ron Walcott
Interim Dean of the Graduate School
The University of Georgia
August 2020

Acknowledgments

First of all, I would like to thank my advisor, Paul Pollack, for his guidance, his encouragement and his patience throughout my Ph.D. studies.

I am thankful to Giorgis Petridis for his encouragement in the last few years, and for being in my thesis committee. I also would like to thank Neil Lyall and Akos Magyar for serving in my thesis committee.

I cannot express how grateful I am to Ertan Elma, my one, for growing up with me through the time zone we shared.

Finally, I would like to thank to my parents for their support from a distance which has not been easy for any of us.

Notation

Let f and g be (real-valued) functions of a real variable x, with $g(x) > 0$. We write $f(x) = O(g(x))$ if $|f(x)| < Cg(x)$ for all sufficiently large x, where $C > 0$ is an absolute constant. Equivalently, we sometimes write $f(x) \ll g(x)$. For a parameter η, if we write $f(x) = O_\eta(g(x))$ or $f(x) \ll_\eta g(x)$, this means that the constant $C = C_\eta$ may depend on η. If $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 0$, that is $|f(x)| < c|g(x)|$ for any $c > 0$ and for all sufficiently large x, we use the notation $f(x) = o(g(x))$. If $\lim_{x\to\infty} \frac{f(x)}{g(x)} = 1$ then we say that $f(x)$ and $g(x)$ are asymptotically equal, and we write $f(x) \sim g(x)$. Other notation will be introduced as needed.

Contents

Chapter 1

Introduction

In this chapter, we introduce some preliminaries and summarize the statement of the results which are going to be detailed in the next chapters.

1.1 Elementary methods

1.1.1 Rational reciprocity laws

Let p be an odd prime and let a be an integer. We define the Legendre symbol as follows:

Definition 1.

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } x^2 \equiv a \bmod p \text{ has a solution and } a \not\equiv 0 \bmod p, \\ -1 & \text{if } x^2 \equiv a \bmod p \text{ does not have a solution,} \\ 0 & \text{if } a \equiv 0 \bmod p. \end{cases}$$

The law of quadratic reciprocity, noticed by Euler and Legendre and proved by Gauss (he actually gave eight different proofs), is one of the fundamental results in number theory.

Theorem 1 (Law of Quadratic Reciprocity, [21])**.** Let p and q be two distinct odd primes. Then we have

$$\left(\frac{p}{q}\right) = (-1)^{\frac{p-1}{2}\frac{q-1}{2}} \left(\frac{q}{p}\right).$$

As a consequence, for distinct odd primes p and q, $\left(\frac{p}{q}\right)$ depends on only on the congruence class of $q \bmod 4p$. We additionally have the following criteria for determining special Legendre symbols.

Theorem 2 (Supplements to Law of Quadratic Reciprocity)**.** Let p be an odd prime. Then we have $\left(\frac{-1}{p}\right) = (-1)^{\frac{p-1}{2}}$, and

$$\left(\frac{2}{p}\right) = \begin{cases} 1 & \text{if} \quad p \equiv \pm 1 \bmod 8, \\ -1 & \text{if} \quad p \equiv \pm 3 \bmod 8. \end{cases}$$

A similar criteria can be asked for the higher power residues. For example, an integer a is called a cubic residue modulo m if the congruence $x^3 \equiv a \bmod m$ has a solution. If q is a prime with $q \equiv 2 \bmod 3$, then every congruence class modulo q is necessarily a cube. We note here the following fact. If $q \equiv 1 \bmod 3$ is a prime then there are integers L and M, uniquely determined up to sign, for which $4q = L^2 + 27M^2$. As in the case of quadratic residues, one can give the characterization of determining prime cubic residues modulo q based on some congruence conditions. The following consequence of the law of cubic reciprocity is due to Z.-H. Sun (see [43, (1.6) and Corollary 2.1]).

Proposition 3. Let q be a prime with $q \equiv 1 \bmod 3$, and let L, M be integers satisfying $4q = L^2 + 27M^2$. Let p be a prime, $p \neq 2, 3$, or q. Then

$$p \text{ is a cubic residue mod } q \text{ if and only if } p \mid L(x^2-1) - M(x^3 - 9x) \text{ for some } x \in \mathbb{Z}.$$

Remark 1. In fact, the restriction to $p \neq 2, 3$ is unnecessary. (See Propositions 7.1 and 7.2 in [29, Chapter 7], or Theorems 2.26 and 2.27 in [39, Chapter 2] for details and the background.)

One of the consequences of Sun's cubic reciprocity law (also keeping in mind our Remark 1) is Nagell's result from 1952, [36], where he proved that for each prime $q \equiv 1 \bmod 3$, $q > 7$, there exists a prime $p < q^{1/2}$ that is a cubic residue modulo q. To see this, first observe that taking $x = 0$ and $x = 1$, by Proposition 3 if a prime $p \neq 2, 3$ divides LM, then p is a cubic residue modulo q. When $q > 7$, $4q = L^2 + 27M^2$ implies that $|LM| > 1$. Now taking any prime p dividing LM produces a cubic residue modulo q with $p < 2q^{1/2}$.

Recalling that each prime $q \equiv 1 \bmod 4$ admits a representation $q = L^2 + 4M^2$, with the integers L, M uniquely determined up to sign, we also quote a form of biquadratic (i.e., fourth power) reciprocity law. We say that an integer a is a biquadratic residue modulo m if the congruence $x^4 \equiv a \bmod m$ has a solution. For an odd prime p, let $p^* = (-1)^{(p-1)/2}p$, so that $p^* = \pm p$ and $p^* \equiv 1 \bmod 4$. The following Proposition 4 is again due to Sun (compare with Theorem 2.2 and Corollary 3.2 of [44]).

Proposition 4. Let q be a prime with $q \equiv 1 \bmod 4$ and let L, M be integers satisfying $q = L^2 + 4M^2$. Let p be an odd prime, $p \neq q$. Then

$$p^* \text{ is a biquadratic residue mod } q \text{ if and only if } p \mid M(x^4 - 6x^2 + 1) - 2L(x^3 - x) \text{ for some } x \in \mathbb{Z}.$$

In Chapter 2, we will show how these reciprocity laws can be used to deduce results on the number of prime quadratic, cubic, biquadratic residues modulo q in the interval (and in subintervals of) $[1, q-1]$.

1.1.2 Sieve techniques

Sieve theory deals with the problem of estimating the size of "sifted sets". Here a sifted set is one which is formed from starting with a given set $\mathcal{A}$ and removing all elements that have a small prime factor from a prescribed set of primes $\mathcal{P}$. The sieve theory is developed to extend the meaning of 'small' in the previous description. Consider a finite sequence (a multiset) $\mathcal{A} = \{a_i\}$, and let $\mathcal{P}$ be a finite set of primes, and denote the number of elements of the subset of $\mathcal{A}$ which consists of elements that are not divisible by any element of $\mathcal{P}$ by $S(\mathcal{A}, \mathcal{P})$. In other words, if we put $P = \prod_{p \in \mathcal{P}} p$, then $S(\mathcal{A}, \mathcal{P}) = \#\{a \in \mathcal{A} : (a, P) = 1\}$. Further, it is sometimes useful to consider a subset of $\mathcal{P}$, where we only would like to consider primes p in $\mathcal{P}$ with $p \leq z$. In this case we put $P(z) = \prod_{\substack{p \in \mathcal{P} \\ p \leq z}} p$, and we use the notation

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

For an integer $d \mid P(z)$, we assume that there exists a multiplicative function $h(.)$ such that

$$A_d(x) := \sum_{\substack{n \leq x \\ d \mid n}} a_n = h(d)X + r_d(x). \tag{1.1}$$

Here, $h(d)$ can be viewed as the density of the masses a_n for $n \equiv 0 \bmod d$, and $r_d(x)$ is an error term. Moreover, X is approximately equal to $A(x) = \sum_{n \leq x} a_n$. Assume that

$$0 \leq h(p) < 1 \text{ if } p \leq z,$$
$$h(p) = 0 \text{ if } p > z.$$

It is important to mention the sieve of Eratosthenes as a first step towards any sieve theoretic result. The idea of the sieve of Eratosthenes is to start with a list of integers up to x

and cross out the multiples of primes (other than themselves) that are $\leq \sqrt{x}$. Then the remaining numbers will only be primes and the number 1. Using this idea and the principle of inclusion-exclusion we have the following form of Sieve of Eratosthenes which is known due to Legendre.

Theorem 5 (Sieve of Eratosthenes–Legendre, Theorem 6.2 [39])**.**

$$S(\mathcal{A}, \mathcal{P}, z) = X \prod_{p|P(z)} (1 - h(p)) + \sum_{d|P(z)} \mu(d) r_d(x).$$

Here, $\mu(n)$ is the Möbius function defined on the natural numbers as

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1, \\ (-1)^k & \text{if } n \text{ is squarefree with } k \text{ distinct prime factors,} \\ 0 & \text{otherwise.} \end{cases}$$

Example 1. Let $\mathcal{A} = \{n(n+2) : n \leq x\}$ and let $\mathcal{P}$ be set of all primes. These sets are natural choices for detecting twin primes. If n and $n+2$ are both prime, then n and $n+2$ have no small prime factors (unless n itself is a small prime); conversely, if n and $n+2$ have no small prime factors up to $\sqrt{x+2}$, then n and $n+2$ are both prime. For this choice of $\mathcal{A}$, let d be a squarefree number, then we can write $A_d = x\frac{\nu(d)}{d} + r_d(x)$, where $\nu(d) = \#\{n \bmod d : n(n+2) \equiv 0 \bmod d\}$. So by Theorem 5, we have

$$\begin{aligned} S(\mathcal{A}, \mathcal{P}, z) =& x \prod_{p \leq z} \left(1 - \frac{\nu(p)}{p}\right) + \sum_{d|P(z)} \mu(d) r_d(x) \\ =& \frac{x}{2} \prod_{2 < p \leq z} \left(1 - \frac{2}{p}\right) + \sum_{d|P(z)} \mu(d) r_d(x) \\ =& 2x \prod_{2 < p \leq z} \left(\frac{1 - \frac{2}{p}}{\left(1 - \frac{1}{p}\right)^2}\right) \prod_{p \leq z} \left(1 - \frac{1}{p}\right)^2 + \sum_{d|P(z)} \mu(d) r_d(x). \end{aligned}$$

Here the main term has order $x/(\log z)^2$ while the error has size $3^{\pi(z)}$, indeed $\left|\sum_{d|P(z)} \mu(d) r_d(x)\right|$ is bounded by $\sum_{d|P(z)} \nu(d) = \prod_{p\leq z}(1+\nu(p)) \leq 3^{\pi(z)}$. In order to obtain a nontrivial estimate, it is necessary to choose z quite small, certainly $z \ll (\log x)^{1+\epsilon}$. But then we cannot deduce an upper bound better than $x/(\log\log x)^2$ from this approach.

Brun [10], worked on improvements of the Sieve of Eratosthenes-Legendre.

Theorem 6 (Brun's pure sieve, Theorem 6.10 [39])**.** For every even integer $m \geq 0$,

$$S(\mathcal{A}, \mathcal{P}, z) = X \prod_{p|P(z)} (1 - h(p)) + O\left(\sum_{d|P(z), \omega(d)\leq m} |r_d(x)|\right) + O\left(X \sum_{d|P(z), \omega(d)\geq m} h(d)\right).$$

Brun applied the above result to the problem described in Example 1. He proved that if $z = z(x) \to \infty$ with $z(x) \leq x^{1/(20\log\log x)}$, then (for the choice of $\mathcal{A}$ and $\mathcal{P}$ as in Example 1)

$$S(\mathcal{A}, \mathcal{P}, z) \sim 2C_2 e^{2\gamma} x/(\log z)^2.$$

This implies the following upper bound for the number of twin prime pairs up to x.

$$\#\{p \leq x : \ p+2 \ \text{ is also prime}\} \ll \frac{x(\log\log x)^2}{(\log x)^2}.$$

Using this upper bound, Brun deduced that the series $\sum_{\substack{p \\ p+2 \text{ prime}}} \frac{1}{p}$ converges.

Sieve theory evolved in the following years to find methods to obtain estimates for $S(\mathcal{A}, \mathcal{P}, z)$, where the aim is to be able to take z as large as possible in terms of x. For example, we would like to get an asymptotic formula when $z \leq x$ is taken as a power of x.

In this thesis we are going to use a sieve result, called the fundamental lemma of the sieve, which under some constraints gives an upper and a lower bound for $S(\mathcal{A}, \mathcal{P}, z)$.

Lemma 7 (Corollary 6.2, [26]). Let $A = (a_n)$ be a sequence. Let x and z be parameters, and let $P(z) = \prod_{p<z} p$ be the product of primes up to z. For an integer $d \mid P(z)$, we assume that there exists a multiplicative function $h(.)$ such that (1.1) holds. Assume that

$$0 \leq h(p) < 1 \text{ if } p \leq z,$$
$$h(p) = 0 \text{ if } p > z.$$

Suppose further that there exists $\kappa > 0$, $K > 1$ such that for any $2 \leq w < z$,

$$\prod_{w \leq p < z} (1 - h(p))^{-1} \leq K \left(\frac{\log z}{\log w} \right)^{\kappa}.$$

Moreover, put $\beta = 9\kappa + 1$ and assume that $s \geq \beta$. Then

$$\sum_{\substack{n \leq x \\ (n, P(z))=1}} a_n < (1 + e^{\beta - s} K^{10}) V(z) + R(x, z^s),$$
$$\sum_{\substack{n \leq x \\ (n, P(z))=1}} a_n > (1 - e^{\beta - s} K^{10}) V(z) - R(x, z^s),$$

where

$$V(z) = \prod_{p \mid P(z)} (1 - h(p)), \quad \text{and} \quad R(x, y) = \sum_{\substack{d \mid P(z) \\ d < y}} |r_d(x)|.$$

We will also use a more precise form of the fundamental lemma of the sieve (the sieve of Diamond–Halberstam–Richert [15]) in order to obtain results on the number of prime divisors of some polynomials. Before stating the lemma we first quote the analytic theorem which introduces the related functions in the statement of Diamond–Halberstam–Richert sieve.

Proposition 8 (Theorem 6.1, [15])**.** For each number $\kappa \geq 1$ for which $2\kappa \in \mathbb{N}$ there exists numbers $\alpha = \alpha_\kappa$ and $\beta = \beta_\kappa$ satisfying

$$\alpha_1 = \beta_1 = 2 \quad \text{and} \quad \alpha_\kappa > \beta_\kappa > 2, \text{ for } \kappa > 1,$$

such that the system of initial conditions

$$\begin{aligned} F(u) =& \frac{1}{j_\kappa(u/2)}, \quad 0 < u \leq \alpha, \\ f(u) =& 0, \quad 0 < u \leq \beta, \end{aligned}$$

the simultaneous difference differential equations

$$\begin{aligned} (u^\kappa F(u))' =& \kappa u^{\kappa-1} f(u-1), \quad \alpha < u, \\ (u^\kappa f(u))' =& \kappa u^{\kappa-1} F(u-1), \quad \beta < u, \end{aligned}$$

and boundary conditions

$$F(u) = 1 + O(e^{-u}), \quad f(u) = 1 + O(e^{-u})$$

has continuous solutions $F = F_\kappa$, $f = f_\kappa$ with the properties that $F(u)$ decreases monotonically and $f(u)$ increases monotonically on $(0, \infty)$. The function j_κ is the continuous solution of the differential delay equation

$$uj'_\kappa = \kappa j_\kappa(u) - \kappa j_\kappa(u-1), \quad u > 1,$$

that is defined for other real values of u by

$$j_\kappa(u) = \begin{cases} 0 & \text{if } u \le 0, \\ \frac{e^{\gamma k} u^\kappa}{\Gamma(\kappa+1)} & \text{if } 0 < u \le 1, \end{cases}$$

where γ denotes the Euler-Mascheroni constant and Γ denotes Euler's gamma function.

Lemma 9 (DHR sieve, Theorem 9.1, [15])**.** Suppose that $\kappa \ge 1$ and that 2κ is an integer. Suppose that for a parameter y with $2 \le y \le z$ and a constant $A > 1$ we have

$$\prod_{w \le p < z} (1 - h(p))^{-1} \le \left(\frac{\log z}{\log w}\right)^\kappa \left(1 + \frac{A}{\log w}\right), \ 2 \le w \le z.$$

Then

$$S(\mathcal{A}, \mathcal{P}, z) \le XV(z) \left\{ F_\kappa \left(\frac{\log y}{\log z}\right) + O\left(\frac{(\log\log y)^2}{(\log y)^{1/(2\kappa+2)}}\right)\right\} + 2 \sum_{\substack{m | P(z) \\ m < y}} 4^{\omega(m)} |R_{\mathcal{A}}(m)|,$$

and

$$S(\mathcal{A}, \mathcal{P}, z) \ge XV(z) \left\{ f_\kappa \left(\frac{\log y}{\log z}\right) - O\left(\frac{(\log\log y)^2}{(\log y)^{1/(2\kappa+2)}}\right)\right\} - 2 \sum_{\substack{m | P(z) \\ m < y}} 4^{\omega(m)} |R_{\mathcal{A}}(m)|,$$

where $\omega(n)$ denotes the number of distinct prime divisors of n, F_κ and f_κ are as defined in Proposition 8 and the constants implied by the O-notation depend at most on κ and A.

The main application of Lemma 9 that we are going to use will be noted in the following proposition. Here the dimension κ of the sieve is the degree of the polynomial.

Proposition 10. Suppose that f is a polynomial with integer coefficients with degree k with no fixed prime divisor, and that f has at most $\min(p-1, k)$ roots modulo every prime

p. Then for every $\theta > 0$, there exists $\eta = \eta(k) > 0$ such that

$$\#\{n \leq p^\theta, f(n) \text{ has no prime divisor less than } p^{\eta\theta}\} \gg_{\theta,k} p^\theta/(\log p)^k$$

provided that p is sufficiently large in terms of θ. The dependence of the implied constant on f is only through its degree k, and not on the precise choice of coefficients.

We will be using the fact that in Proposition 10, η can be taken as any number $> \frac{1}{\beta_k}$, where the values of β_k are given in Table 17.1, [15], p. 227. We will be using the facts that

$$\begin{aligned} \beta_2 &= 4.26645\cdots < 4.27, \\ \beta_3 &= 6.640859\cdots < 7, \\ \beta_4 &= 9.072248\cdots < 9.1. \end{aligned} \tag{1.2}$$

1.1.3 Erdős' result on infinitude of weakly prime numbers

The following question was stated in Mathematics Magazine (Problem 1029) in 1978:

Question. Does there exist any prime number such that if any digit (in base 10) is changed to any other digit, the resulting number is always composite?

In 1979, Erdős answered this question affirmatively, [18], proving actually that there are infinitely many such primes.

Theorem 11 (Erdős)**.** For all sufficiently large positive integers k, there exist primes p,

$$p = \sum_{i=0}^{k} a_i 10^i, \ a_k > 0, \ 0 \leq a_i \leq 9,$$

such that all of the integers $p + t\,10^i$, $0 < |t| < 10$, $0 \leq i \leq k$ are composite.

We will call this type of primes *weakly prime numbers* base 10. Similarly we can define a weakly prime number for any fixed base $a \geq 2$ and Erdős' result can be extended to those bases. Here we include a sketch of the proof of Erdős, as our proof of a quantitative improvement (Theorem 27, below) has the same essence. One of the key results he used in the proof is the Bang-Zsigmondy Theorem for the fact that for each $j \in \mathbb{N}$ there are primes q_j such that the order of 10 $\bmod q_j$ is exactly j. (That is $10^j \equiv 1 \bmod q_j$ and $10^i \not\equiv 1 \bmod q_j$ for $1 \leq i < j$.)

Theorem 12. [Bang-Zsigmondy Theorem, [2], [50], [8]] Let a and n be two integers greater than 1. Then there exists a prime q such that a has order $n \bmod q$, except exactly in the following cases:

- $n = 2$ and $a = 2^k - 1$, where $k \geq 2$.
- $n = 6$ and $a = 2$.

We will also need Linnik's result on the least prime in an arithmetic progression. We will return back to this result in Section 1.2.1.

Theorem 13. [Linnik's Theorem, 1944, [30]] Let a, q be two integers such that $q \geq 1$ and $(a, q) = 1$. There exists a prime p such that $p \equiv a \bmod q$, and $p \ll q^C$ for some positive absolute constant C.

In order to prove the existence of weakly prime numbers, Erdős showed the existence of small prime numbers q and a prime p so that each $p + t10^i$ is divisible by one of the primes q. Our proof of a quantitative improvement of this result is also based on the idea of choosing such primes q in an effective manner.

Sketch Proof of Theorem 11. Let k be a large integer. Put $x = 10^{k+1}$. Let $r := \lfloor \epsilon \sqrt{\log x} \rfloor$. By Bang-Zsigmondy Theorem, for each $j \in \mathbb{N}$ there are primes q_j such that the order of 10

mod q_j is exactly j. We will use such $\{q_j\}$ to determine some congruences by induction on j for $1 \leq j \leq r$. Suppose that we have determined some congruence classes $u_m \bmod q_m$ for $1 \leq m \leq j-1$. Let $b_1, \ldots, b_{s_{j-1}}$ be the integers of the form $t10^i$, $0 < |t| < 10$, $1 \leq i \leq k$ which do not satisfy any of the congruences

$$t10^i \equiv -u_m \bmod q_m,\ 1 \leq m \leq j-1.$$

The numbers $t10^i$ determine at most $18j$ residue classes modulo q_j (since $10^j \equiv 1 \bmod q_j$). Therefore by the Pigeonhole Principle, there is a congruence class $u_j \bmod q_j$ for which $b_L \equiv -u_j \bmod q_j$, $1 \leq L \leq j-1$ is satisfied by at least $\left\lceil \frac{b_{s_{j-1}}}{18j} \right\rceil$ values of L. This determines the congruences

$$p \equiv u_j \bmod q_j,\ \ 1 \leq j \leq r. \tag{1.3}$$

Suppose that $p \leq x$ is a prime satisfying the congruences (1.3). Then the number of integers $t10^j$, $0 < |t| < 10$, $1 \leq j \leq k$ for which $p + t10^j$ is not a multiple of one of the q_j, $1 \leq j \leq r$ is at most

$$18(k+1)\prod_{j=2}^{r}\left(1 - \frac{1}{j}\right) < \frac{18\log x}{r} < \frac{18\sqrt{\log x}}{\epsilon}.$$

Let $\nu_1, \nu_2, \ldots, \nu_s$, $s \leq \frac{18\sqrt{\log x}}{\epsilon}$ be these integers of the form $t10^i$. Let $Q_1, Q_2, \ldots, Q_s$ be the consecutive primes in the list of the first $r+s$ primes which are not equal to any of the q_j's. Put

$$p \equiv -\nu_i \bmod Q_i,\ i = 1, \ldots, s. \tag{1.4}$$

There are $r+s$ congruence conditions given in the equations (1.3) and (1.4) each to a prime

modulus and the product of the moduli satisfies

$$\prod q_j \prod Q_i < x^{\epsilon}.$$

Before completing the proof, we now quote a quantitative form of Linnik's theorem that appeared in [26].

Theorem 14 (Corollary 18.8, p. 442, [26])**.** If q is sufficiently large and $x \geq q^C$, for a sufficiently large constant C, then

$$\#\{\text{primes } p \leq x : p \equiv a \bmod q\} \gg \frac{x}{\sqrt{q}\,\varphi(q)\log q}$$

for any a with $(a, q) = 1$, where the implied constant is absolute.

Hence by Theorem 14 there are at least $x^{1-2\epsilon}$ primes $p < x$ such that all $p + t\,10^i$, $0 < |t| < 10$, $0 \leq i \leq k$ are all divisible by the primes $\{q_j\}, \{Q_i\}$ we determined. Among those primes p fewer than $(\log x)^2$ may have the property that some of $p + t\,10^i$ themselves are prime. This leaves us with primes $p < x$ such that $p + t\,10^i$, $0 < |t| < 10$, $0 \leq i \leq k$ are all composite. □

In 2011, Tao [45] proved that for any integer $K \geq 2$, there exist at least $c_K \frac{x}{\log x}$ primes p in the interval $[x, (1 + K^{-1})x]$ satisfying $|pj \pm a^h k|$ is composite for every $2 \leq a \leq K$, $1 \leq j, k \leq K$ and $1 \leq h \leq K \log x$, where $c_K > 0$ is a constant depending only on K. In a different direction, Pan [37] adopted Tao's methods to prove the following theorem.

Theorem 15 (Pan, 2014)**.** Suppose that $K \geq 2$ is an integer and $\epsilon > 0$ is a small number. Then for all sufficiently large (depending only on K and ϵ) x, there exist at least $x^{1-\epsilon}$ integers $n \in [x, (1+K^{-1})x]$ such that $\omega(nj \pm a^h k) \geq (\log\log\log x)^{\frac{1}{3}-\epsilon}$ for all $2 \leq a \leq K$, $1 \leq j, k \leq K$ and $0 \leq h \leq K \log x$. Here, as usual, $\omega(m)$ denotes the number of distinct prime factors of m.

In [37], Pan also asked if one could improve the quoted lower bound $(\log\log\log x)^{\frac{1}{3}-\epsilon}$ to a bound comparable to $\log\log x$. (This is a natural question as the normal order of $\omega(n)$ is $\log\log n$.) In Chapter 3, we will present a quantitative improvement (Theorem 27) of the Erdős' and Pan's results above.

1.2 Analytic methods

1.2.1 Dirichlet series and primes in an arithmetic progression

Let $a(n)$ be an arithmetic function. The Dirichlet series $f(s)$ corresponding to $a(n)$ is formally defined as

$$f(s) = \sum_{n=1}^{\infty} \frac{a(n)}{n^s}$$

where $s \in \mathbb{C}$. For a given Dirichlet series $f(s)$ as above, we call $a(n)$ the Dirichlet coefficients of $f(s)$.

Example 2. If $a(n) = 1$ for any $n \in \mathbb{N}$, then the Dirichlet series $\sum_{n=1}^{\infty} \frac{a(n)}{n^s}$ defines the Riemann zeta function

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s}, \quad \Re s > 1.$$

The Riemann zeta function $\zeta(s)$ can be meromorphically continued to the whole complex plane with a simple pole at $s = 1$ with residue 1.

$\zeta(s)$ also has an Euler product expansion

$$\zeta(s) = \prod_{p \text{ prime}} \left(1 - \frac{1}{p^s}\right)^{-1}, \quad \Re s > 1.$$

By logarithmic differentiation, we obtain

$$-\frac{\zeta'(s)}{\zeta(s)} = \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}, \quad \Re s > 1,$$

where $\Lambda(n)$ is the von Mangoldt function defined by

$$\Lambda(n) = \begin{cases} \log p & \text{if } n = p^k, \text{ for some prime } p \text{ and } k \geq 1, \\ 0 & \text{otherwise.} \end{cases}$$

Perron's formula, stated below, allows us to estimate the partial sums $\sum_{n \leq x} a(n)$ using the analytic properties of $f(s)$.

Lemma 16 (Lemma 3.12, [46])**.** For $s = \sigma + it$, σ, $t \in \mathbb{R}$, let $g(s) = \sum_{n=1}^{\infty} \frac{a_n}{n^s}$, $(\sigma > 1)$, where $a_n = O(\psi(n))$, $\psi(n)$ being nondecreasing and $\sum_{n=1}^{\infty} \frac{|a_n|}{n^\sigma} = O\left(\frac{1}{(\sigma-1)^\alpha}\right)$, for some $\alpha \geq 0$ as $\sigma \to 1$. Let $c > 0$ so that $\sigma + c > 1$. If x is not an integer and N is the integer nearest to x, then

$$\begin{aligned} \sum_{n \leq x} \frac{a_n}{n^s} =& \frac{1}{2\pi i} \int_{c-iT}^{c+iT} g(s+w) \frac{x^w}{w}\, dw + O\left(\frac{x^c}{T(\sigma + c - 1)^\alpha}\right) \\ &+ O\left(\frac{\psi(2x) x^{1-\sigma} \log x}{T}\right) + O\left(\frac{\psi(N) x^{1-\sigma}}{T|x - N|}\right). \end{aligned} \tag{1.5}$$

If x is an integer, then the corresponding result is

$$\begin{aligned} \sum_{n=1}^{x-1} \frac{a_n}{n^s} + \frac{a_x}{2x^s} =& \frac{1}{2\pi i} \int_{c-iT}^{c+iT} g(s+w) \frac{x^w}{w}\, dw + O\left(\frac{x^c}{T(\sigma + c - 1)^\alpha}\right) \\ &+ O\left(\frac{\psi(2x) x^{1-\sigma} \log x}{T}\right) + O\left(\frac{\psi(x) x^{-\sigma}}{T}\right). \end{aligned} \tag{1.6}$$

Returning to the last example, Perron's formula allows us to describe the sum $\sum_{n \leq x} \Lambda(n)$

in terms of the zeros of the Riemann zeta function $\zeta(s)$ (see [14]):

$$\sum_{n\leq x}{}' \Lambda(n) = x - \sum_{\rho} \frac{x^{\rho}}{\rho} - \frac{\zeta'(0)}{\zeta(0)} - \frac{1}{2}\log(1-x^{-2}),$$

where $\sum'$ indicates that the last term should be halved if x is an integer. Here ρ denotes a nontrivial zero of $\zeta(s)$, that is $\zeta(\rho)=0$ and $0<\Re\rho<1$. And using the information on the location of the zeros of $\zeta(s)$, we obtain the Prime Number Theorem.

Theorem 17 (Prime Number Theorem)**.**

$$\sum_{n\leq x}\Lambda(n) = x + O(x\exp\{-c\sqrt{\log x}\}).$$

Lemma 16 will appear again in Chapter 4, where it will be used to count number fields of a certain type.

Example 3. Another set of examples for functions defined by a Dirichlet series is Dirichlet L-functions $L(s,\chi)$. We define a Dirichlet character $\chi(n)$ (which are the Dirichlet coefficients for $L(s,\chi)$) as follows.

Definition 2. Let $q\geq 2$ be an integer. A totally multiplicative function $\chi:\mathbb{Z}\to\mathbb{C}$ is called a Dirichlet character modulo q if

- $\chi(n+q)=\chi(n)$ for any $n\in\mathbb{N}$,
- $\chi(n)=0$ if and only if $(n,q)>1$.

The set of Dirichlet characters modulo q form a group with $\varphi(q)$ elements with identity element χ_0, called the principal character, defined as $\chi_0(n)=1$ for any $n\in\mathbb{Z}$ with $(n,q)=1$. For any nonprincipal Dirichlet character $\chi \bmod q$, we have

$$\sum_{n \bmod q}\chi(n) = 0. \tag{1.7}$$

Moreover, Dirichlet characters modulo q satisfy the following orthogonality property. For $(a,q)=1$, we have

$$\frac{1}{\varphi(q)}\sum_{\chi \bmod q}\chi(a)\overline{\chi}(b)=\begin{cases}1 & \text{if } a\equiv b \bmod q,\\ 0 & \text{otherwise.}\end{cases}$$

A Dirichlet character $\chi \bmod q$ is called a primitive character modulo q if for every proper divisor d of q there exists an integer $a \equiv 1 \bmod d$, with $(a,q)=1$ and $\chi(a)\neq 1$. Thus in particular, if q is prime, every nonprincipal character modulo q is primitive.

Let χ be a Dirichlet character modulo q. The Dirichlet L-function $L(s,\chi)$ is defined by the series

$$L(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)}{n^s}, \quad \Re s>1.$$

$L(s,\chi)$ can be analytically continued to the whole complex plane, (when $\chi=\chi_0$ with a simple pole at $s=1$ with residue $\frac{q}{\varphi(q)}$).

Logarithmically differentiating the Euler product expansion

$$L(s,\chi)=\prod_{p}\left(1-\frac{\chi(p)}{p^s}\right)^{-1}, \quad \Re s>1$$

of $L(s,\chi)$, we obtain the identity

$$-\frac{L'}{L}(s,\chi)=\sum_{n=1}^{\infty}\frac{\chi(n)\Lambda(n)}{n^s}, \quad \Re s>1.$$

Using this identity and the orthogonality of characters, Dirichlet L-functions play an important role in counting primes in certain arithmetic progressions since for $(a,q)=1$, we have

$$\sum_{\substack{n=1\\ n\equiv a \bmod q}}^{\infty} \frac{\Lambda(n)}{n^s} = \frac{1}{\varphi(q)} \sum_{\chi \bmod q} \overline{\chi}(a) \sum_{n=1}^{\infty} \frac{\chi(n)\Lambda(n)}{n^s}.$$

Using Perron's formula, Lemma 16, we obtain an explicit formula for the partial sums of $\Lambda(n)\chi(n)$,

$$\sum_{n\le x}{}' \chi(n)\Lambda(n) = \begin{cases} -\sum_{\rho_\chi} \frac{x^{\rho_\chi}}{\rho_\chi} & -\frac{L'(0,\chi)}{L(0,\chi)} - \sum_{m=1}^{\infty} \frac{x^{-2m+1}}{2m-1} \quad \text{if } \chi(-1) = -1, \\ -\sum_{\rho_\chi} \frac{x^{\rho_\chi}}{\rho_\chi} & -\log x - b(\chi) - \sum_{m=1}^{\infty} \frac{x^{-2m}}{2m} \quad \text{if } \chi(-1) = 1, \end{cases} \tag{1.8}$$

for a primitive Dirichlet character χ modulo q, where $b(\chi)$ is a constant depending on χ and ρ_χ denotes a nontrivial zero of $L(s,\chi)$. And using orthogonality we derive an expression for the partial sums of $\Lambda(n)$ along the progression $n \equiv a \bmod q$, which is a weighted count of primes (and prime powers) in terms of the zeros of the Dirichlet L-functions $L(s,\chi)$ modulo q. We now recall two important results on these zeros.

Theorem 18 (Landau-Page Theorem, see [9], p. 39)**.** There exists a constant $c_1 > 0$ such that $L(s,\chi) \neq 0$ for $\Re s \ge 1 - \frac{c_1}{\log T}$, for $|t| = |\Im s| \le T$, $T \ge 2$ and for any primitive character modulo $q \le T$ except possibly for at most one exceptional case $L(\beta_1, \chi_1) = 0$. The exceptional zero β_1 is simple, real and the exceptional character χ_1 is a quadratic character, that is $\chi_1^2 = \chi_0$. Moreover, for some constant $c_2 > 0$, the inequality $1 - \beta_1 \ge \frac{c_2}{T^{1/2}\log T}$ holds.

We next quote the lower bounds of $|L(1,\chi)|$ and thus a zero-free region for $L(s,\chi)$.

Theorem 19 (Landau [28] and Siegel's Theorem, [42], also see Chapter 21 in [14])**.** If χ is a non-real character modulo q, we have $L(1,\chi) \gg (\log q)^{-1}$. Moreover, for each $\epsilon > 0$ there

exists $C(\epsilon) > 0$ such that

$$L(1, \chi) > C(\epsilon) q^{-\epsilon}$$

holds for all real Dirichlet characters χ modulo q. Hence there exists $C'(\epsilon) > 0$ such that any zero β of $L(s, \chi)$ satisfies

$$\beta \leq 1 - C'(\epsilon) q^{-\epsilon}.$$

Using Theorem 18, Theorem 19, and the explicit formula (1.8), we derive the Siegel-Walfisz Theorem, [14],

$$\sum_{\substack{n \leq x \\ n \equiv a \bmod q}} \Lambda(n) = \frac{x}{\varphi(q)} + O(x \exp\{-c_A \sqrt{\log x}\}),$$

as long as $q \ll (\log x)^A$ for some $A > 0$.

As mentioned in the previous section, Linnik proved the following theorem in [30]. We restate Theorem 13 here.

Theorem (Linnik's Theorem, 1944)**.** Let a, q be two integers such that $q \geq 1$ and $(a, q) = 1$. There exists a prime p such that $p \equiv a \bmod q$, and $p \ll q^C$ for some positive absolute constant C.

From then forward, there have been improvements on how small C can be taken. The best known result in this direction is that C can be taken as 5 by Xylouris [49], and when the modulus q is prime C can be taken as 4.5 due to the work of Meng, [35]. Following the proof of Linnik's Theorem in [9, p. 39], we obtain the following corollary. Due to lack of suitable reference we include the proof here. We will use this Corollary 1 when we prove Theorem 27 in Chapter 3.

Corollary 1. Let $K > 0$ be fixed. Let a, q be two integers such that $q \geq 1$ and $(a, q) = 1$, and let x be a real number so that $q^c \ll x$, for a sufficiently large constant $c > 0$. Then there are at least $\gg_K \frac{x}{q^2\varphi(q)\log x}$ primes p such that $p \equiv a \bmod q$, and $x < p \leq (1 + K^{-1})x$.

Proof. The result in the case when $q \leq (\log x)^2$ follows by applying the Siegel-Walfisz Theorem. Suppose that $q > (\log x)^2$. We follow Bombieri's notation used in [9]. Here, $L(s, \chi)$ denotes a Dirichlet L-function for $s = \sigma + it$, where σ and t are real numbers, and χ is a Dirichlet character $\bmod q$. Let $c_1 > 0$ be the constant appearing in the Landau-Page Theorem (see Theorem 18, above) such that $L(s, \chi) \neq 0$ for $\sigma \geq 1 - \frac{c_1}{\log T}$, $|t| \leq T$ for all primitive characters $\chi \bmod m$, $m \leq T$ except possibly for one exceptional real character. We let χ_1 denote a character modulo q, induced by an exceptional character, if it exists. In this case we let β_1 denote the exceptional zero of $L(s, \chi_1)$, and we also let $\delta_1 := 1 - \beta_1$.
We put $4A := \frac{\log x}{\log q}$ so that $(1 + K^{-1})x = q^{4c_0A}$, where $c_0 = 1 + \frac{\log(1+1/K)}{4A\log q}$. Then $1 < c_0 < 2$. Using the last equation in the proof of Linnik's Theorem in [9, p. 55], namely,

$$\sum_{\substack{p\leqslant x\\ p\equiv a \bmod q}} \log p = \frac{1}{\varphi(q)}\left(x - \chi_1(a)\frac{x^{\beta_1}}{\beta_1}\right) + O\left(\frac{x}{\varphi(q)}\delta_1(\log q)\exp\left(-c_1A\right)\right) + O\left(\frac{x\log x}{q^4}\right) + O\left(\frac{1}{\varphi(q)}x^{1/2}q^{20}\right),$$

we obtain

$$\begin{aligned}\sum_{\substack{x<p\leqslant(1+K^{-1})x\\ p\equiv a \bmod q}} \log p =& \frac{1}{\varphi(q)}\left(K^{-1}x - \chi_1(a)\frac{((1+K^{-1})^{\beta_1} - 1)x^{\beta_1}}{\beta_1}\right)\\ &+ O\left(\frac{x}{\varphi(q)}\delta_1(\log q)\exp\left(-c'A\right)\right)\\ &+ O\left(\frac{x\log x}{q^4}\right) + O\left(\frac{1}{\varphi(q)}x^{1/2}q^{20}\right). \qquad (1.9)\end{aligned}$$

Note that $\frac{1}{2} < \beta_1 < 1$, so $\frac{K^{-1}}{(2+K^{-1})} < (1+K^{-1})^{\beta_1} - 1 < K^{-1}$. So we have

$$\frac{K^{-1}}{(2+K^{-1})}\frac{x^{\beta_1}}{\beta_1} < \left|\chi_1(a)\frac{((1+K^{-1})^{\beta_1}-1)x^{\beta_1}}{\beta_1}\right| < K^{-1}\frac{x^{\beta_1}}{\beta_1}.$$

If $\chi_1(a) > 0$, then

$$K^{-1}x - \chi_1(a)\frac{((1+K^{-1})^{\beta_1}-1)x^{\beta_1}}{\beta_1} > K^{-1}x - \chi_1(a)K^{-1}\frac{x^{\beta_1}}{\beta_1}.$$

If $\chi_1(a) < 0$, then

$$\begin{aligned} K^{-1}x - \chi_1(a)\frac{((1+K^{-1})^{\beta_1}-1)x^{\beta_1}}{\beta_1} &> K^{-1}x - \frac{K^{-1}}{(2+K^{-1})}\chi_1(a)\frac{x^{\beta_1}}{\beta_1} \\ &> \frac{K^{-1}}{(2+K^{-1})}x - \frac{K^{-1}}{(2+K^{-1})}\chi_1(a)\frac{x^{\beta_1}}{\beta_1}. \end{aligned}$$

Thus we have

$$K^{-1}x - \chi_1(a)\frac{((1+K^{-1})^{\beta_1}-1)x^{\beta_1}}{\beta_1} \gg_K x - \chi_1(a)\frac{x^{\beta_1}}{\beta_1}.$$

For A large enough, the term $x - \chi_1(a)\frac{x^{\beta_1}}{\beta_1}$ is $\gg (\delta_1 \log q)x$. So the main term is $\gg_K \frac{x}{\varphi(q)}q^{-2}$ and the first error term on the right hand side of (1.9) is negligible compared to the main term for large A. Moreover, it follows from the argument given in [9] that $x - \chi_1(a)\frac{x^{\beta_1}}{\beta_1} \gg \frac{x}{q^2}$. Now we note that for A large enough, the sum of the last two error terms on the right-hand side of (1.9) is also negligible. Thus we obtain

$$\sum_{\substack{x<p\leqslant(1+K^{-1})x \\ p\equiv a \bmod q}} \log p \gg_K \frac{x}{\varphi(q)}q^{-2}. \tag{1.10}$$

Since each term of the sum in (1.10) is of size $C\log x$, the desired result follows. □

1.2.2 Character sums and some applications

A central problem in analytic number theory is to understand the size of the character sums

$$\sum_{n \leq x} \chi(n)$$

where χ is a nonprincipal Dirichlet character $\bmod q$. Showing some cancellation in character sums has many applications in number theory an example of which is to bound the smallest quadratic nonresidue modulo q. By (1.7), the character sum over q consecutive integers vanishes, and so we are primarily interested sums over an interval of length $< q$, so-called incomplete sums, for whose absolute value a trivial upper bound is q. In 1919, Pólya and Vinogradov proved the following upper bound which shows cancellations for character sums if the length of the interval is larger that $q^{\frac{1}{2}+\epsilon}$, $\epsilon > 0$.

Theorem 20 (Pólya-Vinogradov Inequality)**.** Let χ be a nonprincipal Dirichlet character $\bmod q$. Then for integers M and N with $N > 0$,

$$\sum_{n=M+1}^{M+N} \chi(n) \ll \sqrt{q} \log q.$$

Here the implicit constant can be taken to be 1 (see [33]). Vinogradov [47] used the Pólya-Vinogradov Inequality (where χ is taken to be quadratic character) and a clever sieving argument to deduce that for sufficiently large primes q, the least positive quadratic nonresidue modulo q is $\ll_\epsilon q^{\frac{1}{2\sqrt{e}}+\epsilon}$.

In 1977, Montgomery and Vaughan showed under the assumption of the Generalized Riemann Hypothesis (GRH) [34] that $\sum_{n \leq x} \chi(n) \ll \sqrt{q} \log\log q$. Up to the constant this is "best possible" since R.E.A.C. Paley [38] had shown, in 1932, that there exist character sums (with real, quadratic characters), that are $\gg \sqrt{q} \log\log q$.

Pólya-Vinogradov Inequality implies that for a given $\epsilon > 0$ the sum $\sum_{n \leq x} \chi(n) = o(x)$ for all $x > q^{\frac{1}{2}+\epsilon}$. We expect to see that such cancellation occurs in a smaller length x of the character sum. The first substantial improvement of Pólya-Vinogradov Inequality in this direction was obtained in 1957 by D. A. Burgess.

Theorem 21 (Burgess, 1957, [11])**.** Let χ be a primitive character modulo $q > 1$ and let $\epsilon > 0$. Then

$$\sum_{n=M+1}^{M+N} \chi(n) \ll N^{1-\frac{1}{r}} q^{\frac{r+1}{4r^2}+\epsilon} \tag{1.11}$$

for $r = 2$, 3 and for any $r \geq 1$ if q is cubefree, with the implied constant depending only on ϵ and r.

Remark. Let $\eta > 0$ be fixed. If q is prime and $N = q^{1/4+\eta}$, then the upper bound in (21) becomes $q^{1/4-\frac{1}{4r}+\frac{r+1}{4r^2}+\epsilon}$ which is less than N for large r . So we see that Burgess bound ensures that cancellation occurs in character sums as long as the length of the sum is at least $q^{1/4+\eta}$.

From here forward, we will assume the modulus q to be a prime. In Vinogradov's proof, if we use Burgess bound instead of Pólya-Vinogradov Inequality, we obtain that the least positive quadratic nonresidue modulo q is $\ll_\epsilon q^{\frac{1}{4\sqrt{e}}+\epsilon}$.

By the total multiplicativity of the characters, the least positive quadratic nonresidue modulo q is necessarily a prime. Hence the proper analogue of the question for residues is to ask for a bound on the least prime quadratic residue modulo q. Vinogradov [47] conjectured that this should be $\ll q^\epsilon$. Linnik and Vinogradov used Burgess estimates to obtain the following best-known upper bound for the least prime quadratic residue modulo q.

Theorem 22 (Linnik-Vinogradov Theorem, [31])**.** Fix $\epsilon > 0$. For all large primes q, the least prime quadratic residue $\bmod q$ is $\ll_\epsilon q^{\frac{1}{4}+\epsilon}$.

Elliott [17] generalized the work of Linnik and Vinogradov for $k \geq 2$.

Theorem 23. Fix an integer $k \geq 2$ and fix $\epsilon > 0$. For all large primes $q \equiv 1 \bmod k$, the smallest prime kth power residue mod q is

$$\ll_{k,\epsilon} q^{\frac{k-1}{4}+\epsilon}.$$

Considering the known forms of Linnik's Theorem on the least prime in an arithmetic progression, Elliott's bound is only interesting for small values of k, as any prime $\equiv 1 \bmod q$ is a kth power modulo q.

In [41], Pollack showed that when $k = 2$, there are many prime quadratic residues satisfying the upper bound of Theorem 22. In fact, Pollack proved a more general theorem.

Theorem 24 (Theorem 1.3, [41])**.** Let $\epsilon > 0$ and let $A > 0$. There is an $m_0 = m_0(\epsilon, A)$ with the following property: If $m > m_0$ and χ is a quadratic character modulo m, then there are at least $(\log m)^A$ primes $p \leq m^{\frac{1}{4}+\epsilon}$ with $\chi(p) = 1$.

In 2017, Pollack proved that for $\epsilon > 0$ and for large enough modulus m there exists $\kappa > 0$ such that there at least m^{κ} prime quadratic nonresidues that are $\leq m^{\frac{1}{4\sqrt{e}}+\epsilon}$ (Pollack actually showed a more general Theorem on the number of small prime character nonresidues, see Theorem 1.1 in [41]). So we expect to have a comparable lower bound for the number of small prime quadratic residues (and possibly for the higher power residues). In Chapter 2, we will present improvements and generalizations of Theorem 24 in this direction, in the case when the modulus m is prime.

1.3 Statements of main results

Using the rational reciprocity laws for quadratic, cubic and biquadratic residues we have the following result for prime moduli (see Theorem 1, 2, and 3 in [6]). This result originally

appeared in [6].

Theorem 25. [Reciprocity Laws Approach] Let $\epsilon > 0$.

(a) For all primes $q \equiv 1 \bmod 3$, with $q > q_0(\epsilon)$, we have that

$$\#\{\text{primes } p < q^{\frac{1}{2}+\epsilon} : p \text{ is a cubic residue mod } q\} > q^{\frac{\epsilon}{30}}.$$

(b) For all primes $q \equiv 1 \bmod 4$, $q > q_1(\epsilon)$, we have that

$$\#\{\text{primes } p < q^{\frac{1}{2}+\epsilon} : p^* \text{ is a biquadratic residue mod } q\} > q^{\frac{\epsilon}{50}}$$

where $p^* = (-1)^{\frac{p-1}{2}} p$.

(c) If $\epsilon < \frac{1}{2}$, for all $q > q_2(\epsilon)$, we have that

$$\#\{\text{primes } p < q^{\frac{1}{2}+\epsilon} : p \text{ is a quadratic residue mod } q\} > q^{\frac{\epsilon}{25}}.$$

Theorem 25 (b) improves the lower bound in Theorem 24 in the case of a prime modulus: the contrast can be seen by the implied bounds on the number of prime quadratic residues $\leq q$. The proof of Theorem 25 implies that one can find at least $q^{\frac{1}{9}}$ primes that are quadratic residue modulo q (see Remark 3 in Chapter 2) and $\leq q$ whereas Theorem 24 can only produce an arbitrary power of $\log q$ of such primes. On the other hand, Theorem 25 only applies when counting quadratic residues up to $q^{\frac{1}{2}+\epsilon}$, whereas Theorem 24 is applicable when counting up to $q^{\frac{1}{4}+\epsilon}$, capturing much smaller primes.

In Chapter 2, together with the proof of Theorem 25, we will also give the proof of the following strengthening of Theorem 24 and Theorem 25, for prime moduli, which applies to all integers $k \geq 2$.

Theorem 26. [Theorem 1, [5]] Let $k \geq 2$ be an integer. Let $0 < \epsilon < \frac{k-1}{3}$. There exists $q_0(\epsilon, k) > 0$ such that if $q \equiv 1 \bmod k$ is a prime with $q > q_0(\epsilon, k)$, then we have

$$\#\{\text{primes } p \leq q^{\frac{k-1}{4}+\epsilon} : p \text{ is a } k\text{th power } \bmod q\} \gg_{\epsilon,k} q^{\frac{9\epsilon}{20k}}.$$

In Chapter 3, we discuss a quantitative improvement of Erdős' result on the infinitude of weakly prime numbers, and Theorem 15.

Theorem 27. (Theorem 1.3, [4]) Let $K \geq 2$ be an integer, $\epsilon > 0$ be a small number. For all sufficiently large positive x, there exist at least $x^{1-\epsilon}$ primes $x < p \leq (1 + K^{-1})x$, such that all of the integers $pj \pm a^h k,\ 2 \leq a \leq K,\ 0 < k \leq K,\ 1 \leq j \leq K,\ 0 \leq h \leq K \log x$ are composite having at least $(\log \log x)^{1-\epsilon}$ distinct prime factors.

In Chapter 4, we present a result on the number of pure number fields of degree p for each odd prime p. Since this result is of a different nature than the ones we discussed so far, we give a little background on the problem here. First we give the following definition.

Definition 3. Fix an integer $k \geq 2$. An integer n is called *k-free* if there are no primes q with $q^k \mid n$.

For an odd prime p and a number field K of degree p, K is said to be a *pure field of degree p* if for a p-free positive integer $n > 1$ we can write $K = \mathbb{Q}(\sqrt[p]{n})$. For $X > 0$, let $P_p(X)$ denote the number of pure fields K of degree p with $|d(K)| \leq X$, where $d(K)$ denotes the discriminant of K. Using elementary methods, Fujisawa [19] gave an upper and a lower bound for $P_p(X)$.

Theorem 28 (Theorem 1 in [19], [20])**.** Let $\epsilon > 0$ and p be an odd prime. Then we have

$$\frac{B_p}{\zeta(2)} X^{\frac{1}{p-1}} \leq P_p(X) \leq C_{p,\epsilon} X^{\frac{1}{p-1}} (\log X)^{p-2+\epsilon},$$

where $\zeta(s)$ is the Riemann zeta function and

$$A_p := \frac{p^{p+1} - p^{p-1} + p^{p-2} - 1}{(p^p - 1)p^p},$$
$$C_{p,\epsilon} := \frac{1}{\zeta(2)^{p-1}} \left(\frac{1}{p^{1/(p-1)}(p-1)} \right)^{p-2} + \epsilon.$$

For a p-free positive integer D, we associate $K = \mathbb{Q}(\sqrt[p]{D})$ with the conductor $f := f(K)$ of the cyclic extension N/k of degree p, where $N = \mathbb{Q}(\zeta, \sqrt[p]{D})$ is the normal closure of K, and $k = \mathbb{Q}(\zeta)$, with ζ denoting p^{th} root of unity. The relationship between the conductor $f(K)$ and the discriminant $d(K)$ is given by the following equality

$$d(K) = (-1)^{\frac{p-1}{2}} p^{p-2} f^{p-1}.$$

In [12], as a special case of a more general result on cubic extensions of number fields, Cohen and Morra obtained a formula for the sum $\sum_{K/\mathbb{Q} \text{ pure cubic}} \frac{1}{f(K)^s}$. Using this formula, they proved the following result.

Theorem 29 (Corollary 7.4 in [12])**.** Let $\epsilon > 0$. Then the number of pure cubic fields K up to isomorphism with the conductor $f(K)$ satisfying $f(K) \leqslant X$ is

$$= CX(\log X + D - 1) + O(X^{2/3+\epsilon})$$

where

$$C = \frac{7}{30} \prod_p \left(1 - \frac{3}{p^2} + \frac{2}{p^3} \right) = 0.0669\ldots,$$
$$D = 2\gamma - \frac{16}{35}\log(3) + 6 \sum_p \frac{\log p}{p^2 + p - 2} = 3.4502\ldots$$

and γ is the Euler-Mascheroni constant.

The following is an asymptotic for the number of pure fields of prime degree $p \geq 5$, whose proof will be given in Chapter 4. The following theorem and its corollary originally appeared in [3].

Theorem 30 (Theorem 3, [3])**.** Let $p \geq 5$ be a prime number. For each $\epsilon > 0$, we have that

$$\#\{K : K \text{ pure field of degree } p,\ |f(K)| \leqslant X\} = XQ_p(\log X) + O_p\left(X^{\frac{p+1}{p+3}+\epsilon}\right),$$

as $X \to \infty$, where $Q_p(x)$ is a polynomial of degree $p-2$.

Using the relation between the conductor $f(K)$ and the discriminant $d(K)$, we obtain the number of pure fields up to a bounded discriminant as a corollary to Theorem 30.

Corollary 2. Let $p \geq 5$ be a prime number. For each $\epsilon > 0$, we have that

$$\begin{aligned}\#\{K : K \text{ pure field of degree } p,\ |d(K)| \leqslant X\} = {} & \sqrt[p-1]{X}\tilde{Q}_p(\log X) \\ & + O_p\left(X^{\frac{p+1}{(p-1)(p+3)}+\epsilon}\right),\end{aligned}$$

as $X \to \infty$, where $\tilde{Q}_p(x)$ is a polynomial of degree $p-2$.

Remark 2. The coefficients of the polynomials $Q_p(x)$ and $\tilde{Q}_p(x)$ are effectively computable. We will explicitly present the leading coefficients in all the cases, and the second leading coefficient in the quintic case.

Chapter 2

Small prime power residues

2.1 Introduction

For each prime q and each integer $k \geq 2$, let $r_k(q)$ denote the smallest prime kth power residue modulo q. Clearly, any prime congruent to 1 modulo q is a kth power residue modulo q, so $r_k(q)$ exists for all pairs k, q. I. M. Vinogradov conjectured that $r_2(q) = O_\epsilon(q^\epsilon)$ for each $\epsilon > 0$, [47], and it is widely believed that the same is true for $r_k(q)$, for every fixed k. (Under the assumption of the Generalized Riemann Hypothesis, it is known that for any $\epsilon > 0$, $r_k(q) \ll_\epsilon q^\epsilon$. See, e.g., the work of Lamzouri, Li, and Soundararajan [27, Theorem 1.4], who present explicit upper bounds improving earlier estimates of Bach and Sorenson [1].) As it was mentioned in the introduction, Elliott, [17], gave an upper bound for $r_k(q)$ generalizing the work of Linnik and Vinogradov concerning the case when $k = 2$.

Theorem. (Theorem 23) Fix an integer $k \geq 2$ and fix $\epsilon > 0$. For all large primes $q \equiv 1 \bmod k$,

$$r_k(q) \ll_{k,\epsilon} q^{\frac{k-1}{4}+\epsilon}.$$

The restriction to primes $q \equiv 1 \bmod k$ is natural since the set of kth powers modulo q coincides with the set of $\gcd(k, q-1)$th powers. Indeed, if a is a kth power modulo q then it is a $\gcd(k, q-1)$th power; conversely if a is a $\gcd(k, q-1)$th power modulo q, then there is x modulo q such that $x^{\gcd(k,q-1)} \equiv a \bmod q$, but then we can find integers u and v such that $u(q-1) + vk = \gcd(k, q-1)$, so that $(x^v)^k \equiv x^{u(q-1)+vk} \equiv a \bmod q$.

Elliott's proof is essentially based on Burgess' character sum bound and the known lower bounds on $|L(1, \chi)|$ for nonprincipal Dirichlet characters χ mod q of order dividing k (recall Theorem 19). Note that Theorem 23 is of interest only for fairly small values of k, as the exponent $\frac{k-1}{4}$ eventually exceeds the exponent in known versions of Linnik's theorem (Theorem 13): By a work of Xylouris, [49], the exponent can be taken as 5, and Meng obtained [35] the better exponent 4.5 when the modulus is prime.

Due to the fact that there are better lower bounds available for $|L(1, \chi)|$ when χ mod q is a complex character, compared to the bounds for the real characters, Elliott observes, [17], that if k is odd then the proof of Theorem 23 can be modified to give a slightly sharper upper bound on $r_k(q)$. As an example, he states that for primes $q \equiv 1 \bmod 3$, there are constants $c, c' > 0$ such that

$$r_3(q) \leq c q^{\frac{1}{2}} \exp(c' \sqrt{\log q \cdot \log \log q}).$$

For the case when $k = 3$, Nagell, before Elliott, published a sharper upper bound for $r_3(q)$ in 1952, [36], namely

$$r_3(q) < 2q^{\frac{1}{2}} \qquad \text{for all } q > 7. \tag{2.1}$$

In contrast, Nagell's proof of (2.1) does not rely on character sum estimates, the proof relies instead on the algebraic theory of cubic residues developed by Gauss, Jacobi, and Eisenstein.

In the first part of this Chapter, we will explore how Nagell's approach can be used to produce more small power residues for the cases $k = 2, 3, 4$.

Next, we will introduce a strengthening and a generalization of these results using methods parallel to that of Elliott-Linnik-Vinogradov.

2.2 Reciprocity Laws approach-Proof of Theorem 25

In this section, we will give the proof of Theorem 25 based on reciprocity laws. We quote Theorem 25 below. As mentioned earlier, this result originally appeared in [6]. We will revisit the proof in this section.

Theorem (Theorem 25)**.** Let $\epsilon > 0$.

(a) For all primes $q \equiv 1 \bmod 3$ with $q > q_0(\epsilon)$, we have that

$$\#\{\text{primes } p < q^{\frac{1}{2}+\epsilon} : p \text{ is a cubic residue mod } q\} > q^{\frac{\epsilon}{30}}.$$

(b) For all primes $q \equiv 1 \bmod 4$ with $q > q_1(\epsilon)$, we have that

$$\#\{\text{primes } p < q^{\frac{1}{2}+\epsilon} : p^* \text{ is a biquadratic residue mod } q\} > q^{\frac{\epsilon}{50}}$$

where $p^* = (-1)^{\frac{p-1}{2}}p$.

(c) If $\epsilon < \frac{1}{2}$ then for all $q > q_2(\epsilon)$, we have that

$$\#\{\text{primes } p < q^{\frac{1}{2}+\epsilon} : p \text{ is a quadratic residue mod } q\} > q^{\frac{\epsilon}{25}}.$$

Recalling the earlier result of Pollack [40] on counting quadratic residues given in Theorem 24, each result given in Theorem 25 is superior in that the number of power residues produced exceeds a certain power of q, not merely an arbitrary power of $\log q$. However, it is necessary to point out that Theorem 24 counts prime quadratic residues in the interval $[1, q^{\frac{1}{4}+\epsilon}]$ whereas

part (c) of Theorem 25 includes a count in a larger range $[1, q^{\frac{1}{2}+\epsilon}]$. On the other hand, if we ask the question of number of prime quadratic residues in $[1, q-1]$, the proof of Theorem 25 implies that there are at least $q^{1/9}$ such primes in contrast to any power of $\log q$ implied by Theorem 24. Due to better bounds for $L(1,\chi)$ for the cubic character compared to the quadratic characters, one expects that the analytic method used in the proof of Theorem 24 would give better results for counting the cubic residues, however when applied to counting cubic residues, this gives only a weaker lower bound than that of Theorem 25 (a) which is

$$q^{c \log\log\log q/\log\log q}$$

for some absolute constant $c > 0$.

If $q \equiv 1 \bmod 8$, then -1 is a biquadratic residue modulo q. So a prime p and p^* are either both biquadratic residues or both biquadratic nonresidues modulo q. So in the case when $q \equiv 1 \bmod 8$, Theorem 25 (b) implies a power-of-q lower bound on the number of prime biquadratic residues $p < q^{1/2+\epsilon}$. In comparison, Theorem 23 only guarantees a single prime biquadratic residue below the significantly larger value $q^{3/4+\epsilon}$. (However, the bound of Theorem 23 applies also when $q \equiv 5 \bmod 8$.)

The proof of Theorem 25 is character-free, based on the reciprocity laws. The main ingredients of the proof are the quadratic reciprocity law, the law of cubic reciprocity given in Proposition 3, and the law of biquadratic reciprocity given in Proposition 4.

Proof of Theorem 25 (a). Let q be a large prime with $q \equiv 1 \bmod 3$. Then we can find integers $L > 0$ and $M > 0$ such that $4q = L^2 + 27M^2$. Define the polynomial $f_0(x)$ with integer coefficients as follows.

$$f_0(x) := L(x^2 - 1) + M(x^3 - 9x).$$

We check for the possible fixed prime divisors of $f_0(x)$, as eventually we would like to use Proposition 10. We first note that $f_0(1) = -8M$, and that $f_0(0) = -L$ so $f_0(x)$ has at least one root modulo 2, and it has two roots modulo 2 if L is even. Now, note that $3 \nmid f_0(0) = -L$, since if $3 \mid L$ then $3^2 \mid L^2 + 27M^2 = 4q$ which is not possible. So $f_0(x)$ has at most two roots modulo 3. Further, we note that since $\gcd(L, M)^2 \mid L^2 + 27M^2 = 4q$, we must have that

$$\gcd(L, M) = 1 \text{ or } 2. \tag{2.2}$$

Expanding the terms in $f_0(x)$ we see that the leading coefficient is M and the constant term is $-L$. So for any prime $p > 3$, $f_0(x)$ cannot reduce to the zero polynomial, so $f_0(x)$ has at most three roots modulo p, in this case. Thus, we see that the only possible fixed prime divisor of $f_0(x)$ is 2.

In order to exclude the possibility of 2 being a fixed prime divisor of f_0, we try to get rid of possible factors of 2 and define a new polynomial $f(x)$ as follows. Since $\gcd(L, M) = 1$ or 2, we have that $2^5 \nmid \gcd(L, 8M)$ so we choose $n_0 \in \{0, 1\}$ with $2^5 \nmid f_0(n_0)$. Let e be the largest integer for which $2^e \mid f_0(n_0)$, so that $e \in \{0, 1, 2, 3, 4\}$. We put

$$f(x) = \frac{1}{2^e} f_0(2^5 x + n_0).$$

By the setup above, $f(x)$ has integer coefficients and $f(x)$ takes only odd values on integers. Moreover, for any prime $p > 3$, as in the case of f_0, f has at most three roots, and f has at most two roots modulo 3 because 2^5 has an inverse modulo p for $p \geq 3$.

Thus by Proposition 10, there is an absolute constant $\eta > 0$ such that if q is sufficiently large in terms of ϵ, then we have that

$$\#\{n \leq q^{\epsilon/4} : n \in \mathbb{N}, f(n) \text{ has no prime divisor less than } q^{\eta\epsilon/4}\} \gg_\epsilon q^{\epsilon/4}/(\log q)^3.$$

In fact, by the sieve of Diamond–Halberstam–Richert, we can take $\eta = 1/7$ recalling the value of β_3 given in (1.2). If we put

$$\mathscr{E} = \{n \le q^{\epsilon/4} : n \in \mathbb{N},\ f(n) \text{ has no prime divisor less than } q^{\epsilon/28}\},$$

and let

$$\mathscr{P} = \{\text{primes } p : p \mid f(n) \text{ for some } n \in \mathscr{E}\},$$

then

$$\#\mathscr{E} \gg_\epsilon q^{\epsilon/4}/(\log q)^3 \qquad \text{and} \qquad \min \mathscr{P} \ge q^{\epsilon/28}.$$

Note that if $n \in \mathbb{N}$, then we have $f(n) = f_0(2^5 n + n_0) = L((2^5 n + n_0)^2 - 1) + M((2^5 n + n_0)^3 - 9(2^5 n + n_0)) \ge L(2^{10} - 1) + M(2^{10} - 9) > 1$. So we can bound $\#\mathscr{E}$ as follows.

$$\#\mathscr{E} \le \sum_{n \in \mathscr{E}} \sum_{\substack{p \mid f(n) \\ p \text{ prime}}} 1.$$

Changing the order of summation, we obtain

$$\sum_{p \in \mathscr{P}} \sum_{\substack{n \le q^{\epsilon/4} \\ p \mid f(n)}} 1 \ge \#\mathscr{E},$$

so by the lower bound on $\#\mathscr{E}$, for large enough primes $q \equiv 1 \bmod 3$, we have

$$\sum_{p \in \mathscr{P}} \sum_{\substack{n \le q^{\epsilon/4} \\ p \mid f(n)}} 1 \gg_\epsilon q^{\epsilon/4}/(\log q)^3. \tag{2.3}$$

Using the fact that for each $p \in \mathscr{P}$, the number of $n \le q^{\epsilon/4}$ for which $p \mid f(n)$ is at most

$3q^{\epsilon/4}/p + O(1)$, we obtain that

$$\sum_{p\in\mathscr{P}} \sum_{\substack{n\le q^{\epsilon/4}\\ p\mid f(n)}} 1 \le 3q^{\epsilon/4} \sum_{p\in\mathscr{P}} \frac{1}{p} + O(\#\mathscr{P})$$

$$\le 3q^{\epsilon/4}\cdot q^{-\epsilon/28}\#\mathscr{P} + O(\#\mathscr{P}).$$

Thus we must have that

$$\#\mathscr{P} > q^{\epsilon/29}$$

since otherwise it contradicts with (2.3) for large q.

We also note that if we put $\mathscr{P}' := \{p \in \mathscr{P} : p \nmid 6LM\}$, then $\#(\mathscr{P} \setminus \mathscr{P}') = O(\log q)$ so $\#\mathscr{P}' > q^{\epsilon/30}$ for large q. Now, let $p \in \mathscr{P}'$. Then $p \mid f(n)$ for some $n \le q^{\epsilon/4}$, so that if we set $m = 2^5 n + n_0$, then $p \mid f_0(m)$. Hence,

$$p \mid L((-m)^2 - 1) - M((-m)^3 - 9(-m)).$$

So by Proposition 3, p is a cubic residue modulo q. Moreover, since $p \mid f_0(m)$ for some $1 \le m \le 2^5 q^{\epsilon/4} + 1$ we have that

$$p \le |f_0(m)| \le \max\{|L|, |M|\}(|m^3 - 9m| + |m^2 - 1|) \ll q^{\frac{1}{2}} m^3.$$

Thus $p \le q^{\frac{1}{2}+\epsilon}$ which finishes the proof. □

Proof of Theorem 25(b). The proof is similar to that of Theorem 25(a). Let $q \equiv 1 \bmod 4$ be a prime. We let L, M be positive integers with $L^2 + 4M^2 = q$, and we define the polynomial $g_0(x)$ with integer coefficients as follows.

$$g_0(x) := M(x^4 - 6x^2 + 1) + 2L(x^3 - x).$$

If $2 \mid M$, then $p = 2$ is a fixed prime divisor of g_0. Noting that $n^3 - n$ is always a multiple of 3, we see that when $3 \mid M$ the prime $p = 3$ is also a fixed divisor of g_0. Now suppose that $p \geq 5$. Since $\gcd(L, M)^2 \mid L^2 + 4M^2 = q$ should hold, we see that $\gcd(L, M) = 1$. The constant term of g_0 is M while the the coefficient of x^3 is $2L$; since $p \geq 5$ and $\gcd(L, M) = 1$, at least one of M and $2L$ is not a multiple of p. Hence, g_0 does not reduce to the zero polynomial modulo p, and so g_0 has at most four roots modulo p.

In order to deal with the possibility of having a fixed prime divisor, as before we try to define a related polynomial. Let 2^e be the highest power of 2 dividing $g_0(0) = M$ and let $3^{e'}$ be the highest power of 3 dividing M.

Let us consider the following cases. If $e \geq 3$, then L should be odd, and $2^2 \mid g_0(2) = -7M + 12L$ but $2^3 \nmid -7M + 12L$. Similarly, if $e' \geq 2$, then $3 \mid g_0(2)$ but $3^2 \nmid g_0(2)$. Keeping these in mind we let

$$m = \begin{cases} 0 & \text{if } 2^3 \nmid M, \\ 2 & \text{if } 2^3 \mid M, \end{cases} \quad \text{and} \quad m' = \begin{cases} 0 & \text{if } 3^2 \nmid M, \\ 2 & \text{if } 3^2 \mid M. \end{cases}$$

Let n_0 be a positive integer solution to the simultaneous congruences

$$n_0 \equiv m \bmod 2^3, \quad n_0 \equiv m' \bmod 3^2$$

with $n_0 \leq 2^3 \cdot 3^2$. Let 2^v be the highest power of 2 dividing $g_0(n_0)$ and let $3^{v'}$ be the highest power of 3 dividing $g_0(n_0)$. Then we have $v \in \{0, 1, 2\}$ and $v' \in \{0, 1\}$. Put

$$g(x) = \frac{1}{2^v 3^{v'}} g_0(2^3 3^2 x + n_0).$$

Then $g(x)$ has integer coefficients by the choice of n_0, v, v' and all the values of g at integers are coprime to 6. So g has no roots modulo 2 and modulo 3. Since $2^3 3^2$ is invertible modulo

every prime $p \geq 5$, our earlier discussion of g_0 implies that g has at most four roots modulo all these p.

We apply Proposition 10 to the polynomial g to get that

$$\#\mathscr{E} := \#\{n \leq q^{\epsilon/5} : n \in \mathbb{N},\, g(n) \text{ has no prime divisor less than } q^{\epsilon/45.5}\} \gg_\epsilon q^{\epsilon/5}/(\log q)^4.$$

Here, we use the value of β_4 noted in the table (1.2), and also note that $5 \cdot 9.1 < 46$. Similarly, as in the proof of part (a) of Theorem 25, we have

$$q^{\epsilon/5}/(\log q)^4 \ll_\epsilon \#\mathscr{E} \leq \sum_{n \in \mathscr{E}} \sum_{\substack{p \mid g(n) \\ p \text{ prime}}} 1 = \sum_{p \in \mathscr{P}} \sum_{\substack{n \leq q^{\epsilon/5} \\ p \mid g(n)}} 1.$$

Now, using the fact that for each $p \in \mathscr{P}$, the number of $n \leq q^{\epsilon/5}$ for which $p \mid g(n)$ is at most $4q^{\epsilon/5}/p + O(1)$, we obtain that

$$\begin{aligned} \sum_{p \in \mathscr{P}} \sum_{\substack{n \leq q^{\epsilon/5} \\ p \mid g(n)}} 1 &\leq 4q^{\epsilon/5} \sum_{p \in \mathscr{P}} \frac{1}{p} + O(\#\mathscr{P}) \\ &\leq 4q^{\epsilon/5} \cdot q^{-\epsilon/45.5} \#\mathscr{P} + O(\#\mathscr{P}). \end{aligned}$$

Thus, we must have that the number of primes p dividing $g(n)$ for some $n \leq q^{\epsilon/5}$ is at least $q^{\epsilon/46}$ for all large q.

Now, as before, put $\mathscr{P}' := \{p \in \mathscr{P} : p \nmid 2LM\}$, then $\#(\mathscr{P} \setminus \mathscr{P}') = O(\log q)$, so $\#\mathscr{P}' > q^{\epsilon/50}$ for large q. Now, let $p \in \mathscr{P}'$. Then $p \mid g(n)$ for some $n \leq q^{\epsilon/5}$, so that if we set $m = 2^3 3^2 n + n_0$, then $p \mid g_0(m)$. Hence,

$$p \mid M(m^4 - 6m^2 + 1) + 2L(m^3 - m).$$

So by Proposition 4, p^* is a biquadratic residue modulo q. Moreover, since $p \mid g_0(m)$ for

some $1 \le m \le 2^3 3^2 q^{\epsilon/5} + 2^2 3^2$ we have that

$$p \le |g_0(m)| \le \max\{|L|, |M|\}(|m^3 - m| + |m^4 + 6m^2 + 1|) \ll q^{\frac{1}{2}} m^4.$$

Thus $p < q^{\frac{1}{2}+\epsilon}$ which finishes the proof. □

Proof of Theorem 25(c). Let q be an odd prime. First assume that $q \equiv 1 \bmod 4$. Let $r = \lfloor \sqrt{q} \rfloor$ and let $f(x) = (x+r)^2 - q$. Then f has no fixed prime divisors, and f has at most two roots modulo every prime p. By Proposition 10 applied to $f(x)$ (where the value of β_2 is used from (1.2), and by the fact that $0.95/4.27 > 2/9$), we obtain that

$$\mathscr{E} = \{n \le q^{0.95\epsilon} : n \in \mathbb{N},\ f(n) \text{ has no prime divisors less than } q^{2\epsilon/9}\} \gg_\epsilon q^{0.95\epsilon}/(\log q)^2.$$

Let

$$\mathscr{P} = \{\text{primes } p : p \mid f(n) \text{ for some } n \in \mathscr{E}\}.$$

Then noting that for each $p \in \mathscr{P}$ the number of $n \le q^{0.95\epsilon}$ for which $p \mid f(n)$ is at most $2q^{0.95\epsilon}/p + O(1)$, by a similar argument as before, we obtain that

$$\#\{\text{odd primes } p : p \mid f(n) \text{ for some } n \le q^{0.95\epsilon}\} > q^{2\epsilon/9}$$

for sufficiently large q. For $n \le q^{0.95\epsilon}$, the integer $f(n) = (n+r)^2 - q$ is positive and smaller than $q^{1/2+\epsilon}$; thus, each prime $p \in \mathscr{P}$ is smaller than $q^{1/2+\epsilon}$. Moreover if $p \in \mathscr{P}$ then $p \mid (n+r)^2 - q$, thus q is a square modulo p. Since $q \equiv 1 \bmod 4$, by the quadratic reciprocity law p is a square modulo q. This completes the proof for the case when $q \equiv 1 \bmod 4$, producing more primes than stated in the theorem in this specific case.

Now, suppose that $q \equiv 3 \bmod 4$. Consider the reduced positive definite ($a > 0$) binary quadratic forms $ax^2 + bxy + cy^2$ of discriminant $q^* = -q$. Note that since $-q = b^2 - 4ac$, we

have $\gcd(a,b,c)=1$ so, such forms are primitive.

Let $h = h(-q)$ be the corresponding class number, the number of reduced binary quadratic forms of discriminant $-q$. Here by a reduced binary quadratic form $ax^2+bxy+cy^2$, we mean the quadratic form which satisfies the following: $-|a| < b < |a| < c$ or $0 \le b \le |a| = c$. Since $-q = b^2 - 4ac$, we have $b^2 \equiv -q \bmod a$. Here, we have $(a,q)=1$ and $|b| \le |a|$, so the number of possible b is at most twice the number of solutions to $b^2 \equiv -q \bmod a$, which is at most $2^{\omega(a)+2}$. Thus we have at most $O(d(a))$ options for b for a given a where $d(a)$ denotes the number of divisors of a. Once a and b are determined, c is determined by the determinant equation. So, if we assume that for all of the forms counted by $h(-q)$, $a \ll h/\log(2h)$ then we would have

$$h \ll \sum_{m \le \frac{h}{\log 2h}} d(m) \ll \frac{h}{\log 2h} \log\left(\frac{2h}{\log 2h}\right);$$

which is eventually incorrect. Thus at least one of the h forms has $a \gg h/\log(2h)$. By Siegel's theorem, we have $h > q^{1/2-\epsilon/3}$ for all large q. Hence, one of the binary quadratic forms described above has $a > q^{1/2-\epsilon/2}$. Since $|b| \le a \le c$, we have

$$ac = \frac{b^2+q}{4} \le \frac{ac+q}{4}$$

so that

$$ac \le \frac{q}{3}.$$

Thus,

$$c \le \frac{q}{3a} < q^{1/2+\epsilon/2}.$$

Let $f_0(x) = ax^2+bx+c$ be one of those forms. Since $\gcd(a,b,c)=1$, f_0 does not reduce to the zero polynomial modulo any prime p, and so f_0 has at most two roots modulo any

prime p. In particular, the only possible fixed prime divisor is $p = 2$. We try to exclude this possibility. We note that $f_0(0) = c$, $a + b + c = f_0(1)$, $4a + 2b + c = f_0(2)$. So if $2^2 \mid f_0(1)$ and $2^2 \mid f_0(0)$ then b should be even, so a should be odd by the primitivity of $f_0(x)$. Let $n_0 \in \{0, 1, 2\}$ for which $2^2 \nmid f_0(n_0)$ and let 2^e be the highest power of 2 for which $2^e \mid f_0(n_0)$, so e is 0 or 1. We define $f(x)$ by

$$f(x) = \frac{1}{2^e} f_0(2^2 x + n_0).$$

Then $f(x)$ has integer coefficients, all the values of f at integers are odd, and f has at most two roots modulo every prime p. Applying Propositon 10 again for $f(x)$, using the value of β_2 from (1.2) we obtain that

$$\#\{n \le q^{\epsilon/5} : n \in \mathbb{N},\ f(n) \text{ has no prime divisors less than } q^{\epsilon/25}\} \gg_\epsilon q^{\epsilon/5}/(\log q)^2.$$

Using the similar type of estimates as before, we have the following bound:

$$\#\mathscr{P} = \#\{\text{odd primes } p : p \mid f(n) \text{ for some } n \le q^{\epsilon/5}\} > q^{\epsilon/25}.$$

Let $p \in \mathscr{P}$, then $p \mid f(n)$ for some $n \le q^{\epsilon/5}$. Put $m = 2^2 n + n_0$. then $m \le q^{0.21\epsilon}$ for large q and $p \mid f_0(m)$. So

$$p \le |f_0(m)| \le am^2 + |b|m + c \le c(m^2 + m + 1) \le q^{1/2+0.5\epsilon} \cdot q^{0.43\epsilon} < q^{1/2+\epsilon}.$$

Moreover, since the discriminant of f_0 is q^*, q^* is a square modulo p. By the quadratic reciprocity law, p is a square modulo q. This completes the proof. □

Remark 3. The parts (a) and (b) of Theorem 25 are effective in the technical sense; given $\epsilon > 0$, there is no theoretical obstacle to compute the value of $q_0(\epsilon)$ or $q_1(\epsilon)$. The same is true

for part (c) in the case when $q \equiv 1 \bmod 4$; however, when $q \equiv 3 \bmod 4$, the use of Siegel's theorem means that we have no way of estimating the required lower bound on q. It seems interesting to note that for the simpler problem of counting prime quadratic residues smaller than q (the specific case $\epsilon = 1/2$ of Theorem 25 (c)), the effectivity is easily restored. One simply applies our sieve argument to $f_0(x) = x^2 + x + \frac{1-q^*}{4}$. In this way, one can show that for all primes q larger than an effectively computable absolute constant, there are more than $q^{1/9}$ prime quadratic residues $p < q$. Here 9 could be replaced with any number larger than $2 \cdot 4.27$. (In addition to being effective, the exponent $1/9$ is better — i.e., larger — than the one that comes directly out of the proof of Theorem 25 (c).)

2.3 Characters approach-Proof of Theorem 26

Let $k \geq 2$ be an integer and q be a prime number with $q \equiv 1 \bmod k$. Let χ be a nonprincipal Dirichlet character modulo q of order k. We note that since q is prime, a nonprincipal Dirichlet character χ modulo q is necessarily primitive. We consider the Dirichlet convolution

$$r_\chi(n) := (\mathbf{1} * \chi * \chi^2 * \cdots * \chi^{k-1})(n) = \sum_{d_0 d_1 \cdots d_{k-1} = n} \chi(d_1)\chi^2(d_2) \cdots \chi^{k-1}(d_{k-1}). \tag{2.4}$$

Note that $r_\chi(n) \geq 0$ for $n \geq 1$ as the numbers $r_\chi(n)$ are the Dirichlet coefficients of $\zeta_K(s)$ where the number field K is the unique degree k cyclic extension of $\mathbb{Q}$ of conductor q. Thus, $r_\chi(n)$ counts the number of (integral) ideals of K with norm n (see Chapter 3 in [48]).

Next, we recall the lower bound for the absolute value of $L(1, \chi)$ which was given in Theorem 19. Although for non-real characters χ, Landau's lower bound is better (in [28] he showed that for a complex character χ modulo q, one has $|L(1, \chi)| \gg (\log q)^{-1}$), we will use Siegel's lower bound ($|L(1, \chi)| \gg_\eta q^{-\eta}$, $\eta > 0$) in order to cover the case when the character is real.

Our next lemma is a result of Pollack, a consequence of Lemma 6 and Lemma 7 in [40]. Here, we state the result using a slightly flexible condition on y which follows from the proof of Lemma 6 and Lemma 7 in [40]. One of the main ingredients of the proof of Lemmas 6 and 7 is the following consequence of Heath-Brown's [24, Lemma 2.4] character sum estimate for primitive characters. Note that there is no restriction here that the modulus is prime.

Proposition 31 (Lemma 3, [40])**.** Let $m > 1$, $k \geq 2$ be integers, and let χ be a primitive character modulo m of order dividing k. Suppose that $0 < \epsilon \leq \frac{1}{3}$. Then for $N \geq m^{\frac{1}{4}+\epsilon}$ we have

$$\sum_{n \leq N} \chi(n) \ll_{\epsilon,k} N^{1-\epsilon^2}.$$

We include the proof of the following lemma, which is essentially the same as one of Pollack's proof in [40], for completeness.

Lemma 32. Let $k \geq 2$ be an integer and q be a large prime such that $q \equiv 1 \bmod k$. Let χ be a character modulo q of order k and let $0 < \delta < \frac{k-1}{3}$. If $q^{\frac{k-1}{4}+\frac{\delta}{2}} \leq y \leq q^{\frac{k-1}{4}+\delta}$ then

$$\sum_{n \leq y} r_\chi(n) = yL(1,\chi)L(1,\chi^2)\cdots L(1,\chi^{k-1}) + O_{\delta,k}\left(y\, q^{-\frac{\delta^2}{(k-1)^2 256}}\right).$$

Proof. Let $0 < \delta < \frac{k-1}{3}$ be given. Assume that $q^{\frac{k-1}{4}+\frac{\delta}{2}} \leq y \leq q^{\frac{k-1}{4}+\delta}$. We start by rewriting the sum $\sum_{n \leq y} r_\chi(n)$ as follows:

$$\begin{aligned}
\sum_{n \leq y} r_\chi(n) &= \sum_{d_0 d_1 \ldots d_{k-1} \leq y} \chi(d_1)\chi^2(d_2)\ldots\chi^{k-1}(d_{k-1}) \\
&= \sum_{d_1 \ldots d_{k-1} \leq y} \chi(d_1)\chi^2(d_2)\ldots\chi^{k-1}(d_{k-1}) \sum_{d_0 \leq \frac{y}{d_1 \ldots d_{k-1}}} 1 \\
&= \sum_{d_1 \ldots d_{k-1} \leq y} \chi(d_1)\chi^2(d_2)\ldots\chi^{k-1}(d_{k-1}) \left\lfloor \frac{y}{d_1 \ldots d_{k-1}} \right\rfloor.
\end{aligned}$$

Since $\left\lfloor \frac{y}{d_1 \dots d_{k-1}} \right\rfloor = \frac{y}{d_1 \dots d_{k-1}} - \left\{ \frac{y}{d_1 \dots d_{k-1}} \right\}$, we have

$$\begin{aligned}\sum_{n \le y} r_\chi(n) =& y \sum_{d_1 \dots d_{k-1} \le y} \frac{\chi(d_1)\chi^2(d_2)\dots\chi^{k-1}(d_{k-1})}{d_1 \dots d_{k-1}} \\ & - \sum_{d_1 \dots d_{k-1} \le y} \chi(d_1)\chi^2(d_2)\dots\chi^{k-1}(d_{k-1}) \left\{ \frac{y}{d_1 \dots d_{k-1}} \right\} \\ =& yS_1 - S_2, \quad \text{say.}\end{aligned}$$

We first deal with S_1. First put $y_0 := y^{\frac{1}{k-1}}$. We partition the sum in S_1 according to the sizes of d_i. For each $(k-1)$-tuple $(d_1, d_2, \dots, d_{k-1})$ with $d_1 d_2 \dots d_{k-1} \le y$, let $\mathscr{S}_{(d_1,d_2,\dots,d_{k-1})} = \{1 \le i \le k-1 : d_i > y_0\}$. For each subset $\mathscr{S} \subset \{1, 2, \dots, k-1\}$, let $\mathscr{I}(\mathscr{S}) = \{(d_1, d_2, \dots, d_{k-1}) : \mathscr{S}_{(d_1,d_2,\dots,d_{k-1})} = \mathscr{S}\}$. Then

$$S_1 = \sum_{d_1 \dots d_{k-1} \le y} \frac{\chi(d_1)\chi^2(d_2)\dots\chi^{k-1}(d_{k-1})}{d_1 \dots d_{k-1}} = \sum_{\mathscr{S}} \sum_{(d_1,d_2,\dots,d_{k-1}) \in \mathscr{I}(\mathscr{S})} \frac{\chi(d_1)\chi^2(d_2)\dots\chi^{k-1}(d_{k-1})}{d_1 \dots d_{k-1}}. \tag{2.5}$$

When $\mathscr{S} = \emptyset$, we have

$$\sum_{(d_1,d_2,\dots,d_{k-1}) \in \mathscr{I}(\emptyset)} \frac{\chi(d_1)\chi^2(d_2)\dots\chi^{k-1}(d_{k-1})}{d_1 \dots d_{k-1}} = \prod_{i=1}^{k-1} \sum_{d_i \le y_0} \frac{\chi^i(d_i)}{d_i}. \tag{2.6}$$

For each $1 \le i \le k-1$, put $S_i(t) := \sum_{n \le t} \chi^i(n)$. Recall that we have $q^{\frac{k-1}{4}+\frac{\delta}{2}} \le y$. By Proposition 31 and the definition of y_0, we have that $S_i(t) \ll_{\delta,k} t^{1-\frac{\delta^2}{4(k-1)^2}}$ for $t \ge y_0$. Thus,

$$\begin{aligned}L(1,\chi^i) - \sum_{d_i \le y_0} \frac{\chi^i(d_i)}{d_i} &= -\frac{S_i(y_0)}{y_0} + \int_{y_0}^{\infty} \frac{S_i(t)}{t^2}\, dt \\ &\ll_{\delta,k} y_0^{-\frac{\delta^2}{4(k-1)^2}} \le q^{-\frac{\delta^2}{4(k-1)^2}\left(\frac{1}{4}+\frac{\delta}{k-1}\right)}.\end{aligned}$$

So using Siegel's Theorem (Theorem 19) as $L(1,\chi) \gg_\delta q^{-\frac{\delta^3}{(k-1)^3 4}}$, we obtain

$$\begin{aligned}\sum_{d_i \le y_0} \frac{\chi^i(d_i)}{d_i} =& L(1,\chi^i)\left(1 + O_{\delta,k}\left(q^{\frac{\delta^3}{(k-1)^3 4}} q^{-\frac{\delta^2}{4(k-1)^2}\left(\frac{1}{4}+\frac{\delta}{k-1}\right)}\right)\right) \\ =& L(1,\chi^i)\left(1 + O_{\delta,k}\left(q^{-\frac{\delta^2}{16(k-1)^2}}\right)\right).\end{aligned}$$

Thus,

$$\begin{aligned}\prod_{i=1}^{k-1} \sum_{d_i \le y_0} \frac{\chi^i(d_i)}{d_i} &= L(1,\chi)L(1,\chi^2)\dots L(1,\chi^{k-1})\left(1 + O_{\delta,k}\left(q^{-\frac{\delta^2}{16(k-1)^2}}\right)\right) \\ &= L(1,\chi)L(1,\chi^2)\dots L(1,\chi^{k-1}) + O_{\delta,k}\left(q^{-\frac{\delta^2}{20(k-1)^2}}\right)\end{aligned}$$

where we use the upper bound $L(1,\psi) \ll \log q$.

Next, we turn to the contribution to S_1 from nonempty $\mathscr{S}$. Fix such a set. Then $i_0 \in \mathscr{S}$ for some $1 \le i_0 \le k-1$. Then by triangle inequality we have

$$\left|\sum_{(d_1,d_2,\dots,d_{k-1})\in\mathscr{I}(\mathscr{S})} \frac{\chi(d_1)\chi^2(d_2)\dots\chi^{k-1}(d_{k-1})}{d_1\dots d_{k-1}}\right| \le \sum_{d_i:\, i\ne i_0} \frac{1}{\prod_{i\ne i_0} d_i}\left|\sum_{y_{i_0}<d_{i_0}\le \frac{y}{\prod_{i\ne i_0} d_i}} \frac{\chi^{i_0}(d_{i_0})}{d_{i_0}}\right|. \tag{2.7}$$

Now, we deal with the innermost sum on the right-hand side of (2.7):

$$\begin{aligned}\sum_{y_{i_0}<d_{i_0}\le \frac{y}{\prod_{i\ne i_0} d_i}} \frac{\chi^{i_0}(d_{i_0})}{d_{i_0}} &= \frac{S_{i_0}\left(\frac{y}{\prod_{i\ne i_0} d_i}\right)}{\frac{y}{\prod_{i\ne i_0} d_i}} - \frac{S_{i_0}(y_{i_0})}{y_{i_0}} + \int_{y_{i_0}}^{\frac{y}{\prod_{i\ne i_0} d_i}} \frac{S_{i_0}(t)}{t^2}\,dt \\ &\ll_{\delta,k} \left(\frac{y}{\prod_{i\ne i_0} d_i}\right)^{-\frac{\delta^2}{4(k-1)^2}} + y_{i_0}^{-\frac{\delta^2}{4(k-1)^2}} \ll y_{i_0}^{-\frac{\delta^2}{4(k-1)^2}}.\end{aligned}$$

Thus using $y_0 \ge q^{\frac{1}{4}+\frac{\delta}{2(k-1)}}$ and $y \le q^{\frac{k-1}{4}+\delta}$, we get

$$\sum_{d_i:\, i\neq i_0} \frac{1}{\prod_{i\neq i_0} d_i} \left| \sum_{y_{i_0} < d_{i_0} \leq \frac{y}{\prod_{i\neq i_0} d_i}} \frac{\chi^{i_0}(d_{i_0})}{d_{i_0}} \right| \ll_{\delta,k} y_{i_0}^{-\frac{\delta^2}{4(k-1)^2}} \sum_{d_i:\, i\neq i_0} \frac{1}{\prod_{i\neq i_0} d_i}$$

$$\leq q^{-\frac{\delta^2}{4(k-1)^2}\left(\frac{1}{4}+\frac{\delta}{2(k-1)}\right)} \left(\sum_{d\leq y} \frac{1}{d}\right)^{k-2}$$

$$\leq q^{-\left(\frac{\delta^2}{(k-1)^2}+\frac{\delta^3}{8(k-1)^3}\right)} (1+\log y)^{k-2} \ll_{\epsilon,k} q^{-\frac{\delta^2}{16(k-1)^2}}.$$

Adding the bounds for $\mathscr{S} = \emptyset$ and for those $\mathscr{S} \neq \emptyset$, we obtain

$$S_1 = L(1,\chi)L(1,\chi^2)\cdots L(1,\chi^{k-1}) + O_{\delta,k}\left(q^{-\frac{\delta^2}{20(k-1)^2}}\right).$$

Now, we estimate S_2. Note that the contribution to S_2 from the tuples $(d_0,\ldots,d_{k-1})$ such that $d_1 d_2 \ldots d_{k-1} \leq y'$ where $y' := \frac{y}{q^{\frac{\delta}{4}}}$ is bounded above by

$$\left| \sum_{d_1\ldots d_{k-1}\leq y'} \chi(d_1)\chi^2(d_2)\ldots\chi^{k-1}(d_{k-1}) \left\{\frac{y}{d_1\ldots d_{k-1}}\right\} \right| \leq \sum_{d_1 d_2\ldots d_{k-1}\leq y'} 1$$

$$\leq y' \left(\sum_{d\leq y'} \frac{1}{d}\right)^{k-2} \leq y' (1+\log y')^{k-2}$$

$$< y q^{\frac{-\delta}{4}} (1+\log q)^{k-2} \ll_{\delta,k} y q^{\frac{-\delta}{5}}.$$

Next, we consider the portion of the sum S_2 where $y' < d_1 d_2 \ldots d_{k-1} \leq y$. Since $y \geq q^{\frac{k-1}{4}+\frac{\delta}{2}}$, we have that $y' = \frac{y}{q^{\frac{\delta}{4}}} \geq q^{\frac{k-1}{4}+\frac{\delta}{4}}$. Thus, if $d_1 d_2 \ldots d_{k-1} > y'$ then for some $1 \leq i \leq k-1$ we have $d_i > q^{\frac{1}{4}+\frac{\delta}{8(k-1)}}$. Moreover, if $d_1 d_2 \ldots d_{k-1} > y'$ then

$$\left\lfloor \frac{y}{d_1\ldots d_{k-1}} \right\rfloor < \frac{y}{y'}.$$

For each tuple $(d_1, \dots, d_{k-1})$ with $y' < d_1 d_2 \dots d_{k-1} \le y$, let $\mathscr{S}_{(d_1,\dots,d_{k-1})} = \{1 \le i \le k-1 : d_i > q^{\frac{1}{4}+\frac{\delta}{8(k-1)}}\}$. Note that by the above argument, $\mathscr{S}_{(d_1,\dots,d_{k-1})}$ is always nonempty. For each nonempty subset $\mathscr{S} \subset \{1, 2, \dots, k-1\}$ and each positive integer $m < \frac{y}{y'}$, let

$$\mathscr{I}(\mathscr{S}, m) := \left\{(d_1, \dots, d_{k-1}) : \mathscr{S}_{(d_1,\dots,d_{k-1})} = \mathscr{S},\ \left\lfloor \frac{y}{d_1 \dots d_{k-1}} \right\rfloor = m \right\}.$$

Then

$$\sum_{d_1 \dots d_{k-1} \le y} \chi(d_1)\chi^2(d_2)\dots\chi^{k-1}(d_{k-1}) \left\{ \frac{y}{d_1 \dots d_{k-1}} \right\}$$
$$= \sum_{\mathscr{S}, m} \sum_{(d_1,\dots,d_{k-1}) \in \mathscr{I}(\mathscr{S},m)} \chi(d_1)\chi^2(d_2)\dots\chi^{k-1}(d_{k-1}) \left\{ \frac{y}{d_1 \dots d_{k-1}} \right\}.$$

Fix a pair $\mathscr{S}$ and m, and fix an $i_0 \in \mathscr{S}$. Suppose that we are given a tuple $\{d_i\}_{i \ne i_0}$ for which $(d_1, \dots, d_{k-1}) \in \mathscr{I}(\mathscr{S}, m)$ for some d_{i_0}. Then the set of d_{i_0} with this property consists exactly of those integers satisfying

$$M < d_{i_0} \le \frac{y}{m \prod}, \quad \text{where} \quad M := \max\left\{ q^{\frac{1}{4}+\frac{\delta}{8(k-1)}},\ \frac{y}{(m+1)\prod},\ \frac{y'}{\prod} \right\} \quad \text{and} \quad \prod := \prod_{i \ne i_0} d_i.$$

Thus,

$$\left| \sum_{(d_1,\dots,d_{k-1}) \in \mathscr{I}(\mathscr{S},m)} \chi(d_1)\chi^2(d_2)\dots\chi^{k-1}(d_{k-1}) \left\{ \frac{y}{d_1 \dots d_{k-1}} \right\} \right|$$
$$\le \sum_{d_i :\, i \ne i_0} \left| \sum_{M < d_{i_0} \le \frac{y}{m\prod}} \chi^{i_0}(d_{i_0}) \left\{ \frac{y}{d_{i_0} \prod} \right\} \right|. \tag{2.8}$$

In the inner sum on the right-hand side of (2.8), $\left\lfloor \frac{y}{d_{i_0}\prod} \right\rfloor$ is constant, so that $\left\{ \frac{y}{d_{i_0}\prod} \right\}$ is a

decreasing function of d_{i_0}; so by Abel's inequality, we see that

$$\left|\sum_{M<d_{i_0}\le \frac{y}{m\prod}} \chi^{i_0}(d_{i_0})\left\{\frac{y}{d_{i_0}\prod}\right\}\right| \le \max_{M<u\le \frac{y}{m\prod}} \left|\sum_{M<d_{i_0}\le u} \chi^{i_0}(d_{i_0})\right|.$$

Since $M \ge q^{\frac{1}{4}+\frac{\delta}{8(k-1)}}$, Proposition 31 gives that the final sum is $\ll_{\delta,k} u^{1-\frac{\delta^2}{64(k-1)^2}}$, and thus the maximum over u is

$$\begin{aligned}\max_{M<u\le \frac{y}{m\prod}} \left|\sum_{M<d_{i_0}\le u} \chi^{i_0}(d_{i_0})\right| &\ll_{\delta,k} \frac{y}{m\prod}\left(\frac{y}{m\prod}\right)^{-\frac{\delta^2}{64(k-1)^2}} \\ &\le \left(\frac{y}{m\prod}\right) M^{-\frac{\delta^2}{64(k-1)^2}} \\ &\le \frac{y}{m\prod} q^{-\frac{\delta^2}{64(k-1)^2}\left(\frac{1}{4}+\frac{\delta}{8(k-1)}\right)}.\end{aligned}$$

Inserting what we have in (2.8), we find that the contribution from the fixed pair $\mathscr{S}$ and m is

$$\begin{aligned}\sum_{(d_1,\dots,d_{k-1})\in\mathscr{I}(\mathscr{S},m)} \chi(d_1)\dots\chi^{k-1}(d_{k-1})\left\{\frac{y}{d_1\dots d_{k-1}}\right\} &\ll_{\delta,k} \frac{y}{m} q^{-\frac{\delta^2}{64(k-1)^2}\left(\frac{1}{4}+\frac{\delta}{8(k-1)}\right)} \sum_{d_i:\, i\neq i_0} \frac{1}{\prod} \\ &\le \frac{y}{m} q^{-\frac{\delta^2}{64(k-1)^2}\left(\frac{1}{4}+\frac{\delta}{8(k-1)}\right)} \left(\sum_{d\le y}\frac{1}{d}\right)^{k-2} \\ &\le \frac{y}{m} q^{-\frac{\delta^2}{64(k-1)^2}\left(\frac{1}{4}+\frac{\delta}{8(k-1)}\right)} (1+\log y)^{k-2}.\end{aligned}$$

Now, summing over all $m \le \frac{y}{y'}$ and over all $O_k(1)$ possibilities for $\mathscr{S}$, we obtain an upper bound for S_2:

$$S_2 \ll_{\delta,k} yq^{-\frac{\delta^2}{64(k-1)^2}\left(\frac{1}{4}+\frac{\delta}{8(k-1)}\right)} (1+\log y)^{k-2} (1+\log y)^{k-2} \ll_{\delta,k} yq^{-\frac{\delta^2}{256(k-1)^2}}.$$

Hence we have

$$\sum_{n\le y} r_\chi(n) = yS_1 - S_2 = yL(1,\chi)L(1,\chi^2)\dots L(1,\chi^{k-1}) + O_{\delta,k}\left(yq^{-\frac{\delta^2}{(k-1)^2 256}}\right).$$

□

We are interested in the sum of $r_\chi(n)$ over positive integers n that do not have 'small' prime divisors. In order to restrict the sum to those n, we apply the sieve. This requires an estimate of the following form.

Proposition 33. Let $k \ge 2$ be an integer and $q \equiv 1 \bmod k$ be a large prime. Let χ be a nonprincipal Dirichlet character modulo q of order k and let $\frac{1}{3} > \epsilon > 0$. Put $x = q^{(k-1)\left(\frac{1}{4}+\epsilon\right)}$. Suppose that e is a squarefree number such that $e \le q^{\frac{(k-1)\epsilon}{2k}}$. Then

$$\sum_{\substack{n\le x\\ e\mid n}} r_\chi(n) = g(e)L(1,\chi)\cdots L(1,\chi^{k-1})x + O_{\epsilon,k}\left(xq^{-\frac{\epsilon^2}{256}}\frac{(2^k-1)^{\omega(e)}}{e}\right)$$

where

$$g(e) = \prod_{p\mid e}\left\{1 - \prod_{j=0}^{k-1}\left(1-\frac{\chi^j(p)}{p}\right)\right\}.$$

Here, as usual, $\omega(n)$ denotes the number of distinct prime divisors of n.

Proof. Let e be a squarefree number such that $e \le q^{\frac{(k-1)\epsilon}{2k}}$. Note that

$$\sum_{\substack{n\le x\\ e\mid n}} r_\chi(n) = \sum_{\substack{d_0d_1\cdots d_{k-1}\le x\\ e\mid d_0d_1\cdots d_{k-1}}} \chi(d_1)\chi^2(d_2)\cdots\chi^{k-1}(d_{k-1}). \tag{2.9}$$

We partition the sum on the right-hand side of (2.9) according to the values of $E_i := (e, d_i)$ noting that then $e \mid d_0d_1\cdots d_{k-1}$ is equivalent to $e \mid E_0E_1\cdots E_{k-1}$. Now, for fixed

$E_0, E_1, \dots, E_{k-1} \mid e$ such that $e \mid E_0E_1\cdots E_{k-1}$ the corresponding contribution to the sum is

$$\sum_{\substack{d_0d_1\cdots d_{k-1}\le x\\ E_i=(e,d_i)\\ \text{for all } i=0,1,2,\dots,k-1}} \chi(d_1)\chi^2(d_2)\cdots\chi^{k-1}(d_{k-1}) = \sum_{\substack{d_0d_1\cdots d_{k-1}\le x\\ E_i\mid d_i,\,(E_i',d_i)=1\\ \text{for all } i=0,1,2,\dots,k-1}} \chi(d_1)\chi^2(d_2)\cdots\chi^{k-1}(d_{k-1})$$

where $E_i' = \frac{e}{E_i}$, for $i = 0, 1, \dots, k-1$. We have

$$\begin{aligned}
&\sum_{\substack{d_0d_1\cdots d_{k-1}\le x\\ E_i\mid d_i,\,(E_i',d_i)=1\\ \text{for all } i=0,1,2,\dots,k-1}} \chi(d_1)\chi^2(d_2)\cdots\chi^{k-1}(d_{k-1})\\
&= \left(\prod_i \chi^i(E_i)\right) \sum_{\substack{d_0d_1\cdots d_{k-1}\le \frac{x}{\prod_i E_i}\\ (E_i',d_i)=1,\,\text{for all } i=0,1,2,\dots,k-1}} \chi(d_1)\chi^2(d_2)\cdots\chi^{k-1}(d_{k-1})\\
&= \left(\prod_i \chi^i(E_i)\right) \sum_{d_0d_1\cdots d_{k-1}\le \frac{x}{\prod_i E_i}} \chi(d_1)\chi^2(d_2)\cdots\chi^{k-1}(d_{k-1}) \prod_i \sum_{\substack{f_i\mid E_i'\\ f_i\mid d_i}} \mu(f_i)\\
&= \left(\prod_i \chi^i(E_i)\right) \sum_{\substack{f_0,f_1,\dots,f_{k-1}\\ f_i\mid E_i' \text{ for all } i=0,\dots,k-1}} \prod_i \mu(f_i) \sum_{\substack{d_0d_1\cdots d_{k-1}\le \frac{x}{\prod_i E_i}\\ f_i\mid d_i}} \chi(d_1)\chi^2(d_2)\cdots\chi^{k-1}(d_{k-1})\\
&= \left(\prod_i \chi^i(E_i)\right) \sum_{\substack{f_0,f_1,\dots,f_{k-1}\\ f_i\mid E_i' \text{ for all } i=0,\dots,k-1}} \prod_i \mu(f_i)\chi^i(f_i) \sum_{d_0d_1\cdots d_{k-1}\le \frac{x}{\prod_i (E_if_i)}} \chi(d_1)\cdots\chi^{k-1}(d_{k-1}).
\end{aligned}$$

By Lemma 32, the innermost sum is

$$= \frac{x}{\prod_i(E_if_i)} \prod_{j=1}^{k-1} L(1,\chi^j) + O\left(\frac{x}{\prod_i(E_if_i)} q^{-\frac{\epsilon^2}{256}}\right)$$

since $e \le \prod_i(E_if_i) \le e^k$ implies that

$$q^{(k-1)\left(\frac{1}{4}+\frac{\epsilon}{2}\right)} \le \frac{x}{\prod_i(E_if_i)} \le q^{(k-1)\left(\frac{1}{4}+\epsilon\right)}.$$

We now sum over all the possible tuples $\{E_0, E_1, \dots, E_{k-1}\}$. There are $(2^k-1)^{\omega(e)}$ such choices. Then the error term becomes

$$\ll_{\epsilon,k} xq^{-\frac{\epsilon^2}{256}} \frac{(2^k-1)^{\omega(e)}}{e}.$$

In order to complete the proof, next we show the following equality:

$$\sum_{\substack{E_0,E_1,\dots,E_{k-1} \\ E_i|e \\ e|E_0E_1\cdots E_{k-1}}} \prod_i \frac{\chi^i(E_i)}{E_i} \prod_i \sum_{f_i|E_i'} \mu(f_i)\frac{\chi^i(f_i)}{f_i} = \prod_{p|e}\left\{1-\prod_{j=0}^{k-1}\left(1-\frac{\chi^j(p)}{p}\right)\right\}. \tag{2.10}$$

To see the identity in (2.10), we note that the left-hand side is a multiplicative function of e, recalling that e is a squarefree number. Thus it is enough to see that the identity holds for primes p. For a prime p, the left hand side of (2.10) is equal to the sum

$$\begin{aligned}
&\sum_{\substack{E_0,E_1,\dots,E_{k-1} \\ E_i|p \\ p|E_0E_1\cdots E_{k-1}}} \prod_i \frac{\chi^i(E_i)}{E_i} \prod_i \sum_{f_i|E_i'} \mu(f_i)\frac{\chi^i(f_i)}{f_i} \\
&\qquad = \sum_{\substack{E_0,E_1,\dots,E_{k-1} \\ E_i=1,p}} \prod_i \frac{\chi^i(E_i)}{E_i} \prod_i \sum_{f_i|E_i'} \mu(f_i)\frac{\chi^i(f_i)}{f_i} \\
&\qquad\quad - \prod_{i=0}^{k-1}\left(1-\frac{\chi^i(p)}{p}\right).
\end{aligned}$$

Thus, it remains to show that

$$\sum_{\substack{E_0,E_1,\dots,E_{k-1} \\ E_i=1,p}} \prod_i \frac{\chi^i(E_i)}{E_i} \prod_i \sum_{f_i|E_i'} \mu(f_i)\frac{\chi^i(f_i)}{f_i} = 1.$$

Put $X_i(n) = \frac{\chi^i(n)}{n}$, and $Y_i(n) = \sum_{d|n} \mu(d)\frac{\chi^i(d)}{d}$. Then we have

$$\begin{aligned}\sum_{\substack{E_0,E_1,\dots,E_{k-1}\\ E_i=1,p}} \prod_i \frac{\chi^i(E_i)}{E_i} \prod_i \sum_{f_i|E_i'} \mu(f_i)\frac{\chi^i(f_i)}{f_i} &= \sum_{\substack{E_0,E_1,\dots,E_{k-1}\\ E_i=1,p}} \prod_i X_i(E_i)Y_i\left(\frac{p}{E_i}\right)\\ &= \prod_{i=0}^{k-1} \sum_{E_i=1,\,p} X_i(E_i)Y_i\left(\frac{p}{E_i}\right)\\ &= \prod_{i=0}^{k-1} \left(X_i(1)Y_i(p) + X_i(p)Y_i(1)\right)\\ &= \prod_{i=0}^{k-1} \left(1\left(1-\frac{\chi^i(p)}{p}\right) + \frac{\chi^i(p)}{p}\right) = 1\end{aligned}$$

which completes the proof.

□

In order to estimate $\sum_{\substack{n\le x\\ (n,P(z))=1}} r_\chi(n)$, we need the fundamental lemma of the sieve in the form it was given in Lemma 7 in the Introduction.

Lemma 34. Let $k \ge 2$ be an integer and let q be a prime with $q \equiv 1 \bmod k$. Suppose that χ is a Dirichlet character modulo q of order k. Let $r_\chi(n)$ be defined as in (2.4). Let $\epsilon > 0$. We let $x = q^{(k-1)\left(\frac{1}{4}+\epsilon\right)}$ and $z \le q^{\frac{(k-1)\epsilon}{2k}}$, we also put $P(z) = \prod_{p<z} p$. Then we have

$$\sum_{\substack{n\le x\\ (n,P(z))=1}} r_\chi(n) \gg_{\epsilon,k} xq^{-\frac{\epsilon^2}{384}}.$$

Proof. We would like to apply Lemma 7 taking Proposition 33 as input. In order to do that, we first note the following estimate. First recall that $g(n)$ is multiplicative and for a squarefree natural number e, we have

$$g(e) = \prod_{p|e} \left\{1 - \prod_{j=0}^{k-1}\left(1-\frac{\chi^j(p)}{p}\right)\right\}.$$

So we have

$$\prod_{p<z}(1-g(p)) = \prod_{p<z}\left(1-\left\{1-\prod_{j=0}^{k-1}\left(1-\frac{\chi^j(p)}{p}\right)\right\}\right)$$
$$= \prod_{p<z}\prod_{j=0}^{k-1}\left(1-\frac{\chi^j(p)}{p}\right) \geq \prod_{p<z}\left(1-\frac{1}{p}\right)^k \gg \frac{1}{(\log z)^k}.$$

So for a large enough constant $K > 1$, we have

$$\prod_{w\leq p<z}(1-g(p))^{-1} \leq K\left(\frac{\log z}{\log w}\right)^k.$$

We now use Lemma 7 with $\kappa = k$ and we choose s large enough so that $e^{9k+1-s}K^{10} < 1$. We obtain that there exists a constant $c = c(\epsilon, k) > 0$ such that the following estimate holds for the sifted sum.

$$\sum_{\substack{n\leq x\\(n,P(z))=1}} r_\chi(n) > c\,xL(1,\chi)\cdots L(1,\chi^{k-1})\prod_{p<z}(1-g(p)) + O_{\epsilon,k}\left(xq^{-\frac{\epsilon^2}{256}}\sum_{\substack{d<z^s\\d|P(z)}}\frac{2^{k\omega(d)}}{d}\right).$$

We also have

$$\sum_{\substack{d<z^s\\d|P(z)}}\frac{2^{k\omega(d)}}{d} \ll \sum_{d|P(z)}\frac{2^{k\omega(d)}}{d} \ll (\log z)^{2^k}.$$

On the other hand, we use Theorem 19, with $|L(1,\psi)| \gg_{k,\epsilon} q^{-\frac{\epsilon^2}{(k-1)512}}$, to obtain

$$\sum_{\substack{n\leq x\\(n,P(z))=1}} r_\chi(n) \gg_{\epsilon,k} xq^{-\frac{\epsilon^2}{384}}$$

for all large q. □

Next we estimate the sifted sum in a different way.

Lemma 35. Let $k \geq 2$ be an integer and let q be a prime with $q \equiv 1 \bmod k$. Suppose that χ is a Dirichlet character modulo q of order k. Let $r_\chi(n)$ be defined as in (2.4). Let $z > 0$, and $x > 0$ be two real numbers such that $z < x$. Assume further that $p_1, p_2, \ldots, p_t$ are the primes such that $z < p_i \leq x$ with $\chi(p_i) = 1$. Then we have

$$\sum_{\substack{n \leq x \\ (n, P(z))=1}} r_\chi(n) \ll x^{\frac{9}{10}} \exp\left(\frac{k\,t}{z^{\frac{9}{10}}}\right).$$

Proof. We start by noting that $r_\chi(q) = 1$. For a squarefree $n \geq 1$, we have $r_\chi(n) = 0$ unless $\chi(p) = 1$ for all $p \mid n$, $p \neq q$. To see this, we first note that $r_\chi(n)$ is multiplicative as the convolution of multiplicative functions is multiplicative. Observe that for a prime $p \neq q$, we have $r_\chi(p) = \sum_{i=0}^{k-1} \chi^i(p)$. Moreover, if $\chi(p) \neq 1$, then $\sum_{i=0}^{k-1} \chi^i(p) = \chi(p) \sum_{i=0}^{k-1} \chi^i(p)$. So $(1 - \chi(p)) \sum_{i=0}^{k-1} \chi^i(p) = 0$ showing that $r_\chi(p) = 0$.

So, we have

$$\begin{aligned}\sum_{\substack{n \leq x \\ (n, P(z))=1}} r_\chi(n) &\leq \sum_{\substack{n_1 n_2 \leq x \\ n_1 \text{ squarefree} \\ n_2 \text{ squarefull} \\ (n_1, n_2)=1 \\ p \mid n_1 \to p = p_i \text{ for some } 1 \leq i \leq t \text{ or } p = q}} r_\chi(n_1 n_2) \\ &\leq \sum_{\substack{n_1 \leq x \\ n_1 \text{ squarefree} \\ p \mid n_1 \to p = p_i \text{ for some } 1 \leq i \leq t \text{ or } p = q}} r_\chi(n_1) \sum_{\substack{n_2 \leq \frac{x}{n_1} \\ n_2 \text{ squarefull} \\ (n_1, n_2)=1}} r_\chi(n_2).\end{aligned}$$

We also note that for any $n \geq 1$, $r_\chi(n) \leq \tau_k(n)$ where $\tau_k(n)$ denotes the k-fold divisor function, that is $\tau_k(n) = \sum_{d_0 d_1 \cdots d_{k-1} = n} 1$. Now, using the crude bound $\tau_k(n) \ll n^{\frac{2}{5}}$, we see

that

$$\begin{aligned} r_\chi(n) &\ll \sum_{\substack{n_1 \le x \\ n_1 \text{ squarefree} \\ p|n_1 \to p=p_i \text{ for some } 1\le i\le t \text{ or } p=q}} r_\chi(n_1)\left(\left(\frac{x}{n_1}\right)^{\frac{1}{2}+\frac{2}{5}}\right) \\ &\ll x^{\frac{9}{10}} \sum_{\substack{n_1 \le x \\ n_1 \text{ squarefree} \\ p|n_1 \to p=p_i \text{ for some } 1\le i\le t \text{ or } p=q}} \frac{r_\chi(n_1)}{n_1^{\frac{9}{10}}} \\ &\ll x^{\frac{9}{10}}\left(1+\frac{1}{q^{\frac{9}{10}}}\right)\prod_{p\in\{p_1,p_2,\ldots,p_t\}}\left(1+\frac{\tau_k(p)}{p^{\frac{9}{10}}}\right) \\ &\ll x^{\frac{9}{10}}\exp\left(\sum_{p\in\{p_1,p_2,\ldots,p_t\}}\frac{k}{p^{\frac{9}{10}}}\right) \ll x^{\frac{9}{10}}\exp\left(\frac{k\,t}{z^{\frac{9}{10}}}\right). \end{aligned}$$

This completes the proof. □

2.4 Proof of Theorem 26

Let $\frac{1}{3} > \epsilon > 0$ be given. As before, let $p_1, p_2, \ldots p_t$ be the primes in the interval $(z, x]$ such that $\chi(p_j) = 1$. Take $x = q^{\frac{k-1}{4}+\epsilon}$. We are looking for an estimate for t. Comparing the lower and the upper bounds obtained in Lemma 34, 35 with $z = q^{\frac{\epsilon}{2k}}$ we have

$$xq^{-\frac{\epsilon^2}{(k-1)^2 384}} \ll x^{\frac{9}{10}}\exp\left(\frac{k\,t}{z^{\frac{9}{10}}}\right).$$

So we obtain the following inequality

$$x^{\frac{1}{10}}q^{-\frac{\epsilon^2}{(k-1)^2 384}} \ll \exp\left(\frac{k\,t}{z^{\frac{9}{10}}}\right),$$

so that we have

$$\log(x^{\frac{1}{10}} q^{-\frac{\epsilon^2}{(k-1)^2 384}}) \leq \frac{k\,t}{z^{\frac{9}{10}}} + O(1)$$

and hence

$$t \gg \frac{z^{\frac{9}{10}} \log(x^{\frac{2}{5}} q^{-\frac{\epsilon^2}{(k-1)^2 384}})}{k} \gg_{\epsilon,k} q^{\frac{9\epsilon}{20k}}.$$

Thus, the number of primes $p \leq x$ with $\chi(p) = 1$ is $\gg_{\epsilon,k} q^{\frac{9\epsilon}{20k}}$. □

Remark 4. In a recent preprint by Dunn, Shparlinski and Zuharescu [16], they improved the bound for the number of small prime quadratic residues (the case when $k = 2$). For example, they show that and for any $\epsilon > 0$ and for all sufficiently large primes q, the number of primes $p \leq q^{\frac{1}{4}+\epsilon}$ such that p is a quadratic residue modulo q is at least $q^{\frac{\epsilon}{3}}$.

Chapter 3

Changes of digits of primes

In this chapter, we prove the quantitative improvement of Erdős' result on the weakly prime numbers. We quote Theorem 27 below.

Theorem (Theorem 27)**.** Let $K \geq 2$ be an integer, $\epsilon > 0$ be a small number. For all sufficiently large positive x, there exist at least $x^{1-\epsilon}$ primes $x < p \leq (1 + K^{-1})x$ such that all of the integers $pj \pm a^h k,\ 2 \leq a \leq K,\ 0 < k \leq K,\ 1 \leq j \leq K,\ 0 \leq h \leq K \log x$, are composite having at least $(\log \log x)^{1-\epsilon}$ distinct prime factors.

The idea Erdős used in the proof of Theorem 11 was to find small prime numbers q and a prime p so that each $p+t10^i$ is divisible by one of the primes q. In order to do that efficiently (using as few small primes as possible), he used Bang-Zsigmondy Theorem (Theorem 12) to choose primes q so that most of the powers 10^i of 10 fall into the same congruence class for some prime q. This made the argument efficient enough to obtain several congruence conditions (whose simultaneous solution exists by the Chinese Remainder Theorem) with a common solution to a small enough modulus so that Linnik's Theorem provides a solution which is a prime number. As in the case of the proof of Theorem 11, Theorem 12 is going to be the key in our argument to prove Theorem 27.

3.1 Proof of Theorem 27

We first state the results which will be used in the proof of Theorem 27. First, we give a technical result as an application of Bang-Zsigmondy Theorem (Theorem 12).

Lemma 36. Let A be a finite set of consecutive positive integers. For each $a \in A$ and each integer $i \geq 2$ for which the pair (a, i) is not an exception to Bang-Zsigmondy Theorem, let $q_{a,i}$ be a prime for which the order of $a \bmod q_{a,i}$ is i. We can choose a family of disjoint sets $\{Q_a\}_{a \in A}$ such that if we write $Q_a = \{q_{a,i_1} < q_{a,i_2} < q_{a,i_3} < ...\}$ then each difference $i_{j+1} - i_j \leq 1 + \#A$.

Proof. We construct the sets Q_a greedily. Proceed through the elements $a \in A$ in order. For each a, add to Q_a the prime $q_{a,i}$, where i is chosen as small as possible subject to the conditions that

(i) $q_{a,i}$ is defined and

(ii) $q_{a,i}$ has not already been included in any of set $Q_{a'}$ $(a' \in A)$.

After having gone through the entire list of a's, we start over and repeat the process. We continue this indefinitely to construct the sets Q_a.

Suppose that the prime added to Q_a at a certain stage is $q_{a,i}$. By the next time we are to add a prime to Q_a, we have used (in the worst case) $\#A$ possible candidates. Since there is at most one index $j \geq 2$ for which $q_{a,j}$ is undefined, the prime we add at this next stage, say $q_{a,i'}$, necessarily satisfies $i' - i \leq \#A + 1$, as desired. □

Now, we are ready to prove Theorem 27.

Proof of Theorem 27. Our proof strategy is as follows: First, note that for an integer m coprime to j, if $p \equiv \frac{-a^h k}{j} \bmod m$ then $pj + a^h k \equiv 0 \bmod m$. In order to find primes p with the desired property, we attempt to find residue classes to many (at least $(\log \log x)^{1-\epsilon}$)

different prime moduli in order for the numbers $\frac{a^h k}{j}$ to be "covered". One way to do this could be assigning congruence conditions to each one of those numbers using different moduli at each step. However, this naive choice is not efficient enough for our purpose: if we apply the Chinese Remainder Theorem after writing down lots of congruence conditions, the modulus to which we can ensure a simultaneous solution would end up being too large to be able to find small enough primes p in our range. Thus, we would like to use the same congruence classes for different $\frac{a^h k}{j}$, whenever there is no obstruction to do so. Here, knowing that we can always find moduli for which a is far from being a primitive root (by Bang-Zsigmondy Theorem) allows us to have an efficient way to decrease the number of moduli we use at the end, and the modulus we find the simultaneous solution for becomes much smaller, allowing us to ensure that we can find prime solutions as small as we need for our purpose.

Let $K \geq 2$ be a given integer and let $\epsilon > 0$ be a fixed small real number. For a given large x, we put $t = \lfloor K \log x \rfloor$. Define the set

$$\mathcal{D}_{K,t} := \{-K, -K+1, \ldots, -1, 1, \ldots, K\} \times \{0, 1, \ldots, t\} \times \{1, 2, \ldots, K\},$$

so that $\#\mathcal{D}_{K,t} = 2K^2(t+1)$.

First, put $r := K\lfloor (\log x)^{\frac{1}{3}} \rfloor$. By Lemma 36, we can construct pairwise disjoint sets $\{\mathcal{Q}_a\}_{a \in \{2,3,\ldots K\}}$ as follows: each $\mathcal{Q}_a = \{q_{a,i_1} < q_{a,i_2} < \ldots\}$ and the indices i_l satisfy $K \leq i_1 < i_2 < \cdots \leq r$, and $i_l - i_{l-1} \leq K$, for all $l > 1$. We enforce $i_1 \geq K$ so that $\mathcal{Q}_a$ has no element $\leq K$, while including only elements indexed by $i_l \leq r$ ensures that the number of elements in $\mathcal{Q}_a$ is at most $r - K + 1$. We put $\mathcal{I}_a := \{i_1, i_2, \ldots : q_{a,i_l} \in \mathcal{Q}_a\}$.

Now, let $n = \lceil (\log\log x)^{1-\epsilon} \rceil$ and let $1 \leq d \leq n$ be an integer. Here, n is the number of times we will repeat our argument and we will divide the process into n pieces associated to the congruence classes modulo n (we use congruence classes as a bookkeeping measure, this division may have been done in a different way without changing the result). We determine

several congruence classes modq_{a,i_l}, for $i_l \in \mathcal{I}_a$ such that $l = d + en$, inductively on e. Fix any congruence class $-u_{a,i_d} \bmod q_{a,i_d}$ and suppose that we have determined the congruences $-u_{a,i_{d+en}} \bmod q_{a,i_{d+en}}$ for each $0 \le e \le c-1$. Let $\mathscr{C}^a_{i_{d+cn}}$ be the set of numbers of the form $\frac{a^h k}{j}$, $(k,h,j) \in \mathcal{D}_{K,t}$ which are not congruent to any of $-u_{a,i_{d+en}} \bmod q_{a,i_{d+en}}$ for any $0 \le e \le c-1$. (Here $\frac{a^h k}{j} \equiv -u$ is equivalent to saying that $a^h k \equiv -ju$.) Now, since the powers of a take exactly i_{d+cn} distinct values mod$q_{a,i_{d+cn}}$, numbers of the form $\frac{a^h k}{j}$ can occupy at most $2K^2\, i_{d+cn}$ residue classes mod$q_{a,i_{d+cn}}$. So by the Pigeonhole Principle, there exists $-u_{i_{d+cn}}$ for which the congruence class $-u_{a,i_{d+cn}} \bmod q_{a,i_{d+cn}}$ is occupied by at least $\left\lceil \frac{\#\mathscr{C}^a_{i_{d+cn}}}{2K^2 i_{d+cn}} \right\rceil$ elements of $\mathscr{C}^a_{i_{d+cn}}$.

We use the bounds for $\mathscr{C}^a_{i_l}$ for various $l \equiv d \bmod n$ iteratively to obtain that for given integers a and d, $1 \le d \le n,\ 2 \le a \le K$, the number $R_{d,a}$ of triples $(k,h,j) \in \mathcal{D}_{K,t}$ for which $\frac{ka^h}{j}$ is not $\equiv -u_{a,i_l} \bmod q_{a,i_l}$ for any $K \le i_l \le r,\ l \equiv d \bmod n$ is

$$\le 2K^2(t+1) \prod_{\substack{i_l \in \mathcal{I}_a \\ l \equiv d \bmod n}} \left(1 - \frac{1}{2K^2\, i_l}\right). \tag{3.1}$$

In order to assign congruence classes for the remainders from each step of this process, we now list the numbers labeled by the triples counted by $\sum_{d=1}^{n} R_{d,a}$, meaning that the remaining elements of the form $\frac{ka^h}{j}$ not covered by the chosen residues classes for each $1 \le d \le n$. We introduce the notation given by the list: $\{v_{a,d,f} : 1 \le f \le R_{d,a},\ 2 \le a \le K,\ 1 \le d \le n\}$. For each element in this list we assign a prime number among the first $\sum_{a=2}^{K} \sum_{d=1}^{n} R_{d,a} + rK$ primes which are not in $\cup_{a=2}^{K} \mathcal{Q}_a$, denoted by the elements of the following list: $\{Q_{a,d,f} : 1 \le f \le R_{d,a},\ 2 \le a \le K,\ 1 \le d \le n\}$. Note that the number of primes in $\cup_{a=2}^{K} \mathcal{Q}_a$ is at most $(K-1)(r-K+1) \le rK$.

Using the construction above, we consider the following system of congruences:

$$\begin{aligned} &p \equiv u_{a,i_l} \bmod q_{a,i_l},\ i_l \in \mathcal{I}_a,\ 2 \le a \le K, \\ &p \equiv -v_{a,d,f} \bmod Q_{a,d,f},\ 1 \le f \le R_{d,a},\ 2 \le a \le K,\ 1 \le d \le n. \end{aligned} \tag{3.2}$$

By the Chinese Remainder Theorem, the solution to the system of congruences (3.2) is unique modulo $\prod q_{a,i_l} \prod Q_{a,d,f}$. If a prime p is a solution to (3.2), then for all triples $(k,h,j) \in \mathcal{D}_{K,t}$, each $pj + a^h k$ is $\equiv 0$ modulo at least n distinct primes. Indeed, let $(k,h,j) \in \mathcal{D}_{K,t}$. For every $1 \le d \le n$, in the above construction we determine a congruence class modulo a prime among either $\{q_{a,i_l}\}$ or $\{Q_{a,d,f}\}$ occupied by $\frac{ka^h}{j}$, call this class $-u \bmod q$. Then $p \equiv u \bmod q \equiv -\frac{ka^h}{j} \bmod q$ which is equivalent to the congruence $pj + a^h k \equiv 0 \mod q$. So for each $pj + a^h k$, we have at least n distinct primes q (one for each choice of d) dividing $pj + a^h k$.

Next, we show that the modulus $\prod q_{a,i_l} \prod Q_{a,d,f}$ is not too large. First note that, by the construction of $\mathcal{Q}_a$ for any $a \in \{2,3,\dots K\}$, and $l \ge 1$ such that $q_{a,i_l} \in \mathcal{Q}_a$, we have $K \le i_l$ and $0 < i_{l+1} - i_l \le K$. Moreover, using the construction given in Lemma 36 for the sets $\mathcal{Q}_a$, we have $i_1 \le 2K+2$. So for any $2 \le d \le n$, we have $i_d \le i_1 + dK \le (d+2)K + 2$, and similarly we have $i_{d+en} \le (d+en+2)K + 2$. Note that there will be at least $\left\lfloor \frac{r-(d+4)K}{nK} \right\rfloor$ elements of the form i_{d+en}, since the i_l only go up to r.

Therefore,

$$\begin{aligned} \sum_{\substack{i_l \in \mathcal{I}_a \\ l \equiv d \bmod n}} \frac{1}{i_l} &\ge \sum_{e=0}^{\left\lfloor \frac{r-(d+4)K}{nK} \right\rfloor} \frac{1}{(d+en+2)K+2} \\ &\ge \frac{1}{K} \sum_{e=0}^{\left\lfloor \frac{r-(d+4)K}{nK} \right\rfloor} \frac{1}{d+en+3} \ge \frac{1}{nK} \sum_{e=0}^{\left\lfloor \frac{r-(d+4)K}{nK} \right\rfloor} \frac{1}{e+5}. \end{aligned}$$

Since

$$\frac{r-(d+4)K}{(n+1)K} \geq (\log x)^{\frac{1}{4}}$$

for large x, we have that

$$\sum_{\substack{i_l \in \mathcal{I}_a \\ l \equiv d \bmod n}} \frac{1}{i_l} \geq \frac{1}{nK}\left(\frac{1}{5}\log\log x\right) \gg (\log\log x)^{\frac{\epsilon}{2}}.$$

Thus,

$$\prod_{\substack{i_l \in \mathcal{I}_a \\ l \equiv d \bmod n}} \left(1-\frac{1}{2K^2 i_l}\right) \leq \exp\left\{\frac{-1}{2K^2}(\log\log x)^{\frac{\epsilon}{2}}\right\} \ll \exp\left\{-(\log\log x)^{\frac{\epsilon}{3}}\right\}.$$

Hence, recalling the upper bound in (3.1), we obtain

$$\begin{aligned}\sum_{a=2}^{K}\sum_{d=1}^{n} R_{d,a} &\ll_K K^2 t \sum_{a=2}^{K}\sum_{d=1}^{n} \exp\left\{-(\log\log x)^{\frac{\epsilon}{3}}\right\} \\ &\ll_K n \log x \exp\left\{-(\log\log x)^{\frac{\epsilon}{3}}\right\} \\ &\ll_K \frac{\log x \log\log x}{(\log\log x)^{\epsilon}\exp\{(\log\log x)^{\frac{\epsilon}{3}}\}} \ll_K \frac{\log x}{\exp\{(\log\log x)^{\frac{\epsilon}{4}}\}}.\end{aligned}$$

Since the product of the first ℓ primes is $\exp\{(1+o(1))\ell\log\ell\}$, and since the primes labeled by $Q_{a,d,f}$ lie in the first $\sum_{a=2}^{K}\sum_{d=1}^{n} R_{d,a} + rK$ primes, we have the following upper bound for the product $\prod Q_{a,d,f}$:

$$\prod Q_{a,d,f} \ll_K \exp\left\{C' \frac{\log x \log\log x}{\exp\left\{(\log\log x)^{\frac{\epsilon}{4}}\right\}}\right\} \ll_K x^{\frac{\epsilon}{2}}. \tag{3.3}$$

On the other hand, as for each $q_{a,i_l} \in \mathcal{Q}_a$, we have $q_{a,i_l} \leq a^{i_l}$,

$$\prod_{a=2}^{K} \prod_{i_l \in \mathcal{I}_a} q_{a,i_l} \leq \prod_{a=2}^{K} \prod_{h=1}^{r} a^h \leq (K!)^{\frac{r(r+1)}{2}} \ll_K \exp\{C(\log x)^{\frac{2}{3}}\} \ll_K x^{\frac{\epsilon}{2}}. \tag{3.4}$$

Thus, combining (3.3) and (3.4), we seek for primes in a certain arithmetic progression where the modulus is $\ll x^{\epsilon}$. Finally, we apply Corollary 1 to complete the proof. $\square$

Chapter 4

Number of pure fields of prime degree

Recall that for an odd prime p and a number field K of degree p, K is said to be a *pure field of degree* p if for a p-free positive integer $n > 1$ we can write $K = \mathbb{Q}(\sqrt[p]{n})$. In this chapter, we prove Theorem 30 and deduce Corollary 2 quoted below.

Theorem (Theorem 30)**.** Let $p \geq 5$ be a prime number. For each $\epsilon > 0$, we have that

$$\#\{K : K \text{ pure field of degree } p,\ |f(K)| \leqslant X\} = XQ_p(\log X) + O_p\left(X^{\frac{p+1}{p+3}+\epsilon}\right),$$

as $X \to \infty$, where $Q_p(x)$ is a polynomial of degree $p-2$.

Corollary (Corollary 2)**.** Let $p \geq 5$ be a prime number. For each $\epsilon > 0$, we have that

$$\#\{K : K \text{ pure field of degree } p,\ |d(K)| \leqslant X\} = \sqrt[p-1]{X}\tilde{Q}_p(\log X) + O_p\left(X^{\frac{p+1}{(p-1)(p+3)}+\epsilon}\right),$$

as $X \to \infty$, where $\tilde{Q}_p(x)$ is a polynomial of degree $p-2$.

4.1 Proof of Theorem 30

We first state the formulas for the discriminants and the conductors of the pure fields of odd prime degree. The following result of Berwick (see [7]) which was reformulated by Mayer in [32] will be the key in our calculations. In the proof of Theorem 30 we will also need Perron's formula, as stated in Lemma 16.

Lemma 37 (Theorem 1 in [32])**.** Let K be a pure field of degree p. Write $K = \mathbb{Q}(\sqrt[p]{D})$, where D is p-free. Let R be the squarefree product of the primes dividing D. Then the associated conductor f satisfies the relation

$$f^{p-1} = \begin{cases} p^2 R^{p-1} & \text{if } D^{p-1} \not\equiv 1 \pmod{p^2}, \\ R^{p-1} & \text{if } D^{p-1} \equiv 1 \pmod{p^2}. \end{cases}$$

Consequently, since for the cyclotomic field $k = \mathbb{Q}(\zeta)$ of p-th roots of unity, $d(K) = d_k f^{p-1}$ and $d_k = (-1)^{\frac{p-1}{2}} p^{p-2}$, the discriminant $d(K)$ is given by

$$d(K) = (-1)^{\frac{p-1}{2}} \begin{cases} p^p R^{p-1} & \text{if } D^{p-1} \not\equiv 1 \pmod{p^2}, \\ p^{p-2} R^{p-1} & \text{if } D^{p-1} \equiv 1 \pmod{p^2}. \end{cases}$$

Remark 5. By definition, every pure field of degree p can be written as $\mathbb{Q}(\sqrt[p]{D})$ for some p-free positive integer D. In fact, there are precisely $p-1$ such values of D. Indeed, if D_0 is any one such value of D, then the full set of D consists of the p-free positive integer representatives of the cosets of D_0, D_0^2, $\ldots$, D_0^{p-1} in the group $\mathbb{Q}^\times/(\mathbb{Q}^\times)^p$. Clearly, all of these D define the same field $\mathbb{Q}(\sqrt[p]{D})$. That these are the only positive, p-free D with $\mathbb{Q}(\sqrt[p]{D}) = \mathbb{Q}(\sqrt[p]{D_0})$ follows from Kummer theory.

4.1.1 Obtaining an expression for the series $\sum \frac{1}{f(K)^s}$

Let $p \geqslant 5$ be a prime number and $s \in \mathbb{C}$ with $\Re s > 1$. In this section, we obtain an identity for the sum

$$\sum_{K \text{ pure field of degree } p} \frac{1}{f(K)^s}$$

which is not a standard Dirichlet series, that is it is not in the form

$$\sum_{n=1}^{\infty} \frac{a_n}{n^s}.$$

However, we will still be able to use the methods stated for the functions represented by a Dirichlet series as the series $\sum \frac{1}{f(K)^s}$ can be written in terms of two Dirichlet series.

Proposition 38. We have

$$\begin{aligned}\sum_{\substack{K \text{ pure field} \\ \text{of degree } p}} \frac{1}{f(K)^s} = -1+\frac{1}{p-1}\Bigg\{ & \frac{1}{p(p-1)}\left(1-\frac{1}{p^{\frac{2s}{p-1}}}\right) \sum_{\substack{\chi \pmod{p^2} \\ \chi^{p-1}\neq\chi_0}} G_{p,\chi}(s) \prod_{k=1}^{p-1} \frac{L(s,\chi^{k(p-1)})}{L(2s,\chi^{2k(p-1)})} \\ & +\frac{1}{p}\left(1-\frac{1}{p^{\frac{2s}{p-1}}}\right)\left(1+\frac{p-1}{p^s}\right)^{-1} G_p(s)\left(\frac{\zeta(s)}{\zeta(2s)}\right)^{p-1} \\ & +\frac{1}{p^{\frac{2s}{p-1}}} G_p(s)\left(\frac{\zeta(s)}{\zeta(2s)}\right)^{p-1}\Bigg\} \end{aligned} \tag{4.1}$$

where

$$G_p(s) := \prod_{q \text{ prime}} \left\{ \left(1+\frac{p-1}{q^s}\right)\left(1+\frac{1}{q^s}\right)^{-(p-1)} \right\}$$

and

$$G_{p,\chi}(s) := \prod_q \left[\left(1 + \frac{\sum_{k=1}^{p-1} \chi^{p-1}(q^k)}{q^s} \right) \prod_{k=1}^{p-1} \left(1 + \frac{\chi^{k(p-1)}(q)}{q^s} \right)^{-1} \right].$$

Proof. If $K = \mathbb{Q}(\sqrt[p]{a_1 a_2^2 \dots a_{p-1}^{p-1}})$ is a pure field of degree p where $a_i \in \mathbb{N}$, $1 \leq i \leq p-1$, are squarefree and pairwise relatively prime, then by Lemma 37, we have

$$f(K)^{p-1} = \begin{cases} p^2 (a_1 a_2 \dots a_{p-1})^{p-1} & \text{if} \quad (a_1 a_2^2 \dots a_{p-1}^{p-1})^{p-1} \not\equiv 1 \pmod{p^2}, \\ (a_1 a_2 \dots a_{p-1})^{p-1} & \text{if} \quad (a_1 a_2^2 \dots a_{p-1}^{p-1})^{p-1} \equiv 1 \pmod{p^2}. \end{cases}$$

So by Remark 5, we have

$$\sum_{\substack{K \text{ pure field} \\ \text{of degree } p}} \frac{1}{f(K)^s} = -1 + \frac{1}{p-1} \left[\sum_{\substack{a_1, a_2, \dots, a_{p-1} \text{ pairwise rel. prime} \\ (a_1 a_2^2 \dots a_{p-1}^{p-1})^{p-1} \equiv 1 \pmod{p^2}}} \frac{\mu^2(a_1 a_2 \dots a_{p-1})}{(a_1 a_2 \dots a_{p-1})^s} \right.$$
$$\left. + \frac{1}{p^{\frac{2s}{p-1}}} \sum_{\substack{a_1, a_2, \dots, a_{p-1} \text{ pairwise rel. prime} \\ (a_1 a_2^2 \dots a_{p-1}^{p-1})^{p-1} \not\equiv 1 \pmod{p^2}}} \frac{\mu^2(a_1 a_2 \dots a_{p-1})}{(a_1 a_2 \dots a_{p-1})^s} \right].$$

Equivalently, letting $\mathrm{rad}(a)$ denote the product of the distinct primes dividing positive integer a, we have

$$\sum_{\substack{K \text{ pure field} \\ \text{of degree } p}} \frac{1}{f(K)^s} = -1 + \frac{1}{p-1} \sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} \left[\sum_{\substack{\mathrm{rad}(a) = n \\ a \, p\text{-free} \\ a^{p-1} \equiv 1 \pmod{p^2}}} 1 + \frac{1}{p^{\frac{2s}{p-1}}} \sum_{\substack{\mathrm{rad}(a) = n \\ a \, p\text{-free} \\ a^{p-1} \not\equiv 1 \pmod{p^2}}} 1 \right]. \quad (4.2)$$

Now, if we put

$$A_p(s) := \sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} \sum_{\substack{\mathrm{rad}(a)=n \\ a\, p\text{-free} \\ a^{p-1} \equiv 1 \pmod{p^2}}} 1,$$

then

$$\sum_{\substack{K \text{ pure field} \\ \text{of degree } p}} \frac{1}{f(K)^s} = -1 + \frac{1}{p-1} \left(\left(1 - \frac{1}{p^{\frac{2s}{p-1}}} \right) A_p(s) + \frac{1}{p^{\frac{2s}{p-1}}} \sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} \sum_{\substack{\mathrm{rad}(a)=n \\ a\, p\text{-free}}} 1 \right).$$

Note that by multiplicativity of the summands, we can write

$$\sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} \sum_{\substack{\mathrm{rad}(a)=n \\ a\, p\text{-free}}} 1 = \prod_{q \text{ prime}} \left(1 + \frac{p-1}{q^s} \right) = \left(\frac{\zeta(s)}{\zeta(2s)} \right)^{p-1} G_p(s)$$

where

$$G_p(s) := \prod_{q \text{ prime}} \left\{ \left(1 + \frac{p-1}{q^s} \right) \left(1 + \frac{1}{q^s} \right)^{-(p-1)} \right\}.$$

Also note that $\frac{G_p(s)}{(\zeta(2s))^{p-1}}$ is analytic for $\Re s \geq \frac{1}{2} + \epsilon$.

We now make the following observation. Let χ be a Dirichlet character modulo k, where $k \geq 2$ is an integer. Let $m \geq 2$ be an integer. Then the following holds:

$$\prod_{q \text{ prime}} \left(1 + \frac{\chi(q)}{q^s} + \frac{\chi(q^2)}{q^s} + \cdots + \frac{\chi(q^{m-1})}{q^s} \right) = \sum_{n \in \mathbb{N}} \frac{\mu^2(n)}{n^s} \sum_{\substack{\mathrm{rad}(a)=n \\ a\, m\text{-free}}} \chi(a). \tag{4.3}$$

By orthogonality property of Dirichlet characters, namely,

$$\sum_{\chi \pmod k} \chi^j(a) = \begin{cases} 0 & \text{if} \quad a^j \not\equiv 1 \pmod k, \\ \varphi(k) & \text{if} \quad a^j \equiv 1 \pmod k, \end{cases}$$

in which we take $k = p^2$, $j = p-1$ and using (4.3) with $m = p$, where χ is replaced by χ^j, we obtain

$$A_p(s) = \frac{1}{\varphi(p^2)} \sum_{\chi \pmod{p^2}} \prod_q \left(1 + \frac{\sum_{k=1}^{p-1} \chi^{p-1}(q^k)}{q^s}\right).$$

Thus, we obtain

$$\sum_{\substack{K \text{ pure field} \\ \text{of degree } p}} \frac{1}{f(K)^s} = -1 + \frac{1}{p-1}\left(\left(1 - \frac{1}{p^{\frac{2s}{p-1}}}\right)\frac{1}{\varphi(p^2)} \sum_{\chi \pmod{p^2}} \prod_q \left(1 + \frac{\sum_{k=1}^{p-1} \chi^{p-1}(q^k)}{q^s}\right) + \frac{1}{p^{\frac{2s}{p-1}}} \sum_{n=1}^{\infty} \frac{\mu^2(n)}{n^s} \sum_{\substack{\mathrm{rad}(a)=n \\ a\, p\text{-free}}} 1\right). \tag{4.4}$$

Now, for a Dirichlet character $\chi \bmod p^2$, we write

$$\prod_q \left(1 + \frac{\sum_{k=1}^{p-1} \chi^{p-1}(q^k)}{q^s}\right) = G_{p,\chi}(s) \prod_{k=1}^{p-1} \frac{L(s, \chi^{k(p-1)})}{L(2s, \chi^{2k(p-1)})}$$

where

$$G_{p,\chi}(s) := \prod_q \left[\left(1 + \frac{\sum_{k=1}^{p-1} \chi^{p-1}(q^k)}{q^s}\right) \prod_{k=1}^{p-1} \left(1 + \frac{\chi^{k(p-1)}(q)}{q^s}\right)^{-1}\right]$$

and $L(s, \chi)$ denotes the Dirichlet L-function.

When $\chi^{p-1} = \chi_0$, we have

$$\begin{aligned} G_{p,\chi}(s) =& G_{p,\chi_0}(s) = \prod_{q \neq p} \left[\left(1 + \frac{p-1}{q^s}\right) \left(1 + \frac{1}{q^s}\right)^{-(p-1)} \right] \\ &= \left(1 + \frac{p-1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{p-1} \prod_{q} \left[\left(1 + \frac{p-1}{q^s}\right) \left(1 + \frac{1}{q^s}\right)^{-(p-1)} \right] \\ &= \left(1 + \frac{p-1}{p^s}\right)^{-1} \left(1 + \frac{1}{p^s}\right)^{p-1} G_p(s). \end{aligned}$$

We also note that $L(s, \chi_0) = \left(1 - p^{-s}\right) \zeta(s)$.

Thus, by (4.4) and the fact that there are exactly $p-1$ characters χ modulo p^2 with $\chi^{p-1} = \chi_0$, we have

$$\begin{aligned} \sum_{\substack{K \text{ pure field} \\ \text{of degree } p}} \frac{1}{f(K)^s} =& -1 + \frac{1}{p-1} \left\{ \frac{1}{\varphi(p^2)} \left(1 - \frac{1}{p^{\frac{2s}{p-1}}}\right) \sum_{\substack{\chi \pmod{p^2} \\ \chi^{p-1} \neq \chi_0}} G_{p,\chi}(s) \prod_{k=1}^{p-1} \frac{L(s, \chi^{k(p-1)})}{L(2s, \chi^{2k(p-1)})} \right. \\ &+ \frac{1}{\varphi(p^2)} \left(1 - \frac{1}{p^{\frac{2s}{p-1}}}\right) \sum_{\substack{\chi \pmod{p^2} \\ \chi^{p-1} = \chi_0}} G_{p,\chi}(s) \prod_{k=1}^{p-1} \frac{L(s, \chi^{k(p-1)})}{L(2s, \chi^{2k(p-1)})} \\ &\left. + \frac{1}{p^{\frac{2s}{p-1}}} G_p(s) \left(\frac{\zeta(s)}{\zeta(2s)}\right)^{p-1} \right\}. \end{aligned}$$

The right-hand side above is equal to

$$\begin{aligned} =& -1 + \frac{1}{p-1} \left\{ \frac{1}{\varphi(p^2)} \left(1 - \frac{1}{p^{\frac{2s}{p-1}}}\right) \sum_{\substack{\chi \pmod{p^2} \\ \chi^{p-1} \neq \chi_0}} G_{p,\chi}(s) \prod_{k=1}^{p-1} \frac{L(s, \chi^{k(p-1)})}{L(2s, \chi^{2k(p-1)})} \right. \\ &+ \frac{1}{\varphi(p^2)} (p-1) \left(1 - \frac{1}{p^{\frac{2s}{p-1}}}\right) G_{p,\chi_0}(s) \left(\frac{L(s, \chi_0)}{L(2s, \chi_0)}\right)^{p-1} \\ &\left. + \frac{1}{p^{\frac{2s}{p-1}}} G_p(s) \left(\frac{\zeta(s)}{\zeta(2s)}\right)^{p-1} \right\}. \end{aligned}$$

Thus, we have

$$\sum_{\substack{K \text{ pure field} \\ \text{of degree } p}} \frac{1}{f(K)^s} = -1 + \frac{1}{p-1}\left\{ \frac{1}{p(p-1)}\left(1-\frac{1}{p^{\frac{2s}{p-1}}}\right) \sum_{\substack{\chi \pmod{p^2} \\ \chi^{p-1}\neq\chi_0}} G_{p,\chi}(s) \prod_{k=1}^{p-1} \frac{L(s,\chi^{k(p-1)})}{L(2s,\chi^{2k(p-1)})} \right.$$
$$+\frac{p-1}{p(p-1)}\left(1-\frac{1}{p^{\frac{2s}{p-1}}}\right)\left(1+\frac{p-1}{p^s}\right)^{-1} G_p(s)\left(\frac{\zeta(s)}{\zeta(2s)}\right)^{p-1}$$
$$\left. +\frac{1}{p^{\frac{2s}{p-1}}} G_p(s)\left(\frac{\zeta(s)}{\zeta(2s)}\right)^{p-1} \right\}.$$

□

4.1.2 Finishing up

We next discuss the following consequence of Perron's formula, Lemma 16.

Lemma 39. Let $\epsilon > 0$. Suppose that $h(s)$ is represented by a convergent Dirichlet series $\sum_{n=1}^{\infty} \frac{a_n}{n^s}$ for $\Re s > 1$ with $a_n = O(n^\epsilon)$. Further suppose that $h(s)$ continues analytically to $\Re s \geq \frac{1}{2} + \epsilon$ except possibly for a pole of order m at $s = 1$ and that $h(s) \ll |t|^{\eta\left(\frac{1}{2}-\frac{\sigma}{2}\right)+\epsilon}$, where $t := \Im s$ and $\sigma := \Re s$, in the region $\sigma \geq \frac{1}{2} + \epsilon$, $|t| \geq 2$, for some $\eta > 0$. Then for $\delta > 0$, we have

$$\sum_{n\leq x} a_n = \mathrm{Res}_{w=1}\left(h(w)\frac{x^w}{w}\right) + O\left(x^{\frac{\eta+2}{\eta+4}+\delta}\right), \qquad \text{as } x \to \infty. \tag{4.5}$$

Proof. Take $c = 1 + \epsilon$, $s = 0$, and $\psi(x) = x^\epsilon$ in Lemma 16. Then if x is half of an odd integer, by (1.5) we have

$$\sum_{n\leq x} a_n = \frac{1}{2\pi i}\int_{1+\epsilon-iT}^{1+\epsilon+iT} h(w)\frac{x^w}{w}\,dw + O\left(\frac{x^{1+2\epsilon}}{T\epsilon^m}\right).$$

Now, we estimate $\frac{1}{2\pi i}\int_{1+\epsilon-iT}^{1+\epsilon+iT} h(w)\frac{x^w}{w}\,dw$. By pulling the contour to the left and applying

the residue theorem, we get

$$\begin{aligned}\int_{1+\epsilon-iT}^{1+\epsilon+iT} h(w)\frac{x^w}{w}\,dw =& 2\pi i \operatorname{Res}_{w=1}\left(h(w)\frac{x^w}{w}\right) - \int_{1+\epsilon+iT}^{\frac{1}{2}+\epsilon+iT} h(w)\frac{x^w}{w}\,dw \\ &- \int_{\frac{1}{2}+\epsilon+iT}^{\frac{1}{2}+\epsilon-iT} h(w)\frac{x^w}{w}\,dw - \int_{\frac{1}{2}+\epsilon-iT}^{1+\epsilon-iT} h(w)\frac{x^w}{w}\,dw.\end{aligned}$$

First we try to find appropriate bounds for the integrals taken over the horizontal lines:

$$\begin{aligned}\int_{1+\epsilon+iT}^{\frac{1}{2}+\epsilon+iT} h(w)\frac{x^w}{w}\,dw \ll& -\int_{1+\epsilon}^{\frac{1}{2}+\epsilon} T^{\eta(\frac{1}{2}-\frac{\sigma}{2})}\frac{x^\sigma}{T}\,d\sigma \\ =& -T^{\frac{p-3}{2}}\int_{1+\epsilon}^{\frac{1}{2}+\epsilon}\left(\frac{x}{T^{\frac{\eta}{2}}}\right)^\sigma d\sigma \\ =& T^{\frac{p-3}{2}}\frac{\left(\frac{x}{T^{\frac{\eta}{2}}}\right)^\sigma}{\log\left(\frac{x}{T^{\frac{\eta}{2}}}\right)}\Bigg|_{\sigma=\frac{1}{2}+\epsilon}^{\sigma=1+\epsilon} \\ =& T^{\frac{p-3}{2}}\frac{\left(\frac{x}{T^{\frac{\eta}{2}}}\right)^{1+\epsilon} - \left(\frac{x}{T^{\frac{\eta}{2}}}\right)^{\frac{1}{2}+\epsilon}}{\log\left(\frac{x}{T^{\frac{\eta}{2}}}\right)}.\end{aligned}$$

A similar estimate holds for $\int_{\frac{1}{2}+\epsilon-iT}^{1+\epsilon-iT} h(w)\frac{x^w}{w}\,dw$. Returning to the left vertical part of the rectangular contour,

$$\int_{\frac{1}{2}+\epsilon+iT}^{\frac{1}{2}+\epsilon-iT} h(w)\frac{x^w}{w}\,dw \ll x^{\frac{1}{2}+\epsilon}\int_1^T \frac{t^{\frac{\eta}{4}-\epsilon}}{t+1}\,dt \ll x^{\frac{1}{2}+\epsilon}T^{\frac{\eta}{4}-\epsilon}.$$

Combining all, we see that if x is half of an integer then

$$\begin{aligned}\sum_{n\le x} a_n =& \operatorname{Res}_{w=1}\left(h(w)\frac{x^w}{w}\right) + O\left(x^{\frac{1}{2}+\epsilon}T^{\frac{\eta}{4}-\epsilon}\right) \\ &+ O\left(T^{\frac{p-3}{2}}\frac{\left(\frac{x}{T^{\frac{\eta}{2}}}\right)^{1+\epsilon} - \left(\frac{x}{T^{\frac{\eta}{2}}}\right)^{\frac{1}{2}+\epsilon}}{\log\left(\frac{x}{T^{\frac{\eta}{2}}}\right)}\right) + O\left(\frac{x^{1+2\epsilon}}{T}\right).\end{aligned}$$

Choosing $T = x^{\frac{2}{\eta+4}}$, and assuming that $\epsilon > 0$ is sufficiently small in terms of δ, we find that the error terms are $O\left(x^{\frac{\eta+2}{\eta+4}+\delta}\right)$.

If x is not half of an odd integer, but still not an integer, then the left-hand side of (4.5) can be evaluated up to the nearest half of an odd integer. On the other hand, on the right-hand side of (4.5), replacing x with the nearest half of an odd integer would have contribution $\ll x^{\epsilon}$ which can be absorbed in the error term. Finally, when x is an integer using (1.6), we can obtain a similar formula where the last term of the sum on the left-hand side of (4.5) is halved. Since we assume $a_x = O(x^{\epsilon})$, the desired result follows. □

As mentioned earlier, the series $\sum_K \frac{1}{f(K)^s}$ given in Proposition 38 is not a standard Dirichlet series for $p > 3$. So we need a little modification before we apply Lemma 39. By (4.2), we write

$$\sum_{K \text{ pure field of degree } p} \frac{1}{f(K)^s} = \frac{1}{p-1}\left[-1 + A_p(s) + \frac{1}{p^{\frac{2s}{p-1}}}B_p(s)\right] \tag{4.6}$$

where

$$B_p(s) = \sum_{n=1}^{\infty}\frac{b_n}{n^s} := \sum_{n=1}^{\infty}\frac{\mu^2(n)}{n^s} \sum_{\substack{\mathrm{rad}(a)=n \\ a\, p\text{-free} \\ a^{p-1}\not\equiv 1 \pmod{p^2}}} 1.$$

Then we have

$$\#\{K \text{ pure field of degree } p : f(K) \le X\} = \frac{1}{p-1}\left[-1 + \sum_{n\le X} a_n + \sum_{n \le \frac{X}{p^{\frac{2}{p-1}}}} b_n\right]. \tag{4.7}$$

We apply Lemma 39 to $A_p(s)$ and $B_p(s)$ which are standard Dirichlet series. Since $\sum_{\substack{\mathrm{rad}(a)=n \\ a\, p\text{-free}}} 1 \ll n^{\epsilon}$, the Dirichlet coefficients a_n and $b_n \ll n^{\epsilon}$. The well-known convexity bounds

imply that $\zeta(s)^{p-1} \ll |t|^{\frac{p-1}{2}-\frac{p-1}{2}\sigma+\epsilon}$ and $L(s,\chi) \ll_p |t|^{\frac{1}{2}-\frac{1}{2}\sigma+\epsilon}$ when $0 < \sigma < 1$ and $|t| \geq 1$ (see Section 5.2 in [26]). Moreover, for $\sigma \geq 1/2+\epsilon$, all of $\frac{1}{L(2s,\chi^{2k(p-1)})}$, $\frac{1}{\zeta(2s)}$, $G_p(s)$ and $G_{p,\chi}(s)$ are $O(1)$. Comparing the expressions (4.1) and (4.6), we see that $A_p(s)$ and $B_p(s)$ satisfy the conditions of Lemma 39 with $\eta = p-1$. Thus by (4.7), for $\delta > 0$ we have

$$\begin{aligned}
&\#\{K \text{ pure field of degree } p : f(K) \leq X\} \\
&= \frac{1}{p-1}\left(\mathrm{Res}_{w=1}\left(A_p(w)\frac{X^w}{w}\right) + \mathrm{Res}_{w=1}\left(B_p(w)\frac{\left(\frac{X}{p^{\frac{2}{p-1}}}\right)^w}{w}\right)\right) + O\left(X^{\frac{p+1}{p+3}+\delta}\right) \\
&= \frac{1}{p-1}\mathrm{Res}_{w=1}\left(\left(A_p(w) + \frac{B_p(w)}{p^{\frac{2w}{p-1}}}\right)\frac{X^w}{w}\right) + O\left(X^{\frac{p+1}{p+3}+\delta}\right) \\
&= \frac{1}{p-1}\mathrm{Res}_{w=1}\left\{\frac{X^w}{w}\sum_{\substack{K \text{ pure field} \\ \text{of degree } p}}\frac{1}{f(K)^s}\right\} + O\left(X^{\frac{p+1}{p+3}+\delta}\right).
\end{aligned}$$

It only remains to consider the residue at $s = 1$. We have

$$\begin{aligned}
&\mathrm{Res}_{s=1}\left\{\frac{X^s}{s}\sum_{K \text{ pure field of degree } p}\frac{1}{f(K)^s}\right\} \\
&= \mathrm{Res}_{s=1}\left\{\frac{X^s}{s}\left[-1 + \frac{1}{p-1}\left\{\left(1-\frac{1}{p^{\frac{2s}{p-1}}}\right)\sum_{\substack{\chi \pmod{p^2} \\ \chi^{p-1}\neq\chi_0}} G_{p,\chi}(s)\prod_{k=1}^{p-1}\frac{L(s,\chi^{k(p-1)})}{L(2s,\chi^{2k(p-1)})}\right.\right.\right. \\
&\qquad + \frac{1}{p}\left(1-\frac{1}{p^{\frac{2s}{p-1}}}\right)\left(1+\frac{p-1}{p^s}\right)^{-1} G_p(s)\left(\frac{\zeta(s)}{\zeta(2s)}\right)^{p-1} \\
&\qquad \left.\left.\left. + \frac{1}{p^{\frac{2s}{p-1}}} G_p(s)\left(\frac{\zeta(s)}{\zeta(2s)}\right)^{p-1}\right\}\right]\right\} \\
&= \mathrm{Res}_{s=1}\left\{\frac{X^s}{s}\left[\frac{G_p(s)}{p-1}\left\{\frac{1}{p}\left(1-\frac{1}{p^{\frac{2s}{p-1}}}\right)\left(1+\frac{p-1}{p^s}\right)^{-1} + \frac{1}{p^{\frac{2s}{p-1}}}\right\}\left(\frac{\zeta(s)}{\zeta(2s)}\right)^{p-1}\right]\right\} \\
&= XQ_p(\log X)
\end{aligned}$$

where $Q_p(t)$ is a polynomial of degree $p-2$, with the leading coefficient ℓ_p which is obtained by comparing Laurent series expansions of the involved functions. We have

$$\begin{aligned}
\ell_p =& \frac{1}{(p-2)!}\left[\frac{1}{p-1}\left\{\frac{1}{p}\left(1-\frac{1}{p^{\frac{2}{p-1}}}\right)\left(1+\frac{p-1}{p}\right)^{-1}+\frac{1}{p^{\frac{2}{p-1}}}\right\}\frac{G_p(1)}{(\zeta(2))^{p-1}}\right] \\
=& \frac{1}{(p-1)!}\left\{\frac{1}{p}\left(1-\frac{1}{p^{\frac{2}{p-1}}}\right)\frac{p}{2p-1}+\frac{1}{p^{\frac{2}{p-1}}}\right\}\frac{G_p(1)}{(\zeta(2))^{p-1}} \\
=& \frac{1}{(p-1)!}\left\{\frac{1}{2p-1}\left(1-\frac{1}{p^{\frac{2}{p-1}}}\right)+\frac{1}{p^{\frac{2}{p-1}}}\right\}\frac{G_p(1)}{(\zeta(2))^{p-1}} \\
=& \frac{1}{(p-1)!}\left\{\frac{1}{p^{\frac{2}{p-1}}}\left(1-\frac{1}{2p-1}\right)+\frac{1}{2p-1}\right\}\frac{G_p(1)}{(\zeta(2))^{p-1}} \\
=& \frac{1}{(p-1)!}\left\{\frac{1}{p^{\frac{2}{p-1}}}\frac{2(p-1)}{2p-1}+\frac{1}{2p-1}\right\}\frac{G_p(1)}{(\zeta(2))^{p-1}} \\
=& \frac{1}{(p-1)!}\left\{\frac{1}{p^{\frac{2}{p-1}}}\frac{2(p-1)}{2p-1}+\frac{1}{2p-1}\right\}\prod_{q\,\text{prime}}\left\{\left(1+\frac{p-1}{q}\right)\left(1-\frac{1}{q}\right)^{p-1}\right\}.
\end{aligned}$$

The numerical values of some of the constants ℓ_p are as follows:

$$\begin{aligned}
\ell_5 &= 0.000867439603\ldots, \\
\ell_7 &= 3.13502861\cdots\times 10^{-6}, \\
\ell_{11} &= 3.55232304\cdots\times 10^{-12}.
\end{aligned}$$

Using the relationship between the conductor $f(K)$ and the discriminant $d(K)$, by Lemma 37 we obtain the leading coefficient $\tilde{\ell}_p$ of $\tilde{Q}_p(x)$:

$$\begin{aligned}
\tilde{\ell}_p = \frac{p-1}{p^{p-2}}\ell_p =& \frac{1}{p^{p-2}(p-2)!}\left\{\frac{1}{p^{\frac{2}{p-1}}}\frac{2(p-1)}{2p-1}+\frac{1}{2p-1}\right\} \\
&\times\prod_{q\,\text{prime}}\left\{\left(1+\frac{p-1}{q}\right)\left(1-\frac{1}{q}\right)^{p-1}\right\}.
\end{aligned}$$

4.1.3 The coefficients of $Q_5(t)$ in the quintic case

In the quintic case, further calculations have been made to obtain the coefficients. If we write $Q_5(t) = C_3t^3 + C_2t^2 + C_1t + C_0$ then

$$C_3 = \ell_5 = \frac{1}{24}\left(\frac{1}{9} + \frac{8}{9\sqrt{5}}\right)\prod_{q\,\text{prime}}\left(1+\frac{4}{q}\right)\left(1-\frac{1}{q}\right)^4,$$

$$\begin{aligned} C_2 = \frac{1}{4}&\left[\left(\frac{1}{18}+\frac{4\sqrt{5}}{45}\right)\left(\frac{G_5'(1)}{G_5(1)} - 8\frac{\zeta'(2)}{\zeta(2)} + 4\gamma - 1\right) + \left(\frac{2}{81}+\frac{2\sqrt{5}}{90}\right)\log 5\right] \\ &\times \prod_{q\,\text{prime}}\left(1+\frac{4}{q}\right)\left(1-\frac{1}{q}\right)^4 \end{aligned}$$

and

$$\begin{aligned} C_1 = \frac{G_5(1)}{4\zeta(2)^4}&\left[\left(\frac{67}{11664}+\frac{1453}{11664\sqrt{5}}\right)(\log 5)^2 + (-4\gamma_1 + 6\gamma^2)\left(\frac{1}{9}+\frac{1}{9\sqrt{5}}\right)\right. \\ &+(4\gamma-1)\left[-\frac{1}{9}-\frac{8}{9\sqrt{5}} + \log 5\left(\frac{4}{81}-\frac{89}{162\sqrt{5}}\right)\right] \\ &+\frac{G_5'(1)}{G_5(1)}\left(\log 5\left(\frac{4}{81}-\frac{32}{27\sqrt{5}}+(4\gamma-1)\left(\frac{1}{9}+\frac{8}{9\sqrt{5}}\right)\right)\right) \\ &+(-8)\frac{\zeta'(2)}{\zeta(2)}\left(\log 5\left(\frac{10}{27}-\frac{23}{27\sqrt{5}}\right)+(4\gamma-1)\left(\frac{1}{9}+\frac{8}{9\sqrt{5}}\right)\right) \\ &\left.+\left(\frac{1}{9}+\frac{8}{9\sqrt{5}}\right)\left(-8\frac{\zeta''(2)}{\zeta(2)}+40\left(\frac{\zeta'(2)}{\zeta(2)}\right)^2+(-8)\frac{\zeta'(2)}{\zeta(2)}\frac{G_5'(1)}{G_5(1)}+\frac{1}{2}\frac{G_5''(1)}{G_5(1)}\right)\right] \end{aligned}$$

where $-\gamma_1$ is the coefficient of $(s-1)$ in the Laurent series expansion of $\zeta(s)$ about $s=1$.

It can be observed from the expressions above that as we move to the secondary terms, the corresponding coefficients become more involved. The coefficient C_0 could also be calculated in terms of $\frac{G_5(1)}{\zeta(2)^4}$, $\frac{\zeta'(2)}{\zeta(2)}$, $\frac{\zeta''(2)}{\zeta(2)}$, $\frac{\zeta'''(2)}{\zeta(2)}$, $\frac{G_5'(1)}{G_5(1)}$, $\frac{G_5''(1)}{G_5(1)}$, $\frac{G_5'''(1)}{G_5(1)}$.

Bibliography

[1] E. Bach, J. Sorenson, *Explicit bounds for primes in residue classes*, Math. Comp. **65** (1996), 1717–1735.

[2] A. S. Bang, *Taltheoretiske undersøgelser*, (Fortsat, Se S. 80), Tidsskrift for Mathematik, vol. 4, (1886), 130-137.

[3] K. Benli, *On the number of pure fields of prime degree*, Colloq. Math., **153**(1), (2018), 39-50.

[4] K. Benli, *On the number of prime factors of the composite numbers resulting after a change of digits of primes*, Journal de Théorie des Nombres de Bordeaux, *to appear.*

[5] K. Benli, *Small prime kth power residues*, Proc. Amer. Math. Soc., *to appear.*

[6] K. Benli, P. Pollack, *Small prime kth power residues for $k = 2, 3, 4$: a reciprocity laws approach*, Proc. Amer. Math. Soc., **147**, (2019), 987–994.

[7] W. E. H. Berwick, *Integral Bases*, Cambridge Tracts in Math. Math. Phys. 22, Stechert-Hafner, New York, 1964.

[8] G. D. Birkhoff, H. S. Vandiver, *On the integral divisors of $a^n - b^n$*. Annals of Mathematics, vol. 5, no. 4, (1904), 173–180.

[9] E. Bombieri, *Le grand crible dans la théorie analytique des nombres*. Astérisque **18** 103, 1987.

[10] V. Brun, *La série* $\frac{1}{5}+\frac{1}{7}+\frac{1}{11}+\frac{1}{13}+\frac{1}{17}+\frac{1}{19}+\frac{1}{29}+\frac{1}{31}+\frac{1}{41}+\frac{1}{43}+\frac{1}{59}+\frac{1}{61}\cdots$ *oú les dénominateurs sont "nombres premiers jumeaux" est convergente ou finie*, Bull. Sci. Math 43 (1919), 100–104, 124-128.

[11] D. A Burgess, *The distribution of quadratic residues and nonresidues,* Mathematika 4 (1957), 106–112.

[12] H. Cohen, A. Morra, *Counting cubic extensions with qiven resolvent*, J. Algebra, 325, (2011), 461-478.

[13] A. Cojocaru, R. Murty, *An Introduction to Sieve Methods and Their Applications*, Cambridge University Press, 2006.

[14] H. Davenport, Multiplicative Number Theory, *Springer Verlag, New York*, 1980.

[15] H. G. Diamond, H. Halberstam, *A Higher-dimensional Sieve Method*, Cambridge Tracts in Mathematics, vol. 177, Cambridge University Press, Cambridge, 2008.

[16] A. Dunn, I. E. Shparlinski, A. Zaharescu, *Bilinear forms in Weyl sums for modular square roots and applications*, preprint, (2019) arXiv:1908.10143.

[17] P. D. T. A. Elliott, *The least prime* $k-$th*-power residue*, J. London Math. Soc. (2), vol. 3, (1971), 205–210.

[18] P. Erdős, *Solution to problem 1029: Erdős and the computer*. Mathematics Magazine **52** (1979), 180–181.

[19] Y. Fujisawa, *Elementary estimates for the number of pure number fields of degree p*, INTEGERS 15, (2015) A4.

[20] Y. Fujisawa, *On some arithmetical functions and the number of pure number fields*, Colloq. Math., **149**(2), (2016), 275–290.

[21] C. F. Gauss, *Disquisitiones Arithmeticae*, Leipzig, Germany, 1801, translated by A. Arthur and S. J. Clark, Yale Univ. Press, New Haven, 1966.

[22] GH from MO (`http://mathoverflow.net/users/11919/gh-from-mo`), *Given a prime p how many primes $\ell < p$ of a given quadratic character mod p?*, MathOverflow, URL: `http://mathoverflow.net/q/52393` (version: 2014-09-03).

[23] A. Granville, K. Soundararajan, *Large character sums*, J. Amer. Math. Soc. **14** (2001), 365–397.

[24] D. R. Heath-Brown, *Zero-free regions for Dirichlet L-functions, and the least prime in an arithmetic progression*, Proc. London Math. Soc. (3) 64, no. 2, (1992), 265-338.

[25] A. Hildebrand, *A note on Burgess's character sum estimate*, C.R. Acad. Sci. Roy. Soc. Canada **8** (1986), 35–37.

[26] H. Iwaniec, E. Kowalski, *Analytic Number Theory*, American Mathematical Society Colloquium Publications, vol 53, American Mathematical Society, Providence, RI, 2004.

[27] Y. Lamzouri, X. Li, K. Soundararajan, *Conditional bounds for the least quadratic non-residue and related problems*, Math. Comp. **84** (2015), 2391–2412, errata in **86** (2017), 2551–2554.

[28] E. Landau, *Über Dirichletsche Reihen mit komplexen Charakteren*, J. Reine Angew. Math., Journal für die Reine und Angewandte Mathematik. [Crelle's Journal], **157**, (1927), 26–32.

[29] F. Lemmermeyer, *Reciprocity Laws: From Euler to Eisenstein*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, 2000.

[30] U. V. Linnik, *On the least prime in an arithmetic progression. I. The basic theorem.* Rec. Math. [Mat. Sbornik] N.S. **15**(57) (1944), 139–178.

[31] Ju. V. Linnik, A. I. Vinogradov, *Hypoelliptic curves and the least prime quadratic residue*, Dokl. Akad. Nauk SSSR, **168**, (1966), 259–261 (Russian).

[32] D. C. Mayer, *Discriminants of metacyclic fields*, Canad. Math. Bull Vol. **36**(1), (1993), 103–107.

[33] H. L. Montgomery, R. C. Vaughan, *Multiplicative Number Theory. I. Classical Theory*, Cambridge Studies in Advanced Mathematics, **97**, Cambridge University Press, Cambridge, 2007.

[34] H. L. Montgomery, R.C. Vaughan, *Exponential sums with multiplicative coefficients*, Invent. Math **43** (1977), 69–82.

[35] Z. Meng, *The distribution of the zeros of L-functions and the least prime in some arithmetic progression*, Sci. China Ser. **A 43**, no. 9, (2000), 937–944.

[36] T. Nagell, *Sur les restes et les non-restes cubiques*, Ark. Mat. **1**, (1952), 579–586.

[37] H. Pan, *On the number of distinct prime factors of* $nj + a^h k$. Monatsh. Math. **175**, no. 2, (2014), 293–305.

[38] R. E. A. C. Paley, *A theorem on characters*, J. London Math. Soc **7** (1932), 28–32.

[39] P. Pollack, *Not Always Buried Deep: A Second Course in Elementary Number Theory*, American Mathematical Society, Providence, RI, 2009.

[40] P. Pollack, *The smallest prime that splits completely in an abelian number field*, Proc. Amer. Math. Soc., **142**, (2014), 1925–1934.

[41] P. Pollack, *Bounds for the first several prime character nonresidues*, Proc. Amer. Math. Soc. **145** (2017), 2815–2826.

[42] C. Siegel, *Über die Classenzahl quadratischer Zahlkörper.* Acta Arithmetica **1.1**, (1935), 83–86.

[43] Z.-H. Sun, *On the theory of cubic residues and nonresidues*, Acta Arith. **84** (1998), 291–335.

[44] Z.-H. Sun, *Supplements to the theory of quartic residues*, Acta Arith. **97** (2001), 361–377.

[45] T. Tao, *A remark on primality testing and decimal expansions.* J. Aust. Math. Soc. **91** (2011), 405–413.

[46] E. C. Titchmarsh, *The Theory of the Riemann Zeta-function*, Second Edition edited by D. R. Heath-Brown, Clarendon Press, Oxford, 1986.

[47] I. M. Vinogradov, *On the distribution of quadratic residues and nonresidues*, J. Phys.-Mat. ob-va Permsk Univ. **2** (1919), 1–16 (Russian).

[48] L. C. Washington, *Introduction to Cyclotomic Fields*, Graduate Texts in Mathematics, vol. 83, Springer-Verlag, New York, 1997.

[49] T. Xylouris, *Über die Nullstellen der Dirichletschen L-Funktionen und die kleinste Primzahl in einer arithmetischen Progression* [The zeros of Dirichlet L-functions and the least prime in an arithmetic progression] (Dissertation for the degree of Doctor of Mathematics and Natural Sciences) Bonn: Universität Bonn, Mathematisches Institut, 2011 (German).

[50] K. Zsigmondy, *Zur Theorie der Potenzreste.* Monatsh. f. Mathematik und Physik **3**, (1892), 265–284.