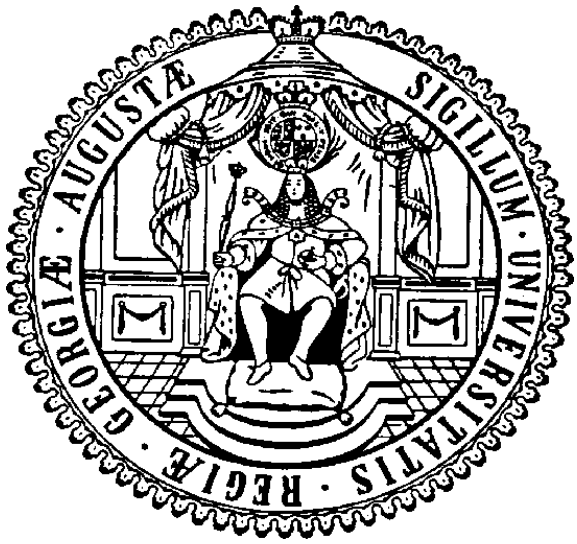
On Artin's Primitive Root Conjecture

Dissertation
zur Erlangung des mathematisch-naturwissenschaftlichen Doktorgrades
"Doctor rerum naturalium"
der Georg-August-Universität Göttingen

im Promotionsprogramm (SMS)
der Georg-August-Universität Göttingen (GAUSS)



vorgelegt von
Christopher Daniel Ambrose
aus Hildesheim

Göttingen, 2014

Betreuungsausschuss

Prof. Dr. Valentin Blomer, Mathematisches Institut Göttingen

Prof. Dr. Preda Mihăilescu, Mathematisches Institut Göttingen

Mitglieder der Prüfungskommission

Referent: Prof. Dr. Valentin Blomer, Mathematisches Institut Göttingen

Koreferent: Prof. Dr. Preda Mihăilescu, Mathematisches Institut Göttingen

Weitere Mitglieder der Prüfungskommission

PD Dr. Ulf-Rainer Fiebig, Institut für Mathematische Stochastik

Prof. Dr. Ina Kersten, Mathematisches Institut Göttingen

Prof. Dr. Russell Luke, Institut für Numerische und Angewandte Mathematik

Prof. Dr. Anita Schöbel, Institut für Numerische und Angewandte Mathematik

Tag der mündlichen Prüfung: 6. Mai 2014

To my Grandmother
Maria

Acknowledgements

At this point I gladly seize the opportunity to thank those who made this thesis possible. I owe deepest gratitude to my supervisor Prof. Dr. Valentin Blomer who always had an open door for fruitful discussions and patiently supported me whenever possible. His creativity and encouragement were of tremendous inspiration from the very beginning and helped me bring this thesis to a satisfactory conclusion. Furthermore, I want to thank my second supervisor and referee Prof. Dr. Preda Mihăilescu for his effort and helpful assistance, and the Volkswagen Foundation whose financial support enabled the completion of this thesis in the first place. I also thank my former colleagues Marc Palm, Deniz Balakci, Sören Kleine and Stefan Baur for their helpfulness and interesting mathematical debates. Particular gratitude goes to Tyge Tiessen, Sönke Behrends, and especially Tobias Bembom, for reading my thesis, giving me valuable hints and being true friends. Last but not least, I wish to thank my family, my friends and my girlfriend for their company, patience and unconditional support during my doctorate and a truly wonderful time.

Contents

Introduction

In this thesis, we study variations of Artin's primitive root conjecture, one of several number theoretical conjectures proposed by Emil Artin. This introduction motivates the problems we are investigating, clarifies our objectives and gives an account of the contribution of this thesis. We start with a historical background.

Historical background on Artin's primitive root conjecture

Artin's primitive root conjecture represents one of the most popular unsolved problems in number theory, and like many other number theoretic problems, it has the feature of being both easily understandable and very involved at the same time. Indeed, the problem was initiated by the following simple observation: Whenever you take a prime number p different from 2 and 5, then the decimal expansion of its reciprocal $1/p$ is periodic:

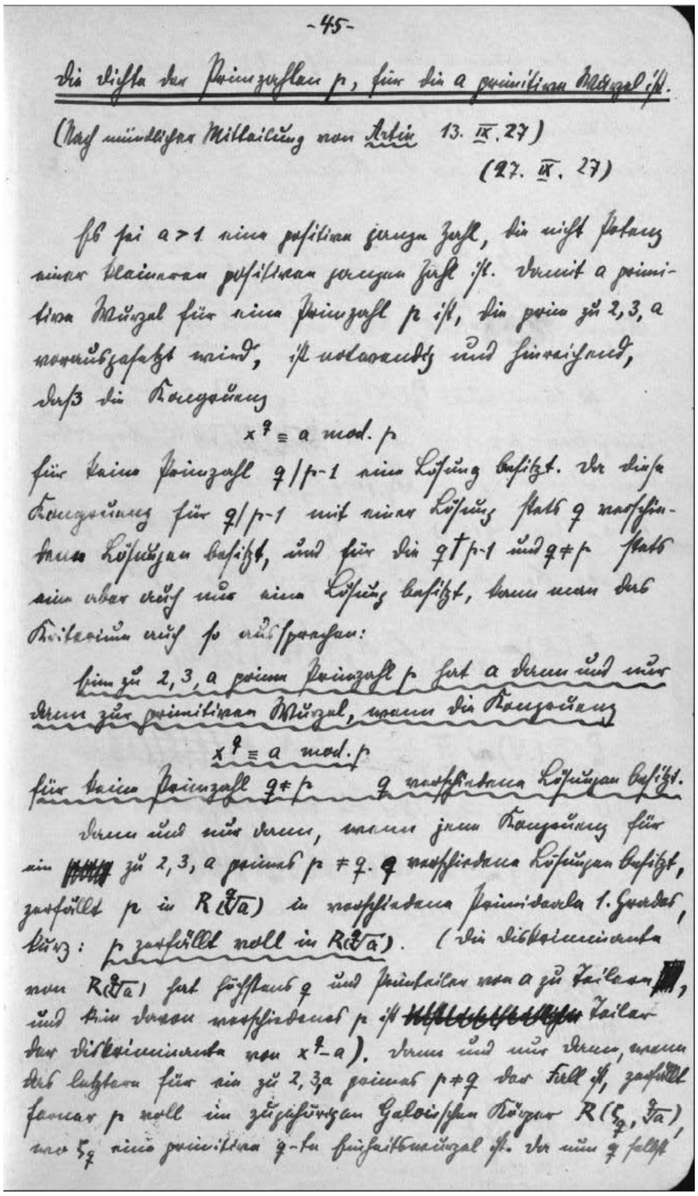
$$\begin{aligned} 1/3 &= 0.\overline{3} & 1/13 &= 0.\overline{076923} \\ 1/7 &= 0.\overline{142857} & 1/17 &= 0.\overline{0588235294117647} \\ 1/11 &= 0.\overline{09} & 1/19 &= 0.\overline{052631578947368421} \end{aligned}$$

Observing these examples, many questions may arise, such as: Why does the period length of $1/7$ equal 6, whereas $1/11$ has a period of length 2? In articles 315–317 of his *Disquisitiones Arithmeticae* (1801) [35], Gauss investigated questions of this kind and the distribution of the period lengths of $1/p$ in general. He showed that this period length coincides with the order of 10 within the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ of $p-1$ elements, i.e. the smallest positive integer n such that p divides $10^n - 1$. Hence, the period length of $1/p$ is always a divisor of $p-1$ and becomes maximal if and only if 10 is a primitive root modulo p. Here, an integer a is called a *primitive root modulo* p, if $p \nmid a$ and a generates $(\mathbb{Z}/p\mathbb{Z})^*$. As the above examples show, 10 is a primitive root modulo 7, 17 and 19, but not modulo 3, 11 or 13. Gauss showed a particular interest in the question of how often 10 would be a primitive root modulo p, as p varies over primes, but made no specific conjecture.

In this regard, a precise prediction is provided by *Artin's primitive root conjecture (AC)* which Artin communicated to Hasse in September 1927 (see [31, 57]): For any integer a, different from 0 and ± 1 and not a square of another integer, there are infinitely many primes p, for which a is a primitive root modulo p. Even more, Artin hypothesised that the set of such primes has a positive density δ_a inside the set of all primes, that is

$$\sharp\{p \leq x : a \text{ is a primitive root modulo } p\} \sim \delta_a \cdot \pi(x),$$

as $x \to \infty$. Here, $\pi(x)$ denotes the number of primes $p \leq x$ which, by the famous prime number theorem, grows asymptotically like $x/\log x$. Artin was led hither by his striking insight in algebraic number theory [3] and heuristic arguments based on the Čebotarev density theorem, a powerful tool to determine densities for a wide class of primes with certain arithmetic properties. We will trace back Artin's intuition in more detail in Chapter 1, but for a quick preview one might take a look at Figure 1.



-45-

Die Dichte der Primzahlen p, für die a primitive Wurzel ist.

(Nach mündlicher Mitteilung von Artin 13. IX. 27)

(27. IX. 27)

FIGURE 1. Entry of HASSE's mathematical notebook from the year 1927 on Artin's primitive root conjecture (taken from [31]).

Since the statement of AC, many mathematicians have attempted a proof (see Chapter 1). Most notably, HOOLEY in 1967 [42], utilized the Brun-Titchmarsh inequality and an effective version of the Čebotarev density theorem, valid under the generalized Riemann hypothesis (GRH), to turn ARTIN's heuristic arguments into a rigorous proof. Furthermore, GUPTA and RAM MURTY in 1984 [36], and later HEATH-BROWN in 1985 [39], applied a sieve argument to show that for "almost all" integers a, there are infinitely many primes p such that a is a primitive root modulo p. In particular, their unconditional approach revealed that this qualitative version of AC holds for some $a \in \{2, 3, 5\}$, but on the other hand it failed to disclose for which of these it is in fact the case. Hence, AC proves to be more complex than it appears at a first glance, and is unsolved until today.

Motivation and objectives

The simple formulation of Artin's primitive root conjecture allows for numerous variations to many fields of mathematical interest. In this thesis, we focus on variants stemming from the area of number fields and elliptic curves.

For any integer a and a prime $p \nmid a$, we define the *residual index* $\operatorname{ind}_a(p)$ and the *residual order* $\operatorname{ord}_a(p)$ *of* a *modulo* p as index and order of the subgroup generated by a inside $(\mathbb{Z}/p\mathbb{Z})^*$. In particular, both quantities divide $p-1$ and satisfy $\operatorname{ind}_a(p) = (p-1)/\operatorname{ord}_a(p)$. If $a \neq 0, \pm 1$ is not a square, AC states that $\operatorname{ind}_a(p) = 1$, or equivalently $\operatorname{ord}_a(p) = p-1$, occurs with positive probability. But what can we say about the distribution of $\operatorname{ind}_a(p)$ and $\operatorname{ord}_a(p)$ as p varies over primes in general? Apart from its significance in number theory, this problem has an influence on cryptography, too. For the Diffie-Hellman key exchange protocol and the ElGamal cryptosystem, for instance, it might be desirable to have information about the distribution of primes p for which a given integer a is a primitive root modulo p or has at least large residual order modulo p.

In a remarkable work from 1977, Lenstra [58] adapted Hooley's method and, assuming GRH, proved a number field analogue of AC. His far reaching result again builds on an effective Čebotarev density theorem under GRH and entails many variations of AC. Subject to the GRH, Lenstra's result e.g. implies that the set of primes p for which $\operatorname{ind}_a(p)$ equals a given positive integer k has a density inside the set of all primes which, as shown by Wagstaff [101] and Moree [76], is positive in most cases, and decreases approximately like $1/k^2$ (see Chapter 2 for details). Roughly speaking, $\operatorname{ord}_a(p)$ is thus typically large and $\operatorname{ind}_a(p)$ is typically small, as p ranges over prime numbers. This principle has been underlined by several other works (see e.g. [24, 51]) and, in more general versions, it will accompany us throughout this thesis. It is our main objective to improve the understanding of the distribution of several variations of $\operatorname{ind}_a(p)$ and $\operatorname{ord}_a(p)$.

Variations for number fields. The most natural generalization of the above discussion is the consideration of number fields. A *number field* $\mathbb{K}$ is a finite field extension of the rational numbers $\mathbb{Q}$ and as such, it inherits many convenient concepts thereof. In particular, there exists a natural generalization of the integers $\mathbb{Z}$ in $\mathbb{K}$, namely the *ring of (algebraic) integers* $\mathcal{O}_{\mathbb{K}}$, i.e. the set of roots inside $\mathbb{K}$ of integer polynomials with leading coefficient equal to 1. Here, ideals and prime ideals of $\mathcal{O}_{\mathbb{K}}$ adopt the roles which integers and prime numbers play in $\mathbb{Z}$. For example, as an analogue of the familiar principle of unique prime factorization, any proper ideal $\mathfrak{a}$ of $\mathcal{O}_{\mathbb{K}}$ admits a unique factorization[1] into a product of finitely many prime ideals $\mathfrak{p}_1, \ldots, \mathfrak{p}_n$. Another interesting role is played by $\mathcal{U}_{\mathbb{K}}$, the *group of units* of $\mathcal{O}_{\mathbb{K}}$. While $\mathcal{U}_{\mathbb{Q}} = \{\pm 1\}$, Dirichlet proved that in general, $\mathcal{U}_{\mathbb{K}}$ is a finitely generated subgroup of $\mathbb{K}$ which is infinite precisely when $\mathbb{K}$ is neither $\mathbb{Q}$ nor an imaginary quadratic field[2]. This feature allows for interesting variations of the above-mentioned problems.

Henceforth, $\mathbb{K}$ will denote a number field and, abusing notation, an *ideal of* $\mathbb{K}$ will always mean an ideal of $\mathcal{O}_{\mathbb{K}}$, for convenience. In virtue of the above discussion, let Γ be a finitely generated but infinite subgroup of $\mathbb{K}^*$. For any prime ideal $\mathfrak{p}$ of $\mathbb{K}$, the group $(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*$ is again cyclic and contains $\mathcal{N}\mathfrak{p} - 1$ residue classes, where for an arbitrary ideal $\mathfrak{a}$ of $\mathbb{K}$, $\mathcal{N}\mathfrak{a}$ denotes the cardinality of $\mathcal{O}_{\mathbb{K}}/\mathfrak{a}$. If $\mathfrak{p}$ is outside some finite exceptional set, then the reduction $\overline{\Gamma}$ of Γ modulo $\mathfrak{p}$ is a subgroup of $(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*$. We express this feature

[1] The analogue statement for algebraic integers instead of ideals is not true in general.
[2] As a simple example, $\sqrt{2}+1$ generates an infinite subgroup of $\mathcal{U}_{\mathbb{Q}(\sqrt{2})}$.

by writing $\overline{\Gamma} \subset (\mathcal{O}_{\mathbb{K}} / \mathfrak{p})^*$. In this case, one may consider the *residual index* $\mathrm{ind}_\Gamma(\mathfrak{p})$ and the *residual order* $\mathrm{ord}_\Gamma(\mathfrak{p})$ *of* Γ *modulo* $\mathfrak{p}$, given by index and order of $\overline{\Gamma}$ inside $(\mathcal{O}_{\mathbb{K}} / \mathfrak{p})^*$. Hence, Γ takes the place of the single integer a, or the subgroup of $\mathbb{Q}^*$ generated thereof, in Artin's original setting, and primes are substituted by prime ideals. We are interested in the following question:

Question 1. *What can we say about* $\mathrm{ind}_\Gamma(\mathfrak{p})$ *and* $\mathrm{ord}_\Gamma(\mathfrak{p})$*, as* $\mathfrak{p}$ *ranges over a suitable family of prime ideals of* $\mathbb{K}$*?*

In this thesis, we contribute to this question by studying average order and moments in general of $\mathrm{ind}_\Gamma(\mathfrak{p})$ and $\mathrm{ord}_\Gamma(\mathfrak{p})$, a problem which has already been studied over $\mathbb{Q}$. Let $a \neq 0, \pm 1$ be an integer. Using effective versions of the Čebotarev density theorem under GRH in combination with the Brun-Titchmarsh inequality, Kurlberg and Pomerance [51] recently proved that $\mathrm{ord}_a(p)$ equals $c_a \cdot p$ on average over p, for some positive constant c_a depending on a, provided that the GRH holds true. A few years earlier, Luca [69] utilized the Siegel-Walfisz theorem or alternatively the Bombieri-Vinogradov theorem to show that this result holds unconditionally, at least on average over a.

As for the residual index, the situation is more difficult. Applying Lenstra's result mentioned above, Wagstaff [101] provided heuristic arguments which suggest that the average order of $\mathrm{ind}_a(p)$ is the product of $\log p$ and a positive constant depending on a. Wagstaff's heuristic certainly agrees with the principle that $\mathrm{ord}_a(p)$ and $\mathrm{ind}_a(p)$ tend to be large and small, respectively. The downside to this principle is, however, that $\mathrm{ind}_a(p)$ is more difficult to handle on average than $\mathrm{ord}_a(p)$, a property which we will frequently encounter throughout this thesis. As a matter of fact, the asymptotic law proposed by Wagstaff is out of reach even under GRH. The best upper bound due to Erdős and Ram Murty [24] for the average order of $\mathrm{ind}_a(p)$ is roughly of size $p^{1/2}$. Moreover, Ram Murty and Srinivasan [83] pointed out that an upper bound of approximate size $p^{1/4}$ would suffice to prove AC. This indicates the complexity and significance of this problem.

So far, the presented problems only concerned reduction modulo primes or prime ideals, and it is natural to consider variations which involve the reduction modulo composite integers or ideals, as well. For an arbitrary ideal $\mathfrak{a}$ of $\mathbb{K}$, again assumed to be outside an exceptional set ($\overline{\Gamma} \subset (\mathcal{O}_{\mathbb{K}} / \mathfrak{a})^*$), it is easy to extend our notion to the *residual index* $\mathrm{ind}_\Gamma(\mathfrak{a})$ and *residual order* $\mathrm{ord}_\Gamma(\mathfrak{a})$ *of* Γ *modulo* $\mathfrak{a}$. Just as in the prime number case, the behaviour of $\mathrm{ord}_a(n)$, with $n \in \mathbb{N}$, has been studied intensively by Erdős, Pomerance, Schmutz and Kurlberg [25, 51]. Since these results again admit generalizations to number fields which may only yield little more information, we omit a treatment of $\mathrm{ord}_\Gamma(\mathfrak{a})$, and instead focus our attention on the following question:

Question 2. *What can we say about* $\mathrm{ind}_\Gamma(\mathfrak{a})$*, as* $\mathfrak{a}$ *varies over all ideals of* $\mathbb{K}$*?*

Of particular interest in this regard is the distribution of $\mathrm{ind}_{\mathcal{U}_{\mathbb{K}}}(\mathfrak{a})$, provided that $\mathcal{U}_{\mathbb{K}}$ is infinite. For this case, Rohrlich [88] has explicitly constructed an infinite family of ideals $\mathfrak{a}$ of $\mathbb{K}$ for which $\mathrm{ind}_{\mathcal{U}_{\mathbb{K}}}(\mathfrak{a})$ is exceptionally large. This construction entailed strong bounds towards the Ramanujan conjecture for GL_n over number fields [72], but on the other hand, the sparseness of this sequence prevented an extension of the Kim-Sarnak bound [48] for GL_2 over $\mathbb{Q}$ to general number fields. We refer to [9] and the survey article [10] of Blomer and Brumley for a detailed discussion. In a recent paper by Rohrlich [89], it is in turn the average order of $\mathrm{ind}_{\mathcal{U}_{\mathbb{K}}}(\mathfrak{a})$ which appears in connection with counting self-dual Artin representations over number fields.

Hence, the understanding of $\mathrm{ind}_\Gamma(\mathfrak{a})$ has an impact on several areas of number theory, and we attend this problem by investigating average order of $\mathrm{ind}_\Gamma(\mathfrak{a})$ and moments thereof

in general. The major difficulty one has to confront here is that, in contrast to the prime ideal case, the group $(\mathcal{O}_{\mathbb{K}} / \mathfrak{a})^*$ is no longer cyclic in general, which results in a much more chaotic behaviour. The aforementioned results for $\mathrm{ord}_a(n)$ and number field variations of AC suggest that $\mathrm{ord}_\Gamma(\mathfrak{a})$ and $\mathrm{ind}_\Gamma(\mathfrak{a})$ are typically large and small, respectively. Nothing changed in this aspect. Establishing upper bounds for the average order of $\mathrm{ind}_\Gamma(\mathfrak{a})$, however, already proves to be harder than expected. Indeed, the best upper bound recently proved by Zelinsky [107] only saves little towards the trivial upper bound $\mathcal{N}\mathfrak{a}$. In this thesis, we will consider lower bounds instead, and establish some unexpected estimates.

Variations for elliptic curves. AC and the problems described above of course allow for variants beyond the number field setting. In this thesis, we study such variations for elliptic curves. A *rational elliptic curve* is the locus of an equation

$$y^2 = x^3 + ax + b \tag{1}$$

with $a, b \in \mathbb{Z}$, satisfying $4a^3+27b^2 \neq 0$, plus a *point O at infinity*. The *rational points* $\mathrm{E}(\mathbb{Q})$ of E, i.e. points on E with rational coordinates and O, form a finitely generated abelian group in virtue of a simple geometric operation. In a similar way, one may introduce elliptic curves defined over other fields, e.g. finite fields $\mathbb{F}_p$, for any prime p. The main difference here is that a and b then lie in $\mathbb{F}_p$ and all equations apply modulo p. If E is an elliptic curve defined over $\mathbb{F}_p$, then the *$\mathbb{F}_p$-rational points* $\mathrm{E}(\mathbb{F}_p)$ of E, i.e. points on E with coordinates in $\mathbb{F}_p$ and O, again form an abelian group with approximately p elements by a famous result due to Hasse. Different to the number field case, however, $\mathrm{E}(\mathbb{F}_p)$ is no longer cyclic in general, but rather a direct sum of at most two cyclic groups. As a variant of Question 1, we are interested in the behaviour of the *residual index* $\mathrm{ind}_Q(\mathrm{E})$ and the *residual order* $\mathrm{ord}_Q(\mathrm{E})$ *of points Q in* $\mathrm{E}(\mathbb{F}_p)$, for suitable families of such groups. In this thesis, we study two basically different types of such families:

Let E be a rational elliptic curve and assume that Q is a rational point on E of infinite order in $\mathrm{E}(\mathbb{Q})$. Henceforth, Q plays the same role as a and Γ did in the number field setting. For all but finitely many primes p, called primes of good reduction for E, the reduction of (1) modulo p yields an elliptic curve E_p defined over $\mathbb{F}_p$. One may also reduce Q modulo p to a point $\overline{Q} \in \mathrm{E}_p(\mathbb{F}_p)$, and define $\mathrm{ind}_Q(\mathrm{E}_p) := \mathrm{ind}_{\overline{Q}}(\mathrm{E}_p)$ and $\mathrm{ord}_Q(\mathrm{E}_p) := \mathrm{ord}_{\overline{Q}}(\mathrm{E}_p)$. If $\mathrm{ind}_Q(\mathrm{E}_p) = 1$, one calls Q a *primitive point of* E *modulo p*, and the elliptic curve analogue of AC amounts to determine whether the set of primes p, for which Q is a primitive point of E modulo p, has a density within the set of all primes. In 1976, Lang and Trotter [56] conjectured that such a density always exists but fell short of an answer. The only improvement on this problem ever since is due to Gupta and Ram Murty [37]. Utilizing effective versions of the Čebotarev density theorem and number field analogues of the Brun-Titchmarsh inequality, they provided a proof under GRH, if E has complex multiplication (CM) by an imaginary quadratic field, a property which usually simplifies the arguments, but applies rather seldom (see Chapter 2 for details).

As above, we are merely interested in the distribution of $\mathrm{ind}_Q(\mathrm{E}_p)$ and $\mathrm{ord}_Q(\mathrm{E}_p)$, as p varies over primes of good reduction for E, a problem about which only little is known. Variations of this problem might also play a role in elliptic curve cryptography. The current state of the above-mentioned *Lang-Trotter conjecture* reveals that the situation is more complex for elliptic curves than for number fields. In fact, several complications which the study of elliptic curves brings along hinder us from a decent treatment of the distribution of $\mathrm{ind}_Q(\mathrm{E}_p)$ and we confine ourselves to the problem:

Question 3. *What can we say about* $\mathrm{ord}_Q(\mathrm{E}_p)$*, as p varies over primes?*

As in the number field case, we approach this question by investigating moments of $\mathrm{ord}_Q(\mathrm{E}_p)$. Inspired by the mentioned work of Gupta and Ram Murty, and impressions from the number field analogues, we expect that the reduction of Q modulo p generates "most" of $\mathrm{E}_p(\mathbb{F}_p)$, for a positive density of primes. As $\mathrm{E}_p(\mathbb{F}_p)$ contains roughly p points, we thus expect that $\mathrm{ord}_Q(\mathrm{E}_p)$ should equal the product of p and some positive constant, depending on Q and E, on average. A recent result in this direction is due to Freiberg and Kurlberg [32], who proved such a result for the exponent of $\mathrm{E}_p(\mathbb{F}_p)$, certainly an upper bound for $\mathrm{ord}_Q(\mathrm{E}_p)$, unconditionally if E has CM, and under GRH otherwise.

Different to the number field setting, elliptic curves are pertinent for another variation of the above problem. Instead of fixing an elliptic curve E and a point Q thereon, and considering the distribution of $\mathrm{ind}_Q(\mathrm{E}_p)$ and $\mathrm{ord}_Q(\mathrm{E}_p)$ over primes p, one may also fix a prime p, assumed to be larger than 3 for convenience, and study how residual index and order of points from a family $\{\mathrm{E}_i : i \in I\}$ of elliptic curves defined over $\mathbb{F}_p$ typically distribute. Different to the preceding problem, however, the groups $\mathrm{E}_i(\mathbb{F}_p)$, $i \in I$, usually have no points in common and are not obtained by reduction of any kind from some other curve. Therefore, we study the following question, again in terms of arbitrary moments.

Question 4. *What can we say about the distribution of "typical" values for* $\mathrm{ind}_Q(\mathrm{E}_i)$ *and* $\mathrm{ord}_Q(\mathrm{E}_i)$ *over a suitable family* $\{\mathrm{E}_i : i \in I\}$ *of elliptic curves defined over* $\mathbb{F}_p$*?*

Contribution of the thesis

In the following, we give a brief outline of the contributions found in this thesis to the above-raised questions and beyond, and give an account of the methods we applied in this regard. At the same time we provide a short overview about content and structure of this thesis which we divided into three major parts.

Part I. The first two chapters of this part can be considered introductory. In Chapter 1, we continue our account of AC. We give a detailed outline of Artin's heuristic arguments and briefly discuss the approaches of Hooley, Gupta, Ram Murty and Heath-Brown named above. In Chapter 2, we address variations of AC which are related to the problems listed above, namely analogues of AC for near-primitive roots, number fields, λ-roots and elliptic curves. We introduce these problems in more detail than above and also quote results which prove to be beneficial for later investigations.

Chapter 3 is not directly related to the questions raised above but of independent interest. Here, we consider the distribution of primitive roots modulo a fixed prime p. We prove that for p large enough, there always exists a primitive root of the form $a^2 + b^2$ modulo p, with integers a and b, which is bounded from above by $p^{\frac{1}{2}+\varepsilon}$.

Theorem 1. *Let* $s^*(p)$ *denote the* least primitive root modulo p which is expressible as a sum of two squares. *Then, for any* $\varepsilon > 0$ *we have*

$$s^*(p) \ll_\varepsilon p^{\frac{1}{2}+\varepsilon}.$$

In fact, we prove a more general statement (cf. Theorem 3.1) which recently appeared in [2] and also holds for λ-roots, a certain generalization of primitive roots to composite moduli. As for the proof, we utilize the usual characterization of sums of two squares in terms of their prime decomposition to translate the problem into a sieve problem of sieve-dimension 1/2. Following ideas of Martin [74], the assertion is then proved by a standard lower bound sieve and Burgess' bound for short character sums [15].

Part II. Here, we elaborately deal with the above-mentioned problems concerning number fields and illuminate Questions 1 and 2. In Chapter 4 we give motivation for these questions, discuss Wagstaff's heuristic in detail and explain the difficulties which prevent adequate estimates for the average order of $\mathrm{ind}_a(p)$. Moreover, we provide a list of tools for prime and prime ideal estimates which are essential for the treatment of these problems and even beyond in Part III. Most of these have already been mentioned before. In Chapters 5, 6 and 7, we then study variations of Questions 1 and 2.

Concerning Question 1. Let $\mathbb{K}$ and Γ be as above, $\kappa > 0$ some real number, $\mathbb{L}$ a finite Galois extension of $\mathbb{K}$ and C a conjugacy class inside the Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. In Chapter 5, we shed some light on Question 1 and study κ-th moments of $\mathrm{ord}_\Gamma(\mathfrak{p})$ over prime ideals in $\mathcal{P}_C(\mathbb{L}/\mathbb{K})$, i.e. prime ideals of $\mathbb{K}$ which are unramified in $\mathbb{L}$ and whose Frobenius symbol inside $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ equals C. Adapting ideas of Kurlberg and Pomerance [51] to number fields, we prove the following result which confirms that $\mathrm{ord}_\Gamma(\mathfrak{p})$ equals a positive multiple of $\mathcal{N}\mathfrak{p}$ on average (cf. Theorem 5.3).

Theorem 2. *Assume GRH. Then there exists an explicitly computable positive constant $c_{\Gamma,C}^{(\kappa)}$ depending on Γ, C, $\mathbb{L}$, $\mathbb{K}$ and κ such that, as $x \to \infty$, we have*

$$\sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ \overline{\Gamma} \subset (\mathcal{O}_\mathbb{K}/\mathfrak{p})^*}} \mathrm{ord}_\Gamma(\mathfrak{p})^\kappa \sim c_{\Gamma,C}^{(\kappa)} \cdot \mathrm{li}(x^{\kappa+1}). \tag{2}$$

Here, $\mathcal{P}_C(x, \mathbb{L}/\mathbb{K})$ consists of those $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}/\mathbb{K})$ which have $\mathcal{N}\mathfrak{p} \leq x$ and, as usual, $\mathrm{li}(x)$ denotes the logarithmic integral of x. Just as in the work of Kurlberg and Pomerance [51], we apply combinatorial arguments combined with standard techniques from algebraic number theory to reduce the problem to estimating sets of prime ideals with certain splitting conditions in Kummer extensions of $\mathbb{L}$. This task is then attended by the Brun-Titchmarsh inequality and an effective Čebotarev density theorem under GRH.

It should be mentioned that, even though we prove an explicit infinite sum expression for $c_{\Gamma,C}^{(\kappa)}$, this does not reveal its positivity, since the sum alternates and involves complicated field degree expressions. Instead, we establish its positivity only on GRH by bounding the left side of (2) from below. However, we expect the positivity to hold unconditionally, and affirm this by computing $c_{\Gamma,C}^{(\kappa)}$ in terms of Euler products for two popular families of field extensions $\mathbb{L}/\mathbb{K}$ (cf. Theorems 5.14 and 5.17).

As brought up above, it is rather hopeless to study moments of $\mathrm{ind}_\Gamma(\mathfrak{p})$, so we consider this problem on average over Γ in Chapter 6. To make this precise, we define

$$\mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) := \sum_{a_1, \dots, a_\gamma \in (\mathcal{O}_\mathbb{K}/\mathfrak{p})^*} \frac{\mathrm{ind}_{\langle a_1, \dots, a_\gamma \rangle}(\mathfrak{p})^\kappa}{(\mathcal{N}\mathfrak{p} - 1)^\gamma}, \tag{3}$$

for any prime ideal $\mathfrak{p}$ of $\mathbb{K}$. Here, $\gamma \geq 1$ denotes the arithmetic rank of Γ, and $\langle a_1, \dots, a_\gamma \rangle$ is the subgroup of $(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*$ generated by the a_i. Under the assumption that the reduction of Γ inside $(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*$ resembles a generic subgroup therein, $\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$ may be seen as an adequate approximation for $\mathrm{ind}_\Gamma(\mathfrak{p})^\kappa$. Due to the additional averaging step, we are able to prove the following precise asymptotic formulae for the average order of $\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$ which confirm appropriate variations of Wagstaff's heuristic (cf. Theorem 6.1).

THEOREM 3. *There exist explicitly computable positive constants $A(\gamma,\kappa)$, depending on γ, κ, $\mathbb{K}$, $\mathbb{L}$ and C such that, as $x\to\infty$, we have*

$$x \ll_{\mathbb{L}} \sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\gamma(\mathfrak{p}) \ll_{\mathbb{K}} x, \tag{4}$$

and

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) \sim \begin{cases} A(\gamma,\kappa)\cdot \mathrm{li}(x) & \text{if } \kappa<\gamma,\\ A(\gamma,\kappa)\cdot \mathrm{li}\left(x^{\kappa-\gamma+1}\right) & \text{if } \kappa>\gamma. \end{cases}$$

Just as in Chapter 5, combinatorial and standard arguments from algebraic number theory break down the proof to estimating certain sets of prime ideals which we overcome by the Brun-Titchmarsh inequality in combination with an unconditional effective Čebotarev density theorem in case $\gamma\neq\kappa$, and number field analogues of the Bombieri-Vinogradov theorem in case $\kappa=\gamma$, where the former does not apply. Under the additional assumption that $\mathbb{L}/\mathbb{Q}$ and $\mathbb{K}/\mathbb{Q}$ are both Galois (cf. Theorem 6.2), we can explicitly compute $A(\gamma,\kappa)$ in terms of the Riemann zeta function and Euler products. Moreover, (4) may then be replaced by an asymptotic equivalence, if one either utilizes an effective Čebotarev density theorem under GRH or number field analogues of the Bombieri-Vinogradov theorem which are only applicable in certain cases. Theorem 3 and the stated variations are to appear in [1].

In Chapter 6, we also briefly discuss how the same techniques apply to study

$$\mathrm{Ord}_\gamma^\kappa(\mathfrak{p}) := \sum_{a_1,\dots,a_\gamma\in(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*} \frac{\mathrm{ord}_{\langle a_1,\dots,a_\gamma\rangle}(\mathfrak{p})^\kappa}{(\mathcal{N}\mathfrak{p}-1)^\gamma} \tag{5}$$

on average over $\mathfrak{p}\in\mathcal{P}_C(\mathbb{L}/\mathbb{K})$. This task turns out to be a lot easier and an unconditional effective Čebotarev density theorem should yield asymptotic formulae which generalize the aforesaid work of LUCA [69] and are in line with Theorem 2. We abstain from going into detail, for the only advantage over Theorem 2 would be a relaxation of the GRH.

Another issue addressed in Chapter 6 is the question, whether one may reduce the summation ranges for the a_i in (3) and (5) to smaller subsets of $(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*$ without effecting the asymptotic behaviour as $\mathcal{N}\mathfrak{p}\to\infty$. To this end, we approximate (3) and (5) by inserting certain "smooth" weight functions. Applying a higher dimensional Poisson summation formula in connection with estimates for higher dimensional Gauß sums, we indeed manage to reduce the summation ranges slightly for the residual index and to a larger amount for the residual order (cf. Theorems 6.13 and 6.18).

Concerning Question 2. In Chapter 7, we address Question 2, or more precisely, the estimation of κ-th moments of $\mathrm{ind}_\Gamma(\mathfrak{a})$ over all ideals of $\mathbb{K}$ for $\kappa>0$. As the main result of this chapter (cf. Theorems 7.1 and 7.2), we prove a slightly stronger version of the following result which will be published in [1]:

THEOREM 4. *As $x\to\infty$, we have*

$$\sum_{\substack{\mathcal{N}\mathfrak{a}\le x\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{a})^*}} \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa \ge \begin{cases} x^{\kappa+0.69+o(1)}, & \text{if } \mathbb{K} \text{ is abelian over } \mathbb{Q},\\ x^{\kappa+0.5+o(1)}, & \text{under GRH.} \end{cases}$$

This result is very surprising in view of the fact that $\mathrm{ind}_\Gamma(\mathfrak{a})$ is typically rather small. Nevertheless, it turns out that there are sufficiently many "highly composite" ideals $\mathfrak{a}$ of $\mathbb{K}$ for which $\mathrm{ind}_\Gamma(\mathfrak{a})$ is exceptionally large, and it is the bottom line of the proof to construct

sufficiently many such ideals. We overcome this problem by a number field adaption of a construction method due to Luca and Sankaranarayanan [70] that indeed gives us

$$\sum_{\substack{\mathcal{N}\mathfrak{a}\leq x\\ \overline{\Gamma}\subset(\mathcal{O}_{\mathbb{K}}/\mathfrak{a})^*}} \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa \geq x^{1+\kappa-\delta+o(1)},$$

with any $\delta > 0$ for which there are "sufficiently many" prime ideals of $\mathbb{K}$ with $\mathcal{N}\mathfrak{p} \leq y$ such that the largest prime divisor of $\mathcal{N}\mathfrak{p}-1$ is less than y^δ. The problem therefore reduces to establishing admissible values δ in virtue of the exponents in Theorem 4, the hardest part of the proof. We attend this problem by generalizing ideas of Balog [6] and Friedlander [34] to number fields. For that purpose, we again make intense use of the Brun-Titchmarsh inequality and effective versions of the Čebotarev density theorem under GRH, or alternatively the Bombieri-Vinogradov theorem if $\mathbb{K}^{(n)}/\mathbb{Q}$ is abelian. Moreover, we utilize a transition between the Brun-Titchmarsh inequality and the Bombieri-Vinogradov theorem due to Bombieri, Friedlander and Iwaniec [11] which enables appropriate estimates for primes in arithmetic progressions to large moduli.

It should be mentioned that any $\delta > 0$ is widely conjectured to be admissible in the above sense. Hence, we expect the surprising lower bound

$$\sum_{\substack{\mathcal{N}\mathfrak{a}\leq x\\ \overline{\Gamma}\subset(\mathcal{O}_{\mathbb{K}}/\mathfrak{a})^*}} \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa \geq x^{1+\kappa+o(1)}$$

which, in view of the trivial upper bound $x^{1+\kappa}$, would determine the asymptotic behaviour of the κ-th moment of $\mathrm{ind}_\Gamma(\mathfrak{a})$ up to a factor of $x^{o(1)}$.

Part III. In this last part, we eventually leave the number field setting and focus on elliptic curves. After a brief introduction in Chapter 8, where basic facts about elliptic curves are provided, we study variations of Questions 3 and 4 in Chapters 9 and 10.

Concerning Question 3. In Chapter 9 we let $\kappa > 0$, fix a rational elliptic curve E and address Question 3 by studying κ-th moments of $\mathrm{ord}_Q(\mathrm{E}_p)$ on average over Q. To this end, we choose a similar approach as in Chapter 6 and define

$$\mathrm{Ord}^\kappa(\mathrm{E}_p) := \sum_{Q\in\mathrm{E}_p(\mathbb{F}_p)} \frac{\mathrm{ord}_Q(\mathrm{E}_p)^\kappa}{\sharp\,\mathrm{E}_p(\mathbb{F}_p)}, \tag{6}$$

for primes p of good reduction for E. We prove the following result (cf. Theorem 9.1) which suggests that $\mathrm{ord}_Q(\mathrm{E}_p)$ should indeed equal a positive multiple of p on average.

Theorem 5. *If* E *has CM by the ring of integers of an imaginary quadratic field, or under GRH if* E *is a non-CM curve, there exists a positive constant* $c_{\mathrm{E}}^{(\kappa)}$ *depending on* κ *and* E *such that, as* $x \to \infty$*, we have*

$$\sum_{\substack{p\leq x\\ p\ of\ g.\ r.}} \mathrm{Ord}^\kappa(\mathrm{E}_p) \sim c_{\mathrm{E}}^{(\kappa)} \cdot \mathrm{li}(x^{1+\kappa}). \tag{7}$$

The main obstacle here is the non-cyclicity of $\mathrm{E}_p(\mathbb{F}_p)$ in general which we already mentioned above. Nevertheless, to prove Theorem 5, we basically proceed as in Chapter 6 and reduce the problem to counting primes with splitting conditions in certain number fields. We estimate these primes by the Brun-Titchmarsh inequality and effective versions of the Čebotarev density theorem. While we need to utilize the latter under GRH if E has no CM, the assumption of the GRH can be circumvented in the CM case by number

field analogues of the Brun-Titchmarsh inequality available in this case. In this way, we obtain (7) with $c_{\mathrm{E}}^{(\kappa)}$ given by an alternating sum whose positivity, similar to Chapter 5, is not obvious from its definition and is confirmed by lower bounds for the left side of (7) which are established with the help of a result of Duke [22].

Concerning Question 4. In Chapter 10, we let $\kappa > 0$, fix a prime $p > 3$, and give an account of Question 4. We consider elliptic curves given by the two-parameter family

$$\mathrm{E}_{a,b}: \quad y^2 \equiv x^3 + ax + b \ (p),$$

where the integers a and b satisfy $4a^3 + 27b^2 \not\equiv 0 \ (p)$, and are taken from some box $|a| \le A$, $|b| \le B$ with parameters $1 \le A, B \le (p-1)/2$. We remain true to our universal framework and model "typical" values for κ-th powers of residual index and residual order of points in $\mathrm{E}_{a,b}(\mathbb{F}_p)$ by $\mathrm{Ind}^\kappa(\mathrm{E}_{a,b})$ and $\mathrm{Ord}^\kappa(\mathrm{E}_{a,b})$ which are defined similar to (6). The precise challenge we are facing is to establish adequate asymptotic estimates for the average orders of these quantities and simultaneously choose A and B as small as possible without effecting the accuracy of these estimates. In fact, we prove the following result which combines Theorems 10.1–10.4 and suggests that residual index and order are typically small and large in $\mathrm{E}_{a,b}(\mathbb{F}_p)$, respectively, just as expected.

Theorem 6. *There exist explicitly computable finite sums $M_{\mathrm{Ord}}(p,\kappa)$ and $M_{\mathrm{Ind}}(p,\kappa)$, given in terms of Kronecker class numbers of binary quadratic forms, which only depend on p and κ such that:*

(i) *As $p \to \infty$, we have*

$$\frac{1}{4AB} \sum_{\substack{|a|\le A, |b|\le B \\ p\nmid 4a^3+27b^2}} \mathrm{Ord}^\kappa(\mathrm{E}_{a,b}) \sim M_{\mathrm{Ord}}(p,\kappa),$$

whenever A and B satisfy $\min(A,B) \ge p^{\frac{1}{4}+\varepsilon}$ and $AB \ge p^{1+\varepsilon}$.

(ii) *As $p \to \infty$, we have*

$$\frac{1}{4AB} \sum_{\substack{|a|\le A, |b|\le B \\ p\nmid 4a^3+27b^2}} \mathrm{Ind}^\kappa(\mathrm{E}_{a,b}) \sim M_{\mathrm{Ind}}(p,\kappa),$$

whenever A and B are chosen according to:

a) $\min(A,B) \ge p^{\frac{1}{4}+\varepsilon}$ *and* $AB \ge p^{1+\varepsilon}$, *if* $\kappa \ge 3$,

b) $\min(A,B) \ge p^{\frac{1}{4}+\varepsilon}$ *and* $AB \ge p^{2-\delta}$, *with some* $\delta > 0$, *if* $1 \le \kappa < 3$,

c) $A = B = (p-1)/2$, *if* $0 < \kappa < 1$.

Moreover, as $p \to \infty$, we have

$$M_{\mathrm{Ord}}(p,\kappa) = p^{\kappa+o(1)} \qquad \text{and} \qquad M_{\mathrm{Ind}(p,\kappa)} = p^{\max\{\kappa-1,0\}+o(1)}.$$

The main ingredient for the proof is a result due to Banks and Shparlinski [7] concerning the distribution of isomorphism classes of elliptic curves defined over $\mathbb{F}_p$ along the family $\mathrm{E}_{a,b}$. From this we infer that, for A and B as in Theorem 6, the sums over $|a| \le A$, $|b| \le B$ are asymptotically equivalent to the corresponding completed versions which sum over all admissible tupels (a,b) from $\mathbb{F}_p^2$. Elementary combinatorial arguments and insights of Deuring [21], Waterhouse [104] and Schoof [92] then allow us to express these completed sums in terms of Kronecker class numbers of binary quadratic forms which yields the first part of Theorem 6. The asymptotic formulae for $M_{\mathrm{Ord}}(p,\kappa)$ and $M_{\mathrm{Ind}}(p,\kappa)$ are derived by standard estimates for L-functions and a result of Vlăduţ.

Notation and Terminology

In the sequel, we introduce notation and terminology which is used most frequently throughout this thesis. A decent treatment of elliptic curves is postponed to Chapter 8, for structural convenience. We assume that the reader is familiar with basic concepts from set theory, algebra, analysis and arithmetic and refer to the accompanied literature for further information. An extensive summary of commonly used notation is provided in the List of Notations and the Index at the end of this thesis.

Numbers and arithmetic functions. As usual, the symbols $\mathbb{N}, \mathbb{Z}, \mathbb{Q}, \mathbb{R}$ and $\mathbb{C}$ denote the positive integers, the integers, the rational, real, and complex numbers, respectively. By $\mathbb{R}_+$ we mean the positive and by $\mathbb{R}_-$ the negative real numbers. The letter p, possibly with subscripts, always refers to a rational prime. For integers a and b we write $a \mid b$ if a divides b and $a \nmid b$ if this is not the case. We write $[a, b]$ for the least common multiple of a and b and, if $(a, b) \neq (0, 0)$, then (a, b) denotes their greatest common divisor. If $a_1, \ldots, a_n$ is an arbitrary family of integers we denote its least common multiple by $\operatorname{lcm}(a_1, \ldots, a_n)$ and, if $(a_1, \ldots, a_n) \neq (0, \ldots, 0)$, its greatest common divisor is denoted by $\gcd(a_1, \ldots, a_n)$. For a prime p, $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ we write $p^n \| a$, if $p^n \mid a$ but $p^{n+1} \nmid a$.

For any $n \in \mathbb{N}$, Euler's totient function $\varphi(n)$, Carmichael's lambda function $\lambda(n)$, the Möbius function $\mu(n)$ and the divisor function $\tau(n)$ have their common meanings. By $\sigma_\kappa(n)$ we denote the sum of κ-th powers of divisors of n for any $\kappa \in \mathbb{R}$, and we simply write $\sigma(n)$ in case $\kappa = 1$. By $\operatorname{rad}(n)$ we understand the largest squarefree divisor of n. The number of distinct prime divisors of n is counted by $\omega(n)$ and $P^+(n)$ denotes the largest prime factor of n, or 1 if $n = 1$. Finally, for any prime p, the p-adic valuation of $a \in \mathbb{Z}$ is given by $\nu_p(a)$, and for any $b \in \mathbb{N}$, $\left(\frac{a}{b}\right)$ denotes the corresponding Legendre-Jacobi symbol. See [45, 100] for more information on arithmetic functions.

Groups. The cardinality of a finite set M is denoted by either $|M|$ or $\sharp M$ and by M^n we mean the cartesian or direct product of n copies of M. If two groups G and G' are isomorphic, we express this by writing $G \cong G'$ and we write $G_1 \oplus \cdots \oplus G_n$ or $\bigoplus_{i=1}^n G_i$ for the direct sum of groups $G_1, \ldots, G_n$. The subgroup of a group G generated by elements $a_1, \ldots, a_n \in G$ is denoted by $\langle a_1, \ldots, a_n \rangle$. If D is a union of conjugacy classes of some finite group G, we write $\|D\|$ for the number of conjugacy classes contained in D, and by C_n we understand the cyclic group with n elements.

Rings and ideals. Let R be a commutative ring. By R^* we denote the unit group of R and we write $\mathrm{GL}_n(R)$ for the group of invertible $n \times n$ matrices with entries in R. The determinant of an arbitrary $n \times n$ matrix A over R is denoted by $\det(A)$, and we also write $\det(A)$ for the determinant of an endomorphism A of a finite-dimensional vector space over some field. The subgroup of matrices A of $\mathrm{GL}_n(R)$ with $\det(A) = 1$ is denoted by $\mathrm{SL}_n(R)$. Principal ideals of R generated by an element r are either denoted by (r) or rR. If $\mathcal{I}$ is an ideal of R, then we denote the associated residue ring by $R/\mathcal{I}$ and its

elements by a mod $\mathcal{I}$ with $a \in R$. If a and b yield the same residue class modulo $\mathcal{I}$, we write $a \equiv b \bmod I$ or simply $a \equiv b\ (r)$, if $\mathcal{I} = (r) = rR$ is a principal ideal.

Fields. Let $\mathbb{F}$ be an arbitrary field. We denote its characteristic by $\mathrm{char}(\mathbb{F})$ and by $\overline{\mathbb{F}}$ we mean an algebraic closure of $\mathbb{F}$. If $\mathbb{F}'$ is another field, we express by $\mathbb{F}' \,/\, \mathbb{F}$ that $\mathbb{F}'$ is a field extension of $\mathbb{F}$ and we write $\mathrm{Gal}(\mathbb{F}' \,/\, \mathbb{F})$ for the corresponding Galois group if $\mathbb{F}' \,/\, \mathbb{F}$ is a Galois extension. Elements of $\mathrm{Gal}(\mathbb{F}' \,/\, \mathbb{F})$ are usually denoted by σ or τ and we write $\sigma|_{\mathbb{F}''}$ for the restriction of σ to any subfield $\mathbb{F}''$ of $\mathbb{F}'$. By id we always mean the identity map. If the extension $\mathbb{F}' \,/\, \mathbb{F}$ is finite, we denote its degree by $[\mathbb{F}' : \mathbb{F}]$. For any subset M of $\mathbb{F}'$ the field $\mathbb{F}(M)$ denotes the field extension of $\mathbb{F}$ which is obtained by adjoining all elements of M to $\mathbb{F}$, i.e. the unique subfield of $\mathbb{F}'$ which contains $\mathbb{F}$ as well as M. Note that we will usually omit set braces, for convenience. The composite field of two fields $\mathbb{F}''$ and $\mathbb{F}'$ is denoted by $\mathbb{F}'' \cdot \mathbb{F}'$. If $\mathbb{F}''$ and $\mathbb{F}'$ are field extensions of $\mathbb{F}$, then the extension $\mathbb{F}'' \cdot \mathbb{F}' \,/\, \mathbb{F}$ is called a *direct product* of the extensions $\mathbb{F}'' \,/\, \mathbb{F}$ and $\mathbb{F}' \,/\, \mathbb{F}$, if $\mathbb{F}'' \cap \mathbb{F}' = \mathbb{F}$. By $\mathbb{F}'' \otimes_{\mathbb{F}} \mathbb{F}'$, we denote the tensor product of $\mathbb{F}''$ and $\mathbb{F}'$ over $\mathbb{F}$. A *quadratic field* always refers to a field $\mathbb{Q}(\sqrt{d})$ with some squarefree non-zero integer d, and it is called *imaginary quadratic* if $d < 0$, and *real quadratic* if $d > 0$. Finally, $\mathbb{F}_q$ always denotes a finite field with q elements. More information on rings and fields is provided in [12, 46, 55].

Number fields and algebraic integers. *Number fields*, i.e. finite field extensions of $\mathbb{Q}$, are denoted by $\mathbb{K}$, $\mathbb{L}$ and $\mathbb{M}$ with or without subscripts. $\mathbb{L}$ will usually refer to an extension of $\mathbb{K}$. By $\mathbb{K}^{(n)}$ and $\mathbb{K}^{ab}$ we denote a normal closure of $\mathbb{K} \,/\, \mathbb{Q}$ and the largest subfield of $\mathbb{K}$ which is abelian over $\mathbb{Q}$, respectively. For an extension $\mathbb{L} \,/\, \mathbb{K}$ of number fields we let $\mathrm{N}_{\mathbb{L} \,/\, \mathbb{K}}$ denote the associated norm map. By $\mathcal{O}_{\mathbb{K}}$ and $\mathcal{U}_{\mathbb{K}}$ we mean the ring of (algebraic) integers of $\mathbb{K}$ and its unit group, respectively. The discriminant of $\mathbb{K}$ is denoted by $\Delta_{\mathbb{K}}$ and by $\zeta_{\mathbb{K}}(s)$ we mean the associated Dedekind zeta function which yields the Riemann zeta function $\zeta(s)$ if $\mathbb{K} = \mathbb{Q}$. The *generalized Riemann hypothesis* or simply *GRH for* $\mathbb{K}$ asserts that all non-trivial zeroes of $\zeta_{\mathbb{K}}(s)$ have real part $1/2$. Omitting the suffix "for $\mathbb{K}$" either indicates that the GRH is assumed for all number fields or that it is clear from the context for which family the assumption is made. By ζ_n we always mean a primitive n-th root of unity in $\mathbb{C}$.

An *ideal of* $\mathbb{K}$ will always refer to an ideal of $\mathcal{O}_{\mathbb{K}}$. Such ideals are denoted by Fraktur letters $\mathfrak{a}$ with or without subscripts and prime ideals are usually represented by $\mathfrak{p}$ or $\mathfrak{P}$. For any ideal $\mathfrak{a}$ of $\mathbb{K}$ the cardinality of $\mathcal{O}_{\mathbb{K}} \,/\, \mathfrak{a}$ is denoted by $\mathcal{N}\,\mathfrak{a}$. By $\mathfrak{a} \mid \mathfrak{a}'$ we express that $\mathfrak{a}$ divides $\mathfrak{a}'$ in the sense of Dedekind. If $\mathfrak{a}'$ is a principal ideal we may replace it by a generator in this notation. If $\mathbb{L} \,/\, \mathbb{K}$ is an extension of number fields and $\mathfrak{P}$ and $\mathfrak{p}$ prime ideals of $\mathbb{L}$ and $\mathbb{K}$, respectively, such that $\mathfrak{P} \cap \mathbb{K} = \mathfrak{p}$ holds, we write $\mathfrak{P} \mid \mathfrak{p}$ and say that $\mathfrak{P}$ *lies over* $\mathfrak{p}$. In case $\mathbb{K} = \mathbb{Q}$ and $\mathfrak{p} = p\,\mathbb{Z}$, we simply write $\mathfrak{P} \mid p$. A prime ideal $\mathfrak{p}$ is called a *linear prime ideal*, if $\mathfrak{p}$ is unramified over $\mathbb{Q}$ with inertia degree 1 over its underlying prime number.

Let $\mathbb{K}$ be number field and Γ a finitely generated subgroup of $\mathbb{K}^*$. If $\mathfrak{a}$ is an ideal of $\mathbb{K}$ for which the $\mathfrak{p}$-adic valuation of a is zero for any $a \in \Gamma$ and any prime ideal $\mathfrak{p} \mid \mathfrak{a}$ of $\mathbb{K}$, we express this by $\overline{\Gamma} \subset (\mathcal{O}_{\mathbb{K}} \,/\, \mathfrak{a})^*$, where $\overline{\Gamma}$ denotes the reduction of Γ in $\mathcal{O}_{\mathbb{K}} \,/\, \mathfrak{a}$. Whenever $\overline{\Gamma} \subset (\mathcal{O}_{\mathbb{K}} \,/\, \mathfrak{a})^*$ holds, we define the *residual index* $\mathrm{ind}_{\Gamma}(\mathfrak{a})$ and the *residual order* $\mathrm{ord}_{\Gamma}(\mathfrak{a})$ *of* Γ *modulo* $\mathfrak{a}$ as the index and order of $\overline{\Gamma}$ in $(\mathcal{O}_{\mathbb{K}} \,/\, \mathfrak{a})^*$, respectively. We use the same notation if Γ itself is a subgroup of $(\mathcal{O}_{\mathbb{K}} \,/\, \mathfrak{a})^*$. If Γ is generated by a single element a we write $\mathrm{ind}_a(\mathfrak{a})$ and $\mathrm{ord}_a(\mathfrak{a})$, for convenience. Also, we will write $\mathrm{ind}_a(\alpha)$ and $\mathrm{ord}_a(\alpha)$ if $\mathfrak{a}$ is a principal ideal generated by $\alpha \in \mathcal{O}_{\mathbb{K}}$. For any $n \in \mathbb{N}$, we define $\mathbb{K}_{\Gamma,n} := \mathbb{K}(\zeta_n, \sqrt[n]{\Gamma})$ as the finite Galois extension of $\mathbb{K}$ obtained by adjoining all n-th roots of elements of Γ. Note

that $\mathbb{K}_{\Gamma,n}$ becomes $\mathbb{K}(\zeta_n)$ if one chooses $\Gamma = \{1\}$. If Γ is generated by a single element $a \in \mathbb{K}$, we simply write $\mathbb{K}_{a,n}$ instead.

For any number field $\mathbb{K}$ we denote by $\mathcal{P}(\mathbb{K})$ the set of all prime ideals $\mathfrak{p}$ of $\mathbb{K}$. If $\mathbb{L}$ is a finite Galois extension of $\mathbb{K}$ and $\mathfrak{p} \in \mathcal{P}(\mathbb{K})$ is unramified in $\mathbb{L}$, then $\left[\frac{\mathbb{L}|\mathbb{K}}{\mathfrak{p}}\right]$ denotes the *Frobenius symbol* inside $\mathrm{Gal}(\mathbb{L}\,/\,\mathbb{K})$, i.e. the conjugacy class inside $\mathrm{Gal}(\mathbb{L}\,/\,\mathbb{K})$ of all Frobenius automorphisms corresponding to prime ideals $\mathfrak{P}$ of $\mathbb{L}$ which lie over $\mathfrak{p}$. If C is a union of conjugacy classes inside $\mathrm{Gal}(\mathbb{L}\,/\,\mathbb{K})$, then $\mathcal{P}_C(\mathbb{L}\,/\,\mathbb{K})$ shall denote the set of all prime ideals $\mathfrak{p}$ of $\mathbb{K}$, unramified in $\mathbb{L}$, which satisfy $\left[\frac{\mathbb{L}|\mathbb{K}}{\mathfrak{p}}\right] \subset C$. Prime ideals which satisfy such a property are often said to have a certain *splitting behaviour* or satisfy a certain *splitting condition* in $\mathbb{L}$. For explanation and further details we refer to [54, 68, 86].

Analytic number theory. For any complex number x, we denote by $|x|$ denotes its absolute value, by $\overline{x}$ its complex conjugate and we write interchangeably either $\exp(x)$ or e^x, where e denotes Euler's constant. Further, we set $e(x) := \exp(2\pi i x)$, where the imaginary unit i and π have their common meanings. If $x \in \mathbb{R}_+$, the natural logarithm of x is denoted by $\log x$, $\mathrm{li}(x) := \int_2^x dt/\log t$ shall denote the *logarithmic integral* of x and for any real number α we will often write $\log^\alpha x$ instead of $(\log x)^\alpha$.

For two complex valued functions $f, g : D \to \mathbb{C}$ defined on some infinite set $D \subset \mathbb{R}$, we write $f(x) \ll g(x)$, $g(x) \gg f(x)$, or $f(x) = O(g(x))$ synonymously, if there exists a positive constant c, the so called *implied constant*, such that $|f(x)| \leq c \cdot |g(x)|$ holds for all $x \in D$. If we want to stress a dependency of c on some parameter t, we add t as a subscript and write $\ll_t$, $\gg_t$ and O_t instead. If $f(x)$ and $g(x)$ are *asymptotically equivalent*, i.e. $\lim_{x\to\infty} f(x)/g(x) = 1$, we write $f(x) \sim g(x)$, as $x \to \infty$, and we write $f(x) = o(g(x))$ if $\lim_{x\to\infty} f(x)/g(x) = 0$. By an *effective version* of an asymptotic equivalence $f(x) \sim g(x)$ we mean an asymptotic formula of the form

$$f(x) = g(x) + o(g(x)).$$

The error terms in such a formula are often denoted by the letter E with or without subscripts.

Let $\mathbb{K}$ be a number field, T an infinite set of ideals of $\mathbb{K}$ and S a subset of T. If

$$\lim_{x\to\infty} \frac{\sharp\{\mathfrak{a} \in S : \mathcal{N}\mathfrak{a} \leq x\}}{\sharp\{\mathfrak{a} \in T : \mathcal{N}\mathfrak{a} \leq x\}}$$

exists and equals some $\delta \in \mathbb{R}$, then we say that S has *natural density* δ in T, and we write $\boldsymbol{\delta}(S)$ for this density if T is clear from the context. As the corresponding results in this thesis also remain true in the context of Dirichlet density, we usually write *density* instead of natural density. Eventually, a property is said to hold for *almost all* elements of T if the subset of T on which it fails has density zero in T.

As usual, we denote by $\pi(x)$ and $\pi(x; a, q)$ the number of primes $p \leq x$ and the number of primes $p \leq x$ which satisfy $p \equiv a \ (q)$, with $a \in \mathbb{Z}$ and $q \in \mathbb{N}$. Primes of the latter form are called *primes in the arithmetic progression* a *modulo* q or simply *primes in arithmetic progression*. By the *prime number theorem* and Dirichlet's *prime number theorem for primes in arithmetic progression*, we have

$$\pi(x) \sim \mathrm{li}(x) \sim \frac{x}{\log x} \qquad \text{and} \qquad \pi(x; a, q) \sim \frac{\pi(x)}{\varphi(q)},$$

as $x \to \infty$, provided that a and q are coprime. That is, primes in the arithmetic progression a modulo q have density $1/\varphi(q)$ in the set of all primes. If $\mathbb{L}\,/\,\mathbb{K}$ is a Galois extension of number fields and C a union of conjugacy classes in $\mathrm{Gal}(\mathbb{L}\,/\,\mathbb{K})$, then $\mathcal{P}(x, \mathbb{K})$ and

$\mathcal{P}_C(x, \mathbb{L}\,/\,\mathbb{K})$ denote the set of $\mathfrak{p} \in \mathcal{P}(\mathbb{K})$ and $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}\,/\,\mathbb{K})$ with $\mathcal{N}\mathfrak{p} \leq x$, respectively. The corresponding counting functions are denoted by $\pi(x, \mathbb{K})$ and $\pi_C(x, \mathbb{L}\,/\,\mathbb{K})$. The *prime ideal theorem* and the *Čebotarev density theorem* state

$$\pi(x, \mathbb{K}) \sim \operatorname{li}(x) \qquad \text{and} \qquad \pi_C(x, \mathbb{L}\,/\,\mathbb{K}) \sim \frac{\sharp C}{[\mathbb{L} : \mathbb{K}]} \cdot \pi(x, \mathbb{K}),$$

as $x \to \infty$, respectively, if C is not empty. This generalizes the above formulae for $\pi(x)$ and $\pi(x; a, q)$ and implies that $\mathcal{P}_C(\mathbb{L}\,/\,\mathbb{K})$ has density $\sharp C/[\mathbb{L} : \mathbb{K}]$ in $\mathcal{P}(\mathbb{K})$. For more details on analytic number theory, the reader should consult [**13**, **45**, **54**, **100**].

Part I

Artin's Primitive Root Conjecture and Related Problems

CHAPTER 1

Artin's Primitive Root Conjecture

Since Artin stated his celebrated conjecture in 1927, numerous mathematicians have been attracted by this problem. Nevertheless, despite all effort made, Artin's primitive root conjecture remains unresolved to date.

It is the purpose of this chapter to continue our historical outline started in the Introduction. On the one hand, we will go into Artin's intuition in Section 1.1 and retrace the ideas which led him to his conjecture and appear frequently in connection with related problems, as we will see later on. On the other hand, we will present the development of this problem by stating the most important improvements towards a resolution in Sections 1.2 and 1.3 and briefly explain the methods which underlie these. Our account basically builds on the survey papers [75] of Moree and [80] of Ram Murty, the articles [31, 57] and the *Collected Papers* [3] of Artin. We refer to these resources for more information.

1.1. Artin's intuition

To start with, we give a precise formulation of *Artin's primitive root conjecture (AC)*.

Conjecture 1.1 (Artin, 1927). *Let a be an integer different from $0, \pm 1$ and not a square. Then there are infinitely many primes p such that a is a primitive root modulo p. Moreover, the set of such primes has a positive density inside the set of all primes, i.e., if $N_a(x)$ counts the number of such primes $\leq x$, there exists a positive constant $\delta_a \in (0, 1]$ depending on a such that*

$$N_a(x) \sim \delta_a \cdot \frac{x}{\log x},$$

as $x \to \infty$.

This conjecture naturally divides into two variants: A *qualitative AC*, asserting the infinitude of primes for which a is a primitive root, and a stronger *quantitative AC* which predicts that these primes even yield a positive portion of all rational primes. Clearly, the quantitative AC implies the qualitative one. As for the constraints on a in Conjecture 1.1, it is rather easy to verify their necessity for either of these variants. If a is either 0 or ± 1 this is obvious, and if a is a square and p odd, then it is impossible for a to generate any of the $(p-1)/2$ non-squares modulo p.

Let us now recapitulate Artin's intuition which led him to Conjecture 1.1 and a precise formula for the predicted density δ_a. The starting point of his arguments is the simple observation that an integer a fails to be a primitive root modulo $p \nmid a$ if and only if there exists a prime divisor q of $p-1$ such that

$$a^{(p-1)/q} \equiv 1 \ (p). \tag{1.1}$$

By a famous result from algebraic number theory due to Dedekind (cf. [86, p. 50]), this condition is equivalent to a specific splitting behaviour of p in certain number fields. Indeed, the condition $q \mid p-1$ is equivalent to the complete splitting of p in the cyclotomic

field $\mathbb{Q}(\zeta_q)$, and the additional condition (1.1) is true if and only if the congruence

$$X^q \equiv a \ (p)$$

admits exactly q distinct roots modulo p which is equivalent to the complete splitting of p in $\mathbb{Q}(\sqrt[q]{a})$ for some q-th root of a. Consequently, a is a primitive root modulo $p \nmid a$ if and only if p does not split completely in the Kummer field $\mathbb{Q}_{a,q} = \mathbb{Q}(\sqrt[q]{a}, \zeta_q)$ for any prime q. The latter is equivalent to saying that p is not contained in $\mathcal{P}_{\{\mathrm{id}\}}(\mathbb{Q}_{a,q} \,/\, \mathbb{Q})$, by standard properties of the Frobenius symbol [68, p. 124]. The density proposed by Conjecture 1.1, if it exists, would therefore equal

$$\boldsymbol{\delta}\left(\bigcap_q \left(\mathcal{P}(\mathbb{Q}) \setminus \mathcal{P}_{\{\mathrm{id}\}}(\mathbb{Q}_{a,q} \,/\, \mathbb{Q})\right)\right),$$

where the intersection is taken over all primes q. Assuming that the sets $\mathcal{P}_{\{\mathrm{id}\}}(\mathbb{Q}_{a,q} \,/\, \mathbb{Q})$ are "independent" in a probabilistic sense, Artin concluded that the conjectural density δ_a should agree with the product[3]

$$\prod_q \left(1 - \boldsymbol{\delta}\left(\mathcal{P}_{\{\mathrm{id}\}}(\mathbb{Q}_{a,q} \,/\, \mathbb{Q})\right)\right)$$

taken over all primes q. By the Čebotarev density theorem, the sets $\mathcal{P}_{\{\mathrm{id}\}}(\mathbb{Q}_{a,q} \,/\, \mathbb{Q})$ have density $1/[\mathbb{Q}_{a,q} : \mathbb{Q}]$. If a is not a q-th power in $\mathbb{Z}$, then the fields $\mathbb{Q}_{a,q}$ have degree $q(q-1)$ over $\mathbb{Q}$. Otherwise, this degree equals $q-1$. Hence, if h denotes the largest integer for which a is a perfect h-th power in $\mathbb{Z}$, Artin proposed the conjectural density

$$\delta(h) := \prod_{p \nmid h} \left(1 - \frac{1}{p(p-1)}\right) \prod_{p \mid h} \left(1 - \frac{1}{p-1}\right), \tag{1.2}$$

a positive rational multiple of the constant

$$\delta_{Artin} := \prod_p \left(1 - \frac{1}{p(p-1)}\right) = 0.3739558136\ldots,$$

commonly known as *Artin's constant*.

Apart from the fact that these arguments are only of a heuristic kind and far away from a rigorous proof, computations by Derrick and Emma Lehmer from 1957 revealed a discrepancy between (1.2) and numerical data. A short correspondence between Artin and the Lehmers started off (see [3, 99] for details) with the effect that Artin became aware of the problem and corrected his conjectural density accordingly. The underlying issue is that the sets $\mathcal{P}_{\{\mathrm{id}\}}(\mathbb{Q}_{a,q} \,/\, \mathbb{Q})$ were assumed to be independent which they are actually not. To make this clear, we observe that a prime splits completely in $\mathbb{Q}_{a,q_1}, \ldots, \mathbb{Q}_{a,q_n}$, with distinct primes q_i, if and only if it splits completely in the composite field $\mathbb{Q}_{a,q_1 \cdots q_n}$. Hence, the sets $\mathcal{P}_{\{\mathrm{id}\}}(\mathbb{Q}_{a,q_1} \,/\, \mathbb{Q}), \ldots, \mathcal{P}_{\{\mathrm{id}\}}(\mathbb{Q}_{a,q_n} \,/\, \mathbb{Q})$ may be considered "independent" if and only if the degree of $\mathbb{Q}_{a,q_1 \cdots q_n}$ over $\mathbb{Q}$ coincides with the product of the degrees of $\mathbb{Q}_{a,q_i}$ over $\mathbb{Q}$. But this is not true in general. An easy example is provided in case $a = 5$, for here one has $\sqrt{a} \in \mathbb{Q}(\zeta_5)$ and therefore

$$[\mathbb{Q}_{a,10} : \mathbb{Q}] = 20 \neq 2 \cdot 20 = [\mathbb{Q}_{a,2} : \mathbb{Q}][\mathbb{Q}_{a,5} : \mathbb{Q}].$$

[3] Disregarding the independence, this is not true in general. As an example (cf. also [58]) one may consider a numbering of the primes, $p_1, p_2, \ldots$ say, and check that each set $M_n := \{p_i : i \geq n\}$ has indeed density equal to 1 in the set of all primes while the intersection $\bigcap_n M_n$ is clearly empty.

Nevertheless, this problem of dependency may be circumvented by a simple inclusion-exclusion argument which suggests

$$\delta_a = \sum_k \frac{\mu(k)}{[\mathbb{Q}_{a,k} : \mathbb{Q}]} \tag{1.3}$$

as the correct density. Using standard techniques from algebraic number theory, one easily shows that, if a is a perfect h-th power in $\mathbb{Z}$, and one writes $a = a_1 a_2^2$ with a_1 squarefree, then (cf. [42, p. 214])

$$[\mathbb{Q}_{a,k} : \mathbb{Q}] = \begin{cases} \frac{n\varphi(k)}{2(k,h)}, & \text{if } 2a_1 \mid n \text{ and } a_1 \equiv 1 \ (4), \\ \frac{n\varphi(k)}{(k,h)}, & \text{otherwise,} \end{cases} \tag{1.4}$$

holds for any squarefree $k \in \mathbb{N}$. From this it becomes clear that (1.3), if expressed as an Euler product, indeed agrees with Artin's originally predicted density (1.2), provided that $a \equiv 2, 3 \ (4)$. Hence Artin was initially right in this case, and to his benefit one should remark that Artin only considered the case $a = 2$ in the first place (cf. [99]). This indicates that he was just a bit hasty in generalizing his conjecture to all of $\mathbb{N}$. Nevertheless, Artin had to correct his conjectural density in case $a_1 \equiv 1 \ (4)$, and suggested the correction factor

$$1 - \mu(|a_1|) \prod_{\substack{p \mid a_1 \\ p \mid h}} \left(\frac{1}{p-2} \right) \prod_{\substack{p \mid a_1 \\ p \nmid h}} \left(\frac{1}{p^2 - p - 1} \right)$$

which may be derived from (1.4) by computing (1.3) in terms of Euler products. See [3, 42] for details. Summing up, Artin eventually proposed

$$\delta_a := \delta(h) \tag{1.5}$$

if $a_1 \equiv 2, 3 \ (4)$, and

$$\delta_a := \delta(h) \left(1 - \mu(|a_1|) \prod_{\substack{p \mid a_1 \\ p \mid h}} \left(\frac{1}{p-2} \right) \prod_{\substack{p \mid a_1 \\ p \nmid h}} \left(\frac{1}{p^2 - p - 1} \right) \right) \tag{1.6}$$

if $a_1 \equiv 1 \ (4)$. These expressions clearly yield positive rational multiples of Artin's constant, a fact which is by no means obvious from (1.3). Moreover, these densities are eventually in agreement with the data provided by the Lehmer's computations, and should therefore yield the correct expression for the conjectural density.

1.2. Hooley's proof under GRH

The first significant improvement concerning AC had been a long time coming. In 1967, i.e. 40 years after Artin's announcement, Hooley [42] turned Artin's heuristic arguments, as described in the previous section, into a rigorous proof subject to the correctness of the GRH for certain number fields. The precise statement of Hooley goes as follows.

Proposition 1.2 (Hooley, 1967). *Let a be an integer different from $0, \pm 1$ and not a square. If one assumes the GRH for the fields $\mathbb{Q}_{a,q}$, then*

$$N_a(x) = \delta_a \cdot \frac{x}{\log x} + O_a\left(\frac{x \log\log x}{\log^2 x} \right),$$

with δ_a given by (1.5) and (1.6).

We give a brief outline of HOOLEY's proof for several reasons. On the one hand, this will indicate the necessity of the GRH to make ARTIN's heuristic applicable. On the other hand, we thereby get in contact with techniques to estimate prime numbers with certain arithmetic properties which appear frequently throughout this thesis. For a more detailed account, we refer to HOOLEY's original work [42].

HOOLEY's proof sets in with the definition of the two quantities

$$N_a(x,\eta) := \sharp\{p \leq x : p \text{ does not split completely in } \mathbb{Q}_{a,q}, \text{ for all primes } q \leq \eta\}$$

and

$$M(x,\eta_1,\eta_2) := \sharp\{p \leq x : p \text{ splits completely in } \mathbb{Q}_{a,q}, \text{ for some prime } q : \eta_1 < q < \eta_2\}.$$

By ARTIN's heuristic approach presented in the previous section, one clearly has

$$N_a(x) = N_a(x,x),$$

but it is hopeless to tackle $N_a(x,x)$ by the inclusion-exclusion principle and effective versions of the Čebotarev density theorem, even under GRH (see Section 4.3.2). Therefore, HOOLEY instead starts from the elementary formula

$$N_a(x) = N_a(x,\xi_1) + O(M(x,\xi_1,\xi_2)) + O(M(x,\xi_2,\xi_3)) + O(M(x,\xi_3,x-1)) \tag{1.7}$$

and chooses the parameters ξ_1, ξ_2 and ξ_3 according to

$$\xi_1 := \frac{1}{6}\log x, \qquad \xi_2 := \frac{\sqrt{x}}{\log^2 x}, \qquad \xi_3 := \sqrt{x}\log x.$$

These choices made, it turns out that $N_a(x,\xi_1)$ is the main term in (1.7) which similar to (1.3) may be written as

$$N_a(x,\xi_1) = \sum_n \mu(n)\cdot \pi_{\{\mathrm{id}\}}(x,\mathbb{Q}_{a,n}\,/\,\mathbb{Q}), \tag{1.8}$$

by the inclusion-exclusion principle, where the sum is over squarefree $n \in \mathbb{N}$ composed of primes not exceeding ξ_1. The two rightmost terms in (1.7) may be estimated as follows: To bound $M(x,\xi_2,\xi_3)$, it suffices to observe that primes p which split completely in $\mathbb{Q}_{a,q}$ satisfy $p \equiv 1\ (q)$. An application of the Brun-Titchmarsh inequality (cf. Proposition 4.2) combined with Mertens' formula (cf. Proposition 4.6) yields

$$M(x,\xi_2,\xi_3) = O\left(\frac{x\log\log x}{\log^2 x}\right).$$

The rightmost term in (1.7) may be estimated by a rather elementary but ingenious argument. For any prime p contained in $M(x,\xi_3,x-1)$, we have $\mathrm{ord}_a(p) \leq \frac{x}{\xi_3} = \frac{\sqrt{x}}{\log x}$, whence p must divide $a^m - 1$ for some $m < \sqrt{x}/\log x$. Hence,

$$2^{M(x,\xi_3,x-1)} \leq \prod_{m<\frac{\sqrt{x}}{\log x}} (a^m - 1),$$

which implies

$$M(x,\xi_3,x-1) = O_a\left(\frac{x}{\log^2 x}\right),$$

as one can easily verify.

Unfortunately, appropriate estimates of $M(x,\xi_1,\xi_2)$ and $N_a(x,\xi_1)$ are not within the scope of the preceding arguments for the following reasons: By the definition of ξ_1, the summation variables n in (1.8) are $\leq x^{1/3}$. This range, however, may not be shortened significally, to n less than a power of $\log x$ say. The summation range for n in (1.8) and the

range between ξ_1 and ξ_2, as well, are thus too large for an application of an unconditional effective Čebotarev density theorem (cf. Proposition 4.8), and an appropriate generalization of a Bombieri-Vinogradov theorem (cf. Proposition 4.3) is not available (see [81] for explanations). Therefore, one must resort to an effective Čebotarev density theorem valid only under GRH for the fields $\mathbb{Q}_{a,q}$ (cf. Proposition 4.7) which indeed allows to treat the terms $M(x,\xi_1,\xi_2)$ and $N_a(x,\xi_1)$ appropriately. In fact, Proposition 4.7 combined with rather elementary arguments eventually yields the estimates

$$M(x,\xi_1,\xi_2) = O_a\left(\frac{x}{\log^2 x}\right)$$

and

$$N_a(x,\xi_1) = \delta_a \cdot \frac{x}{\log x} + O_a\left(\frac{x}{\log^2 x}\right).$$

This proves Proposition 1.2 and indicates the necessity of the GRH for Hooley's arguments to apply.

1.3. Unconditional results of Gupta, Murty and Heath-Brown

Hooley's work is still state of the art regarding the quantitative AC. As for the qualitative AC, however, Gupta and Ram Murty [36] unconditionally showed its correctness for infinitely many integers. More precisely, they proved:

Proposition 1.3 (Gupta–Ram Murty, 1984). *Let r,s,t be three distinct primes, and set*

$$S := \left\{rt^2, r^3s^2, r^2s, s^3t^2, s^2t, r^2t^3, rs^3, r^3st^2, st^3, r^2s^3t, r^3t, rs^2t^3, rst\right\}.$$

For some $a \in S$, there exists $\delta > 0$ such that for at least $\delta x/\log^2 x$ primes $p \le x$, a is a primitive root modulo p.

Their method is based on a lower bound sieve which yields the existence of $\gg x/\log^2 x$ primes up to x such that all odd prime divisors of $p-1$ are larger than $x^{\frac{1}{4}-\varepsilon}$, for $\varepsilon > 0$ arbitrarily small. For such primes p, the residual order $\mathrm{ord}_a(p)$ has only "few choices" and one can show that $(\mathbb{Z}/p\mathbb{Z})^*$ is typically generated by r, s and t. Hence, for $\gg x/\log^2 x$ primes p, one may find a generator of the cyclic group $(\mathbb{Z}/p\mathbb{Z})^*$ of the form $r^u s^v t^w$ for appropriate positive integers u, v, and w. Some combinatorial arguments then allow to bound u, v, and w by 3 which in the end leads to Proposition 1.3.

Only one year later, Heath-Brown [39] refined this method by an improvement of the utilized sieve result. This enabled him to prove the existence of $\gg x/\log^2 x$ primes up to x such that, for appropriate $e \in \mathbb{N}$, either $p-1 = 2^e q$, for some odd prime q, or $p-1 = 2^e q_1 q_2$ holds, with odd primes q_1 and q_2 satisfying $q_1 \in [p^{1/4}, p^{1/2}]$. Following the lines of Gupta and Ram Murty this allowed Heath-Brown to prove the following improvement of Proposition 1.3.

Proposition 1.4 (Heath-Brown, 1985). *Let r,s,t be multiplicative independent[4] integers such that none of $r,s,t,-3rs,-3rt,-3st$ or rst is a square. Then*

$$\sharp\{p \le x : r,s \text{ or } t \text{ generate } (\mathbb{Z}/p\mathbb{Z})^*\} \gg \frac{x}{\log^2 x}.$$

In particular the qualitative AC holds for one of r,s and t.

[4]Integers $a_1,\dots,a_n$ are called multiplicative independent, if $a_1^{e_1}\cdots a_n^{e_n} = 1$, with $e_i \in \mathbb{Z}$, is only satisfied with $e_i = 0$ for $i = 1,\dots,n$.

This result entails the following remarkable consequences.

COROLLARY 1.5. *There are at most two primes and at most three squarefree integers larger than* 1 *for which the qualitative AC fails. Moreover, if* $T \subset \mathbb{Z}$ *denotes the set of all integers* a *for which the qualitative AC fails, then*

$$\sharp\{a \in T : |a| \leq x\} \ll \log^2 x.$$

Hence, choosing an integer a at random, the qualitative AC for a holds true[5] with probability 1, and taking three distinct primes, e.g. 2, 3 and 5, it even fails for at most two of them. Nonetheless, these results still fail to prove the qualitative AC for any fixed single integer which is different from $0, \pm 1$ and not a perfect square. This phenomenon may be seen as a classical side-effect of sieve methods.

[5]Note that the qualitative AC is trivially fulfilled for all perfect squares, for they are excluded from consideration in Conjecture 1.1

CHAPTER 2

Related Problems and Generalizations

Due to its simple formulation, Artin's primitive root conjecture naturally entails many generalizations and variations. This chapter serves to present only a few of these, namely the ones which will be of importance for the remainder of this thesis. A more extensive summary of variants of Artin's primitive root conjecture is provided in the survey paper of Moree [75].

2.1. Near-primitive roots

Let $a \neq 0, \pm 1$ be an integer. Artin's primitive root conjecture asserts that the set of primes $p \nmid a$ for which $\mathrm{ind}_a(p)$ equals 1 is infinite and has a positive density, provided that a is different from ± 1 and not a square. As a natural variation, one may consider an arbitrary $k \in \mathbb{N}$, and ask whether the same holds true if one instead requires that p satisfies $\mathrm{ind}_a(p) = k$. In this case we shall call a a *near-primitive root modulo p of index k*, and we denote by $N_{a,k}$ the set of primes p for which a is a near-primitive root of index k. The *analogue of AC for near-primitive roots* then amounts to ask whether $N_{a,k}$ has a (positive) density.

This question was first considered by Lenstra [58] in his impressive '77 paper concerning number field analogues of AC and Euklid's algorithm in global fields. Amongst other results, Lenstra proved that, under GRH, $N_{a,k}$ always has a density.

Proposition 2.1 (Lenstra, 1977). *Let $a \neq 0, \pm 1$ be an integer, $k \in \mathbb{N}$ and assume GRH for the fields $\mathbb{Q}_{a,nk}$, with $n \in \mathbb{N}$ squarefree. Then $N_{a,k}$ has a density $\delta_{a,k}$ given by*

$$\delta_{a,k} := \sum_{n=1}^{\infty} \frac{\mu(n)}{[\mathbb{Q}_{a,nk} : \mathbb{Q}]}.$$

To explain the expression for $\delta_{a,k}$, note that a prime p fulfils $\mathrm{ind}_a(p) = k$ if and only if $p \equiv 1 \ (k)$, $X^k \equiv a \ (p)$ is solvable and $X^{(p-1)/(qk)} \equiv a \ (p)$ is not solvable for any prime divisor q of $(p-1)/k$. By translating these properties into appropriate splitting conditions in the fields $\mathbb{Q}(\zeta_{nk}, a^{1/nk})$, the expression for $\delta_{a,k}$ arises by the same heuristic arguments as in Section 1.1.

Different to the classical case of AC, Lenstra also pointed out various cases in which $\delta_{a,k}$ happens to be zero, and provided necessary and sufficient criteria[6] for this to happen. An easy example for this is provided in the case where k is odd, $a \mid k$ and $a \equiv 1 \ (4)$: For any odd prime counted by $N_{a,k}$, we necessarily have $p \equiv 1 \ (a)$, and hence

$$\left(\frac{a}{p}\right) = \left(\frac{p}{a}\right) = \left(\frac{1}{a}\right) = 1$$

by quadratic reciprocity (cf. [54]). On the other hand, we know that a cannot be a square modulo p, as $\mathrm{ind}_a(p) = k$ is odd. Thus, $N_{a,k}$ contains 2 at most, and we have $\delta_{a,k} = 0$.

[6] Lenstra proved that $\delta_{a,k} = 0$ holds if, and under GRH only if, $N_{a,k}$ is finite.

Wagstaff [101] and Moree [76] explicitly computed $\delta_{a,k}$ in terms of Euler products and proved that $\delta_{a,k}$ is a rational multiple of Artin's constant. From this expression one may on the one hand determine the cases in which $\delta_{a,k}$ vanishes, and on the other hand it shows that $\delta_{a,k}$, for fixed a, is roughly of size $1/k^2$. In particular, this indicates that, for fixed $a \neq 0, \pm 1$, the quantities $\mathrm{ind}_a(p)$ and $\mathrm{ord}_a(p)$ are typically small and large, respectively (cf. Figures 2.1 and 2.2). Indeed, Erdős and Ram Murty [24] have proved:

Proposition 2.2 (Erdős–Ram Murty, 1996). *Let $a \neq 0, \pm 1$ be an integer. Then there exist $\alpha > 0$ and $\delta > 0$ such that*

$$\mathrm{ord}_a(p) \geq \sqrt{p} \cdot \exp\left(\log^{\delta} p\right)$$

holds for all but $O(x/(\log x)^{1+\alpha})$ primes $p \leq x$. If we assume GRH for the fields $\mathbb{Q}_{a,n}$, $n \in \mathbb{N}$, and let $\epsilon(x)$ be a function tending to infinity as $x \to \infty$, then we have

$$\mathrm{ord}_a(p) \geq p/\epsilon(p),$$

for all but $o(x/\log x)$ primes $p \leq x$.

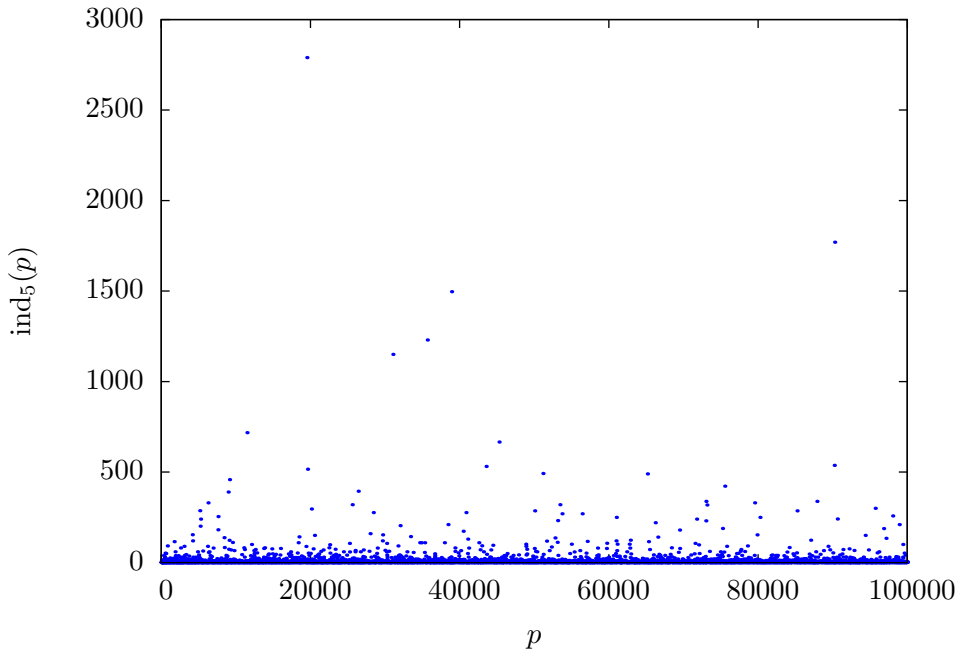


Figure 2.1. The residual index $\mathrm{ind}_5(p)$ over primes $p \neq 5$ is typically small.

During our discussion of Wagstaff's heuristic in Section 4.1, we will come upon the question for explicit asymptotic formulae for $N_{a,k}(x)$, the counting function of primes in $N_{a,k}$, which are uniform in a and k. In this regard, Murata [78] adapted Hooley's method and proved the following result, valid only for positive squarefree integers a.

Proposition 2.3 (Murata, 1991). *Let $a \geq 2$ be a squarefree integer and $k \in \mathbb{N}$. Assuming GRH for the fields $\mathbb{Q}_{a,n}$, $n \in \mathbb{N}$, one has*

$$N_{a,k}(x) = \delta_{a,k} \cdot \mathrm{li}(x) + O\left((k^{\varepsilon} \log\log x + \log a)\, \frac{x}{\log^2 x}\right),$$

where the implied constant only depends on ε.

For more details on the distribution of $\operatorname{ind}_a(p)$ and $\operatorname{ord}_a(p)$ and near-primitive roots, we refer to [30, 58, 78, 101] and especially the article [76] of Moree from which we took most of the information provided in this section.

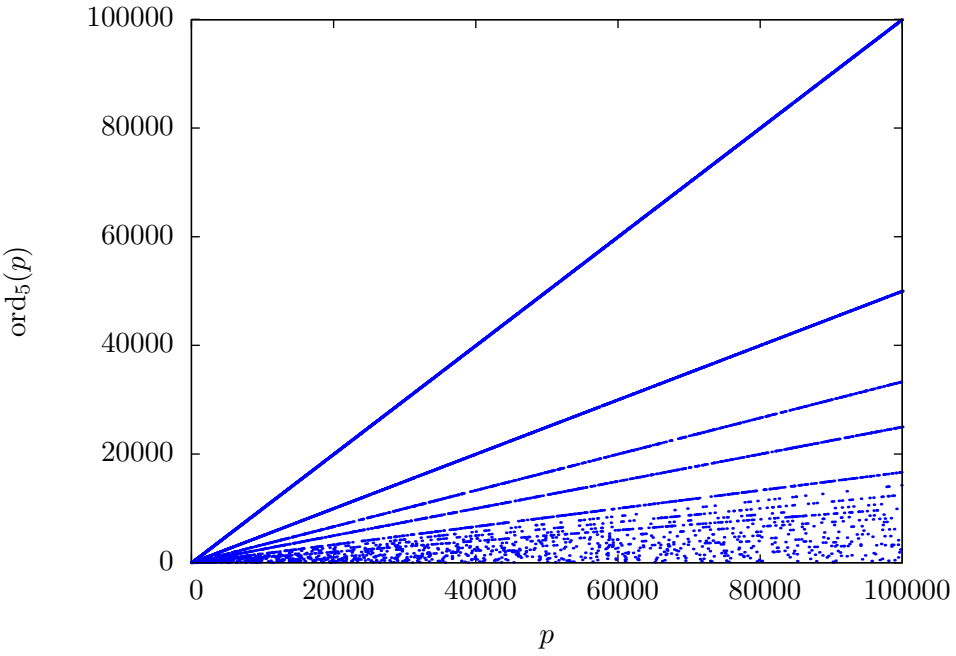


Figure 2.2. The residual order $\operatorname{ord}_5(p)$ over primes $p \neq 5$ is typically large.

2.2. Number field analogues

Let $\mathbb{K}$ be a number field with algebraic integers $\mathcal{O}_{\mathbb{K}}$. Since $(\mathcal{O}_{\mathbb{K}} / \mathfrak{p})^*$ is cyclic for any prime ideal $\mathfrak{p}$ of $\mathbb{K}$, one may ask if there are infinitely many prime ideals $\mathfrak{p}$ of $\mathbb{K}$, for which a given algebraic integer $a \in \mathcal{O}_{\mathbb{K}}$ generates $(\mathcal{O}_{\mathbb{K}} / \mathfrak{p})^*$, and whether the set of such prime ideals even has a positive density in the set of all prime ideals. In this way a natural *number field analogue of AC* arises.

In this regard the most exhaustive work has been done by Lenstra [58] in connection with his research on Euclidean number fields. We have already encountered part of his work in the preceding section. In fact, Lenstra has considered a further reaching generalization and proved the following result (cf. Theorem 3.1 of [58]) which extends a work of Cooke and Weinberger [20], who established a similar result in a more restricted setting two years earlier.

Proposition 2.4 (Lenstra, 1977). *Let $\mathbb{L} / \mathbb{K}$ be a Galois extension of number fields, C a union of conjugacy classes of $\operatorname{Gal}(\mathbb{L} / \mathbb{K})$, Γ a finitely generated subgroup of $\mathbb{K}^*$ of arithmetic rank ≥ 1 and $k \in \mathbb{N}$. Further, set $q(n) := \prod_{p \mid n} p \cdot p^{\nu_p(k)}$, for any squarefree $n \in \mathbb{N}$. Assuming GRH for the fields $\mathbb{K}_{\Gamma, q(n)}$, $n \in \mathbb{N}$, the set of prime ideals $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L} / \mathbb{K})$, for which $\operatorname{ind}_\Gamma(\mathfrak{p})$ divides k, has a density inside the set of all prime ideals of $\mathbb{K}$ given by*

$$\sum_{n=1}^{\infty} \frac{\mu(n) \cdot \sharp \left(C \cap \operatorname{Gal}(\mathbb{L} / \mathbb{L} \cap \mathbb{K}_{\Gamma, q(n)}) \right)}{[\mathbb{L}_{\Gamma, q(n)} : \mathbb{K}]}.$$

REMARK 2.5. As a matter of fact, LENSTRA [58] more generally treated the problem for finite Galois extensions $\mathbb{L}/\mathbb{K}$ of arbitrary *global fields*, i.e. number fields and function fields in one variable over some finite field. In the latter case, LENSTRA's result holds unconditionally, since the generalized Riemann hypothesis for function fields was proved to be correct by WEIL in 1948 [105], and extends a work of BILHARZ [8] from 1937.

The sum expression for the density supposed in Proposition 2.4 may again be derived by an appropriate number field adaption of Artin's heuristic arguments presented in Section 1.1. We omit this deduction and refer to [58] for details and to Chapters 5 and 6 for applications of similar arguments. As in the preceding section, the density proposed in Proposition 2.4 may happen to be zero. LENSTRA proved that this happens if, and under GRH only if, the considered set of prime ideals is finite, and he established necessary and sufficient criteria for this to happen. In fact, he proved the following result (cf. Theorem 4.1 of [58]) which will be of great value for us in Section 5.2.3.

PROPOSITION 2.6 (LENSTRA, 1977). *Let $\mathbb{K}$, Γ, $\mathbb{L}$, C and k as in Proposition 2.4, and let h be the product of those primes p for which Γ is contained in $\mathbb{K}^{*q(p)}$. Then the density proposed in Proposition 2.4 is positive if and only if there exists $\sigma \in \mathrm{Gal}(\mathbb{L}(\zeta_h)/\mathbb{K})$ such that $\sigma|_{\mathbb{L}} \in C$ and $\sigma|_{\mathbb{K}_{\Gamma,q(p)}} \neq \mathrm{id}$ hold, for every prime p for which $\mathbb{K}_{\Gamma,q(p)} \subset \mathbb{L}(\zeta_h)$.*

Propositions 2.4 and 2.6 provide a powerful tool to tackle a wide class of AC-like problems. Here we only mention the following example (cf. [58, p. 216]) which closes the connection to the preceding section. Apart from this, LENSTRA provides further examples in Sections 8 and 9 of his paper.

EXAMPLE 2.7. Consider an integer $a \neq \pm 1, 0$ and set $\mathbb{K} = \mathbb{Q}$ and $\Gamma = \langle a \rangle \subset \mathbb{K}^*$. Now fix an integer $k \in \mathbb{N}$, define $\mathbb{L} = \mathbb{Q}(\zeta_k, \sqrt[k]{a})$ and set $C = \{\mathrm{id}\} \subset \mathrm{Gal}(\mathbb{L}/\mathbb{K})$. The set $\mathcal{P}_C(\mathbb{L}/\mathbb{K})$ then consists exactly of those primes p that split completely in $\mathbb{L}$ which is equivalent to saying that $k \mid \mathrm{ind}_a(p)$ as explained in Sections 1.1 and 2.1. If one additionally restricts to those primes p which fulfil $\mathrm{ind}_a(p) \mid k$, then one obtains the set $N_{a,k}$ as defined in the preceding section. Hence, Proposition 2.4 yields Proposition 2.1 as a special case, and Proposition 2.6 determines the cases in which $\delta_{a,k}$ vanishes.

We get back to the number field setting considered by LENSTRA in our investigation of residual index and order in number fields in Part II. To conclude this section, we present another possible way of generalizing AC to number fields. Instead of the above problem, one may consider rational primes p, unramified in $\mathbb{K}$, for which the index of the reduction of Γ in $(\mathcal{O}_{\mathbb{K}}/p\,\mathcal{O}_{\mathbb{K}})^*$ has a certain property. An additional difficulty which arises here is that $(\mathcal{O}_{\mathbb{K}}/p\,\mathcal{O}_{\mathbb{K}})^*$ is only cyclic if p is inert in $\mathbb{K}$. However, one could ask whether there exist infinitely many primes p for which the order of the reduction of Γ in $(\mathcal{O}_{\mathbb{K}}/(p))^*$ is as big as possible. This has been studied by ROSKAM in [90] for a real quadratic field $\mathbb{K}$, and Γ generated by a fundamental unit of $\mathbb{K}$. Assuming GRH, ROSKAM adapted HOOLEY's and LENSTRA's methods to establish appropriate positive density results. Similar problems have also been considered unconditionally by adapting the sieve argument of GUPTA and RAM MURTY [36] to number fields. See [16, 84] for examples.

2.3. Composite moduli and λ-roots

Observing the content so far, one may wonder why we were only concerned with the reduction of (algebraic) integers modulo primes and prime ideals, respectively. In fact, there is a priori no reason which prevents from considering reduction modulo composite integers as well. But how would one formulate an analogue of AC then?

Recall that, different to the prime number case, the group of units of $\mathbb{Z}/n\mathbb{Z}$ is in general no longer cyclic for arbitrary integers n. However, it is evident from computations that the residual order $\mathrm{ord}_a(n)$ of some integer a modulo n is still typically large as n ranges over integers coprime to a. In fact, Kurlberg [50] proved the following result under GRH which confirms this fact building on the methods provided by Hooley's treatment of AC.

Proposition 2.8 (Kurlberg, 2003). *Let $a \neq 0, \pm 1$ be an integer and assume GRH for the fields $\mathbb{Q}_{a,k}$, $k \in \mathbb{N}$. Then, the set of $n \in \mathbb{N}$ with $\mathrm{ord}_a(n) \ll n^{1-\varepsilon}$ has density zero, i.e. the number of such $n \leq x$ is $o(x)$.*

In accordance with this observation, there is a natural way of generalizing the notion of primitive roots to composite moduli as suggested by Carmichael: For $a \in \mathbb{Z}$ and $n \in \mathbb{N}$ with $(a, n) = 1$, we call a a *λ-root* modulo n if $\mathrm{ord}_a(n)$ is as large as possible. Thus, a is a λ-root modulo n if $\mathrm{ord}_a(n) = \lambda(n)$, since the Carmichael function yields nothing but the exponent of $(\mathbb{Z}/n\mathbb{Z})^*$. Accordingly, one could suppose the following optimistic *analogue of AC for λ-roots*: Given an integer a which is not in an exceptional set[7], yet to be determined, there exists a positive constant Ω_a depending on a such that, as $x \to \infty$,

$$M_a(x) \sim \Omega_a \cdot x, \tag{2.1}$$

where $M_a(x)$ denotes the number of integers $n \leq x$ with $(a, n) = 1$ and $\mathrm{ord}_a(n) = \lambda(n)$.

In 2008, Li [61] proved $M_a(x) = o(x)$, for any element of the set $\mathcal{E}$ consisting of perfect powers with exponent larger than 1 and squares times either -1 or ± 2. Thus, $\mathcal{E}$ is a fair candidate for an exceptional set in the above sense. However, in the same paper it is also shown that

$$\liminf_{x\to\infty} \frac{M_a(x)}{x} = 0$$

holds for any integer a. Hence, there is no $a \in \mathbb{Z}$ for which (2.1) holds with a positive constant Ω_a. In fact, it turns out that the function $M_a(x)/x$ oscillates a lot, and for any $a \notin \mathcal{E}$, the ratio $M_a(x)/x$ does rather not seem to tend to a limit at all, as $x \to \infty$. Indeed, Li conjectured that

$$\limsup_{x\to\infty} \frac{M_a(x)}{x} > 0$$

should hold whenever $a \notin \mathcal{E}$ and, in colaboration with Pomerance, established a proof therefor under the assumption of the GRH [65].

Proposition 2.9 (Li–Pomerance, 2003). *Assuming GRH, there exists a positive number B such that, for any $a \notin \mathcal{E}$, we have*

$$\limsup_{x\to\infty} \frac{M_a(x)}{x} \geq B \cdot \frac{\varphi(|a|)}{|a|}.$$

In the same paper the authors conjectured that even more is true and made the following guess which, however, has not been resolved yet, even under GRH:

Conjecture 2.10 (Li–Pomerance, 2003). *For each prime p let*

$$F_p := \liminf_{t\to\infty} \sum_{j=0}^{\infty} \frac{\exp\left(tp^{-j-1}\right) - 1}{\exp\left(t/\varphi(p^j)\right)}$$

[7] such as the set containing 0, ± 1 and all perfect squares in Section 1.1

and set

$$\alpha := \prod_p (1 - F_p).$$

Then

$$\limsup_{x\to\infty} \frac{M_a(x)}{x} = \alpha \cdot \frac{\varphi(|a|)}{|a|}$$

holds for any $a \in \mathbb{Z}\setminus\mathcal{E}$*, and the* lim sup *is attained on a set which is independent of* a*.*

For similar problems and further reading concerning the results presented in this section we recommend the reader to consult the papers [60, 62, 63, 66, 77], and the articles [64, 65] of Li and Pomerance on which the major part of this section builds on. In Chapters 3 and 7 we deal with further problems concering composite integers or ideals of a number field.

2.4. Primitive points on elliptic curves

From an abstract point of view, one may obtain an analogue of AC whenever one has a group G equipped with an infinite family of homomorphisms $\psi_i : G \to G_i$, by taking an element $g \in G$ and ask whether there are infinitely many indices i, for which $\psi_i(g)$ generates all of G_i. So far, we have considered such families provided by number fields. In this section we present an analogue of AC for the reductions modulo primes of a rational elliptic curve, a setting we come back to in Part III. Our account is based on the survey papers [75] of Moree and [17] of Cojocaru. For background on elliptic curves and explanation of used terminology, we refer to Chapter 8 as well as [17, 44, 96].

Let E be a rational elliptic curve, i.e. the locus of an equation

$$y^2 = x^3 + ax + b, \tag{2.2}$$

with $a, b \in \mathbb{Z}$ satisfying $4a^3 + 27b^2 \neq 0$ plus a point O at infinity. Assume that the group $\mathrm{E}(\mathbb{Q})$ of rational points on E contains a point $Q \in \mathrm{E}(\mathbb{Q})$ of infinite order. For any prime p of good reduction for E, let E_p denote the reduction of E modulo p and consider the reduction $\overline{Q}$ in $\mathrm{E}_p(\mathbb{F}_p)$, the group of $\mathbb{F}_p$-rational points of E_p. If $\overline{Q}$ generates $\mathrm{E}_p(\mathbb{F}_p)$, one calls Q a *primitive point of* E *modulo* p, and obtaines an *elliptic curve analogue of AC* by asking whether there exist infinitely many primes p for which Q is a primitive point of E modulo p, and whether the set of these primes has a density. In this regard Lang and Trotter [56] proposed the following conjecture, commonly known as the *Lang-Trotter conjecture*.

Conjecture 2.11 (Lang–Trotter, 1977). *Let* Q *be a rational point of* $\mathrm{E}/\mathbb{Q}$ *of infinite order and let* $N_{\mathrm{E},Q}(x)$ *be the number of primes* $p \leq x$ *such that* Q *is a primitive point of* E *modulo* p*. Then there exists* $\delta_{\mathrm{E},Q} \geq 0$ *such that*

$$N_{\mathrm{E},Q}(x) \sim \delta_{\mathrm{E},Q} \cdot \frac{x}{\log x}.$$

Just as AC itself, this problem has not been resolved yet. The most notable result in this direction is due to Gupta and Ram Murty [37]. Under GRH they adapted Hooley's method to elliptic curves and proved the subsequent theorem which, however, is only valid if E has complex multiplication (CM) by the ring of integers of an imaginary quadratic field and restricts to primes which split completely in the CM field of E. This illustrates the difficulty of the Lang-Trotter conjecture, for in many cases the CM property allows for unconditional results.

Proposition 2.12 (Gupta–Ram Murty, 1986). *Let* E *be a rational elliptic curve with CM by the ring of integers* $\mathcal{O}_{\mathbb{K}}$ *of an imaginary quadratic field* $\mathbb{K}$*, and let* Q *be a rational point on* E *of infinite order. Further, let* $N'_{\mathrm{E},Q}(x)$ *denote the number of primes counted by* $N_{\mathrm{E},Q}(x)$ *which split completely in* $\mathbb{K}$*. Then, under GRH, there exists* $\delta'_{\mathrm{E},Q} \geq 0$ *such that*

$$N'_{\mathrm{E},Q}(x) = \delta'_{\mathrm{E},Q} \cdot \frac{x}{\log x} + O\left(\frac{x \log\log x}{\log^2 x}\right).$$

If 2 *and* 3 *are inert in* $\mathbb{K}$*, or* $\mathbb{K} = \mathbb{Q}(\sqrt{-11})$*, then* $\delta'_{\mathrm{E},Q} > 0$*.*

Gupta and Ram Murty also established an expression for the density $\delta_{\mathrm{E},Q}$ which looks much alike the one for δ_a in the classical case and may be obtained by similar heuristic arguments. The role of the Kummer fields $\mathbb{Q}_{a,k}$ is replaced by certain elliptic curve analogues. For more details we refer to [37].

One of the obstructions which prevent better results for the Lang-Trotter conjecture is the following. For Q to be a primitive point of E modulo p, it is necessary that $\mathrm{E}_p(\mathbb{F}_p)$ is cyclic in the first place. Different to the number field case, however, $\mathrm{E}_p(\mathbb{F}_p)$ is no longer cyclic in general, but rather a direct sum of (at most) two cyclic groups. It is therefore natural to ask whether the set of primes p for which $\mathrm{E}_p(\mathbb{F}_p)$ is cyclic has a (positive) density. Assuming GRH, Serre [93] used an adaption of Hooley's method to prove that the set of such primes indeed has a density which is positive if and only if the 2-division field of E is different from $\mathbb{Q}$, i.e. if the right side of (2.2) has an irrational root. If E has CM, this holds unconditionally by an argument of Ram Murty [79] which was later simplified by Cojocaru [18]. In the non-CM case, the latter could relax the GRH to a quasi 3/4-GRH. Here, a *quasi* δ*-GRH* asserts that the non-trivial zeroes of the respective Dedekind zeta function have real part $\leq \delta$. Finally, it has been proved unconditionally by Gupta and Ram Murty [38] that $\mathrm{E}_p(\mathbb{F}_p)$ is cyclic infinitely often, if and only if the 2-division field of E is different from $\mathbb{Q}$, and the number of such primes $\leq x$ is then $\gg x/\log^2 x$.

Let us return to the Lang-Trotter conjecture. In [37], Gupta and Ram Murty also considered a slightly modified problem which circumvents the non-cyclicity problem. Letting Λ be a free subgroup of $\mathrm{E}(\mathbb{Q})$, and thus automatically of finite rank λ say, by the Mordell-Weil theorem [96, p. 239], they considered the set of primes p for which the reduction of Λ modulo p generates $\mathrm{E}_p(\mathbb{F}_p)$. Subject to the GRH they were able to prove the existence of a density for this set, even for non-CM curves.

Proposition 2.13 (Gupta–Ram Murty, 1986). *Let* E *be a rational elliptic curve, and let* $N_{\mathrm{E},\Lambda}(s)$ *denote the number of primes* $p \leq x$ *such that the reduction of* Λ *modulo* p *generates* $\mathrm{E}_p(\mathbb{F}_p)$*. Then, under GRH*[8]*, there exists* $\delta_{\mathrm{E},\Lambda} \geq 0$ *such that, as* $x \to \infty$*,*

$$N_{\mathrm{E},\Lambda}(x) \sim \delta_{\mathrm{E},\Lambda} \cdot \frac{x}{\log x},$$

if either E *has no CM and* $\lambda \geq 18$*, or* E *has CM and* $\lambda \geq 10$*.*

As for unconditional results, Gupta and Ram Murty also provided the following lower bound result for $N_{\mathrm{E},\Lambda}(x)$ which is proved by avoiding the GRH by a lower bound sieve argument. As a remarkable piece of history, Gupta and Ram Murty noticed that the same method applies to the qualitative AC which eventually led to Propositions 1.3 and 1.4.

[8] Gupta and Ram Murty also proved a similar result with a quasi $\lambda/(\lambda+1)$-GRH.

PROPOSITION 2.14 (GUPTA–RAM MURTY, 1986). *If the rational elliptic curve* E *has CM, and* $\lambda \geq 6$*, then*

$$N_{\mathrm{E},\Lambda}(x) \gg \frac{x}{\log^2 x}.$$

More information on the announced topics and similar problems concerning elliptic curves and their reductions modulo primes is provided in [17, 75]. We will address related problems in Chapter 9.

CHAPTER 3

On the Least Primitive Root Expressible as a Sum of Two Squares

Artin's primitive root conjecture deals with the distribution of primes for which a given integer a is a primitive root. From a different point of view, one may take a fixed prime p, and ask for the distribution of primitive roots modulo p. Clearly, there exist exactly $\varphi(p-1)$ primitive roots modulo p inside $\{1, 2, \dots, p\}$, but their distribution in dependence of p is hardly understood. In this chapter we shed some light on this problem and establish upper bounds for the least primitive root expressible as a sum of two squares. Up to minor changes the content of this chapter coincides with the author's article [2].

We start with a brief introduction of the problem and state our main result in Section 3.1. Afterwards, in Section 3.2, we gather necessary tools from sieve theory, and in Section 3.3 we describe how our problem may be translated into a lower bound sieve problem of sieve-dimension $1/2$. In Section 3.4 we finally prove our main result.

3.1. Introduction and statement

A problem which has been studied intensively in the past is the search for upper bounds for $g(p)$, the *least primitive root modulo* p. Burgess [14] proved $g(p) = O(p^{\frac{1}{4}+\varepsilon})$, and Elliott [23] has shown $g(p) \ll (\log p)^{B(\varepsilon)}$, for all but $O(Y^{\varepsilon})$ primes $p \leq Y$. Recalling Proposition 1.4 of Heath-Brown, one moreover knows that $g(p) \leq 5$ holds infinitely often. Under GRH, the best upper bound so far is due to Shoup [95], who proved

$$g(p) \ll \omega(p-1)^4 (\log(\omega(p-1)) + 1)^4 \log^2 p,$$

for all primes p.

As a nearby variation of this problem, one may ask for primitive roots modulo p with certain arithmetic properties. In this regard it is natural to consider prime primitive roots modulo p instead. According to a folklore conjecture, all but finitely many primes p admit a positive prime primitive root modulo p which is smaller than p. This problem, however, has not been resolved yet. Writing $g^*(p)$ for the *least prime primitive root modulo* p, Martin [73] showed $g^*(p) \ll (\log p)^{B(\varepsilon)}$, for all but $O(Y^{\varepsilon})$ primes $p \leq Y$. Even though only stated for primitive roots, Shoup's result [95] from above holds for prime primitive roots, too, i.e. conditionally under GRH, we have the uniform estimate (see also [74])

$$g^*(p) \ll \omega(p-1)^4 (\log(\omega(p-1)) + 1)^4 \log^2 p.$$

Further information concerning $g(p)$ and $g^*(p)$ is provided in Paragraph 27 of Section 9.7 of Moree's survey article [75] on which the preceding account is based.

In this chapter we are interested in unconditional results valid for all primes, and therefore weaken the condition that the primitive root be a prime. Instead, as a natural variation, we ask for the *least primitive root expressible as a sum of two squares*. From a sieve-theoretic point of view this may be regarded as half way towards prime primitive roots. As it amounts to no extra effort, we treat the case of arbitrary moduli n. Of course,

$(\mathbb{Z}/n\mathbb{Z})^*$ may not have a primitive root in general and, following Section 2.3, we consider λ-roots modulo n instead. In this regard we write $s^*(n)$ for the *least λ-root modulo n expressible as a sum of two squares*, and prove the following main result of this chapter.

THEOREM 3.1. *For $n \in \mathbb{N}$, let n_c denote the largest odd cube-free divisor of n. Then, for any $\varepsilon > 0$ we have*

$$s^*(n) \ll_\varepsilon n_c^{\frac{1}{2}+\varepsilon}.$$

According to Theorem 3.1 there always exists a λ-root modulo n in the range $[1, n_c^{\frac{1}{2}+\varepsilon}]$, provided that n is sufficiently large. As we will see in the proof, it is even possible to find such a λ-root which is odd and free of prime divisors $p \equiv 3\ (4)$. The proof itself uses ideas of MARTIN [74], who treated the case of almost-primitive roots, i.e. primitive roots with only "few" prime divisors. It is based on a semi-linear lower bound sieve, i.e. a lower bound sieve of sieve-dimension $1/2$, and BURGESS' bound (cf. [15]) for short character sums. The semi-linear sieve is applicable here because primes represented by $x^2 + y^2$, i.e. 2 and primes $p \equiv 1\ (4)$, have density $1/2$ in the set of all primes. We thus note that, as a generalization of Theorem 3.1, our method also works if one considers λ-roots represented by any binary quadratic form of class number[9] 1.

3.2. The semi-linear sieve

We now provide the necessary tools from sieve theory needed to prove Theorem 3.1. For a more detailed introduction, we refer to [33]. As usual in sieve theory, $\mathcal{A}$ shall denote a subset of $\mathbb{N}$, and for any $d \in \mathbb{N}$, we let $\mathcal{A}_d := \{a \in \mathcal{A} \mid a \equiv 0\ (d)\}$. For a set $\mathcal{P}$ of rational primes, and a positive parameter z, we let $\mathcal{P}(z)$ be the product of all primes $p \in \mathcal{P}$ smaller than z. The predominant goal in sieve theory consists of estimating the quantity

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

To this end, one assumes that for any $d \in \mathbb{N}$, an asymptotic formula

$$\sharp\mathcal{A}_d = h(d)X + r_d \tag{3.1}$$

holds. Here the so called *density function* $h(d)$ is a multiplicative function, and X is a real parameter which serves as an approximation to the size of $\mathcal{A}$. The remainder terms r_d are intended to be rather small (at least on average over d). In a probabilistic sense one may then expect that X multiplied with

$$V(z) := \prod_{\substack{p \in \mathcal{P} \\ p < z}} (1 - h(p))$$

yields a good approximation for $\mathcal{S}(\mathcal{A}, z)$. This is indeed true under appropriate assumptions, and we state the following result which is a special case of a beta sieve of sieve-dimension $1/2$ (cf. [33, p. 207, 275]). Since we are merely interested in lower bounds for $\mathcal{S}(\mathcal{A}, z)$, we omit the upper bound version.

PROPOSITION 3.2. *Assume that the function $h(d)$ in (3.1) satisfies*

$$\prod_{\substack{w \le p < z \\ p \in \mathcal{P}}} (1 - h(p))^{-1} \le \left(\frac{\log z}{\log w}\right)^{\frac{1}{2}} \left(1 + \frac{L}{\log w}\right), \tag{3.2}$$

[9] Different to the definition in Chapter 10, the class number of a binary quadratic form is here understood without additional weighting by its automorphism group. See Section 10.2.1 for explanation.

for all $2 \leq w \leq z$ *with some constant* $L \geq 1$. *Then, for* $s \geq 1$ *we have*

$$\mathcal{S}(\mathcal{A}, z) \geq XV(z) \left\{ f(s) + O\left((\log D)^{-\frac{1}{6}} \right) \right\} + O\left(\sum_{\substack{d \mid \mathcal{P}(z) \\ d < D}} |r_d| \right),$$

where $s = \log D / \log z$, *and the first implied constant depends on* L. *For* $1 \leq s \leq 3$ *the function* $f(s)$ *is given by*

$$f(s) := \sqrt{\frac{e^{\gamma}}{\pi s}} \log\left(1 + 2(s-1) + 2\sqrt{s(s-1)}\right)$$

with γ *denoting the Euler-Mascheroni constant.*

3.3. Counting λ-roots expressible as a sum of two squares

Let us now translate our problem into an appropriate sieve setting in order to make Proposition 3.2 applicable. Henceforth, we fix a positive integer n, let $x \in \mathbb{R}_+$ be a real parameter, and set

$$\mathcal{A} := \{1 \leq a < x \mid a \text{ is a } \lambda\text{-root modulo } n,\ a \equiv 1\ (4)\}.$$

Furthermore, $\mathcal{P}$ will be the set of primes $p \equiv 3\ (4)$. Then we aim to bound

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

from below for a suitable choice of the parameters z and x. Indeed, if $\mathcal{S}(\mathcal{A}, z) \geq 1$ for $z > \sqrt{x}$, there exists a λ-root modulo n less than x which is expressible as a sum of two squares, since a member of $\mathcal{A}$ must have an even number of prime divisors in $\mathcal{P}$.

Before we can apply Proposition 3.2 to our problem, it is essential to derive an asymptotic formula for $\sharp\,\mathcal{A}_d$ as in (3.1). Therefore, we let $\delta_n(k)$ denote the *characteristic function of λ-roots modulo* n, i.e. $\delta_n(k) = 1$, if k is a λ-root modulo n, and $\delta_n(k) = 0$, otherwise. Since $\delta_n(k)$ is periodic with period n, and with support inside the set of integers coprime to n, it admits a unique expression as a linear combination of Dirichlet characters modulo n. This linear combination has been determined in Lemmas 4 and 5 of [74] which we summarize in the following lemma.

LEMMA 3.3. *Let* $\mathcal{G}$ *be the subgroup of Dirichlet characters modulo* n *given by*

$$\mathcal{G} := \left\{ \chi^{\frac{\lambda(n)}{\mathrm{rad}(\lambda(n))}} : \chi \text{ Dirichlet character modulo } n \right\}.$$

For every prime p *dividing* $\varphi(n)$, *let* $m(p)$ *denote the number of independent characters of order* p *in* $\mathcal{G}$. *For every character* χ *modulo* n, *let* $\sigma(\chi)$ *denote its order. Then, for any integer* k, *we have*

$$\delta_n(k) = \sum_{\chi \bmod n} c_\chi \chi(k),$$

where the sum ranges over Dirichlet characters modulo n. *The coefficients* c_χ *are given by*

$$c_\chi := \begin{cases} \prod_{p \mid \sigma(\chi)} \left(\frac{-1}{p^{m(p)}} \right) \prod_{\substack{p \mid \varphi(n) \\ p \nmid \sigma(\chi)}} \left(1 - \frac{1}{p^{m(p)}} \right), & \text{if } \chi \in \mathcal{G}, \\ 0, & \text{otherwise,} \end{cases}$$

and satisfy the equation

$$\sum_{\chi \bmod n} |c_\chi| = 2^{\omega(\varphi(n))} c_0,$$

where $c_0 := c_{\chi_0}$, *and* χ_0 *is the principal character modulo* n.

The error term in the asymptotic formula for $\sharp\,\mathcal{A}_d$, which we proceed to prove in the subsequent section, involves short sums of consecutive values of characters $\chi \in \mathcal{G}$. To this end, we state the following result (cf. Lemma 7 in [74]) which yields appropriate estimates for such sums, and is based on a more general result of Burgess (cf. [15]).

Lemma 3.4. *For every* $\mathcal{G} \ni \chi \neq \chi_0$, $M, N \geq 1$, *and* $0 < \eta < 1$, *we have*

$$\sum_{M<k\leq M+N} \chi(k) \ll N \left(\frac{n_c^{1/4+\eta}}{N}\right)^{\eta}.$$

3.4. Proof of Theorem 3.1

We begin with the deduction of an asymptotic formula for $\sharp\,\mathcal{A}_d$ as in (3.1).

Lemma 3.5. *Let* $n \in \mathbb{N}$, $x \in \mathbb{R}_+$ *and set* $X := \frac{c_0 x \varphi(2n)}{4n}$ *with* c_0 *as in Lemma 3.3. For a positive integer* $d \leq x$ *we have*

$$\sharp\,\mathcal{A}_d = h(d)X + r_d,$$

where $h(d)$ *is a multiplicative function given by*

$$h(d) := \begin{cases} 0, & \text{if } (d, 2n) > 1, \\ \frac{1}{d}, & \text{otherwise.} \end{cases}$$

For any $0 < \eta < 1$, $\varepsilon > 0$, *and* $0 < D \leq x$ *the remainder terms* r_d *satisfy*

$$\sum_{\substack{d|\mathcal{P}(z)\\ d<D}} |r_d| \ll_{\varepsilon,\eta} X n_c^{\varepsilon} \left(\frac{n_c^{1/4+\eta}}{x}\right)^{\eta} D^{\eta}.$$

Proof. If $(d, n) > 1$, or $2 \mid d$ we clearly have $\mathcal{A}_d = \varnothing$. For d odd, and $(d, n) = 1$ we deduce by Lemma 3.3

$$\begin{aligned} \sharp\,\mathcal{A}_d &= \sum_{\substack{k\leq x\\ k\equiv 1\ (4)\\ k\equiv 0\ (d)}} \delta_n(k) = \sum_{\substack{k\leq x/d\\ kd\equiv 1\ (4)}} \sum_{\chi\in\mathcal{G}} c_\chi \chi(kd) \\ &= c_0\chi_0(d) \sum_{\substack{k\leq x/d\\ k\equiv d\ (4)}} \chi_0(k) + \sum_{\substack{\chi\in\mathcal{G}\\ \chi\neq\chi_0}} c_\chi \chi(d) \sum_{\substack{k\leq x/d\\ k\equiv d\ (4)}} \chi(k). \end{aligned} \tag{3.3}$$

By Möbius inversion the first sum in (3.3) equals

$$\begin{aligned} \sum_{\substack{k\leq x/d\\ k\equiv d\ (4)\\ (k,n)=1}} 1 &= \sum_{\substack{k\leq x/d\\ k\equiv d\ (4)}} \sum_{\substack{f|k\\ f|n}} \mu(f) = \sum_{f|n} \mu(f) \sum_{\substack{lf\leq x/d\\ lf\equiv d\ (4)}} 1 = \frac{x}{4d} \sum_{\substack{f|n\\ 2\nmid f}} \frac{\mu(f)}{f} + O\left(2^{\omega(n)}\right) \\ &= \frac{x}{4d} \cdot \frac{\varphi(2n)}{n} + O\left(2^{\omega(n)}\right). \end{aligned} \tag{3.4}$$

The second sum in (3.3) can be estimated using Lemma 3.3 and 3.4. If $d_0 \equiv d\ (4)$ with $d_0 \in \{1,3\}$, and m is an integer satisfying $4m \equiv 1\ (n)$, we obtain

$$\begin{aligned}\sum_{\substack{\chi\in\mathcal{G}\\ \chi\neq\chi_0}} c_\chi\chi(d) \sum_{\substack{k\leq x/d\\ k\equiv d\ (4)}} \chi(k) &\ll \sum_{\substack{\chi\in\mathcal{G}\\ \chi\neq\chi_0}} |c_\chi| \left|\chi(m) \sum_{0\leq l\leq \frac{x}{4d}-\frac{d_0}{4}} \chi(4l+d_0)\right| \\ &\ll \sum_{\substack{\chi\in\mathcal{G}\\ \chi\neq\chi_0}} |c_\chi| \left| \sum_{0\leq l\leq \frac{x}{4d}-\frac{d_0}{4}} \chi(l+md_0)\right| \\ &\ll c_0 2^{\omega(\varphi(n))}\cdot \frac{x}{d}\left(\frac{d}{x}n_c^{1/4+\eta}\right)^\eta.\end{aligned}$$

By (3.3) and (3.4) the remainder term r_d is therefore

$$\ll c_0 2^{\omega(n)} + c_0 2^{\omega(\varphi(n))}\cdot \frac{x}{d}\left(\frac{d}{x}n_c^{1/4+\eta}\right)^\eta \ll_\varepsilon \frac{1}{d}\cdot\frac{c_0 x\varphi(2n)}{4n}\cdot n_c^\varepsilon\left(\frac{d}{x}n_c^{1/4+\eta}\right)^\eta,$$

since $d\leq x$ and $\eta<1$. Using the definition of X, we finally deduce

$$\sum_{\substack{d\mid\mathcal{P}(z)\\ d<D}} |r_d| \leq \sum_{d<D}|r_d| \ll_\varepsilon X n_c^\varepsilon\left(\frac{n_c^{1/4+\eta}}{x}\right)^\eta \sum_{d<D} d^{\eta-1} \ll_\eta X n_c^\varepsilon\left(\frac{n_c^{1/4+\eta}}{x}\right)^\eta D^\eta.$$

□

Using Proposition 3.2 and Lemma 3.5, we are finally in the position to prove the following modification of Theorem 3.1.

THEOREM 3.6. *Let $n\in\mathbb{N}$ and $x\in\mathbb{R}_+$. Let further $\mathcal{S}(\mathcal{A})$ denote the number of odd λ-roots q modulo n in the range $0<q<x$, such that q is expressible as a sum of two squares, and set $X := \frac{c_0 x\varphi(2n)}{4n}$ with c_0 as in Lemma 3.3. Then, for any $0<\eta<\frac{1}{2}$ there exists $x_0(\eta)\geq 1$ such that*

$$\mathcal{S}(\mathcal{A}) \gg_\eta \frac{X}{\sqrt{\log x}}$$

holds, whenever $x > \max\left\{x_0(\eta), n_c^{\frac{1}{2}+\frac{5\eta}{1-2\eta}}\right\}$.

PROOF. Inserting the multiplicative function $h(d)$ from Lemma 3.5 into the definition of $V(z)$, one can easily verify that (3.2) is satisfied, and $V(z)\sim\frac{c_n}{\sqrt{\log z}}$ holds with some constant $c_n\geq 1$ depending on n (cf. [33, p. 277f]). Hence, Proposition 3.2 is applicable. If $z>\sqrt{x}$, we clearly have

$$\begin{aligned}\mathcal{S}(\mathcal{A}) &\geq \mathcal{S}(\mathcal{A},z) \\ &\gg \frac{X}{\sqrt{\log x}}\left\{f(s)+O\left((\log D)^{-\frac{1}{6}}\right)\right\} + O_{\eta,\varepsilon}\left(X n_c^\varepsilon\left(\frac{n_c^{1/4+\eta}}{x}\right)^\eta D^\eta\right)\end{aligned}$$

by Proposition 3.2 and Lemma 3.5. Now we define $D := \frac{x^{1-\eta}}{n_c^{2\eta+1/4}}$, and set $\varepsilon := \eta^2$. With these choices the above error term becomes $o(X/\sqrt{\log x})$. If we choose x according to the condition

$$x > n_c^{\frac{1}{2}+\frac{5\eta}{1-2\eta}},$$

we obtain $D>x^{1/2}$, and hence $f(s)>0$. This completes the proof. □

At last, it is rather easy to show that Theorem 3.1 is a simple consequence of Theorem 3.6. Indeed, for any $0 < \eta < \frac{1}{2}$, Theorem 3.6 implies that $\mathcal{S}(\mathcal{A})$ is positive, whenever

$$x > x_0(\eta) n_c^{\frac{1}{2}+\frac{5\eta}{1-2\eta}}$$

is satisfied. Since $\mathcal{S}(\mathcal{A})$ is a counting function, it must therefore be ≥ 1, and Theorem 3.1 follows. □

Part II

Residual Index and Residual Order in Number Fields

CHAPTER 4

Wagstaff's Heuristic and Related Problems

After the preceding chapters which were, except for Chapter 3, of rather introductory nature, we are now facing the main part of this thesis, namely the study of the distribution of residual index and residual order over certain families of ideals of a number field.

We give a brief outline of certain heuristic considerations of Wagstaff [101] in Section 4.1 and starting from this, we utilize Section 4.2 to motivate the problems we are investigating in Chapters 5, 6 and 7. Afterwards, in Section 4.3, we provide the main tools from algebraic and analytic number theory which are needed to face these tasks and, beyond that, prove beneficial for problems considered in Part III. These are basically the same tools which led to the results of Hooley, Lenstra et al. which we presented in Chapters 1 and 2.

4.1. Wagstaff's heuristic

Let us fix an integer $a \neq 0, \pm 1$, and assume GRH. In Section 2.1 we observed that, for any $k \in \mathbb{N}$, the set of primes p, for which $\operatorname{ind}_a(p) = k$ holds, has a density in the set of all primes which is positive in most cases (cf. Sections 2.1 and 2.2). It is natural to study the distribution of $\operatorname{ind}_a(p)$ over primes p, and ask for its average order, or even arbitrary moments in general. Probably the first result in this direction is due to Wagstaff [101], who considered the average order of $\operatorname{ind}_a(p)$ over primes $p \nmid a$ by the following heuristic approach: Recall that, for any $k \in \mathbb{N}$, the density of primes which satisfy $\operatorname{ind}_a(p) = k$ is denoted by $\delta_{a,k}$, and $N_{a,k}(x)$ denotes the counting function of such primes $p \leq x$. As $\delta_{a,k}$ decreases roughly like $1/k^2$ (see Section 2.1), one would expect

$$\sum_{\substack{p \leq x \\ p \nmid a}} \operatorname{ind}_a(p) = \sum_{k \leq x} k N_{a,k}(x) \sim \pi(x) \sum_{k \leq x} k \delta_{a,k} \sim A_a \cdot x, \tag{4.1}$$

as $x \to \infty$, with some positive constant A_a depending on a. This is in line with computational data (see Figure 4.1) and a conjecture of Fomenko [29], and suggests that $\operatorname{ind}_a(p)$ is a positive multiple of $\log p$ on average. Wagstaff proved that the rightmost equivalence in (4.1) is indeed true (cf. Section 6 of [101]). However, the implicit error terms involved in Proposition 2.1 (see also Proposition 2.3) are too big, to prove the middle equivalence and make this approach rigorous. In the sequel, we will refer to (4.1) and the presented heuristic arguments concerning the average order of $\operatorname{ind}_a(p)$ as *Wagstaff's heuristic*.

The problem of proving (4.1) turns out to be a very delicate one, and it is yet unsolved. Proceeding similarly to Wagstaff's heuristic, one can (unconditionally) prove (cf. [27])

$$\frac{1}{\pi(x)} \sum_{\substack{p \leq x \\ p \nmid a}} \operatorname{ind}_a(p) \gg \log \log x,$$

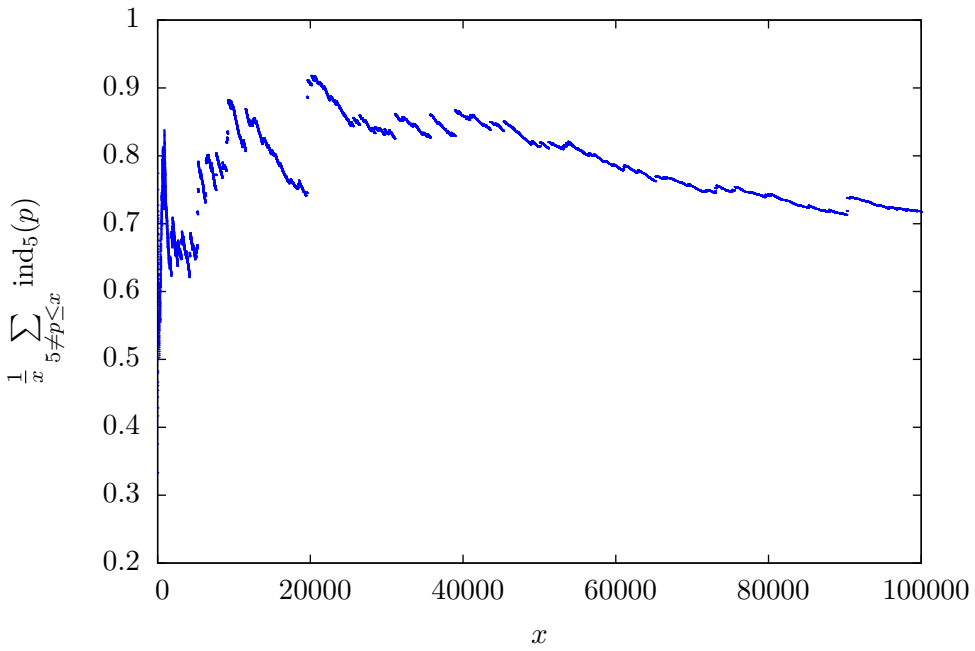


FIGURE 4.1. Average behaviour of $\mathrm{ind}_5(p)$ over primes $p \neq 5$.

and under GRH one may even derive (cf. [26, p. 112])

$$\frac{1}{\pi(x)} \sum_{\substack{p \leq x \\ p \nmid a}} \mathrm{ind}_a(p) \gg \log x.$$

As for upper bounds, the best result in this direction, due to ERDŐS and RAM MURTY [24], is given by

$$\frac{1}{\pi(x)} \sum_{\substack{p \leq x \\ p \nmid a}} \mathrm{ind}_a(p) \ll \frac{\sqrt{x}}{\log^{\eta} x},$$

for some $\eta > 0$. This upper bound is still far away from the expected growth. Moreover, RAM MURTY and SRINIVASAN [83] pointed out that an upper bound of the form $O(x^{1/4} \log x)$ would suffice to prove AC. This underlines the complexity of the problem and indicates that every step towards a proof of Wagstaff's heuristic would indeed be worthwhile. In this regard, work of PAPPALARDI [87] and FELIX and RAM MURTY [28] must be mentioned. Instead of summing $\mathrm{ind}_a(p)$, they considered a modified problem and studied the average behaviour of $f(\mathrm{ind}_a(p))$ for certain truncation functions f. If f increases sufficiently slowly, then, assuming GRH, they proved results which affirm (4.1).

4.2. Wagstaff's heuristic in number fields and related problems

Following Section 2.2, the above problem admits a natural generalization to number fields. Henceforth, let $\mathbb{K}$ be a number field and Γ a finitely generated, not necessarily torsion-free, infinite subgroup of $\mathbb{K}^*$, say with arithmetic rank $\gamma \in \mathbb{N}$. The most popular example for such a group is given by the unit group $\mathcal{U}_{\mathbb{K}}$ of $\mathbb{K}$, if $\mathbb{K}$ is neither $\mathbb{Q}$ nor an

imaginary quadratic field. Moreover, we let $\mathbb{L}/\mathbb{K}$ be a finite Galois extension with Galois group $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$ and consider a union of conjugacy classes C therein.

Inspired by Wagstaff and Lenstra, we are interested in the distribution of $\mathrm{ind}_\Gamma(\mathfrak{p})$ over prime ideals of $\mathcal{P}_C(\mathbb{L}/\mathbb{K})$, i.e. prime ideals of $\mathbb{K}$ which are unramified in $\mathbb{L}$ and satisfy $\left[\frac{\mathbb{L}|\mathbb{K}}{\mathfrak{p}}\right] = C$. In particular, we are curious about the asymptotic behaviour of

$$\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*}} \mathrm{ind}_\Gamma(\mathfrak{p})^\kappa,$$

for any parameter $\kappa\in\mathbb{R}_+$. Note that the condition $\overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*$ excludes only finitely many prime ideals. In the sequel we refer to the above quantity as the *κ-th moment*[10] *of* $\mathrm{ind}_\Gamma(\mathfrak{p})$ *over prime ideals in* $\mathcal{P}_C(\mathbb{L}/\mathbb{K})$. In view of Wagstaff's heuristic (4.1), or a generalization to κ-th moments thereof, we expect the following to hold

$$\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*}} \mathrm{ind}_\Gamma(\mathfrak{p})^\kappa \sim \begin{cases} A_1\cdot \mathrm{li}(x), & \text{if } \gamma>\kappa,\\ A_2\cdot x, & \text{if } \gamma=\kappa,\\ A_3\cdot \mathrm{li}(x^{\kappa-\gamma+1}), & \text{if } \gamma<\kappa,\end{cases} \tag{4.2}$$

with positive constants A_i possibly depending on $\mathbb{L}$, $\mathbb{K}$, C, Γ, and κ. Of course, the generalization step to number fields will not change the complexity of the problem, so that just as in the classical case, a proof of (4.2) seems out of reach, even under GRH. However, in Chapter 6 we will affirm (4.2) by, partly conditionally upon GRH, proving its correctness at least on average over Γ (cf. Theorems 6.1 and 6.2). Moreover, there are many variations of the presented problem which are easier to handle and we will address two of these in Chapters 5 and 7:

In Chapter 5 we consider the same problem as above, only with $\mathrm{ind}_\Gamma(\mathfrak{p})$ replaced by $\mathrm{ord}_\Gamma(\mathfrak{p})$. It turns out that, on average, the residual order is much easier to handle than the residual index. This is due to the general observation that the residual order is typically large while the residual index is typically rather small (cf. Propositions 2.1, 2.2 and 2.8). Consequently, Kurlberg and Pomerance [51] have, conditionally on GRH, established an asymptotic formula for the average order of $\mathrm{ord}_\Gamma(\mathfrak{p})$ in the case where $\mathbb{K}=\mathbb{L}=\mathbb{Q}$ and Γ is generated by a single rational number $a\neq 0,\pm 1$, i.e. they proved an asymptotic formula

$$\sum_{\substack{p\leq x\\ p\nmid a}} \mathrm{ord}_a(p) \sim c_a\cdot \mathrm{li}(x^2),$$

which suggests that $\mathrm{ord}_a(p)$ equals some positive constant c_a times p on average (cf. Proposition 5.1). In Chapter 5 we generalize their method to number fields, and, relying on GRH, prove analogue asymptotic formulae for

$$\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*}} \mathrm{ord}_\Gamma(\mathfrak{p})^\kappa,$$

the *κ-th moment of* $\mathrm{ord}_\Gamma(\mathfrak{p})$ *over prime ideals in* $\mathcal{P}_C(\mathbb{L}/\mathbb{K})$ which suggests that $\mathrm{ord}_\Gamma(\mathfrak{p})^\kappa$ equals $\mathcal{N}\mathfrak{p}^\kappa$ on average (cf. Theorem 5.3).

[10] This notion certainly differs from the usual notion of κ-th moments, as we abstain from dividing by the number of prime ideals under consideration, for convenience.

In Chapter 7 we study a related problem which surprisingly appears frequently in different fields of number theory, i.e. the distribution of $\mathrm{ind}_{\mathcal{U}_\mathbb{K}}(\mathfrak{a})$ over all ideals of $\mathbb{K}$, if $\mathcal{U}_\mathbb{K}$ is infinite. As already explained in the Introduction, the size of $\mathrm{ind}_{\mathcal{U}_\mathbb{K}}(\mathfrak{a})$, as $\mathfrak{a}$ ranges over ideals of $\mathbb{K}$, plays a crucial role in connection with the Ramanujan conjecture for GL_n over number fields (see Chapter 7 and [9, 10] for details). In a recent work, Rohrlich [89] was concerned with the average order of $\mathrm{ind}_{\mathcal{U}_\mathbb{K}}(\mathfrak{a})$ in connection with counting self-dual Artin representations over number fields, and it is exactly this problem which we address in Chapter 7 in more generality. More precisely, we study lower bounds of

$$\sum_{\substack{\mathcal{N}\mathfrak{a}\leq x\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{a})^*}} \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa,$$

the *κ-th moment of* $\mathrm{ind}_\Gamma(\mathfrak{a})$ *over all ideals of* $\mathbb{K}$. While, as we have seen above, $\mathrm{ind}_\Gamma(\mathfrak{p})$ is expected to be small on average, we are proving a surprising results which suggest that $\mathrm{ind}_\Gamma(\mathfrak{a})$ is in fact rather close to $\mathcal{N}\mathfrak{a}$ on average (cf. Theorems 7.1 and 7.2).

4.3. Tools for prime number and prime ideal estimates

Before we get to business in the next chapters, we make some arrangements. In the remainder of this thesis we will frequently need to handle primes in arithmetic progression or, more generally, prime ideals of a number field which give rise to the same Frobenius symbol in a finite Galois extension. This section serves to provide the corresponding tools from analytic and algebraic number theory, most of which have already been referred to frequently in previous chapters.

4.3.1. Primes in arithmetic progression. According to the *prime number theorem for primes in arithmetic progression*, a classical result due to Dirichlet, we have

$$\pi(x;a,q)\sim\frac{\pi(x)}{\varphi(q)}, \tag{4.3}$$

provided that $a\in\mathbb{Z}$ and $q\in\mathbb{N}$ are coprime, with

$$\pi(x)\sim\mathrm{li}(x)\sim\frac{x}{\log x}$$

by the classical *prime number theorem* (see [100] for details). For further applications, however, the asymptotic equivalence (4.3) often turns out to be little practical and we are more interested in effective versions, upper and lower bounds and so on. As for effective versions, the *Siegel-Walfisz theorem* [13, p. 114] often proves useful.

Proposition 4.1 (Siegel-Walfisz theorem). *For any $A>0$, there exists a constant $C=C(A)>0$ such that*

$$\pi(x;a,q)=\frac{\mathrm{li}(x)}{\varphi(q)}+O\left(xe^{-C\sqrt{\log x}}\right)$$

holds uniformly, for any $q\in\mathbb{N}$ in the range $q\leq\log^A x$ and any $a\in\mathbb{Z}$ with $(a,q)=1$.

Subject to the GRH for the cyclotomic fields $\mathbb{Q}(\zeta_q)$, it can be shown that Proposition 4.1 remains true with an improved error term $O(\sqrt{x}\log x)$ and a larger range $q\leq x$ (cf. [13, p. 116] and [4, p. 229]). In Section 4.3.2 we will encounter number field generalizations of this statement and Proposition 4.1, namely effective versions of the Čebotarev density theorem.

The estimation of $\pi(x;a,q)$ or even sums thereof for large moduli q does not lie within the scope of the asymptotic formula given by Proposition 4.1, and we are often forced to resort to upper bounds and average results, instead. In this regard, classical tools are provided by the *Brun-Titchmarsh inequality* (cf. [100, p. 73]) and the *Bombieri-Vinogradov theorem* (cf. [33, p. 170]).

PROPOSITION 4.2 (Brun-Titchmarsh inequality). *Let $x, y \in \mathbb{R}_+$ and let $a \in \mathbb{Z}$ and $q \in \mathbb{N}$. If $y/q \to \infty$, we have*

$$\pi(x+y;a,q) - \pi(x;a,q) \leq \big(2+o(1)\big)\frac{y}{\varphi(q)\log(y/q)}.$$

PROPOSITION 4.3 (Bombieri-Vinogradov theorem). *For any $A > 0$ there exists a positive constant $B = B(A)$ such that*

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

In Section 7.4.2 we need to handle sums of $\pi(x;a,q)$ for moduli q which slightly exceed $x^{1/2}$. In this case the Bombieri-Vinogradov theorem is not applicable and the Brun-Titchmarsh inequality is too imprecise, at least for our needs. For this purpose, we quote the following result of BOMBIERI, FRIEDLANDER and IWANIEC [11], which represents a continuous transition between these two statements.

PROPOSITION 4.4 (BOMBIERI–FRIEDLANDER–IWANIEC, 1989). *Let $a \neq 0$ be an integer, $A > 0$ and $2 \leq Q \leq x^{3/4}$. Let $\mathcal{Q}$ be the set of all positive integers q, prime to a, from an interval $Q' < q \leq Q$. Then*

$$\sum_{q\in\mathcal{Q}} \left|\pi(x;a,q) - \frac{\mathrm{li}(x)}{\varphi(q)}\right| \leq \left[L\left(\theta - \frac{1}{2}\right)^2 \frac{x}{\log x} + O_A\left(\frac{x\log^3\log x}{\log^3 x}\right)\right] \sum_{q\in\mathcal{Q}} \frac{1}{\varphi(q)} + O_{a,A}\left(\frac{x}{\log^A x}\right),$$

where $\theta = \log Q/\log x$ and L is an absolute constant.

Due to these estimates, we are frequently confronted with sums of the type $\sum_n \frac{1}{n^r\varphi(n)^s}$, with real numbers $r, s \geq 0$ satisfying $r + s > 1$ and n either in the range $1 \leq n \leq x$ or $x < n$, for some $x \in \mathbb{R}_+$. For convenience, we once and for all state the following commonly known statement which may be proved by elementary methods using the identity

$$\frac{1}{\varphi(n)} = \frac{1}{n}\sum_{s|n} \frac{\mu^2(s)}{\varphi(s)}.$$

LEMMA 4.5. *For any $x \in \mathbb{R}_+$, and any $r, s \geq 0$ such that $s + r > 1$ we have*

$$\sum_{n>x} \frac{1}{n^r\varphi(n)^s} = O_{r,s}(x^{1-r-s}) \qquad \text{and} \qquad \sum_{n\leq x} \frac{1}{\varphi(n)} = O(\log x).$$

Another problem which occurs quite frequently in this context is the estimation of certain sums and products over primes. To this end, we note the following classical results due to MERTENS [100, p. 16ff], both of which are referred to as *Mertens' formula*.

PROPOSITION 4.6 (Mertens' formula). *For $x \geq 2$ we have the uniform estimates*

$$\sum_{p \leq x} \frac{1}{p} = \log\log x + O(1) \qquad \text{and} \qquad \prod_{p \leq x} \left(1 - \frac{1}{p}\right) = \frac{e^{-\gamma}}{\log x} + O\left(\frac{1}{\log^2 x}\right),$$

where γ denotes the Euler-Mascheroni constant.

4.3.2. Prime ideals with given Frobenius symbol. Let us now turn to the prime ideal case in general. Let $\mathbb{L}/\mathbb{K}$ be a Galois extension of number fields and $C \subset \mathrm{Gal}(\mathbb{L}/\mathbb{K})$ a conjugacy class. We are interested in $\pi_C(x, \mathbb{L}/\mathbb{K})$, the number of prime ideals of $\mathbb{K}$ which are unramified in $\mathbb{L}$ and satisfy $\mathcal{N}\mathfrak{p} \leq x$ as well as $\left[\frac{\mathbb{L}|\mathbb{K}}{\mathfrak{p}}\right] = C$. By the *Čebotarev density theorem*, we have the asymptotic equivalence (cf. [54, p. 169])

$$\pi_C(x, \mathbb{L}/\mathbb{K}) \sim \frac{|C|}{[\mathbb{L}:\mathbb{K}]} \cdot \pi(x, \mathbb{K}) \tag{4.4}$$

with

$$\pi(x, \mathbb{K}) \sim \mathrm{li}(x) \sim \frac{x}{\log x}$$

by the *prime ideal theorem* (cf. [53]). Note that in the case $\mathbb{L} = \mathbb{Q}(\zeta_q)$ and $\mathbb{K} = \mathbb{Q}$ we have $\pi_C(x, \mathbb{L}/\mathbb{K}) = \pi(x; a, q)$, where a corresponds to the choice of C by the Frobenius symbol. This observation uncovers DIRICHLET's prime number theorem for primes in arithmetic progression as a special case of the Čebotarev density theorem and will beyond that often be useful in the sequel.

Again, (4.4) is not sufficient for practical purposes and we quote the following result of LAGARIAS and ODLYZKO [52] which we refer to as the *effective (version of the) Čebotarev density theorem under GRH*.

PROPOSITION 4.7 (LAGARIAS–ODLYZKO, 1977). *If the GRH for $\mathbb{L}$ holds true, then for every $x > 2$ we have*

$$\left|\pi_C(x, \mathbb{L}/\mathbb{K}) - \frac{|C|}{[\mathbb{L}:\mathbb{K}]}\,\mathrm{li}(x)\right| \ll \frac{|C|}{[\mathbb{L}:\mathbb{K}]} \cdot x^{1/2} \log\left(\Delta_{\mathbb{L}} x^{[\mathbb{L}:\mathbb{Q}]}\right) + \log(\Delta_{\mathbb{L}}),$$

where the implied constant is absolute.

As for unconditional statements, LAGARIAS and ODLYZKO [52] also proved the following *unconditional effective (version of the) Čebotarev density theorem* which may be viewed as a generalization of the Siegel-Walfisz theorem quoted above. Possible non-trivial zeroes of the Dedekind zeta function $\zeta_{\mathbb{L}}(s)$ associated to $\mathbb{L}$ which are away from the critical line are taken into account and just as in Proposition 4.1 effect a larger error term and a shorter range for admissible fields $\mathbb{L}$ than in Proposition 4.7.

PROPOSITION 4.8 (LAGARIAS–ODLYZKO, 1977). *There exist positive absolute constants c_1 and c_2 such that, if*

$$\log x \geq 10[\mathbb{L}:\mathbb{Q}](\log \Delta_{\mathbb{L}})^2,$$

then

$$\left|\pi_C(x, \mathbb{L}/\mathbb{K}) - \frac{|C|}{[\mathbb{L}:\mathbb{K}]}\,\mathrm{li}(x)\right| \leq \frac{|C|}{[\mathbb{L}:\mathbb{K}]}\,\mathrm{li}(x^{\beta_0(\mathbb{L})}) + c_1 x e^{-c_2\left(\frac{\log x}{[\mathbb{L}:\mathbb{Q}]}\right)^{1/2}}.$$

Here, the so called Siegel zero *$\beta_0(\mathbb{L})$ of $\zeta_{\mathbb{L}}$, if existent, denotes the only zero of $\zeta_{\mathbb{L}}(s)$, $s = \sigma + it$, in the strip*

$$1 - (4\log \Delta_{\mathbb{L}})^{-1} \leq \sigma \leq 1, \ |t| \leq (4\log \Delta_{\mathbb{L}})^{-1},$$

and must therefore be simple and real.

Problems involving field extensions $\mathbb{L}\,/\,\mathbb{K}$ with degree essentially larger than $\log x$, however, cannot be handled unconditionally by Proposition 4.8. Therefore, we provide the following *number field analogue of the Bombieri-Vinogradov theorem* which combines a result established by Ram Murty and Kumar Murty (1987) [81] and a recent generalization of this by Ram Murty and Petersen (2013) [82]. These statements yield an appropriate estimate for the average error term in Proposition 4.8 which, in special situations, is as good as the one obtained under GRH in Proposition 4.7.

Proposition 4.9 (Ram Murty–Kumar Murty–Petersen). *For $a \in \mathbb{Z}$ and $q \in \mathbb{N}$ let $\pi_C(x; a, q)$ denote the number of prime ideals $\mathfrak{p}$ of $\mathbb{K}$ which are unramified in $\mathbb{L}$ and satisfy $\mathcal{N}\mathfrak{p} \leq x$, $\mathcal{N}\mathfrak{p} \equiv a \ (q)$ and $\left[\frac{\mathbb{L}|\mathbb{K}}{\mathfrak{p}}\right] = C$. Let H be the largest abelian subgroup of $\mathrm{Gal}(\mathbb{L}\,/\,\mathbb{K})$ such that $H \cap C \neq \varnothing$. Further, let $\mathbb{M}$ be the fixed field of H and set $\eta := \max\{[\mathbb{M} : \mathbb{Q}] - 2, 2\}$ and $Q := x^{\frac{1}{\eta}-\varepsilon}$. Then, for any $A > 0$ we have*

$$\sum_{\substack{q \leq Q \\ \mathbb{L} \cap \mathbb{Q}(\zeta_q) = \mathbb{Q}}} \max_{(a,q)=1} \max_{y \leq x} \left| \pi_C(y; a, q) - \frac{|C|}{\varphi(q)[\mathbb{L} : \mathbb{K}]} \cdot \pi(y) \right| \ll_{\varepsilon, A} \frac{x}{\log^A x}.$$

If $\mathbb{K} = \mathbb{Q}$, then this result remains true with $Q = x^{\frac{1}{\eta}} \log^{-B} x$, where $B = B(A)$ is a positive constant depending on A.

4.3.3. Estimates for Siegel zeroes and discriminants. For later applications of Propositions 4.7 and 4.8 we need good upper bounds for possible Siegel zeroes and number field discriminants. A sufficient result for the first problem is given by the following statement due to Stark (cf. [97, p. 148]).

Proposition 4.10 (Stark, 1974). *Let $\mathbb{L}$ be a number field and set $m_{\mathbb{L}} := 4$ if $\mathbb{L}\,/\,\mathbb{Q}$ is Galois, $m_{\mathbb{L}} := 16$ if there exists a field tower $\mathbb{Q} = \mathbb{M}_0 \subset \mathbb{M}_1 \subset \cdots \subset \mathbb{M}_s = \mathbb{L}$ with each field Galois over the preceding one, and $m_{\mathbb{L}} := 4[\mathbb{L} : \mathbb{Q}]!$ otherwise. Then there exists an absolute positive constant c_3, such that*

$$\beta_0(\mathbb{L}) < \max\left\{1 - \frac{1}{m_{\mathbb{L}} \log \Delta_{\mathbb{L}}},\ 1 - \frac{1}{c_3 \Delta_{\mathbb{L}}^{1/[\mathbb{L}:\mathbb{Q}]}}\right\}.$$

As for upper bounds for number field discriminants, we note the following result due to Serre [94].

Proposition 4.11 (Serre, 1981). *Let $\mathbb{L}\,/\,\mathbb{Q}$ be a finite Galois extension which is ramified only at the primes $p_1, \ldots, p_n$. Then*

$$\log |\Delta_{\mathbb{L}}| \leq [\mathbb{L} : \mathbb{Q}] \left(\log[\mathbb{L} : \mathbb{Q}] + \sum_{i=1}^{n} \log p_i \right).$$

To conclude this chapter, we invoke Proposition 4.11 to prove upper bounds for discriminants of the fields $\mathbb{K}_{\Gamma,k} = \mathbb{K}(\sqrt[k]{\Gamma}, \zeta_k)$, for fields of this type occur quite frequently throughout this thesis.

Lemma 4.12. *Let $\mathbb{K}$ be a number field and Γ a finitely generated subgroup[11] of $\mathbb{K}^*$ of arithmetic rank γ. Then there exist positive constants c_4 and c_5, depending on Γ and $\mathbb{K}$, such that*

$$\Delta_{\mathbb{K}_{\Gamma,k}} \leq \left(c_4 \operatorname{rad}(k) \varphi(k) k^{\gamma}\right)^{c_5 [\mathbb{K}_{\Gamma,k} : \mathbb{Q}]}$$

holds for every positive integer k.

[11] Note that we allow Γ to be finite here, to extend the assertion to cyclotomic extensions $\mathbb{K}(\zeta_n) = \mathbb{K}_{\{1\},n}$.

PROOF. Let $\mathcal{P}$ be the set of primes which ramify in $(\mathbb{K}_{\Gamma,k})^{(n)}$, the normal closure of $\mathbb{K}_{\Gamma,k}$ over $\mathbb{Q}$. Since $\Delta_{\mathbb{K}_{\Gamma,k}}$ divides $\Delta_{(\mathbb{K}_{\Gamma,k})^{(n)}}$ (cf. [86, p. 213]), Proposition 4.11 yields

$$\Delta_{\mathbb{K}_{\Gamma,k}} \leq \left([(\mathbb{K}_{\Gamma,k})^{(n)} : \mathbb{Q}] \prod_{p \in \mathcal{P}} p \right)^{[(\mathbb{K}_{\Gamma,k})^{(n)} : \mathbb{Q}]}. \tag{4.5}$$

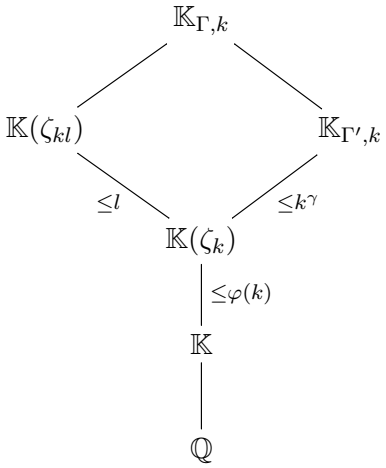
Since $\mathbb{K}^{(n)}(\zeta_k)$ is Galois over $\mathbb{Q}$, the same holds for $\mathbb{K}^{(n)}(\zeta_k, \sqrt[k]{\Gamma})$. This field, however, contains $\mathbb{K}_{\Gamma,k}$. We thus obtain

$$[(\mathbb{K}_{\Gamma,k})^{(n)} : \mathbb{Q}] \leq [\mathbb{K}^{(n)}(\zeta_k, \sqrt[k]{\Gamma}) : \mathbb{Q}] \leq [\mathbb{K}^{(n)} : \mathbb{K}] \cdot [\mathbb{K}_{\Gamma,k} : \mathbb{Q}], \tag{4.6}$$

by basic facts from Galois theory (cf. [46]) and set

$$c_5 := [\mathbb{K}^{(n)} : \mathbb{K}].$$

If ζ_l, $l \in \mathbb{N}$, is a generator of the torsion part of Γ and Γ' denotes the free part of Γ, then we clearly have $\mathbb{K}_{\Gamma,k} = \mathbb{K}(\zeta_{kl}) \cdot \mathbb{K}_{\Gamma',k}$. Hence, the display



yields

$$[\mathbb{K}_{\Gamma,k} : \mathbb{Q}] \leq l[\mathbb{K} : \mathbb{Q}]\varphi(k)k^{\gamma},$$

again by standard arguments from Galois theory. Next we observe that $\mathcal{P}$ consists of primes which divide k, ramify in $\mathbb{K}^{(n)}$ or divide a generator of Γ (cf. [54, p. 62,74]). Thus, the set $\mathcal{P}'$ of primes in $\mathcal{P}$ which do not divide k or ramify in $\mathbb{K}^{(n)}$ only depends on Γ. If we set

$$c_4 := l[\mathbb{K}^{(n)} : \mathbb{Q}] \prod_{p \in \mathcal{P}'} p,$$

then the assertion finally follows by (4.5) and (4.6). □

CHAPTER 5

Moments of the Residual Order over Prime Ideals

As explained in detail in Chapter 4, studying moments of $\mathrm{ind}_\Gamma(\mathfrak{p})$ is a hard if not hopeless task. Things, however, become much easier if one considers the residual order instead, a problem we will address in this chapter. In fact, subject to the GRH for certain number fields, we prove asymptotic formulae for moments of $\mathrm{ord}_\Gamma(\mathfrak{p})$, and thereby generalize a work of Kurlberg and Pomerance [51]. In the first section we provide a brief introduction to the problem and state the main result of this chapter which is proved in Section 5.2. Afterwards, in Sections 5.3 and 5.4, we illustrate this statement by applying it to two prominent examples.

5.1. Generalizing a work of Kurlberg and Pomerance

In [51], Kurlberg and Pomerance have recently considered the average order of $\mathrm{ord}_a(p)$, for a single rational number $a \neq 0, \pm 1$ over primes $p \nmid a$. Using techniques similar to the ones in Hooley's proof of AC under GRH, they managed to establish the following asymptotic formula under GRH.

Proposition 5.1 (Kurlberg–Pomerance, 2013). *Let $a = \alpha/\beta$ be a rational number different from $0, \pm 1$ with $(\alpha, \beta) = 1$, and set*

$$c_a := \sum_{k=1}^{\infty} \frac{\varphi(k)\,\mathrm{rad}(k)(-1)^{\omega(k)}}{k^2[\mathbb{Q}_{a,k} : \mathbb{Q}]}.$$

Then c_a converges absolutely, is positive, and, assuming GRH for the fields $\mathbb{Q}_{a,k}$, $k \in \mathbb{N}$,

$$\sum_{p \leq x} \mathrm{ord}_a(p) = c_a \cdot \mathrm{li}(x^2) + O\left(\frac{x^2}{(\log x)^{2-4/\log\log\log x}}\right)$$

holds uniformly, whenever $|\alpha|, |\beta| \leq x$.

Remark 5.2. Kurlberg and Pomerance pointed out that c_a is a rational multiple of the so called *Stephens' constant*

$$c_{Stephens} := \prod_p \left(1 - \frac{p}{p^3 - 1}\right) = 0.57599689\ldots.$$

This constant plays a crucial role in a result of Luca [69], who unconditionally proved Proposition 5.1 on average over a. We come back to this result in Section 6.4.

Let us now turn to the analogue problem in the number field setting introduced in Section 4.2. Let $\mathbb{L}/\mathbb{K}$ be a finite Galois extension of number fields, Γ a finitely generated, not necessarily torsion-free, infinite subgroup of $\mathbb{K}^*$ with arithmetic rank $\gamma \in \mathbb{N}$, and let

C be a conjugacy class[12] in $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. We are interested in the asymptotic behaviour of

$$\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*}} \mathrm{ord}_\Gamma(\mathfrak{p})^\kappa, \tag{5.1}$$

the κ-th moment of $\mathrm{ord}_\Gamma(\mathfrak{p})$ over prime ideals in $\mathcal{P}_C(\mathbb{L}/\mathbb{K})$, for any $\kappa\in\mathbb{R}_+$. Adapting the ideas of Kurlberg and Pomerance we establish asymptotic formulae for (5.1) under GRH which generalize Proposition 5.1. To give a precise statement, we define

$$C(\Gamma,n) := \left\{\sigma\in\mathrm{Gal}(\mathbb{L}_{\Gamma,n}/\mathbb{K}) : \sigma|_\mathbb{L}\in C,\ \sigma|_{\mathbb{K}_{\Gamma,n}}=\mathrm{id}\right\}, \tag{5.2}$$

for any $n\in\mathbb{N}$, noting that the fields $\mathbb{K}_{\Gamma,n}$ and $\mathbb{L}_{\Gamma,n}$ are both finite Galois extensions of $\mathbb{K}$. The exact statement of our main results goes as follows.

Theorem 5.3. *Let $\mathbb{K}$ be a number field and Γ a finitely generated infinite subgroup of $\mathbb{K}^*$ of arithmetic rank γ. Let $\mathbb{L}$ be a finite Galois extension of $\mathbb{K}$ and C a conjugacy class in $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$. Further, let $\kappa\in\mathbb{R}_+$, define $\psi_\kappa(n):=\sum_{s|n}\mu(s)s^\kappa$, and set*

$$c_{\Gamma,C}^{(\kappa)} := \sum_{n\geq 1}\frac{\psi_\kappa(n)|C(\Gamma,n)|}{n^\kappa[\mathbb{L}_{\Gamma,n}:\mathbb{K}]}.$$

Then $c_{\Gamma,C}^{(\kappa)}$ converges absolutely. Assuming GRH for the fields $\mathbb{L}_{\Gamma,n}$, $n\in\mathbb{N}$, this constant is positive and we have

$$\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*}} \mathrm{ord}_\Gamma(\mathfrak{p})^\kappa = c_{\Gamma,C}^{(\kappa)}\cdot \mathrm{li}(x^{\kappa+1}) + O\left(\frac{x^{\kappa+1}}{(\log x)^{2-3/\log\log\log x}}\right),$$

whenever $x>2$. Here, the O-term[13] depends on Γ, $\mathbb{L}$ and κ.

Remark 5.4. Note that we seemingly saved a bit upon the error term in Proposition 5.1. The reason for this is simply that, different to Theorem 5.3, the error term in Proposition 5.1 is uniform, if absolute value of nominator and denominator of a do not exceed x. Moreover, the 3 appearing in the O-term of Theorem 5.3 may even be replaced by any real number larger than $4\cdot\log 2$. This will become clear in the proof of Lemma 5.8.

Because of the alternating nature of $\psi_\kappa(n)$, it is by no means obvious whether $c_{\Gamma,C}^{(\kappa)}$ is positive or zero, and how this depends on $\mathbb{K}$, $\mathbb{L}$, C, κ, or Γ. In the rational case Kurlberg and Pomerance established the positivity by expressing c_a in terms of Euler products. Unfortunately, we failed to derive such an expression in general, and only managed to prove the positivity of $c_{\Gamma,C}^{(\kappa)}$ under GRH using a different approach which is based on ideas of Lenstra. This proof will be given in Section 5.2.3. Nevertheless, we believe in this positivity, and it seems that appropriate expressions for $c_{\Gamma,C}^{(\kappa)}$ may easily be established which underline this property, whenever one considers a fixed choice for $\mathbb{K}$, $\mathbb{L}$, Γ and C. In Sections 5.3 and 5.4 we will in fact confirm this claim by deducing precise formulae for $c_{\Gamma,C}^{(\kappa)}$ in two prominent examples which prove positivity in both cases. To start with, however, let us prove Theorem 5.3.

[12] In the present and the subsequent chapter we restrict to conjugacy classes, for convenience. The case of a union of conjugacy classes may be easily derived from this.

[13] For the remainder of this chapter and Chapter 6 we agree on the convention that a dependence of an implied constant on $\mathbb{L}$ may also include dependencies on C and $\mathbb{K}$ if we don't need the precision.

5.2. Proof of Theorem 5.3

Throughout this section we tacitly assume the occurring prime ideals of $\mathbb{K}$ to satisfy $\overline{\Gamma} \subset (\mathcal{O}_{\mathbb{K}} / \mathfrak{p})^*$, for notational convenience, as this condition fails only for finitely many prime ideals which do not effect our arguments. For all such prime ideals we recall the elementary identity

$$\operatorname{ord}_\Gamma(\mathfrak{p}) = \frac{\mathcal{N}\mathfrak{p} - 1}{\operatorname{ind}_\Gamma(\mathfrak{p})}.$$

To prove the asymptotic formula of Theorem 5.3, we let $x > 2$, set $z := \log x$ and proceed as in [51]. First, we separate prime ideals in $\mathcal{P}_C(x, \mathbb{L} / \mathbb{K})$ according to the size of $\operatorname{ind}_\Gamma(\mathfrak{p})$:

$$\begin{aligned}\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \frac{\operatorname{ord}_\Gamma(\mathfrak{p})^\kappa}{(\mathcal{N}\mathfrak{p}-1)^\kappa} &= \sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \frac{1}{\operatorname{ind}_\Gamma(\mathfrak{p})^\kappa} \\ &= \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}/\mathbb{K}) \\ \operatorname{ind}_\Gamma(\mathfrak{p}) \le z}} \frac{1}{\operatorname{ind}_\Gamma(\mathfrak{p})^\kappa} + \sum_{\substack{p \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ \operatorname{ind}_\Gamma(\mathfrak{p}) > z}} \frac{1}{\operatorname{ind}_\Gamma(\mathfrak{p})^\kappa} \\ &= \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ \operatorname{ind}_\Gamma(\mathfrak{p}) \le z}} \sum_{rs \mid \operatorname{ind}_\Gamma(\mathfrak{p})} \frac{\mu(s)}{r^\kappa} + \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ \operatorname{ind}_\Gamma(\mathfrak{p}) > z}} \frac{1}{\operatorname{ind}_\Gamma(\mathfrak{p})^\kappa}. \end{aligned} \tag{5.3}$$

Here we used the elementary identity

$$\frac{1}{n^\kappa} = \sum_{rs \mid n} \frac{\mu(s)}{r^\kappa},$$

valid for any $n \in \mathbb{N}$. Note that we are summing $\operatorname{ord}_\Gamma(\mathfrak{p})^\kappa / (\mathcal{N}\mathfrak{p}-1)^\kappa$ instead of $\operatorname{ord}_\Gamma(\mathfrak{p})^\kappa$ as it turns out to be more convenient and may easily be reverted by a simple partial summation argument. Next, we split the first term of (5.3) once more, so that (5.3) becomes

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \sum_{\substack{rs \mid \operatorname{ind}_\Gamma(\mathfrak{p}) \\ rs \le z}} \frac{\mu(s)}{r^\kappa} - \underbrace{\sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ \operatorname{ind}_\Gamma(\mathfrak{p}) > z}} \sum_{\substack{rs \mid \operatorname{ind}_\Gamma(\mathfrak{p}) \\ rs \le z}} \frac{\mu(s)}{r^\kappa}}_{=:E_2} + \underbrace{\sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ \operatorname{ind}_\Gamma(\mathfrak{p}) > z}} \frac{1}{\operatorname{ind}_\Gamma(\mathfrak{p})^\kappa}}_{=:E_1}. \tag{5.4}$$

We treat the three terms in (5.4) separately. The first of these will turn out to be the dominating term, and is treated first in Section 5.2.1. We postpone the treatment of the error terms E_1 and E_2 to Section 5.2.2.

5.2.1. Treatment of the main term. In this subsection we aim to deduce an asymptotic formula for the first term in (5.4). After a change of summation order, the aforesaid term becomes

$$\sum_{rs \le z} \frac{\mu(s)}{r^\kappa} \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}/\mathbb{K}) \\ rs \mid \operatorname{ind}_\Gamma(\mathfrak{p})}} 1. \tag{5.5}$$

We treat the inner sum of (5.5) by Proposition 4.7, the effective Čebotarev density theorem under GRH. To enable its application, it is necessary to prove the subsequent lemma.

LEMMA 5.5. *For any $n \in \mathbb{N}$ we have that $C(\Gamma, n)$ is either empty or a conjugacy class in $\operatorname{Gal}(\mathbb{L}_{\Gamma,n} / \mathbb{K})$ of size $|C|$.*

PROOF. Assume that $C(\Gamma, n)$ is not empty and let $\sigma \in C(\Gamma, n)$. Note that $C(\Gamma, n)$ is clearly closed under conjugation because $\mathbb{L}$ and $\mathbb{K}_{\Gamma,n}$ are Galois over $\mathbb{K}$. Since $\tau\sigma\tau^{-1}|_{\mathbb{L}}$ runs through C as τ runs through $\mathrm{Gal}(\mathbb{L}_{\Gamma,n} / \mathbb{K})$, $C(\Gamma, n)$ contains a conjugacy class of $\mathrm{Gal}(\mathbb{L}_{\Gamma,n} / \mathbb{K})$ with at least $|C|$ elements. On the other hand, $C(\Gamma, n) \to C$, $\sigma \mapsto \sigma|_{\mathbb{L}}$ is an injective map, since $\mathbb{L}_{\Gamma,n} = \mathbb{L} \cdot \mathbb{K}_{\Gamma,n}$ (cf. [46, p. 154]). This yields $|C(\Gamma, n)| \leq |C|$, and also proves that $C(\Gamma, n)$ must be a conjugacy class. □

Now let $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L} / \mathbb{K})$, and observe that $n \mid \mathrm{ind}_\Gamma(\mathfrak{p})$ is equivalent to $n \mid \mathrm{ind}_a(\mathfrak{p})$ for every $a \in \Gamma$, since $(\mathcal{O}_\mathbb{K} / \mathfrak{p})^*$ is a cyclic group. By a result due to DEDEKIND (cf. [86, p. 50]), this is, for all but finitely many $\mathfrak{p}$, equivalent to requiring that $\mathfrak{p}$ splits completely in $\mathbb{K}_{\Gamma,n}$. Thus we find

$$\sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L} / \mathbb{K}) \\ n \mid \mathrm{ind}_\Gamma(\mathfrak{p})}} 1 = \pi_{C(\Gamma,n)}(x, \mathbb{L}_{\Gamma,n} / \mathbb{K}) + O(1),$$

where the implied constant may depend on Γ and $\mathbb{L}$ (cf. [86, p. 50]). Proposition 4.7, Lemma 5.5 and Lemma 4.12 then yield[14]

$$\sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L} / \mathbb{K}) \\ n \mid \mathrm{ind}_\Gamma(\mathfrak{p})}} 1 - \frac{|C(\Gamma, n)|}{[\mathbb{L}_{\Gamma,n} : \mathbb{K}]} \mathrm{li}(x) \ll \frac{|C|}{[\mathbb{L}_{\Gamma,n} : \mathbb{K}]} x^{1/2} \log\left(\Delta_{\mathbb{L}_{\Gamma,n}} x^{[\mathbb{L}_{\Gamma,n} : \mathbb{Q}]}\right) + \log\left(\Delta_{\mathbb{L}_{\Gamma,n}}\right)$$

$$\ll_{\mathbb{L},\Gamma} x^{1/2} \log x.$$

Hence, (5.5) becomes

$$\mathrm{li}(x) \sum_{rs \leq z} \frac{\mu(s)}{r^\kappa} \cdot \frac{|C(\Gamma, rs)|}{[\mathbb{L}_{\Gamma,rs} : \mathbb{K}]} + O_{\mathbb{L},\Gamma}\left(\sum_{n \leq z} x^{1/2} \log x \left| \sum_{rs=n} \frac{\mu(s)}{r^\kappa} \right|\right). \tag{5.6}$$

The inner sum of the O-term is ≤ 1 since $\kappa \in \mathbb{R}_+$. Hence

$$\sum_{n \leq z} x^{1/2} \log x \left| \sum_{rs=n} \frac{\mu(s)}{r^\kappa} \right| \leq z x^{1/2} \log x. \tag{5.7}$$

The next step consists of showing that the sum over rs in (5.6) converges absolutely, as $z \to \infty$, and computing its limit. To this end, we note the following estimate[15] for the field degrees $[\mathbb{K}_{\Gamma,n} : \mathbb{K}]$.

LEMMA 5.6. *For any $n \in \mathbb{N}$ we have*

$$[\mathbb{K}_{\Gamma,n} : \mathbb{K}] \gg n\varphi(n),$$

where the implied constant depends on $\mathbb{K}$ and Γ.

PROOF. We only give a proof for the case where $\mathbb{K} / \mathbb{Q}$ is abelian. The general case may be handled by similar arguments but is more elaborate. Let $a = \alpha/\beta \in \Gamma$, with $\alpha, \beta \in \mathcal{O}_\mathbb{K}$, be of infinite order in Γ. By the estimate

$$[\mathbb{K}_{\Gamma,n} : \mathbb{K}] \geq [\mathbb{K}(\sqrt[n]{a}, \zeta_n) : \mathbb{K}],$$

we may restrict to bounding the degree $[\mathbb{K}(\sqrt[n]{a}, \zeta_n) : \mathbb{K}]$ from below. Since $\mathbb{K}(\sqrt[n]{a}, \zeta_n)$ coincides with $\mathbb{K}(\sqrt[n]{\beta^{n-1}\alpha}, \zeta_n)$, we may without loss of generality assume $a \in \mathcal{O}_\mathbb{K}$. By

[14] Note that the assertion of Proposition 4.7 trivially holds if $C(\Gamma, n)$ is empty.

[15] It should be mentioned that Lemma 5.6 is not sharp and could presumably be replaced by the stronger bound $[\mathbb{K}_{\Gamma,n} : \mathbb{K}] \gg n^\gamma \varphi(n)$ instead. However, the corresponding proof appears more involved and Lemma 5.6 suffices for our purposes, so we abstain from this precision, for convenience.

Lemma 1.6 of [103] we may then choose an embedding of $\mathbb{K}$ into $\mathbb{C}$ such that $a\overline{a} \in \mathbb{R}$ is different from 1, because a is not a root of unity. Here, $\overline{a}$ denotes the complex conjugate of a. The obvious estimate

$$\begin{aligned}[\mathbb{K}(\sqrt[n]{a}, \zeta_n) : \mathbb{K}] &= [\mathbb{K}(\sqrt[n]{a}, \zeta_n) : \mathbb{K}(\zeta_n)] \cdot [\mathbb{K}(\zeta_n) : \mathbb{K}] \\ &\gg_{\mathbb{K}} [\mathbb{K}(\sqrt[n]{a}, \zeta_n) : \mathbb{K}(\zeta_n)] \cdot \varphi(n)\end{aligned}$$

breaks down the problem to appropriately bound $[\mathbb{K}(\sqrt[n]{a}, \zeta_n) : \mathbb{K}(\zeta_n)]$ from below. By Kummer theory (cf. [12, p. 205ff]) this degree equals n/m, where m is the largest divisor of n such that a is an m-th power in $\mathbb{K}(\zeta_n)$. Since $\mathbb{K} \,/\, \mathbb{Q}$ is assumed abelian, the same holds true for $\mathbb{K}(\zeta_n) / \mathbb{Q}$ and we clearly have $\sqrt[m]{a\overline{a}} \in \mathbb{K}(\zeta_n)$. Hence, $\mathbb{Q}(\sqrt[m]{a\overline{a}})$ must also be abelian over $\mathbb{Q}$. By the choice of the complex embedding from above, this however implies that m is bounded from above by a constant only depending[16] on a, and we finally obtain

$$[\mathbb{K}(\sqrt[n]{a}, \zeta_n) : \mathbb{K}] \gg_{\mathbb{K}} [\mathbb{K}(\sqrt[n]{a}, \zeta_n) : \mathbb{K}(\zeta_n)] \cdot \varphi(n) \gg_a n\varphi(n)$$

which proves the assertion. □

Now, recall the definition of $\psi_\kappa(n)$ in Theorem 5.3 which gives us

$$\sum_{rs \le z} \frac{\mu(s)}{r^\kappa} \cdot \frac{|C(\Gamma, rs)|}{[\mathbb{L}_{\Gamma,rs} : \mathbb{K}]} = \sum_{n \le z} \frac{\psi_\kappa(n) |C(\Gamma, n)|}{n^\kappa [\mathbb{L}_{\Gamma,n} : \mathbb{K}]}.$$

By Lemmas 5.5, 5.6 and 4.5 and the obvious estimate $|\psi_\kappa(n)| \le \operatorname{rad}(n)^\kappa$, this sum converges absolutely, as $z \to \infty$:

$$\sum_{n > z} \frac{\psi_\kappa(n) |C(\Gamma, n)|}{n^\kappa [\mathbb{L}_{\Gamma,n} : \mathbb{K}]} \ll_{\Gamma,\mathbb{K}} \sum_{n > z} \frac{\operatorname{rad}(n)^\kappa}{\varphi(n) n^{\kappa+1}} \le \sum_{n > z} \frac{1}{\varphi(n) n} \ll \frac{1}{z}.$$

Combining this estimate with (5.5), (5.6) and (5.7), we finally obtain

$$\sum_{rs \le z} \frac{\mu(s)}{r^\kappa} \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(\mathbb{L} \,/\, \mathbb{K}) \\ rs \mid \operatorname{ind}_\Gamma(\mathfrak{p})}} 1 = c_{\Gamma,C}^{(\kappa)} \cdot \operatorname{li}(x) + O_{\Gamma,\mathbb{L}}\left(z x^{1/2} \log x + \frac{x}{z \log x} \right), \tag{5.8}$$

with $c_{\Gamma,C}^{(\kappa)}$ as asserted in Theorem 5.3.

5.2.2. Treatment of the error terms. To complete the proof of the asserted asymptotic formula in Theorem 5.3, it remains to give reasonable upper bounds for the remainder terms E_1 and E_2 defined in (5.4). For this purpose we prove the following lemma, a simple number field generalization[17] of Theorem 6 of [51].

Lemma 5.7. *Assume the GRH for the fields $\mathbb{L}_{\Gamma,n}$, $n \in \mathbb{N}$. Then for $x > 2$ and $1 \le L \le \log x$, we have*

$$\left| \left\{ \mathfrak{p} \in \mathcal{P}(x, \mathbb{K}) : \operatorname{ord}_\Gamma(\mathfrak{p}) \le \frac{\mathcal{N}\mathfrak{p} - 1}{L} \right\} \right| \ll \frac{\pi(x)}{L} + \frac{x \log\log x}{\log^2 x},$$

where the implied constant depends on Γ and $\mathbb{K}$.

[16] The constant accounts for possible powers of $a\overline{a}$ which are contained in $\mathbb{Q}$ and hence in $\mathbb{K}$. Since $(\alpha\overline{\alpha})/(\beta\overline{\beta})$ is an l-th power in $\mathbb{K}$ for some $l \mid n$ if and only if the same holds for $\alpha\overline{\alpha}\beta^{n-1}\overline{\beta^{n-1}}$, it was warrantable to assume $a \in \mathcal{O}_\mathbb{K}$ in the beginning.

[17] In Lemma 5.7, one may replace L by L^γ in the denominator, if Lemma 5.6 holds with the stronger bound $[\mathbb{K}_{\Gamma,n} : \mathbb{K}] \gg n^\gamma \varphi(n)$.

PROOF. To begin with, we note that one may for convenience restrict to prime ideals of $\mathbb{K}$ which are linear, for the contribution of the remaining prime ideals is $O_{\mathbb{K}}(\sqrt{x}/\log x)$. Thus it suffices to bound the cardinality of

$$\left\{\mathfrak{p} \in \mathcal{P}(x, \mathbb{K}) \text{ linear} : \operatorname{ord}_\Gamma(\mathfrak{p}) \leq \frac{\mathcal{N}\mathfrak{p} - 1}{L}\right\}$$

from above. We proceed as in the corresponding proof in [51], but only deal with those prime ideals which satisfy $\operatorname{ind}_\Gamma(\mathfrak{p}) > x^{1/2}\log^2 x$. For the remaining prime ideals one simply uses Proposition 4.7 and Lemma 5.6 to generalize the arguments in [51]. Let $a = \alpha/\beta$, with $\alpha, \beta \in \mathcal{O}_{\mathbb{K}}$, be of infinite order in Γ. Since $\operatorname{ord}_a(\mathfrak{p}) \leq \operatorname{ord}_\Gamma(\mathfrak{p})$, it is sufficient to estimate the size of

$$M := \left\{\mathfrak{p} \in \mathcal{P}(x, \mathbb{K}) \text{ linear} : \operatorname{ord}_a(\mathfrak{p}) \leq \frac{\mathcal{N}\mathfrak{p} - 1}{x^{1/2}\log^2 x}\right\}.$$

To do so, we generalize HOOLEY's argument [42] presented in Section 1.2 to number fields (cf. also [47, p. 353]). If $a^t \equiv 1 \bmod \mathfrak{p}$, we clearly have $\mathfrak{p} \mid \alpha^t - \beta^t$. Hence, we obtain

$$\prod_{\mathfrak{p}\in M} \mathfrak{p} \Bigg| \prod_{t \leq \sqrt{x}/\log^2 x} (\alpha^t - \beta^t).$$

From this one deduces

$$2^{\frac{|M|}{[\mathbb{K}:\mathbb{Q}]}} \leq \prod_{\substack{p \leq x \\ M \ni \mathfrak{p} \mid p}} p \Bigg| \prod_{t \leq \sqrt{x}/\log^2 x} \left|\mathrm{N}_{\mathbb{K}/\mathbb{Q}}\left(\alpha^t - \beta^t\right)\right|$$

since prime ideals in M are linear, and there are at most $[\mathbb{K} : \mathbb{Q}]$ prime ideals of $\mathbb{K}$ lying over the same rational prime. If σ runs through the $[\mathbb{K} : \mathbb{Q}]$ embeddings of $\mathbb{K}$ into $\mathbb{C}$, we clearly have

$$\begin{aligned}\left|\mathrm{N}_{\mathbb{K}/\mathbb{Q}}\left(\alpha^t - \beta^t\right)\right| &= \prod_\sigma \left|\sigma(\alpha)^t - \sigma(\beta)^t\right| \\ &\leq \prod_\sigma \left(|\sigma(\alpha)|^t + |\sigma(\beta)|^t\right) \\ &\leq A^{t[\mathbb{K}:\mathbb{Q}]},\end{aligned}$$

because $t \geq 1$, where we put $A := 2 \cdot \max_\sigma \{\sigma(\alpha), \sigma(\beta)\}$. Finally, we obtain

$$|M| \leq [\mathbb{K} : \mathbb{Q}]^2 \log A \sum_{t \leq \sqrt{x}/\log^2 x} t \leq [\mathbb{K} : \mathbb{Q}]^2 \log A \cdot \frac{x}{\log^4 x}. \qquad \square$$

From this lemma we infer the following upper bounds for the remainders E_1 and E_2.

LEMMA 5.8. *Under GRH for the fields $\mathbb{L}_{\Gamma,n}$, $n \in \mathbb{N}$, we have*

$$E_1 \ll_{\Gamma,\mathbb{K}} \frac{x \log\log x}{(\log x)^{2+\kappa}} \qquad \text{and} \qquad E_2 \ll_{\Gamma,\mathbb{K}} \frac{x}{(\log x)^{2-3/\log\log\log x}}.$$

PROOF. From Lemma 5.7 and the arrangement $z = \log x$ one immediately deduces

$$E_1 = \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K}) \\ \operatorname{ind}_\Gamma(\mathfrak{p})>z}} \frac{1}{\operatorname{ind}_\Gamma(\mathfrak{p})^\kappa} \ll_{\Gamma,\mathbb{K}} \frac{1}{z^\kappa}\left(\frac{\pi(x)}{z} + \frac{x\log\log x}{\log^2 x}\right) \ll \frac{x\log\log x}{\log^{2+\kappa} x}.$$

To estimate E_2, we proceed as in [51], and observe

$$\alpha_z(n) := \Big|\sum_{\substack{rs|n\\ rs\le z}} \frac{\mu(s)}{r^\kappa}\Big| \le \sum_{\substack{d|n\\ d\le z}} \Big|\sum_{s|d} \frac{\mu(s)s^\kappa}{d^\kappa}\Big| = \sum_{\substack{d|n\\ d\le z}} \frac{|\psi_\kappa(d)|}{d^\kappa}. \tag{5.9}$$

From this we easily infer the estimates

$$\alpha_z(n) \le z \tag{5.10}$$

and

$$\alpha_z(n) \le \prod_{\substack{p^e\|n\\ p\le z}} \left(1 + \frac{p^\kappa - 1}{p^\kappa} + \cdots + \frac{p^\kappa - 1}{p^{\kappa e}}\right) < 2^{\omega_z(n)}, \tag{5.11}$$

where $\omega_z(n)$ shall denote the number of distinct prime divisors $\le z$ of n. We have

$$|E_2| \le \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathrm{ind}_\Gamma(\mathfrak{p})>z}} \alpha_z(\mathrm{ind}_\Gamma(\mathfrak{p})) \le E_{2,1} + E_{2,2} + E_{2,3}$$

with

$$E_{2,1} := \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathrm{ind}_\Gamma(\mathfrak{p})>z\\ \omega_z(\mathrm{ind}_\Gamma(\mathfrak{p}))\le w}} \alpha_z(\mathrm{ind}_\Gamma(\mathfrak{p})), \qquad E_{2,2} := \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ z<\mathrm{ind}_\Gamma(\mathfrak{p})\le x^{1/2}\log^2 x\\ \omega_z(\mathrm{ind}_\Gamma(\mathfrak{p}))>w}} \alpha_z(\mathrm{ind}_\Gamma(\mathfrak{p})),$$

$$E_{2,3} := \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathrm{ind}_\Gamma(\mathfrak{p})>x^{1/2}\log^2 x}} \alpha_z(\mathrm{ind}_\Gamma(\mathfrak{p})),$$

where $w := 4\log z/\log\log z$. Combining Lemma 5.7 with (5.11) immediately yields

$$\begin{aligned} E_{2,1} &\le 2^w \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathrm{ind}_\Gamma(\mathfrak{p})>z}} 1 \ll_{\Gamma,\mathbb{K}} 2^w\left(\frac{x}{z\log x} + \frac{x\log\log x}{\log^2 x}\right) \ll 2^w\cdot\frac{x\log\log x}{\log^2 x} \\ &\ll \frac{x}{\log^2 x}\exp\left(\frac{4\log 2\log\log x}{\log\log\log x} + \log\log\log x\right) \ll \frac{x}{(\log x)^{2-3/\log\log\log x}} \end{aligned} \tag{5.12}$$

since $4\cdot\log 2 < 3$. As for $E_{2,3}$, we proceed as in the proof of Lemma 5.7, and utilizing (5.10) we easily obtain

$$E_{2,3} \le z \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathrm{ind}_\Gamma(\mathfrak{p})>x^{1/2}\log^2 x}} 1 \ll_{\Gamma,\mathbb{K}} \frac{zx}{\log^4 x} = \frac{x}{\log^3 x}. \tag{5.13}$$

The estimation of $E_{2,2}$ is the hardest part and we only show how to break it down to the corresponding problem in [51]. To start with, we interchange summation order and obtain

$$E_{2,2} \le z \sum_{\substack{z<n<x^{1/2}\log^2 x\\ \omega_z(n)>w}} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathrm{ind}_\Gamma(\mathfrak{p})=n}} 1 \le z \sum_{\substack{z<n<x^{1/2}\log^2 x\\ \omega_z(n)>w}} \sum_{\substack{\mathfrak{p}\in\mathcal{P}(x,\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (n)}} 1 \tag{5.14}$$

by (5.10). Separating prime ideals of $\mathbb{K}$ by their inertia degree $f_{\mathfrak{p}}$ over $\mathbb{Q}$, the Brun-Titchmarsh inequality yields

$$\begin{aligned}\sum_{\substack{\mathfrak{p}\in\mathcal{P}(x,\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (n)}} 1 &= \sum_{\substack{\mathfrak{p}\in\mathcal{P}(x,\mathbb{K})\\ f_{\mathfrak{p}}=1\\ \mathcal{N}\mathfrak{p}\equiv 1\ (n)}} 1 + \sum_{\substack{\mathfrak{p}\in\mathcal{P}(x,\mathbb{K})\\ f_{\mathfrak{p}}=2\\ \mathcal{N}\mathfrak{p}\equiv 1\ (n)}} 1 + O(x^{1/3})\\ &\ll_{\mathbb{K}} \pi(x;1,n) + \pi(x^{1/2};1,n) + \pi(x^{1/2};-1,n) + x^{1/3}\\ &\ll \frac{x}{\varphi(n)\log x} + x^{1/3}.\end{aligned}$$

Inserting this into (5.14) and recalling the definition z, we obtain

$$E_{2,2} \ll_{\mathbb{K}} \frac{zx}{\log x} \sum_{\substack{z<n<x^{1/2}\log^2 x\\ \omega_z(n)>w}} \frac{1}{\varphi(n)} = x \sum_{\substack{z<n<x^{1/2}\log^2 x\\ \omega_z(n)>w}} \frac{1}{\varphi(n)}.$$

As shown in [51], the sum over n is $O(\log^{-2} x)$ and hence $E_{2,2} \ll_{\mathbb{K}} x/\log^2 x$. Combining this estimate with (5.12) and (5.13), we obtain the desired estimate for E_2. □

Combining (5.3), (5.4) with (5.8) and Lemma 5.8, and recalling that $z = \log x$, we finally obtain

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \frac{\mathrm{ord}_\Gamma(\mathfrak{p})^\kappa}{(\mathcal{N}\mathfrak{p}-1)^\kappa} = c^{(\kappa)}_{\Gamma,C}\cdot \mathrm{li}(x) + O\left(\frac{x}{(\log x)^{2-3/\log\log\log x}}\right), \tag{5.15}$$

where the implied constant may depend on $\mathbb{L}$, Γ and κ. A simple partial summation argument completes the proof of the asserted asymptotic formula in Theorem 5.3. □

5.2.3. The positivity of $c^{(\kappa)}_{\Gamma,C}$ under GRH. Let us now take a closer look at $c^{(\kappa)}_{\Gamma,C}$. Unfortunately, the involved field degrees prevent us from expressing this constant in terms of Euler products, and due to the alternating of $\psi_\kappa(n)$, we failed to establish its positivity in general. However, we managed to prove this fact at least under GRH.

Lemma 5.9. *Assume GRH for the fields $\mathbb{L}_{\Gamma,n}$, $n\in\mathbb{N}$. Then the constant $c^{(\kappa)}_{\Gamma,C}$ is positive for every choice of $\mathbb{K}$, Γ, $\mathbb{L}$, C and κ.*

To prove this statement, we disregard the definition of $c^{(\kappa)}_{\Gamma,C}$ and choose a rougher approach. The key idea is the following. For any $n\in\mathbb{N}$, we have the trivial bound

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \frac{\mathrm{ord}_\Gamma(\mathfrak{p})^\kappa}{(\mathcal{N}\mathfrak{p}-1)^\kappa} \geq \frac{1}{n^\kappa} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathrm{ind}_\Gamma(\mathfrak{p})\mid n}} 1. \tag{5.16}$$

By results of Lenstra [58], valid under GRH, the sum on the right of (5.16) runs either over a finite set of prime ideals, or over a set of prime ideals of positive density. For a fixed choice of $\mathbb{K},\mathbb{L},\Gamma$, and C, it is easy to show that the first case does not occur for infinitely many n. For such n, the right side of (5.16) is then $\gg x/\log x$ which proves Lemma 5.9 and completes the proof of Theorem 5.3. We proceed with a rigorous account of these arguments.

Proof. Let $n\in\mathbb{N}$. Following Lenstra (cf. Proposition 2.4), we set $q(l) := l\cdot l^{\nu_l(n)}$, for every rational prime l, and assume GRH. Let h denote the product of primes l for which $\Gamma\subset\mathbb{K}^{*q(l)}$, a finite number by Lemma 5.1 of [58]. By Proposition 2.6, the set

$$M(n) := \{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K}) : \mathrm{ind}_\Gamma(\mathfrak{p}) \mid n\}$$

has positive density if and only if there exists $\sigma \in \mathrm{Gal}(\mathbb{L}(\zeta_h)/\mathbb{K})$ such that

$$\sigma\,|_{\mathbb{L}} \in C \qquad \text{and} \qquad \sigma\,|_{\mathbb{L}_{\Gamma,q(l)}} \neq \mathrm{id}\,, \text{ whenever } \mathbb{L}_{\Gamma,q(l)} \subset \mathbb{L}(\zeta_h). \tag{5.17}$$

Certainly, h does not increase if we enlarge n by multiplying it with some positive integer. Therefore, we may choose n a sufficiently large multiple of h, so that $\mathbb{L}_{\Gamma,q(l)} \not\subset \mathbb{L}(\zeta_h)$ for any prime l. For such n, condition (5.17) is obviously true, and the assertion follows. □

Remark 5.10. Another way to prove Lemma 5.9 under GRH is to utilize Lemma 5.7 with L sufficiently small, so that the left side of (5.15) is bounded from below by a function of x which dominates the error term in (5.15). We will use a similar argument to prove the positivity of an asymptotic constant in a related elliptic curve problem which we consider in Chapter 9.

Now that we have convinced ourselves of the positivity of $c^{(\kappa)}_{\Gamma,C}$, at least under GRH, we spend the remainder of this chapter to address its computation in two special cases: In Section 5.3 we consider a real quadratic field $\mathbb{K}$ and compute the asymptotic constant for κ-th moments of the residual order of its group of units $\mathcal{U}_{\mathbb{K}}$ over all prime ideals of $\mathbb{K}$. Afterwards, in Section 5.4, we deal with the distribution of $\mathrm{ord}_a(p)$ for a positive rational number a over primes p in an arithmetic progression modulo an odd prime q.

5.3. Residual order of units of a real quadratic field modulo prime ideals

As a first example for the computation of the asymptotic constant of Theorem 5.3, we consider moments of the residual order of the group of units of a real quadratic field over all of its prime ideals. Hence, we let $\mathbb{K} := \mathbb{Q}(\sqrt{d})$, with squarefree $d \in \mathbb{N}$, and set $\Gamma := \mathcal{U}_{\mathbb{K}} = \langle \pm\varepsilon \rangle$, where $\varepsilon \geq 1$ denotes a fundamental unit of $\mathbb{K}$. The discriminant of $\mathbb{K}$ will be denoted by Δ, i.e. $\Delta = d$ if $d \equiv 1\ (4)$, and $\Delta = 4d$ otherwise. As we consider the reduction of Γ modulo all prime ideals of $\mathbb{K}$, we set $\mathbb{L} := \mathbb{K}$, thence $C := \{\mathrm{id}\}$. For any $n \in \mathbb{N}$, we infer $C(\Gamma, n) = \{\mathrm{id}\}$, straight from its definition (5.2). Hence, by Theorem 5.3 we have

$$c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}} = \sum_{n\geq 1} \frac{\psi_\kappa(n)}{n^\kappa [\mathbb{K}(\zeta_n,\, \sqrt[n]{\varepsilon},\, \sqrt[n]{-\varepsilon}) : \mathbb{K}]} = \sum_{n\geq 1} \frac{\psi_\kappa(n)}{n^\kappa [\mathbb{K}(\zeta_{2n},\, \sqrt[n]{\varepsilon}) : \mathbb{K}]}, \tag{5.18}$$

for any $\kappa \in \mathbb{R}_+$. Thus, the main part of computing $c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}}$ consists of determining the field degrees $[\mathbb{K}(\sqrt[n]{\varepsilon}, \zeta_{2n}) : \mathbb{K}]$. Beforehand, we wish to stress the necessity to distinguish between the cases $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = 1$ and $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = -1$. The underlying issue is the following: In the latter case, $\mathbb{K}(\sqrt{\varepsilon})$ is clearly not Galois over $\mathbb{Q}$ which turns out to be very convenient for the computation of the field degrees $[\mathbb{K}(\sqrt[n]{\varepsilon}, \zeta_{2n}) : \mathbb{K}]$. In case $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = 1$, however, $\mathbb{K}(\sqrt{\varepsilon})$ is Galois over $\mathbb{Q}$ with Galois group isomorphic to $C_2 \oplus C_2$. Apart from $\mathbb{K}$ there are then two other quadratic subfields of $\mathbb{K}(\sqrt{\varepsilon})$ which causes difficulties in the computation of $[\mathbb{K}(\sqrt[n]{\varepsilon}, \zeta_{2n}) : \mathbb{K}]$. The aforesaid quadratic subfields are given by

$$\mathbb{K}^+ := \mathbb{Q}(\sqrt{\varepsilon} + \sqrt{\varepsilon}^{-1}) \qquad \text{and} \qquad \mathbb{K}^- := \mathbb{Q}(\sqrt{\varepsilon} - \sqrt{\varepsilon}^{-1}),$$

with respective discriminants Δ^+ and Δ^- (cf. [90]). Note that the odd parts of Δ^+ and Δ^- are coprime, and one has $\mathbb{K} = \mathbb{Q}(\sqrt{\Delta^+ \cdot \Delta^-})$. Both properties are easily inferred from the definition of $\mathbb{K}^+$ and $\mathbb{K}^-$. As for the field degrees $[\mathbb{K}(\sqrt[n]{\varepsilon}, \zeta_{2n}) : \mathbb{K}]$, we obtain the following statement.

LEMMA 5.11. *For any $n \in \mathbb{N}$, we have*

$$[\mathbb{K}(\sqrt[n]{\varepsilon}, \zeta_{2n}) : \mathbb{K}] = \frac{n\varphi(2n)}{\vartheta(n)},$$

with

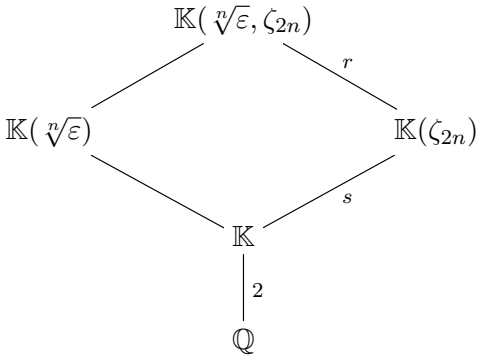
$$\vartheta(n) := \begin{cases} 2, & \text{if } \Delta \mid 2n, \\ 1, & \text{otherwise,} \end{cases}$$

if $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = -1$, *and*

$$\vartheta(n) := \begin{cases} 4, & \text{if } \operatorname{lcm}(\Delta, \Delta^+, \Delta^-) \mid 2n, \\ 1, & \text{if } \Delta^+ \nmid 2n \text{ and } \Delta^- \nmid 2n, \\ 2, & \text{otherwise,} \end{cases}$$

if $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = 1$.

PROOF. We proceed similar to the proofs of Lemma 7 in [90] and Proposition 4.1 in [101]. Let $n \in \mathbb{N}$, and consider the following diagram of field extensions:



To determine s, we first note that

$$s = \begin{cases} \varphi(2n), & \text{if } \sqrt{d} \notin \mathbb{Q}(\zeta_{2n}), \\ \frac{\varphi(2n)}{2}, & \text{if } \sqrt{d} \in \mathbb{Q}(\zeta_{2n}). \end{cases}$$

If $d \equiv 1 \ (4)$, we have $\sqrt{d} \in \mathbb{Q}(\zeta_{2n})$ if and only if $d \mid n$. If $d \equiv 2, 3 \ (4)$, then $\mathbb{Q}(\sqrt{d})$ is contained in $\mathbb{Q}(\zeta_{2n})$ if and only if $2d \mid n$. These are easy consequences of Theorem 8.3 of [86, p. 50] and the theory of cyclotomic fields (see e.g. [54, p. 76f]). It remains to compute r according to the sign of $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon)$.

Assume that $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = -1$, and let p be a prime dividing n. If ε was a p-th power in $\mathbb{K}(\zeta_{2n})$, the extension $\mathbb{Q}(\sqrt[p]{\varepsilon})/\mathbb{Q}$ would be a subextension of the abelian extension $\mathbb{K}(\zeta_{2n})/\mathbb{Q}$, and hence abelian too. But $\mathbb{Q}(\sqrt[p]{\varepsilon})/\mathbb{Q}$ is not even Galois. (Since $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = -1$ this also holds for $p = 2$ as mentioned above.) So ε cannot be a p-th power in $\mathbb{K}(\zeta_{2n})$. Now assume that $4 \mid n$, and -4ε is a 4-th power in $\mathbb{K}(\zeta_{2n})$. Since $\varepsilon > 0$ and $1 + i \in \mathbb{K}(\zeta_{2n})$ this would yield the existence of $x \in \mathbb{K}(\zeta_{2n}) \cap \mathbb{R}$ such that

$$4\varepsilon = |-4\varepsilon| = |x + ix|^4 = 4x^4.$$

But as we have seen, this is impossible, for ε cannot be a perfect power in $\mathbb{K}(\zeta_{2n})$. Thus, $X^n - \varepsilon$ is irreducible over $\mathbb{K}(\zeta_{2n})$ (cf. [46, p. 170]), and we have $r = n$.

Now assume $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = 1$. By Kummer theory the degree r equals n/m where m is the largest integer such that ε is an m-th power in $\mathbb{K}(\zeta_{2n})$ (cf. [12, p. 205ff]). As before, one may easily show that m is not divisible by an odd prime. Also m is not divisible by

4. For otherwise $\mathbb{Q}(\sqrt[4]{\varepsilon})/\mathbb{Q}$, which is clearly not normal, would be a subextension of the abelian extension $\mathbb{K}(\zeta_{2n})/\mathbb{Q}$. Thus we have $r = n/2$ if $\sqrt{\varepsilon} \in \mathbb{K}(\zeta_{2n})$ and $r = n$ otherwise. Clearly, $\sqrt{\varepsilon} \in \mathbb{K}(\zeta_{2n})$ holds if and only if one of $\sqrt{\Delta^+}$ or $\sqrt{\Delta^-}$ (and hence the other, too) is contained in $\mathbb{K}(\zeta_{2n})$. If one of Δ^+ and Δ^- divides $2n$, then $\sqrt{\Delta^+}$ and $\sqrt{\Delta^-}$ are contained in $\mathbb{K}(\zeta_{2n})$ by the same arguments as above. If both Δ^+ and Δ^- do not divide $2n$, then Δ cannot divide $2n$ either. Hence, neither of K, $\mathbb{K}^+$ and $\mathbb{K}^-$ is a subfield of $\mathbb{Q}(\zeta_{2n})$, whence the degree of the composite field $\mathbb{Q}(\sqrt{\varepsilon}) \cdot \mathbb{Q}(\zeta_{2n})$ over $\mathbb{Q}$ equals $4\varphi(2n)$ and $\sqrt{\varepsilon}$ is not contained in $\mathbb{K}(\zeta_{2n})$. □

To be in the position of giving a concise expression for $c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}}$, let us introduce some auxiliary notation. For any $n \in \mathbb{N}$, we define

$$f_\kappa(n) := \frac{\psi_\kappa(n)}{n^{\kappa+1}\varphi(n)},$$

clearly a multiplicative function, and set

$$F_\kappa(n) := \prod_{p \mid n} \frac{p^{\kappa+2}}{p^{\kappa+2}-1} \qquad \text{and} \qquad G_\kappa(n) := \prod_{p \mid n} \left(1 - \frac{p^\kappa - 1}{p-1} \frac{p}{p^{\kappa+2}-1}\right). \tag{5.19}$$

The following relation between these quantities will be of great value.

Lemma 5.12. *For $a, b \in \mathbb{N}$ such that $b \mid a$ we have*

$$\sum_{\substack{n \geq 1 \\ \mathrm{rad}(n) \mid a}} f_\kappa(bn) = \frac{f_\kappa(b) F_\kappa(b) G_\kappa(a)}{G_\kappa(b)}.$$

Proof. Since $f_\kappa(n)$ is multiplicative, we have

$$\sum_{\substack{n \geq 1 \\ \mathrm{rad}(n) \mid a}} f_\kappa(bn) = \sum_{\substack{l \geq 1 \\ \mathrm{rad}(l) \mid b}} \sum_{\substack{m \geq 1 \\ (m,b)=1 \\ \mathrm{rad}(m) \mid a}} f_\kappa(blm) = \sum_{\substack{l \geq 1 \\ \mathrm{rad}(l) \mid b}} f_\kappa(bl) \sum_{\substack{m \geq 1 \\ (m,b)=1 \\ \mathrm{rad}(m) \mid a}} f_\kappa(m). \tag{5.20}$$

Using the mutliplicativity of $f_\kappa(n)$ again, the sum over m is easily expressed in terms of geometric sums:

$$\sum_{\substack{m \geq 1 \\ (m,b)=1 \\ \mathrm{rad}(m) \mid a}} f_\kappa(m) = \prod_{\substack{p \mid a \\ p \nmid b}} \left(1 + \sum_{i \geq 1} \frac{1 - p^\kappa}{p^{(\kappa+1)i}\varphi(p^i)}\right) = \frac{G_\kappa(a)}{G_\kappa(b)}.$$

To treat the sum over l in (5.20), we note that

$$f_\kappa(p^{e_1}p^{e_2}) = \frac{f_\kappa(p^{e_1})}{p^{e_2(\kappa+2)}}$$

holds for any prime p, and integers $e_1 \geq 1$ and $e_2 \geq 0$. Thus we obtain

$$\sum_{\substack{l \geq 1 \\ \mathrm{rad}(l) \mid b}} f_\kappa(bl) = f_\kappa(b) \sum_{\substack{l \geq 1 \\ \mathrm{rad}(l) \mid b}} \frac{1}{l^{\kappa+2}} = f_\kappa(b) F_\kappa(b),$$

which completes the proof. □

To make life even easier, we introduce further notation. If $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = -1$, we write

$$D := \begin{cases} \Delta, & \text{if } \Delta \equiv 1 \ (4), \\ \frac{\Delta}{2}, & \text{if } \Delta \equiv 0 \ (4). \end{cases}$$

If $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = 1$, we let

$$D := \begin{cases} \mathrm{lcm}(\Delta, \Delta^+, \Delta^-), & \text{if } \mathrm{lcm}(\Delta, \Delta^+, \Delta^-) \equiv 1 \ (4), \\ \mathrm{lcm}(\Delta, \Delta^+, \Delta^-)/2, & \text{if } \mathrm{lcm}(\Delta, \Delta^+, \Delta^-) \equiv 0 \ (4), \end{cases}$$

and set

$$D^+ := \begin{cases} \Delta^+, & \text{if } \Delta^+ \equiv 1 \ (4), \\ \frac{\Delta^+}{2}, & \text{if } \Delta^+ \equiv 0 \ (4), \end{cases} \quad \text{and} \quad D^- := \begin{cases} \Delta^-, & \text{if } \Delta^- \equiv 1 \ (4), \\ \frac{\Delta^-}{2}, & \text{if } \Delta^- \equiv 0 \ (4). \end{cases}$$

Furthermore, we set

$$c^{(\kappa)} := \prod_p \left(1 - \frac{p^\kappa - 1}{p-1} \frac{p}{p^{\kappa+2}-1}\right). \tag{5.21}$$

REMARK 5.13. Note that $c^{(1)}$ yields the Stephens' constant introduced in Remark 5.2. The subsequent theorem reveals that $c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}}$ is a positive rational multiple of $c^{(\kappa)}$, and in Section 5.4 we will convince ourselves of the same phenomenon in another setting. We believe that this phenomenon holds true in general, and $c^{(\kappa)}_{\Gamma,C}$ is a positive rational multiple of $c^{(\kappa)}$, whenever Γ has arithmetic rank γ equal to 1. Hence, $c^{(\kappa)}$ yields an adequate generalization of $c_{Stephens}$ to the κ-th moment case if $\gamma = 1$, and we speak of $c^{(\kappa)}$ as the *generalized Stephens' constant (of rank 1)*. In a similar way, one may introduce *generalized Stephens' constants of rank* γ for any $\gamma \in \mathbb{N}$.

THEOREM 5.14. *Let $\mathbb{K} = \mathbb{Q}(\sqrt{d})$ be a real quadratic field of discriminant Δ. Then, using the notation introduced above, we have*

$$c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}} = c^{(\kappa)} \cdot \eta_\kappa(d)$$

with a correction factor

$$\eta_\kappa(d) := 1 - \frac{f_\kappa(2)F_\kappa(2)}{2G_\kappa(2)} + \frac{f_\kappa(D)F_\kappa(D)}{G_\kappa(D)} - \frac{f_\kappa([2,D])F_\kappa(2D)}{2G_\kappa(2D)}$$

if $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = -1$, and

$$\begin{aligned} \eta_\kappa(d) := 1 &- \frac{f_\kappa(2)F_\kappa(2)}{2G_\kappa(2)} + \frac{2f_\kappa(D)F_\kappa(D)}{G_\kappa(D)} - \frac{f_\kappa([2,D])F_\kappa(2D)}{G_\kappa(2D)} \\ &+ \frac{f_\kappa(D^+)F_\kappa(D^+)}{G_\kappa(D^+)} + \frac{f_\kappa(D^-)F_\kappa(D^-)}{G_\kappa(D^-)} - \frac{f_\kappa([D^+,D^-])F_\kappa(D^+D^-)}{G_\kappa(D^+D^-)} \\ &- \frac{f_\kappa([2,D^+])F_\kappa(2D^+)}{2G_\kappa(2D^+)} - \frac{f_\kappa([2,D^-])F_\kappa(2D^-)}{2G_\kappa(2D^-)} + \frac{f_\kappa(\mathrm{lcm}(2,D^+,D^-))F_\kappa(2D^+D^-)}{2G_\kappa(2D^+D^-)} \end{aligned}$$

if $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = 1$. In particular, $c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}}$ is a positive rational multiple of $c^{(\kappa)}$.

PROOF. We proceed similarly to the proof of Proposition 3 in [51]. Let us first assume $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = -1$ and note that $\varphi(2n) = n$ if n is odd and $\varphi(2n) = 2\varphi(n)$ if n is even. By Lemma 5.11, we have

$$[\mathbb{K}(\sqrt[n]{\varepsilon}, \zeta_{2n}) : \mathbb{K}] = \begin{cases} \frac{n\varphi(n)}{2}, & \text{if } D \mid n, 2 \nmid n, \\ n\varphi(n), & \text{if } D \mid n, 2 \mid n \text{ or if } D \nmid n, 2 \nmid n, \\ 2n\varphi(n), & \text{if } D \nmid n, 2 \mid n, \end{cases} \tag{5.22}$$

for any $n \in \mathbb{N}$. By (5.18) and (5.22) we thus obtain

$$\begin{aligned} c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}} &= 2 \sum_{\substack{n\geq 1 \\ D\mid n, 2\nmid n}} f_\kappa(n) + \sum_{\substack{n\geq 1 \\ D\mid n, 2\mid n}} f_\kappa(n) + \sum_{\substack{n\geq 1 \\ D\nmid n, 2\nmid n}} f_\kappa(n) + \frac{1}{2} \sum_{\substack{n\geq 1 \\ D\nmid n, 2\mid n}} f_\kappa(n) \\ &= 2\sum_{\substack{n\geq 1 \\ D\mid n}} f_\kappa(n) - \sum_{\substack{n\geq 1 \\ D\mid n, 2\mid n}} f_\kappa(n) + \sum_{\substack{n\geq 1 \\ D\nmid n}} f_\kappa(n) - \frac{1}{2} \sum_{\substack{n\geq 1 \\ D\nmid n, 2\mid n}} f_\kappa(n) \\ &= \sum_{n\geq 1} f_\kappa(n) + f_\kappa(Dn) - \frac{f_\kappa(2n)}{2} - \frac{f_\kappa([2,D]n)}{2}. \end{aligned}$$

By the multiplicativity of $f_\kappa(n)$, $c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}}$ equals

$$\Bigg(\sum_{\substack{n\geq 1 \\ \mathrm{rad}(n)\mid [2,D]}} f_\kappa(n) + f_\kappa(Dn) - \frac{f_\kappa(2n)}{2} - \frac{f_\kappa([2,D]n)}{2} \Bigg) \Bigg(\sum_{\substack{n\geq 1 \\ (2D,n)=1}} f_\kappa(n) \Bigg). \tag{5.23}$$

As in the proof of Lemma 5.12 the right sum in (5.23) can be easily expressed as an Euler product:

$$\sum_{\substack{n\geq 1 \\ (2D,n)=1}} f_\kappa(n) = \prod_{p\nmid 2D} \Bigg(1 + \sum_{i\geq 1} \frac{1-p^\kappa}{p^{(\kappa+1)i}\varphi(p^i)} \Bigg) = \frac{c^{(\kappa)}}{G_\kappa(2D)}$$

To treat the first sum in (5.23), we invoke Lemma 5.12 and obtain

$$c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}} = c^{(\kappa)} \left(1 + \frac{f_\kappa(D)F_\kappa(D)}{G_\kappa(D)} - \frac{f_\kappa(2)F_\kappa(2)}{2G_\kappa(2)} - \frac{f_\kappa([2,D])F_\kappa(2D)}{2G_\kappa(2D)} \right)$$

which proves the asserted formula for $c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}}$ in case $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = -1$.

Let us now consider the more fiddly case $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = 1$. Just as above, Lemma 5.11 and (5.18) yield

$$\begin{aligned} c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}} &= 4 \sum_{D\mid n, 2\nmid n} + 2 \sum_{\substack{D\nmid n, 2\nmid n \\ D^+\mid n \text{ or } D^-\mid n}} + 2 \sum_{[2,D]\mid n} + \sum_{\substack{2\nmid n \\ D^+\nmid n, D^-\nmid n}} + \sum_{\substack{2\mid n, D\nmid n \\ D^+\mid n \text{ or } D^-\mid n}} + \frac{1}{2} \sum_{\substack{2\mid n \\ D^+\nmid n, D^-\nmid n}} \\ &= 4\sum_{D\mid n} - 2 \sum_{[2,D]\mid n} + 2 \sum_{\substack{D\nmid n \\ D^+\mid n \text{ or } D^-\mid n}} - \sum_{\substack{2\mid n, D\nmid n \\ D^+\mid n \text{ or } D^-\mid n}} + \sum_{D^+\nmid n, D^-\nmid n} - \frac{1}{2} \sum_{\substack{2\mid n \\ D^+\nmid n, D^-\nmid n}} \end{aligned}$$

with each sum ranging over $n \in \mathbb{N}$ and summing $f_\kappa(n)$. By the definition of D, D^+ and D^-, it is clear that $D \mid n$ already implies $D^+ \mid n$ and $D^- \mid n$. Thus, using basic

set-theoretic arguments, we infer

$$\begin{aligned} c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}} &= 2\sum_{D|n} - \sum_{[2,D]|n} + 2 \sum_{D^+|n \text{ or } D^-|n} - \sum_{\substack{2|n \\ D^+|n \text{ or } D^-|n}} + \sum_{D^+\nmid n, D^-\nmid n} -\frac{1}{2} \sum_{\substack{2|n \\ D^+\nmid n, D^-\nmid n}} \\ &= 2\sum_{D|n} - \sum_{[2,D]|n} + \sum -\frac{1}{2}\sum_{2|n} + \sum_{D^+|n \text{ or } D^-|n} -\frac{1}{2} \sum_{\substack{2|n \\ D^+|n \text{ or } D^-|n}} \\ &= \sum -\frac{1}{2}\sum_{2|n} + 2\sum_{D|n} - \sum_{[2,D]|n} \\ &\quad + \sum_{D^+|n} + \sum_{D^-|n} - \sum_{[D^+,D^-]|n} - \frac{1}{2}\sum_{[2,D^+]|n} - \frac{1}{2}\sum_{[2,D^-]|n} + \frac{1}{2}\sum_{[2,D^+,D^-]|n} . \end{aligned}$$

Proceeding as above one easily deduces the asserted formula for $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon) = 1$. A rather tedious calculation finally establishes the asserted positivity of $c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}}$ in both cases. □

To conclude this section with, we provide some numerical data for the constants $c^{(\kappa)}$ and the correction factors $\eta_\kappa(d)$. Table 5.1 shows a small selection of approximate values for $c^{(\kappa)}$ and the limit

$$c_\infty := \lim_{\kappa\to\infty} c^{(\kappa)} = \prod_p \left(1 - \frac{1}{p^2 - p}\right) \tag{5.24}$$

to which $c^{(\kappa)}$ decreasingly tends to, as $\kappa \to \infty$.

κ	$c^{(\kappa)} \approx$	κ	$c^{(\kappa)} \approx$
1	0.57595997	4	0.39266027
2	0.45893750	5	0.38307636
3	0.41305713	∞	0.37395582

TABLE 5.1. A sample of approximate values for $c^{(\kappa)}$. For all computations we used the formulae (5.21) and (5.24) running over primes less than 10^7.

As for the correction factors $\eta_\kappa(d)$, the Tables 5.2 and 5.3 provide samples of exact and approximate values for $\eta_1(d)$ according to the the sign of $\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(\varepsilon)$. From this data it becomes evident that the correction factor in case $\kappa = 1$ is approximately $6/5$. This is not surprising as $\eta_\kappa(d)$ is, at least for large d, typically dominated by the term

$$1 + \frac{f_\kappa(2)F_\kappa(2)}{2G_\kappa(2)} = \frac{3\cdot 2^\kappa}{2^{\kappa+1}+1}$$

which equals $6/5$ if $\kappa = 1$, and increasingly tends to $3/2$, as $\kappa \to \infty$. Moreover, this behaviour indicates that the particular choice of the real quadratic field has only little influence on the size of $c^{(\kappa)}_{\mathcal{U}_{\mathbb{K}},\{\mathrm{id}\}}$, especially if d gets large in the norm -1 case.

d	ε	$\eta_1(d)$	$\eta_1(d) \approx$
2	$1+\sqrt{2}$	19/16	1.1875
5	$1/2+\sqrt{5}/2$	684/595	1.14957983193
10	$3+\sqrt{10}$	11429/9520	1.20052521008
13	$3/2+\sqrt{13}/2$	2604/2183	1.19285387082
17	$4+\sqrt{17}$	29268/24475	1.19583248212
26	$5+\sqrt{26}$	209581/174640	1.20007443885
29	$5/2+\sqrt{29}/2$	29196/24359	1.19857136992
37	$6+\sqrt{37}$	303468/253075	1.19912278969
41	$32+5\sqrt{41}$	413028/344395	1.19928570392

TABLE 5.2. Correction factors $\eta_1(d)$ for fundamental units of norm -1.

d	ε	$\eta_1(d)$	$\eta_1(d) \approx$
3	$2+\sqrt{3}$	2191/1840	1.19076086957
6	$5+2\sqrt{6}$	559/460	1.2152173913
7	$8+3\sqrt{7}$	31839/26800	1.18802238806
11	$10+3\sqrt{11}$	125327/105520	1.18770849128
14	$15+4\sqrt{14}$	3993/3350	1.19194029851
15	$4+\sqrt{15}$	263209/218960	1.2020871392
19	$170+39\sqrt{19}$	649743/547120	1.1875694546
21	$5/2+\sqrt{21}/2$	1895/1541	1.22972096042
22	$197+42\sqrt{22}$	31373/26380	1.18927217589
23	$24+5\sqrt{23}$	1153631/971440	1.18754735238
30	$11+2\sqrt{30}$	126027/109480	1.15114176105
31	$1520+273\sqrt{31}$	2827167/2380720	1.18752604254
33	$23+4\sqrt{33}$	186199/151685	1.22753733065
34	$35+6\sqrt{34}$	46341/39160	1.18337589377
35	$6+\sqrt{35}$	3829513/3189200	1.20077542957
38	$37+6\sqrt{38}$	162507/136780	1.18809036409
39	$25+4\sqrt{39}$	61194/50209	1.21878547671
42	$13+2\sqrt{42}$	18581/15410	1.20577547047
43	$3482+531\sqrt{43}$	7549071/6357040	1.18751352831
46	$24335+3588\sqrt{46}$	144247/121430	1.18790249526
47	$48+7\sqrt{47}$	9858719/8302000	1.18751132257

TABLE 5.3. Correction factors $\eta_1(d)$ for fundamental units of norm $+1$.

5.4. Residual order of rational numbers modulo primes in arithmetic progression

A recurring procedure in number theory is to generalize questions concerning prime numbers to primes in arithmetic progression. In view of the work of KURLBERG and POMERANCE [51], it is therefore natural to ask for average order, or even moments in

general, of the residual order of a single rational number $a \neq 0, \pm 1$, written as $a = \alpha/\beta$, with coprime integers α and $\beta \neq 0$, over primes in an arithmetic progression, say $p \equiv b\ (q)$ with $q \in \mathbb{N}$ and $(q, b) = 1$. This problem is attackable by Theorem 5.3. We therefore set $\mathbb{K} := \mathbb{Q}$, $\Gamma := \langle a \rangle \subset \mathbb{Q}^*$, $\mathbb{L} := \mathbb{Q}(\zeta_q)$, and let $C_{b,q}$ be the singleton containing the automorphism σ_b of $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ which acts on $\mathbb{Q}(\zeta_q)$ by $\sigma_b(\zeta_q) = \zeta_q^b$. Then, assuming GRH, we indeed obtain

$$\sum_{\substack{p \leq x \\ p \equiv b\ (q) \\ p \nmid \alpha, \beta}} \mathrm{ord}_a(p)^\kappa = \sum_{p \in \mathcal{P}_{C_{b,q}(x, \mathbb{Q}(\zeta_q)/\mathbb{Q})} \atop p \nmid \alpha, \beta} \mathrm{ord}_a(p)^\kappa \sim c^{(\kappa)}_{\langle a \rangle, C_{b,q}} \mathrm{li}(x^{1+\kappa}),$$

as $x \to \infty$, with

$$c^{(\kappa)}_{\langle a \rangle, C_{b,q}} = \sum_{n \geq 1} \frac{\psi_\kappa(n) |C_{b,q}(\langle a \rangle, n)|}{n^\kappa [\mathbb{Q}(\sqrt[n]{a}, \zeta_{[q,n]}) : \mathbb{Q}]}. \tag{5.25}$$

Recall that

$$C_{b,q}(\langle a \rangle, n) = \left\{ \sigma \in \mathrm{Gal}(\mathbb{Q}(\sqrt[n]{a}, \zeta_{[n,q]})/\mathbb{Q}) : \sigma|_{\mathbb{Q}(\zeta_q)} = \sigma_b,\ \sigma|_{\mathbb{Q}(\sqrt[n]{a}, \zeta_n)} = \mathrm{id} \right\},$$

as defined in (5.2), and $\mathbb{Q}(\sqrt[n]{a}, \zeta_{[q,n]})$ is the composite field of $\mathbb{Q}(\sqrt[n]{a}, \zeta_n)$ and $\mathbb{Q}(\zeta_q)$.

By Lemma 5.9, we already know that the constant in (5.25) is positive, at least under GRH, and we proceed to confirm this fact by computing (5.25) explicitly. However, we restrict to a rather moderate setting, i.e. we only consider the case that a be positive and q be an odd prime, for this avoids many complications and clarifies the arguments. As in the preceding section we start with the determination of the degrees $[\mathbb{Q}(\sqrt[n]{a}, \zeta_{[q,n]}) : \mathbb{Q}]$. To this end, we proceed as in [51], and introduce some more notation to make life easier in the sequel. We write $a = a_0^h$, where $h \in \mathbb{N}$ and a_0 is a positive rational number which is not a perfect power in $\mathbb{Q}$. Further, we set $e := \nu_2(h)$, and let $a_0 = a_1 a_2^2$ with $a_1 \in \mathbb{Z}$ squarefree and $a_2 \in \mathbb{Q}$. Finally, we define

$$\rho(a) := \begin{cases} [2^{e+1}, a_1], & \text{if } a_1 \equiv 1\ (4), \\ [2^{e+1}, 4a_1], & \text{if } a_1 \equiv 2, 3\ (4), \end{cases} \tag{5.26}$$

and note that the odd part of $\rho(a)$ is squarefree. We obtain the following statement.

Lemma 5.15. *For any positive rational number a, any prime q and any $n \in \mathbb{N}$ we have*

$$[\mathbb{Q}(\sqrt[n]{a}, \zeta_{[q,n]}) : \mathbb{Q}] = \frac{n\varphi([q,n])}{(n,h)\beta_a([q,n])},$$

where, for any $k \in \mathbb{N}$, we define

$$\beta_a(k) := \begin{cases} 2, & \text{if } \rho(a) \mid k, \\ 1, & \text{otherwise.} \end{cases}$$

Proof. By Kummer theory the degree of $\mathbb{Q}(\sqrt[n]{a}, \zeta_{[q,n]})$ over $\mathbb{Q}(\zeta_{[q,n]})$ is the smallest $k \in \mathbb{N}$ such that the k-th power of $\sqrt[n]{a}$ is contained in $\mathbb{Q}(\zeta_{[q,n]})$ (cf. [12, p. 205ff]). The assertion then follows by the same arguments as in Lemma 5.11. □

Different to the preceding section, the size of $C_{b,q}(\langle a \rangle, n)$ is no longer constant, but may vary with n between the values 0 and 1 (cf. Lemma 5.5). This makes the computation of (5.25) more involved. We address this problem in the subsequent lemma.

LEMMA 5.16. *Let a be a positive rational number, q an odd prime, and $b \in \mathbb{Z}$ coprime to q. For any $n \in \mathbb{N}$ we have $C_{b,q}(\langle a\rangle, n) = \{\mathrm{id}\}$ if $b \equiv 1\ (q)$. If $b \not\equiv 1\ (q)$, then we have*

$$|C_{b,q}(\langle a\rangle, n)| = \begin{cases} 1, & \text{if } q \nmid n, \\ 0, & \text{otherwise,} \end{cases}$$

if $q \nmid \rho(a)$, and

$$|C_{b,q}(\langle a\rangle, n)| = \begin{cases} 1, & \text{if } q \nmid n \text{ and } \frac{\rho(a)}{q} \nmid n, \text{ or if } q \nmid n \text{ and } \left(\frac{b}{q}\right) = 1, \\ 0, & \text{otherwise,} \end{cases}$$

if $q \mid \rho(a)$.

PROOF. If $b \equiv 1\ (q)$, then σ_b is the identity in $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$, and one clearly has $\mathrm{id} \in C_{b,q}(\langle a\rangle, n)$. By Lemma 5.5 the assertion follows for $b \equiv 1\ (q)$.

Now assume $b \not\equiv 1\ (q)$. Then $\sigma_b \neq \mathrm{id}$ in $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$. By Lemma 5.15 we have

$$[\mathbb{Q}(\sqrt[n]{a}, \zeta_{[q,n]}) : \mathbb{Q}] = \frac{n\varphi([q,n])}{(n,h)\beta_a([q,n])}$$

on the one hand, and

$$[\mathbb{Q}(\sqrt[n]{a}, \zeta_n) : \mathbb{Q}] = \frac{n\varphi(n)}{(n,h)\beta_a(n)}$$

on the other. Using basic facts from Galois theory (cf. [46, p. 153ff]) and the elementary identity

$$\varphi(m)\varphi(n) = \varphi([m,n])\varphi((m,n)), \tag{5.27}$$

we find

$$[\mathbb{Q}(\sqrt[n]{a}, \zeta_n) \cap \mathbb{Q}(\zeta_q) : \mathbb{Q}] = \begin{cases} \varphi((q,n)), & \text{if } \beta_a([q,n]) = \beta_a(n), \\ 2\varphi((q,n)), & \text{otherwise.} \end{cases}$$

If q divides n, then $\mathbb{Q}(\zeta_q)$ is contained in $\mathbb{Q}(\sqrt[n]{a}, \zeta_n)$, and $C_{b,q}(\langle a\rangle, n)$ must be empty. Thus, we may assume $q \nmid n$, thence $\varphi((q,n)) = 1$.

If $\beta_a([q,n]) = \beta_a(n)$, then the natural map from $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{a}, \zeta_{[q,n]})$ into the direct product of $\mathrm{Gal}(\mathbb{Q}(\sqrt[n]{a}, \zeta_n)/\mathbb{Q})$ and $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ is an isomorphism, and therefore $C_{b,q}(\langle a\rangle, n)$ consists of exactly one automorphism. One easily checks that under the assumption $q \nmid n$ the condition $\beta_a([q,n]) = \beta_a(n)$ is true for all n, if $q \nmid \rho(a)$, and if $q \mid \rho(a)$, it is true, whenever $\frac{\rho(a)}{q} \nmid n$.

Finally, assume $\beta_a([q,n]) \neq \beta_a(n)$. In this case the intersection $\mathbb{M} := \mathbb{Q}(\sqrt[n]{a}, \zeta_n) \cap \mathbb{Q}(\zeta_q)$ is the unique quadratic subfield of $\mathbb{Q}(\zeta_q)$. (Note that $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ is cyclic, because q is prime.) The extension $\mathbb{Q}(\sqrt[n]{a}, \zeta_{[q,n]})/\mathbb{M}$ is the direct product of the Galois extensions $\mathbb{Q}(\sqrt[n]{a}, \zeta_n)/\mathbb{M}$ and $\mathbb{Q}(\zeta_q)/\mathbb{M}$ and hence Galois itself. If σ_b is contained in $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{M})$, it may be lifted uniquely to $C_{b,q}(\langle a\rangle, n)$, whence $|C_{b,q}(\langle a\rangle, n)| = 1$. If $\sigma_b \notin \mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{M})$, then $C_{b,q}(\langle a\rangle, n)$ is clearly empty. Since σ_b is contained in $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{M})$ if and only if b is a square in $(\mathbb{Z}/q\mathbb{Z})^*$, the assertion follows. □

We are now well prepared to prove the subsequent theorem which yields precise expressions for $c^{(\kappa)}_{\langle a\rangle, C_{b,q}}$ and confirms its positivity.

THEOREM 5.17. *Let a be a positive rational number, and h and $\rho(a)$ as defined at the beginning of this section. Let q be an odd prime, b some integer coprime to q, and $\kappa \in \mathbb{R}_+$. Define*

$$f_\kappa(h,q,n) := \frac{\psi_\kappa(n)(n,h)\varphi\big((q,n)\big)}{n^{\kappa+1}\varphi(n)}$$

and set $F_\kappa(h,q,p) := \sum_{i\geq 0} f_\kappa(h,q,p^i)$ and $F_\kappa(h,q,p,t) := \sum_{i<t} f_\kappa(h,q,p^i)$ for any prime p and any non-negative integer t. Finally, set $\tilde{\rho}(a) := \rho(a)/(q,\rho(a))$.

(i) *If $b \equiv 1\ (q)$, we have*

$$c^{(\kappa)}_{\langle a\rangle, C_{b,q}} = \frac{1}{\varphi(q)}\Big(\prod_p F_\kappa(h,q,p)\Big)\Big(1+\prod_{p\mid\tilde{\rho}(a)}\Big(1-\frac{F_\kappa(h,q,p,\nu_p(\tilde{\rho}(a)))}{F_\kappa(h,q,p)}\Big)\Big).$$

(ii) *If $b \not\equiv 1\ (q)$, and either $\left(\frac{b}{q}\right) = 1$ or $q \nmid \rho(a)$, then we have*

$$c^{(\kappa)}_{\langle a\rangle, C_{b,q}} = \frac{1}{\varphi(q)}\Big(\prod_{p\neq q} F_\kappa(h,q,p)\Big)\Big(1+\prod_{p\mid\tilde{\rho}(a)}\Big(1-\frac{F_\kappa(h,q,p,\nu_p(\tilde{\rho}(a)))}{F_\kappa(h,q,p)}\Big)\Big).$$

(iii) *If $\left(\frac{b}{q}\right) = -1$ and $q \mid \rho(a)$, then*

$$c^{(\kappa)}_{\langle a\rangle, C_{b,q}} = \frac{1}{\varphi(q)}\Big(\prod_{p\neq q} F_\kappa(h,q,p)\Big)\Big(1-\prod_{p\mid\tilde{\rho}(a)}\Big(1-\frac{F_\kappa(h,q,p,\nu_p(\tilde{\rho}(a)))}{F_\kappa(h,q,p)}\Big)\Big).$$

In particular $c^{(\kappa)}_{\langle a\rangle, C_{b,q}}$ is a positive rational multiple of $c^{(\kappa)}$.

PROOF. Our proof uses ideas of the proof of Proposition 3 of [51]. For convenience we write $g_\kappa(n) := |C_{b,q}(n)|f_\kappa(h,q,n)$. By Lemma 5.15, (5.25) and (5.27), we easily obtain

$$c^{(\kappa)}_{\langle a\rangle, C_{b,q}} = \frac{1}{\varphi(q)}\sum_{n\geq 1} g_\kappa(n) + \frac{1}{\varphi(q)}\sum_{\substack{n\geq 1\\ \rho(a)\mid[q,n]}} g_\kappa(n).$$

From the definition of $\tilde{\rho}(a)$, it is clear that $\rho(a)$ divides $[n,q]$ if and only if $\tilde{\rho}(a)$ divides n, because q is odd, and the odd part of $\rho(a)$ is squarefree. Hence, we have

$$c^{(\kappa)}_{\langle a\rangle, C_{b,q}} = \frac{1}{\varphi(q)}\sum_{n\geq 1}\Big(g_\kappa(n) + g_\kappa(\tilde{\rho}(a)n)\Big). \tag{5.28}$$

Let us first compute (5.28) in one of the cases $\left(\frac{b}{q}\right) = 1$ or $q \nmid \rho(a)$, for in these cases $|C_{b,q}(\langle a\rangle, n)|$, and hence $g_\kappa(n)$ too, is multiplicative in n (cf. Lemma 5.16). Under this assumption, (5.28) becomes

$$c^{(\kappa)}_{\langle a\rangle, C_{b,q}} = \frac{1}{\varphi(q)}\sum_{\substack{n\geq 1\\ \mathrm{rad}(n)\mid\tilde{\rho}(a)}}\Big(g_\kappa(n) + g_\kappa(\tilde{\rho}(a)n)\Big)\sum_{\substack{n\geq 1\\ (n,\tilde{\rho}(a))=1}} g_\kappa(n). \tag{5.29}$$

The rightmost sum in (5.29) can easily be expressed as an Euler product:

$$\sum_{\substack{n\geq 1\\ (n,\tilde{\rho}(a))=1}} g_\kappa(n) = \prod_{p\nmid\tilde{\rho}(a)}\sum_{i\geq 0} g_\kappa(p^i). \tag{5.30}$$

The first sum in (5.29) may be split up into two sums, the first of which being treated as in (5.30):

$$\sum_{\substack{n\geq 1\\ \mathrm{rad}(n)\mid\tilde{\rho}(a)}} g_\kappa(n) = \prod_{p\mid\tilde{\rho}(a)}\sum_{i\geq 0} g_\kappa(p^i). \tag{5.31}$$

As for the remaining sum, we may write

$$\begin{aligned}\sum_{\substack{n\geq 1\\ \mathrm{rad}(n)\mid\tilde{\rho}(a)}} g_\kappa(\tilde{\rho}(a)n) &= \prod_{p\mid\tilde{\rho}(a)}\sum_{i\geq \nu_p(\tilde{\rho}(a))} g_\kappa(p^i)\\ &= \prod_{p\mid\tilde{\rho}(a)}\Bigg(\sum_{i\geq 0} g_\kappa(p^i) - \sum_{i<\nu_p(\tilde{\rho}(a))} g_\kappa(p^i)\Bigg).\end{aligned} \tag{5.32}$$

Combining equations (5.29)–(5.32) we are led to

$$c^{(\kappa)}_{\langle a\rangle,C_{b,q}} = \frac{1}{\varphi(q)}\Bigg(\prod_p\sum_{i\geq 0} g_\kappa(n)\Bigg)\Bigg(1+\prod_{p\mid\tilde{\rho}(a)}\Bigg(1-\frac{\sum_{i<\nu_p(\tilde{\rho}(a))} g_\kappa(p^i)}{\sum_{i\geq 0} g_\kappa(p^i)}\Bigg)\Bigg).$$

Now we note that $|C_{b,q}(\langle a\rangle, n)|$ depends only on the squarefree part of n (cf. Lemma 5.16), whence $|C_{b,q}(\langle a\rangle, p^i)| = |C_{b,q}(\langle a\rangle, p)|$ holds for any prime p and $i\in\mathbb{N}$. Therefore, the sum $\sum_{i\geq 0} g_\kappa(n)$ equals $\sum_{i\geq 0} f_\kappa(h,q,n)$ if $|C_{b,q}(\langle a\rangle, p)| = 1$, and it equals 1 otherwise. In case $b\equiv 1\ (q)$, we have $C_{b,q}(\langle a\rangle, n) = 1$ for any $n\in\mathbb{N}$, and thus obtain

$$c^{(\kappa)}_{\langle a\rangle,C_{b,q}} = \frac{1}{\varphi(q)}\Bigg(\prod_p F_\kappa(h,q,p)\Bigg)\Bigg(1+\prod_{p\mid\tilde{\rho}(a)}\Bigg(1-\frac{F_\kappa(h,q,p,\nu_p(\tilde{\rho}(a)))}{F_\kappa(h,q,p)}\Bigg)\Bigg)$$

in this case. Now assume $b\not\equiv 1\ (q)$. By Lemma 5.16 we have $C_{b,q}(\langle a\rangle, p) = \varnothing$ if and only if $p = q$. Thus

$$c^{(\kappa)}_{\langle a\rangle,C_{b,q}} = \frac{1}{\varphi(q)}\Bigg(\prod_{p\neq q} F_\kappa(h,q,p)\Bigg)\Bigg(1+\prod_{p\mid\tilde{\rho}(a)}\Bigg(1-\frac{F_\kappa(h,q,p,\nu_p(\tilde{\rho}(a)))}{F_\kappa(h,q,p)}\Bigg)\Bigg).$$

Let us now assume $q\mid\rho(a)$ and $\left(\frac{b}{q}\right) = -1$, so that $g_\kappa(n)$ is no longer multiplicative. However, by Lemma 5.16, we at least have

$$|C_{b,q}(\langle a\rangle, mn)| = |C_{b,q}(\langle a\rangle, m)|\cdot|C_{b,q}(\langle a\rangle, n)|$$

if $(\tilde{\rho}(a), n) = 1$. Hence, (5.29) and (5.30) remain valid. As for the first sum in (5.29), we note that $g_\kappa(\tilde{\rho}(a)n) = 0$ holds for all $n\in\mathbb{N}$ by Lemma 5.16. Accordingly, we obtain

$$\begin{aligned}\sum_{\substack{n\geq 1\\ \mathrm{rad}(n)\mid\tilde{\rho}(a)}}\Big(g_\kappa(n)+g_\kappa(\tilde{\rho}(a)n)\Big) &= \sum_{\substack{n\geq 1\\ \mathrm{rad}(n)\mid\tilde{\rho}(a)\\ \tilde{\rho}(a)\nmid n}} f_\kappa(h,q,n)\\ &= \sum_{\substack{n\geq 1\\ \mathrm{rad}(n)\mid\tilde{\rho}(a)}} f_\kappa(h,q,n) - \sum_{\substack{n\geq 1\\ \mathrm{rad}(n)\mid\tilde{\rho}(a)\\ \tilde{\rho}(a)\mid n}} f_\kappa(h,q,n)\\ &= \Bigg(\prod_{p\mid\tilde{\rho}(a)} F_\kappa(h,q,p)\Bigg)\Bigg(1-\prod_{p\mid\tilde{\rho}(a)}\Bigg(1-\frac{F_\kappa(h,q,p,\nu_p(\tilde{\rho}(a)))}{F_\kappa(h,q,p)}\Bigg)\Bigg),\end{aligned}$$

since $f_\kappa(h,q,n)$ is multiplicative in n. By the same arguments as above, Lemma 5.16 finally yields

$$c^{(\kappa)}_{\langle a\rangle,C_{b,q}} = \frac{1}{\varphi(q)}\Big(\prod_{p\neq q} F_\kappa(h,q,p)\Big)\Big(1-\prod_{p\mid\tilde\rho(a)}\Big(1-\frac{F_\kappa(h,q,p,\nu_p(\tilde\rho(a)))}{F_\kappa(h,q,p)}\Big)\Big).$$

It is an easy exercise to show that the obtained expressions are positive and, expressing $F_\kappa(h,q,p)$ in terms of geometric sums, reveals that $c^{(\kappa)}_{\langle a\rangle,C_{b,q}}$ is a rational multiple of $c^{(\kappa)}$. □

Remark 5.18. Theorem 5.17 reveals a somewhat surprising phenomenon. Intuitively, one might expect that $\mathrm{ord}_a(p)$ distributes equally over the residue classes of $(\mathbb{Z}/q\mathbb{Z})^*$ on average. Theorem 5.17 shows that this is not true in general. Indeed, if $q\nmid\rho(a)$, then $c^{(\kappa)}_{\langle a\rangle,C_{b,q}}$ is constant on residue classes $b\in(\mathbb{Z}/q\mathbb{Z})^*\backslash\{1\}$, whereas $c^{(\kappa)}_{\langle a\rangle,C_{1,q}}$ is smaller by the factor $F_\kappa(h,q,q)<1$ than any of these. If $q\mid\rho(a)$, then $c^{(\kappa)}_{\langle a\rangle,C_{b,q}}$ is not even constant on residue classes $b\not\equiv 1\ (q)$ and its value differs according to whether b is a square modulo q or not. In fact, $c^{(\kappa)}_{\langle a\rangle,C_{b,q}}$ happens to be larger for squares b modulo q if and only if $\rho(a)$ has an even number of square divisors.

To conclude this section, we provide a small computation to affirm that our results agree with the results of Kurlberg and Pomerance [51]. Let a, q and b be as above and recall the definition of the constant c_a given in Proposition 5.1. This constant should naturally arise from the constants computed in Theorem 5.17 by the relation

$$c_a = \sum_{b=1}^{q-1} c^{(1)}_{\langle a\rangle,C_{b,q}}. \tag{5.33}$$

We illustrate this in the (easier) case $q\nmid\rho(a)$. Let therefore $f(h,n):=\frac{\mathrm{rad}(n)(-1)^{\omega(n)}(n,h)}{n^3}$ and set $F(h,p):=\sum_{i\geq 0}f(h,p^i)$ and $F(h,p,t):=\sum_{i<t}f(h,p^i)$ for any prime p and any non-negative integer t. Kurlberg and Pomerance proved (cf. Proposition 3 of [51])

$$c_a = \prod_p F(h,p)\Big(1+\prod_{p\mid\rho(a)}\Big(1-\frac{F(h,p,\nu_p(\rho(a)))}{F(h,p)}\Big)\Big).$$

To validate (5.33), we first note the elementary relations

$$\varphi(q)\cdot f(h,q^i)=f_1(h,q,q^i),\qquad \varphi(q)\cdot(F(h,q)-1)=F_1(h,q)-1,$$

and

$$f(h,p^i)=f_1(h,q,p^i),\qquad F(h,p)=F_1(h,p),\qquad F(h,p,t)=F_1(h,p,t)$$

which are easily verified for any prime $p\neq q$ and $i\geq 1$. By Theorem 5.17 we then deduce

$$\begin{aligned}\sum_{b=1}^{q-1} c^{(1)}_{\langle a\rangle,C_{b,q}} &= \Big(c^{(1)}_{\langle a\rangle,C_{1,q}}+(\varphi(q)-1)c^{(1)}_{\langle a\rangle,C_{2,q}}\Big)\\ &= \frac{1}{\varphi(q)}\Big(F_1(h,q,q)+\varphi(q)-1\Big)\prod_{p\neq q}F(h,p)\Big(1+\prod_{p\mid\rho(a)}\Big(1-\frac{F(h,p,\nu_p(\rho(a)))}{F(h,p)}\Big)\Big)\\ &= \prod_p F(h,p)\Big(1+\prod_{p\mid\rho(a)}\Big(1-\frac{F(h,p,\nu_p(\rho(a)))}{F(h,p)}\Big)\Big)\\ &= c_a\end{aligned}$$

which proves (5.33) if $q\nmid\rho(a)$. The other case may be handled similarly.

CHAPTER 6

Double Averaging of the Residual Index over Prime Ideals

In the preceding chapter we investigated moments of the residual order over prime ideals in a suitable number field setting. In this chapter we return to the corresponding problem for the residual index. As already mentioned in Chapter 4, this task appears much more delicate, and not attackable by common methods. To simplify the question, we consider it on average which, as we will see, allows for asymptotic formulae in the spirit of (4.2). Most of this chapter is to appear in the author's article [1].

In Section 6.1 we provide a precise formulation of the problem we are investigating and state the main theorems of this chapter. The subsequent section serves to establish rather elementary results about moments of index and order in finite abelian groups which prove beneficial throughout the remainder of this thesis. In Section 6.3 we make up for the proofs of the theorems stated in Section 6.1, making intense use of the tools provided in Section 4.3. Afterwards, for the sake of completeness, we address the corresponding problem for the residual order, and quote a result of Luca which settles the problem in the rational case. To conclude with, we present a method to reduce the summation range of the considered "double average sums" by the Poisson summation formula.

6.1. Wagstaff's heuristic on average

As before, we let $\kappa \in \mathbb{R}_+$, choose a Galois extension $\mathbb{L}/\mathbb{K}$ of number fields, fix a conjugacy class C of $\mathrm{Gal}(\mathbb{L}/\mathbb{K})$, and consider a finitely generated, not necessarily torsion-free, infinite subgroup Γ of $\mathbb{K}^*$ with arithmetic rank $\gamma \in \mathbb{N}$. Originally, we were interested in asymptotic formulae for the κ-th moment of $\mathrm{ind}_\Gamma(\mathfrak{p})$ over prime ideals in $\mathcal{P}_C(\mathbb{L}/\mathbb{K})$:

$$\sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*}} \mathrm{ind}_\Gamma(\mathfrak{p})^\kappa.$$

As explained in detail in Section 4.1, however, it seems hopeless to attack this task by common methods. Instead, we modify the problem and consider the average order of

$$\mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) := \sum_{a_1,\dots,a_\gamma\in(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*} \frac{\mathrm{ind}_{\langle a_1,\dots,a_\gamma\rangle}(\mathfrak{p})^\kappa}{(\mathcal{N}\mathfrak{p}-1)^\gamma}, \tag{6.1}$$

over prime ideals $\mathfrak{p}\in\mathcal{P}_C(\mathbb{L}/\mathbb{K})$. Obviously, $\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$ is the κ-th moment of $\mathrm{ind}_{\langle a_1,\dots,a_\gamma\rangle}(\mathfrak{p})$ averaged over all tupels $(a_1,\dots,a_\gamma)\in(\mathcal{O}_\mathbb{K}/\mathfrak{p})^{*\gamma}$. One may hope that the behaviour of the reduction of Γ modulo $\mathfrak{p}$ (whenever $\overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*$) resembles that of a generic subgroup of $(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*$, so that $\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$ yields a reasonable approximation[18] of $\mathrm{ind}_\Gamma(\mathfrak{p})^\kappa$.

It turns out that $\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$ is much easier to handle than $\mathrm{ind}_\Gamma(\mathfrak{p})^\kappa$. Due to the additional averaging process, precise asymptotic estimates for the average order of $\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$ over prime ideals in $\mathcal{P}_C(\mathbb{L}/\mathbb{K})$ become available. We formulate these in the subsequent theorem. The result is unconditional and depends on whether $\gamma=\kappa$, $\gamma>\kappa$ or $\gamma<\kappa$. The latter two

[18] Of course one must keep track of a possible torsion part of Γ which is not taken into account.

cases turn out to be easier and admit asymptotic formulae while in the first case we at least determined the corresponding growth rate.

THEOREM 6.1. *Let $\mathbb{K}$, $\mathbb{L}$, C, κ and γ be as above. For $n \in \mathbb{N}$, we set*

$$c_C(n) := \begin{cases} |C|, & \text{if } \{\sigma \in C : \sigma|_{\mathbb{L}\cap\mathbb{K}(\zeta_n)} = \mathrm{id}\} \neq \varnothing, \\ 0, & \text{otherwise.} \end{cases}$$

Let furthermore $\varphi_t(n)$ be the multiplicative function defined by $\varphi_t(p^e) := p^e\left(1 - \frac{1}{p^t}\right)$ for any prime power p^e, $e \in \mathbb{N}$, and any $t \in \mathbb{R}_+$.

(i) *If $\gamma > \kappa$, then*

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) = \mathrm{li}(x)\sum_{n\geq 1}\frac{c_C(n)\varphi_\kappa(n)}{n^{\gamma-\kappa+1}[\mathbb{L}(\zeta_n):\mathbb{K}]} + O\left(\frac{\mathrm{li}(x)}{(\log\log x)^{\frac{\gamma(\gamma-\kappa)}{2\gamma-\kappa}-\varepsilon}}\right),$$

where the implied constant depends[19] *on $\mathbb{L}$, γ, κ and ε, and the sum over n is convergent and positive.*

(ii) *If $\gamma = \kappa$, then*

$$x \ll_{\mathbb{L}} \sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) \ll_{\mathbb{K}} x.$$

(iii) *If $\gamma < \kappa$, then*

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) = \mathrm{li}(x^{\kappa-\gamma+1})\sum_{n\geq 1}\frac{c_C(n)\varphi_\gamma(n)}{n^{\kappa-\gamma+1}[\mathbb{L}(\zeta_n):\mathbb{K}]} + O\left(\frac{\mathrm{li}(x^{\kappa-\gamma+1})}{(\log\log x)^{\frac{\kappa(\kappa-\gamma)}{2\kappa-\gamma}-\varepsilon}}\right),$$

where the implied constant depends on $\mathbb{L}$, γ, κ and ε, and the sum over n is convergent and positive.

As Theorem 6.2 will show, the asymptotic constant and the error term in Theorem 6.1 (i) can be simplified and improved, respectively, and Theorem 6.1 (ii) can be replaced by an asymptotic formula under GRH, if one additionally assumes that $\mathbb{L}$ and $\mathbb{K}$ are both Galois over $\mathbb{Q}$. We conjecture that such an asymptotic formula holds in general.

THEOREM 6.2. *With the notations of Theorem 6.1, assume that $\mathbb{L}$ and $\mathbb{K}$ are Galois over $\mathbb{Q}$, and let m be some positive integer such that $\mathbb{L}^{ab}$, the abelian part of $\mathbb{L}$, is contained in $\mathbb{Q}(\zeta_m)$. Set*

$$A_{\gamma,C}^{(\kappa)} := \frac{|C|}{[\mathbb{L}:\mathbb{K}]}\sum_{\substack{d\mid m\\ c_C(d)\neq 0}}\frac{[\mathbb{L}\cap\mathbb{Q}(\zeta_d):\mathbb{Q}]\varphi_{\gamma-\kappa+1}\left(\frac{m}{d}\right)a_\gamma^{(\kappa)}(m,d)}{md^{\gamma-\kappa}},$$

with certain positive real numbers $a_\gamma^{(\kappa)}(m,d)$ given by Euler products which only depend on κ, γ, m and d and will be defined in Lemma 6.11. Then $A_{\gamma,C}^{(\kappa)}$ is positive and we have:

(i) *If $\gamma > \kappa$, then*

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) = \zeta(\gamma-\kappa+1)\cdot A_{\gamma,C}^{(\kappa)}\cdot\mathrm{li}(x) + O\left(\frac{\mathrm{li}(x)}{(\log x)^{\frac{\gamma(\gamma-\kappa)}{6\gamma-3\kappa}-\varepsilon}}\right),$$

[19] Just as in Chapter 5, a dependency on $\mathbb{L}$ may also include dependencies on $\mathbb{K}$ and C.

where $\zeta(s)$ is the Riemann zeta function and the implied constant depends on $\mathbb{L}$, γ, κ and ε.

(ii) *If $\gamma = \kappa$ and one assumes the GRH for the fields $\mathbb{L}(\zeta_n)$, $n \geq 1$, then*

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) = A_{\gamma,C}^{(\kappa)} \cdot x + O_{\mathbb{L}}\left(\frac{x \log\log x}{\log x}\right),$$

(iii) *If $\gamma < \kappa$, then*

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) = \zeta(\kappa - \gamma + 1) \cdot A_{\kappa,C}^{(\gamma)} \cdot \mathrm{li}(x^{\kappa-\gamma+1}) + O\left(\frac{\mathrm{li}(x^{\kappa-\gamma+1})}{(\log x)^{\frac{\kappa(\kappa-\gamma)}{6\kappa-3\gamma}-\varepsilon}}\right),$$

where the implied constant depends on $\mathbb{L}$, γ, κ and ε.

Remark 6.3. By the Kronecker-Weber theorem (cf. [68, p. 273]), an integer m as in Theorem 6.2 always exists. Although not obvious from its definition, the constant $A_{\gamma,C}^{(\kappa)}$ in Theorem 6.2 does not depend on the choice of m as will become clear in Section 6.3.3. Moreover, if $\kappa = 1$, then $a_\gamma^{(1)}(m, d) = 1$ holds, for any $\gamma \in \mathbb{N}$ and all $d \mid m$ (cf. Lemma 6.11) which simplifies $A_{\gamma,C}^{(\kappa)}$ substantially.

Theorem 6.2 supports (4.2) and Wagstaff's heuristic in particular. Theorem 6.2 (ii) remains true unconditionally if Proposition 4.9, the number field analogue of the Bombieri-Vinogradov theorem, is applicable. This is the case, if $\mathbb{L} \cap \mathbb{Q}(\zeta_n) = \mathbb{Q}$ holds for all $n \in \mathbb{N}$, and the largest abelian subgroup H of $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ for which $H \cap C \neq \varnothing$ has index ≤ 4 inside $\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$ (see the paragraph after (6.27) in Section 6.3.3 for more details). In particular, Theorem 6.2 (ii) holds unconditionally if $\mathbb{L} = \mathbb{Q}$. In case $\gamma = \kappa = 1$ this result was independently proved by Felix [27].

At last, the asymptotic formulae in Theorem 6.1 (i) and (iii) hold with the better error terms of Theorem 6.2 if there exists a field tower $\mathbb{Q} = \mathbb{M}_0 \subset \mathbb{M}_1 \subset \cdots \subset \mathbb{M}_s = \mathbb{K}$ in which each field is Galois over the preceding one. This is a consequence of stronger upper bounds for possible Siegel zeroes of Dedekind zeta functions (cf. Proposition 4.10). Further explanations will be provided in Section 6.3.1.

6.2. Index and order in finite abelian groups

Throughout this section let G be an arbitrary finite abelian group. For any $\gamma \in \mathbb{N}$, and any $\kappa \in \mathbb{R}_+$, we define

$$\mathrm{Ind}_\gamma^\kappa(G) := \frac{1}{|G|^\gamma} \sum_{a_1,\ldots,a_\gamma \in G} \frac{|G|^\kappa}{|\langle a_1, \ldots, a_\gamma\rangle|^\kappa},$$

and

$$\mathrm{Ord}_\gamma^\kappa(G) := \frac{1}{|G|^\gamma} \sum_{a_1,\ldots,a_\gamma \in G} |\langle a_1, \ldots, a_\gamma\rangle|^\kappa.$$

These quantities represent the κ-th moment of index and order of $\langle a_1, \ldots, a_\gamma\rangle$ inside G, respectively, averaged over all $(a_1, \ldots, a_\gamma) \in G^\gamma$. Let furthermore $\lambda_\gamma(G)$ denote the cardinality of the largest subgroup of G generated by γ elements. This quantity clearly satisfies

$$\lambda_\gamma(G) = \prod_{p \| |G|} \lambda_\gamma(G_p), \tag{6.2}$$

where G_p denotes the p-Sylow subgroup of G. For convenience, we write $\lambda(G)$ instead of $\lambda_1(G)$ for the exponent of G. For any divisor d of $\lambda_\gamma(G)$, we define

$$f_{G,\gamma}(d) := \sharp\{(a_1,\dots,a_\gamma) \in G^\gamma : |\langle a_1,\dots,a_\gamma\rangle| = d\}$$

and its associated summatory function

$$h_{G,\gamma}(d) := \sum_{e|d} f_{G,\gamma}(e).$$

Then we clearly have

$$\mathrm{Ind}_\gamma^\kappa(G) = \frac{1}{|G|^{\gamma-\kappa}} \sum_{d|\lambda_\gamma(G)} \frac{f_{G,\gamma}(d)}{d^\kappa}, \tag{6.3}$$

and

$$\mathrm{Ord}_\gamma^\kappa(G) = \frac{1}{|G|^\gamma} \sum_{d|\lambda_\gamma(G)} f_{G,\gamma}(d) d^\kappa. \tag{6.4}$$

The aim of this section is to derive basic properties of $\mathrm{Ind}_\gamma^\kappa(G)$ and $\mathrm{Ord}_\gamma^\kappa(G)$. We will establish explicit formulae for these for special families of groups G which frequently occur in the context of residue rings in number fields and elliptic curves defined over finite fields. On the other hand, we also prove upper and lower bounds for $\mathrm{Ind}_\gamma^1(G)$ which prove beneficial in Section 7.5. Our account is inspired by the work of Luca and Shparlinski who investigated $\mathrm{Ord}_1^1(G)$ in [71].

To start with, we prove the following observation which reduces the problem of determining $\mathrm{Ind}_\gamma^\kappa(G)$ and $\mathrm{Ord}_\gamma^\kappa(G)$ to the case where G is a finite p-group.

Lemma 6.4. *Let $\kappa \in \mathbb{R}_+$ and $\gamma \in \mathbb{N}$. Let further $G \cong \bigoplus_{p||G|} G_p$ be the decomposition of a finite abelian group G into its p-Sylow subgroups and d a divisor of $\lambda_\gamma(G)$. Then:*

$$f_{G,\gamma}(d) = \prod_{p||G|} f_{G_p,\gamma}(p^{\nu_p(d)}), \tag{6.5}$$

$$h_{G,\gamma}(d) = \prod_{p||G|} h_{G_p,\gamma}(p^{\nu_p(d)}), \tag{6.6}$$

$$\mathrm{Ind}_\gamma^\kappa(G) = \prod_{p||G|} \mathrm{Ind}_\gamma^\kappa(G_p), \tag{6.7}$$

$$\mathrm{Ord}_\gamma^\kappa(G) = \prod_{p||G|} \mathrm{Ord}_\gamma^\kappa(G_p). \tag{6.8}$$

Proof. Let $A_{G,\gamma}(d) := \{(a_1,\dots,a_\gamma) \in G^\gamma : |\langle a_1,\dots,a_\gamma\rangle| = d\}$. By definition, we obviously have $f_{G,\gamma}(d) = |A_{G,\gamma}(d)|$. As one can easily verify, the natural isomorphism $\psi : G^\gamma \to \prod_{p||G|} G_p^\gamma$ induces a bijection

$$A_{G,\gamma}(d) \overset{1:1}{\longleftrightarrow} \prod_{p|\lambda_\gamma(G)} A_{G_p,\gamma}(p^{\nu_p(d)})$$

which yields (6.5). From this one deduces (6.6) immediately. Equations (6.7) and (6.8) then follow from (6.2)–(6.5). □

This lemma enables us to establish explicit formulae for $\mathrm{Ind}_\gamma^\kappa(G)$ and $\mathrm{Ord}_\gamma^\kappa(G)$ which may be of independent interest, and yield an easy tool to compute $\mathrm{Ind}_\gamma^\kappa(G)$ and $\mathrm{Ord}_\gamma^\kappa(G)$ for specific choices of G.

LEMMA 6.5. *Let G be a finite abelian group, $\kappa \in \mathbb{R}_+$, $\gamma \in \mathbb{N}$ and for any prime $p \mid |G|$ let G_p denote the corresponding p-Sylow subgroup. Then we have*

$$\mathrm{Ind}_\gamma^\kappa(G) = \frac{|G|^\kappa}{\lambda_\gamma(G)^\kappa} \prod_{p||G|} \left[1 + \left(1 - \frac{1}{p^\kappa}\right) \frac{\lambda_\gamma(G_p)^\kappa}{|G_p|^\gamma} \sum_{j=0}^{\alpha_p - 1} \frac{h_{G_p,\gamma}(p^j)}{p^{j\kappa}} \right],$$

and

$$\mathrm{Ord}_\gamma^\kappa(G) = \lambda_\gamma(G)^\kappa \prod_{p||G|} \left[1 - \frac{p^\kappa - 1}{|G_p|^\gamma \lambda_\gamma(G_p)^\kappa} \sum_{j=0}^{\alpha_p - 1} p^{j\kappa} h_{G_p,\gamma}(p^j) \right],$$

where α_p is defined by $\lambda_\gamma(G_p) = p^{\alpha_p}$.

PROOF. By the previous lemma, it suffices to consider the case where G is a finite abelian p-group, $G = C_{p^{\alpha_1}} \oplus \cdots \oplus C_{p^{\alpha_n}}$ say, with integers $\alpha_1 \geq \cdots \geq \alpha_n \geq 1$. Recall that C_n denotes the cyclic group of n elements. For convenience, we set $\alpha := \sum_{i=1}^{\min(\gamma,n)} \alpha_i$, and observe $\lambda_\gamma(G) = p^\alpha$. By partial summation, we obtain

$$\begin{aligned}
\mathrm{Ind}_\gamma^\kappa(G) &= \frac{1}{|G|^{\gamma-\kappa}} \sum_{i=0}^{\alpha} \frac{f_{G,\gamma}(p^i)}{p^{i\kappa}} \\
&= \frac{|G|^\kappa}{|G|^\gamma} \left[\frac{h_{G,\gamma}(p^\alpha)}{\lambda_\gamma(G)^\kappa} - \sum_{j=0}^{\alpha-1} \left(\frac{1}{p^{(j+1)\kappa}} - \frac{1}{p^{j\kappa}} \right) h_{G,\gamma}(p^j) \right] \\
&= \frac{|G|^\kappa}{\lambda_\gamma(G)^\kappa} \left[1 + \left(1 - \frac{1}{p^\kappa}\right) \frac{\lambda_\gamma(G)^\kappa}{|G|^\gamma} \sum_{j=0}^{\alpha-1} \frac{h_{G,\gamma}(p^j)}{p^{j\kappa}} \right],
\end{aligned}$$

since $h_{G,\gamma}(p^\alpha)$ is the number of all elements in G^γ. The same argument yields the assertion for $\mathrm{Ord}_\gamma^\kappa(G)$. □

For an arbitrary finite abelian group G the determination of $h_{G,\gamma}(d)$, and hence of $\mathrm{Ind}_\gamma^\kappa(G)$ and $\mathrm{Ord}_\gamma^\kappa(G)$, seems very involved, for arbitrary $\gamma \in \mathbb{N}$. In case $\gamma = 1$, the reader may find an exact expression for $h_{G,1}(d)$ in [71]. We briefly address the computation of these quantities for two types of groups with a "sufficiently nice" structure which frequently occur in the sequel, not least in this chapter.

As a first example we assume G to be a finite cyclic group. This situation arises in the present chapter, as the groups $(\mathcal{O}_\mathbb{K} / \mathfrak{p})^*$ are cyclic of order $\mathcal{N}\mathfrak{p} - 1$, for every prime ideal $\mathfrak{p}$ of $\mathbb{K}$. In this case an easy computation reveals the following nice result.

LEMMA 6.6. *Let G be a finite cyclic group, $\gamma \in \mathbb{N}$ and d a divisor of $\lambda_\gamma(G) = |G|$. Then we have*

$$f_{G,\gamma}(d) = \sum_{e \mid d} \mu(e) \left(\frac{d}{e}\right)^\gamma \qquad \text{and} \qquad h_{G,\gamma}(d) = d^\gamma,$$

and for any $\kappa \in \mathbb{R}_+$ we have

$$\mathrm{Ord}_\gamma^\kappa(G) = |G|^\kappa \prod_{p^e ||| |G|} \left(1 - \frac{p^{(\gamma+\kappa)e} - 1}{p^{(\gamma+\kappa)e}} \cdot \frac{p^\kappa - 1}{p^{\gamma+\kappa} - 1} \right),$$

as well as

$$\mathrm{Ind}_\gamma^\gamma(G) = \prod_{p^e ||| |G|} \left(1 + \left(1 - \frac{1}{p^\gamma}\right) e \right)$$

and

$$\mathrm{Ind}_\gamma^\kappa(G) = \prod_{p^e \| |G|} \left(1 + \left(1 - \frac{1}{p^\kappa}\right) \frac{1 - p^{(\kappa-\gamma)e}}{p^{\gamma-\kappa} - 1}\right),$$

if $\gamma \neq \kappa$.

Proof. Let d divide $|G|$. Since G is cyclic, there is exactly one subgroup H of G with d elements and we have $H \supset \langle a_1, \dots, a_\gamma \rangle$ for $a_i \in G$ if and only if all a_i are contained in H. Hence $h_{G,\gamma}(d) = |H|^\gamma = d^\gamma$, and the formula for $f_{G,\gamma}(d)$ follows by Möbius inversion. Now assume $G = C_{p^e}$, for some prime p and $e \in \mathbb{N}$. Then, by Lemma 6.5 we easily get

$$\mathrm{Ord}_\gamma^\kappa(G) = |G|^\kappa \left(1 - \frac{p^\kappa - 1}{p^{(\gamma+\kappa)e}} \sum_{j=0}^{e-1} p^{(\gamma+\kappa)j}\right) = |G|^\kappa \left(1 - \frac{p^\kappa - 1}{p^{(\gamma+\kappa)e}} \cdot \frac{p^{(\gamma+\kappa)e} - 1}{p^{\gamma+\kappa} - 1}\right)$$

and

$$\mathrm{Ind}_\gamma^\kappa(G) = 1 + \left(1 - \frac{1}{p^\kappa}\right) p^{(\kappa-\gamma)e} \sum_{j=0}^{e-1} p^{(\gamma-\kappa)j}.$$

In case $\gamma = \kappa$, this immediately yields

$$\mathrm{Ind}_\gamma^\gamma(G) = 1 + \left(1 - \frac{1}{p^\gamma}\right) e,$$

and if $\gamma \neq \kappa$, we easily get

$$\mathrm{Ind}_\gamma^\kappa(G) = 1 + \left(1 - \frac{1}{p^\kappa}\right) p^{(\kappa-\gamma)e} \cdot \frac{p^{(\gamma-\kappa)e} - 1}{p^{\gamma-\kappa} - 1} = 1 + \left(1 - \frac{1}{p^\kappa}\right) \frac{1 - p^{(\kappa-\gamma)e}}{p^{\gamma-\kappa} - 1}.$$

□

The second example we are discussing is motivated by the theory of elliptic curves over finite fields which we get back to in Part III. If E is an elliptic curve defined over $\mathbb{F}_p$, for some prime p, then the group of $\mathbb{F}_p$-rational points $\mathrm{E}(\mathbb{F}_p)$ has the form $C_d \oplus C_{de}$ with appropriate $d, e \in \mathbb{N}$. See Chapter 8 for details. We restrict to $\gamma = 1$, the only case that matters for us, and obtain the following precise expressions for $h_{G,1}(\cdot)$ and $f_{G,1}(\cdot)$ and a sufficient lower bound for $\mathrm{Ord}_1^\kappa(G)$.

Lemma 6.7. *Let* $d, e \in \mathbb{N}$ *and* $G \cong C_d \oplus C_{de}$. *For any divisor* k *of* $\lambda(G) = de$ *we have*

$$f_{G,1}(k) = \sum_{l|k} \frac{\mu(l)k}{l} \left(\frac{k}{l}, d\right) \qquad \text{and} \qquad h_{G,1}(k) = k(k, d),$$

and

$$\mathrm{Ord}_1^\kappa(G) \geq (de)^\kappa \prod_{p \| |G|} \left(1 - \frac{1}{p} - \frac{1}{p^2}\right)$$

Proof. By Lemma 6.4 it suffices to consider $G = C_{p^m} \oplus C_{p^n}$ with a prime p and integers $0 \leq m \leq n$. Let $k = p^i$ with an integer $0 \leq i \leq n$. Elements of the form $(a_1, a_2) \in G$ with $a_1 \in C_{p^m}$ and $a_2 \in C_{p^n}$ are counted by $h_{G,1}(k)$ if and only if a_1 and a_2 are contained in a subgroup of C_{p^m} and C_{p^n} with $p^{\min\{i,m\}}$ and p^i elements, respectively.

Hence, we have $h_{G,1}(k) = k(k,p^n)$ and by Möbius inversion the assertion for $f_{G,1}(k)$ follows. Combining this with Lemma 6.5 yields

$$\begin{aligned}
\mathrm{Ord}_1^\kappa(G) &= p^{n\kappa}\left[1 - \frac{p^\kappa - 1}{p^{m+n}p^{n\kappa}} \sum_{j=0}^{\alpha_p - 1} p^{j\kappa} p^j (p^j, p^m)\right] \\
&= p^{n\kappa}\left[1 - \frac{p^\kappa - 1}{p^{m+n}p^{n\kappa}} \left(\sum_{j=0}^{m-1} p^{j(\kappa+2)} + p^m \sum_{j=m}^{n-1} p^{j(\kappa+1)}\right)\right] \\
&= p^{n\kappa}\left[1 - \frac{p^\kappa - 1}{p^{m+n}p^{m\kappa}} \left(\frac{p^{(\kappa+2)m} - 1}{p^{\kappa+2} - 1} + p^{2m} \cdot \frac{p^{(\kappa+1)(n-m)} - 1}{p^{\kappa+1} - 1}\right)\right] \\
&> p^{n\kappa}\left[1 - \frac{p^\kappa - 1}{p^{\kappa+2} - 1} \cdot \frac{p^{(\kappa+2)m}}{p^{m+n}p^{n\kappa}} - \frac{p^\kappa - 1}{p^{\kappa+1} - 1} \cdot \frac{p^{(\kappa+1)(n-m)}}{p^{n-m}p^{n\kappa}}\right] \\
&\geq p^{n\kappa}\left[1 - \frac{p^\kappa - 1}{p^{\kappa+2} - 1} - \frac{p^\kappa - 1}{p^{\kappa+1} - 1}\right] > p^{n\kappa}\left(1 - \frac{1}{p} - \frac{1}{p^2}\right),
\end{aligned}$$

where in the last line we utilized $0 \leq m \leq n$. □

To conclude this section we return to the treatment of an arbitrary finite abelian group G, and prove upper and lower bounds for $\mathrm{Ind}_\gamma^1(G)$. These estimates become of interest in Chapter 7, where they are applied to the groups $(\mathcal{O}_\mathbb{K} / \mathfrak{a})^*$ for an arbitrary ideal $\mathfrak{a}$ of $\mathbb{K}$ which are not cyclic in general. Similar results may be obtained for $\kappa > 1$ or $\mathrm{Ord}_\gamma^\kappa(G)$ (see also [71]), but are omitted because they won't be needed any further in the sequel.

THEOREM 6.8. *Let G be a finite abelian group and $\gamma \in \mathbb{N}$. Then*

$$\frac{|G|}{\lambda(G)} \leq \mathrm{Ind}_1^1(G) \leq \tau(\lambda(G)) \cdot \frac{|G|}{\lambda(G)}$$

and if $\gamma > 1$ we have

$$\frac{|G|}{\lambda_\gamma(G)} \leq \mathrm{Ind}_\gamma^1(G) \leq 2^{\omega(|G|)} \cdot \frac{|G|}{\lambda(G)}.$$

PROOF. The lower bounds are in both cases obvious from Lemma 6.5. As for the upper bounds, by Lemma 6.4 it suffices to consider the case of a finite, abelian p-group, because $\tau(n)$ and $2^{\omega(n)}$ are multiplicative. Hence, assume that $G = C_{p^{\alpha_1}} \oplus \cdots \oplus C_{p^{\alpha_n}}$ holds with $\alpha_1 \geq \ldots \alpha_n \geq 1$, and define α and β by $\lambda_\gamma(G) = p^\alpha$ and $|G| = p^\beta$. Then

$$h_{G,\gamma}(p^k) \leq h_{G,1}(p^k)^\gamma \leq p^{\gamma \sum_{i=1}^n \min(k,\alpha_i)}$$

holds for any $k = 0, \ldots, \alpha - 1$, since $|\langle a_1, \ldots, a_\gamma\rangle| \mid p^k$ certainly implies $|\langle a_i\rangle| \mid p^k$ for all $i = 1, \ldots, \gamma$. By Lemma 6.5, we thus obtain

$$\mathrm{Ind}_\gamma^1(G) \cdot \frac{\lambda_\gamma(G)}{|G|} \leq 1 + \left(1 - \frac{1}{p}\right) \frac{p^\alpha}{p^{\beta\gamma}} \sum_{k=0}^{\alpha-1} \frac{p^{\gamma \sum_{i=1}^n \min(k,\alpha_i)}}{p^k}. \tag{6.9}$$

In case $\gamma = 1$, this yields

$$\mathrm{Ind}_1^1(G) \cdot \frac{\lambda(G)}{|G|} \leq 1 + \left(1 - \frac{1}{p}\right) \sum_{k=0}^{\alpha_1 - 1} \frac{p^{\min(k,\alpha_1)}}{p^k} \leq \alpha_1 + 1 = \tau(\lambda(G)).$$

If $\gamma > 1$, we set $\alpha_0 := \alpha$ and $\alpha_{n+1} := 0$ and the right side of (6.9) is

$$\begin{aligned}
&= 1 + \left(1 - \frac{1}{p}\right) p^{\alpha} \sum_{j=0}^{n} \sum_{k=\alpha_{j+1}}^{\alpha_j - 1} \frac{p^{\gamma \sum_{i=1}^{j} k - \alpha_i}}{p^k} \\
&= 1 + \left(1 - \frac{1}{p}\right) \left(p^{\alpha} \sum_{k=\alpha_1}^{\alpha-1} p^{-k} + \sum_{j=1}^{n} p^{\alpha - \gamma \sum_{i=1}^{j} \alpha_i} \sum_{k=\alpha_{j+1}}^{\alpha_j - 1} p^{(\gamma j - 1)k} \right) \\
&= p^{\alpha - \alpha_1} + \left(1 - \frac{1}{p}\right) \sum_{j=1}^{n} p^{\alpha - \gamma \sum_{i=1}^{j} \alpha_i} \cdot \frac{p^{(\gamma j - 1)(\alpha_j - \alpha_{j+1})} - 1}{p^{\gamma j - 1} - 1} \cdot p^{(\gamma j - 1)\alpha_{j+1}} \\
&\overset{\gamma > 1}{\leq} p^{\alpha - \alpha_1} + \sum_{j=1}^{n} p^{\alpha - \gamma \sum_{i=1}^{j} \alpha_i} \cdot p^{(\gamma j - 1)\alpha_j - \gamma j + 1} \\
&\leq p^{\alpha - \alpha_1} + p^{\alpha - \alpha_1} \sum_{j=1}^{n} p^{-\gamma j + 1} \\
&\overset{\gamma > 1}{\leq} 2p^{\alpha - \alpha_1}.
\end{aligned}$$

This proves the assertion. □

6.3. Proofs of Theorems 6.1 and 6.2

Let us now return to the original problem and investigate the average behaviour of $\mathrm{Ind}_{\gamma}^{\kappa}(\mathfrak{p})$ over $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}/\mathbb{K})$, for arbitrary $\kappa \in \mathbb{R}_+$ and $\gamma \in \mathbb{N}$. Since $\mathrm{Ind}_{\gamma}^{\kappa}(\mathfrak{p})$ equals $\mathrm{Ind}_{\gamma}^{\kappa}((\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*)$ as defined in Section 6.2, we may apply the results from Section 6.2. By Lemma 6.6 and (6.3) we have

$$\mathrm{Ind}_{\gamma}^{\kappa}(\mathfrak{p}) = \sum_{d \mid \mathcal{N}\mathfrak{p} - 1} \frac{1}{d^{\gamma - \kappa}} \sum_{f \mid \frac{\mathcal{N}\mathfrak{p} - 1}{d}} \frac{\mu(f)}{f^{\gamma}}. \tag{6.10}$$

Summing over $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}/\mathbb{K})$, we thus obtain

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \mathrm{Ind}_{\gamma}^{\kappa}(\mathfrak{p}) = \sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \sum_{d \mid \mathcal{N}\mathfrak{p} - 1} \frac{1}{d^{\gamma - \kappa}} \sum_{f \mid (\mathcal{N}\mathfrak{p} - 1)/d} \frac{\mu(f)}{f^{\gamma}}. \tag{6.11}$$

This formula turns out to be a vital tool in case $\gamma \geq \kappa$. In case $\kappa > \gamma$, however, the term $1/d^{\gamma - \kappa}$ causes serious troubles, and it is more convenient to consider

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \frac{\mathrm{Ind}_{\gamma}^{\kappa}(\mathfrak{p})}{(\mathcal{N}\mathfrak{p} - 1)^{\kappa - \gamma}} = \sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \sum_{d \mid \mathcal{N}\mathfrak{p} - 1} \frac{1}{d^{\kappa - \gamma}} \sum_{f \mid d} \frac{\mu(f)}{f^{\gamma}}, \tag{6.12}$$

which is easily derived from Lemma 6.6 and (6.3) if one exchanges the roles of d and $(\mathcal{N}\mathfrak{p} - 1)/d$. We start with the proof of Theorem 6.1 and first consider parts (i) and (iii), as it turns out to be more convenient to treat the cases $\kappa = \gamma$ and $\kappa \neq \gamma$ separately.

6.3.1. Proof of Theorem 6.1 (i) and (iii). Let us first consider the case $\gamma \neq \kappa$. Rearranging the right sides of (6.11) and (6.12), yields

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \mathrm{Ind}_{\gamma}^{\kappa}(\mathfrak{p}) = \sum_{f \leq x} \frac{\mu(f)}{f^{\gamma}} \sum_{d \leq x} \frac{1}{d^{\gamma - \kappa}} \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ \mathcal{N}\mathfrak{p} \equiv 1 \ (df)}} 1 \tag{6.13}$$

in case $\gamma > \kappa$, and

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \frac{\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})}{(\mathcal{N}\mathfrak{p}-1)^{\kappa-\gamma}} = \sum_{f\le x}\frac{\mu(f)}{f^\kappa}\sum_{d\le x}\frac{1}{d^{\kappa-\gamma}} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}} 1 \tag{6.14}$$

for $\gamma < \kappa$. Observing (6.13) and (6.14), we notice that the respective right sides are almost identical, only κ and γ have swapped their roles. It therefore suffices to study the case $\gamma > \kappa$ by the right side of (6.13), and transfer the results to the case $\kappa > \gamma$ later on.

Henceforth, we thus assume $\gamma > \kappa$ until further notice. To get rid of the terms for large d and f, we prove the following lemma.

LEMMA 6.9. *Let $\kappa \in \mathbb{R}_+$ and $\gamma \in \mathbb{N}$ satisfy $\gamma > \kappa$. For any positive parameters $1 < y, z \le x^\alpha$, with $0 < \alpha < 1/2$, we have*

$$\begin{aligned}\sum_{f\le x}\frac{\mu(f)}{f^\gamma}\sum_{d\le x}\frac{1}{d^{\gamma-\kappa}} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}} 1 &= \sum_{f\le y}\frac{\mu(f)}{f^\gamma}\sum_{d\le z}\frac{1}{d^{\gamma-\kappa}} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}} 1 \\ &\quad + O\left(x^{2/3} + \frac{x}{x^{\alpha(\gamma-\kappa)}} + \frac{\mathrm{li}(x)}{y^\gamma} + \frac{\mathrm{li}(x)}{z^{\gamma-\kappa}}\right),\end{aligned}$$

where the implied constant depends on $\mathbb{K}$, γ and κ.

PROOF. The sum over $\mathfrak{p}$ is trivially bounded from above by $[\mathbb{K}:\mathbb{Q}]x/(df)$. Recalling that $\gamma \ge 1$ and $\gamma > \kappa$, we thus obtain

$$\sum_{f>x^\alpha}\frac{\mu(f)}{f^\gamma}\sum_{d\le x}\frac{1}{d^{\gamma-\kappa}} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}} 1 \ll_{\mathbb{K}} x\sum_{f>x^\alpha}\frac{1}{f^{\gamma+1}}\sum_{d\le x}\frac{1}{d^{\gamma-\kappa+1}} \ll_{\gamma,\kappa} x^{1-\gamma\alpha} \ll \frac{x}{x^{\alpha(\gamma-\kappa)}},$$

and

$$\sum_{f\le x}\frac{\mu(f)}{f^\gamma}\sum_{d>x^\alpha}\frac{1}{d^{\gamma-\kappa}} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}} 1 \ll_{\mathbb{K}} x\sum_{f\le x}\frac{1}{f^{\gamma+1}}\sum_{d>x^\alpha}\frac{1}{d^{\gamma-\kappa+1}} \ll_{\gamma,\kappa} \frac{x}{x^{\alpha(\gamma-\kappa)}}.$$

It remains to estimate the terms with $d, f \le x^\alpha$ and $f > y$ or $d > z$. The contribution of non-linear prime ideals of $\mathbb{K}$ is bounded by $O_{\mathbb{K}}(x^{2/3})$ as one can easily see from (6.11) and standard estimates for divisor functions (cf. [100, p. 81f]). By the Brun-Titchmarsh inequality, we obtain

$$\begin{aligned}\sum_{y<f\le x^\alpha}\frac{\mu(f)}{f^\gamma}\sum_{d\le x^\alpha}\frac{1}{d^{\gamma-\kappa}} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}} 1 &\ll_{\mathbb{K}} \sum_{y<f\le x^\alpha}\frac{\mu(f)}{f^\gamma}\sum_{d\le x^\alpha}\frac{\pi(x;1,df)}{d^{\gamma-\kappa}} + x^{2/3} \\ &\ll_{\gamma,\kappa} \frac{\mathrm{li}(x)}{y^\gamma} + x^{2/3}.\end{aligned}$$

Here we used the trivial estimate $\varphi(mn) \ge \varphi(m)\varphi(n)$ and Lemma 4.5. In the same way one deduces

$$\sum_{f\le x^\alpha}\frac{\mu(f)}{f^\gamma}\sum_{z<d\le x^\alpha}\frac{1}{d^{\gamma-\kappa}} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}} 1 \ll_{\mathbb{K},\gamma,\kappa} \frac{\mathrm{li}(x)}{z^{\gamma-\kappa}} + x^{2/3},$$

and the assertion follows. □

We choose parameters $1 \le y, z \le x^{1/3}$ which are specified later and obtain

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) = \sum_{f\le y}\frac{\mu(f)}{f^\gamma}\sum_{d\le z}\frac{1}{d^{\gamma-\kappa}} \sum_{\substack{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})\\ \mathcal{N}\mathfrak{p}\equiv 1\ (df)}} 1 + O\left(x^{2/3} + \frac{x}{x^{(\gamma-\kappa)/3}} + \frac{\mathrm{li}(x)}{y^\gamma} + \frac{\mathrm{li}(x)}{z^{\gamma-\kappa}}\right) \tag{6.15}$$

by Lemma 6.9, with an implied constant depending on $\mathbb{K}$, γ and κ. Now we recall that $\mathbb{K}(\zeta_n)$ and $\mathbb{L}(\zeta_n)$ are both finite Galois extensions of $\mathbb{K}$. By a standard argument from algebraic number theory, the condition $\mathcal{N}\mathfrak{p} \equiv 1\ (df)$ is equivalent to the complete splitting of $\mathfrak{p}$ in the Galois extension $\mathbb{K}(\zeta_{df})$ of $\mathbb{K}$ (cf. [86, p. 50]). Thus, the prime ideals $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}/\mathbb{K})$ which satisfy $\mathcal{N}\mathfrak{p} \equiv 1\ (df)$ are exactly those which are unramified in $\mathbb{L}(\zeta_{df})$ and satisfy $\left[\frac{\mathbb{L}(\zeta_{df})|\mathbb{K}}{\mathfrak{p}}\right] \subset C(df)$, where

$$C(n) := \{\sigma \in \mathrm{Gal}(\mathbb{L}(\zeta_n)/\mathbb{K}) : \sigma|_{\mathbb{L}} \in C, \sigma|_{\mathbb{K}(\zeta_n)} = \mathrm{id}\}$$

for any positive integer n.

Lemma 6.10. *$C(n)$ is either empty or a conjugacy class in $\mathrm{Gal}(\mathbb{L}(\zeta_n)/\mathbb{K})$, and we have*

$$|C(n)| = c_C(n),$$

where $c_C(n)$ is as defined in the statement of Theorem 6.1.

Proof. By Lemma 5.5, $C(n)$ is either empty or a conjugacy class of size $|C|$ in $\mathrm{Gal}(\mathbb{L}(\zeta_n)/\mathbb{K})$ (take $\Gamma = \{1\}$ in Lemma 5.5). It remains to show $|C(n)| = c_C(n)$.

Clearly $|C(n)| \ne 0$ implies $c_C(n) \ne 0$. If $c_C(n) \ne 0$, let σ lie in the intersection of C and $\mathrm{Gal}(\mathbb{L}/\mathbb{L}\cap\mathbb{K}(\zeta_n))$. Since $\mathbb{L}(\zeta_n)/\mathbb{L}\cap\mathbb{K}(\zeta_n)$ is the direct product of the extensions $\mathbb{L}/\mathbb{L}\cap\mathbb{K}(\zeta_n)$ and $\mathbb{K}(\zeta_n)/\mathbb{L}\cap\mathbb{K}(\zeta_n)$, there exists a lift $\tilde\sigma$ of σ in $\mathrm{Gal}(\mathbb{L}(\zeta_n)/\mathbb{L}\cap\mathbb{K}(\zeta_n))$ satisfying $\tilde\sigma|_{\mathbb{K}(\zeta_n)} = \mathrm{id}$ (cf. [46, p. 153f]). Hence we have $\tilde\sigma \in C(n)$ which shows that $C(n)$ is empty if and only if $c_C(n) = 0$. The assertion then follows from Lemma 5.5. □

The sum over $\mathfrak{p}$ on the right side of (6.15) may thus be written as $\pi_{C(df)}(x, \mathbb{L}(\zeta_{df})/\mathbb{K})$ which we will estimate by Proposition 4.8, the unconditional effective Čebotarev density theorem. To this end, choose y and z according to the condition $\log x \gg_{\mathbb{L}} (yz)^3 \log^2(yz)$. By Proposition 4.8 and Lemma 6.10, we infer from (6.15)

$$\begin{aligned}\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) &= \mathrm{li}(x)\sum_{f\le y}\frac{\mu(f)}{f^\gamma}\sum_{d\le z}\frac{c_C(df)}{d^{\gamma-\kappa}[\mathbb{L}(\zeta_{df}):\mathbb{K}]} + O\left(\frac{\mathrm{li}(x)}{y^\gamma} + \frac{\mathrm{li}(x)}{z^{\gamma-\kappa}}\right) + E\\ &= \mathrm{li}(x)\sum_{f\ge 1}\frac{\mu(f)}{f^\gamma}\sum_{d\ge 1}\frac{c_C(df)}{d^{\gamma-\kappa}[\mathbb{L}(\zeta_{df}):\mathbb{K}]} + O\left(\frac{\mathrm{li}(x)}{y^\gamma} + \frac{\mathrm{li}(x)}{z^{\gamma-\kappa}}\right) + E\\ &= \mathrm{li}(x)\sum_{n\ge 1}\frac{c_C(n)\varphi_\kappa(n)}{n^{\gamma-\kappa+1}[\mathbb{L}(\zeta_n):\mathbb{K}]} + O\left(\frac{\mathrm{li}(x)}{y^\gamma} + \frac{\mathrm{li}(x)}{z^{\gamma-\kappa}}\right) + E \end{aligned} \tag{6.16}$$

with an implied constant depending on γ, κ and $\mathbb{L}$, since

$$[\mathbb{L}(\zeta_n):\mathbb{K}] \ge [\mathbb{L}(\zeta_n):\mathbb{L}] = \frac{[\mathbb{L}(\zeta_n):\mathbb{Q}(\zeta_n)]\cdot[\mathbb{Q}(\zeta_n):\mathbb{Q}]}{[\mathbb{L}:\mathbb{Q}]} \gg_{\mathbb{L}} \varphi(n). \tag{6.17}$$

The sum in (6.16) clearly converges absolutely because of $0 \le c_C(n) \le C$, $\gamma > \kappa$ and (6.17), and it is positive because the first summand is so, and all others are ≥ 0.

To estimate the error term E coming from Proposition 4.8, we note that, for n large enough, the possible Siegel zeroes $\beta_0(\mathbb{L}(\zeta_n))$ of $\zeta_{\mathbb{L}(\zeta_n)}(s)$ which occur in E (cf. Proposition 4.8) satisfy

$$\beta_0(\mathbb{L}(\zeta_n)) \le 1 - \frac{1}{8[\mathbb{L}(\zeta_n):\mathbb{Q}]\cdot[\mathbb{L}(\zeta_n):\mathbb{Q}]!\log n} \le 1 - \frac{1}{(n[\mathbb{L}:\mathbb{Q}])^{n[\mathbb{L}:\mathbb{Q}]}} \tag{6.18}$$

by Proposition 4.10, Lemma 4.12 and Stirling's formula (cf. [100, p. 8]). Hence, by Proposition 4.8, Lemma 4.12, and (6.18) there exists a constant $c > 0$ depending on $\mathbb{L}$ such that[20]

$$E \ll_{\mathbb{L}} \sum_{f\le y}\frac{1}{f^{\gamma}}\sum_{d\le z}\frac{1}{d^{\gamma-\kappa}}\left[\frac{1}{\varphi(df)}\operatorname{li}\bigl(x^{\beta_0(\mathbb{L}(\zeta_{df}))}\bigr) + xe^{-c\left(\frac{\log x}{[\mathbb{L}(\zeta_{df}):\mathbb{Q}]}\right)^{1/2}}\right] \tag{6.19}$$

$$\ll_{\mathbb{L}} \operatorname{li}(x)\exp\left(-\frac{\log x}{(yz[\mathbb{L}:\mathbb{Q}])^{yz[\mathbb{L}:\mathbb{Q}]}}\right) + zxe^{-c'\left(\frac{\log x}{yz}\right)^{1/2}}. \tag{6.20}$$

Here c' is another appropriate positive constant depending on $\mathbb{L}$. In view of (6.16) and (6.20), we set

$$y := (\log\log x)^{\frac{\gamma-\kappa}{(2\gamma-\kappa)}-\varepsilon} \qquad \text{and} \qquad z := (\log\log x)^{\frac{\gamma}{(2\gamma-\kappa)}-\varepsilon}$$

which yields the asserted asymptotic formula

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})}\operatorname{Ind}_{\gamma}^{\kappa}(\mathfrak{p}) = \operatorname{li}(x)\sum_{n\ge1}\frac{c_C(n)\varphi_\kappa(n)}{n^{\gamma-\kappa+1}[\mathbb{L}(\zeta_n):\mathbb{K}]} + O\left(\frac{\operatorname{li}(x)}{(\log\log x)^{\frac{\gamma(\gamma-\kappa)}{2\gamma-\kappa}-\varepsilon}}\right), \tag{6.21}$$

with an implied constant depending on $\mathbb{L}$, γ, κ and ε. The corresponding asymptotic formula in case $\kappa > \gamma$ may be deduced from (6.14) by the same methods as above, followed by a simple partial summation argument. This proves Theorem 6.1.

While we are on the subject of error terms, let us for the ease of readability include at this point the corresponding estimations in the situation of Theorem 6.2 and briefly show how to improve the error term in (6.21) if we assume the existence of a field tower $\mathbb{Q} = \mathbb{M}_0 \subset \mathbb{M}_1 \subset \cdots \subset \mathbb{M}_s = \mathbb{K}$ in which each field is Galois over the preceding one. In this case, such a tower exists for any $\mathbb{L}(\zeta_n)$, too, and Proposition 4.10 and Lemma 4.12 provide the stronger bound $\beta_0(\mathbb{L}(\zeta_n)) \le 1-(c_3n^2)^{-1}$ instead of (6.18), if n is large enough. From (6.19) we thus derive

$$E \ll_{\mathbb{L}} \operatorname{li}(x)e^{-\frac{\log x}{c_3(yz)^2}} + zxe^{-c'\left(\frac{\log x}{yz}\right)^{1/2}}.$$

Collecting error terms and recalling the condition $\log x \gg_{\mathbb{L}} (yz)^3\log^2(yz)$, an optimization of y and z provides the choice

$$y := (\log x)^{\frac{\gamma-\kappa}{(6\gamma-3\kappa)}-\varepsilon} \qquad \text{and} \qquad z := (\log x)^{\frac{\gamma}{(6\gamma-3\kappa)}-\varepsilon}$$

and yields

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})}\operatorname{Ind}_{\gamma}^{\kappa}(\mathfrak{p}) = \operatorname{li}(x)\sum_{n\ge1}\frac{c_C(n)\varphi_\kappa(n)}{n^{\gamma-\kappa+1}[\mathbb{L}(\zeta_n):\mathbb{K}]} + O\left(\frac{\operatorname{li}(x)}{(\log x)^{\frac{\gamma(\gamma-\kappa)}{6\gamma-3\kappa}-\varepsilon}}\right), \tag{6.22}$$

with an implied constant depending on $\mathbb{L}$, γ, κ and ε. Just as above, it is easy to derive an analogue error term in case $\kappa > \gamma$. In this way we have confirmed the remark in the last paragraph of Section 6.1 and already proved a good part of Theorem 6.2, too. □

[20] Note that $\mathbb{L}(\zeta_n) = \mathbb{L}_{\{1\},n}$ for any $n \in \mathbb{N}$.

6.3.2. Proof of Theorem 6.1 (ii). From (6.10) we initially infer the estimate

$$\operatorname{Ind}_\gamma^\kappa(\mathfrak{p}) \le \sum_{d \mid \mathcal{N}\mathfrak{p}-1} d^{\kappa-\gamma} \le \max\{1, (\mathcal{N}\mathfrak{p}-1)^{\kappa-\gamma}\} \cdot \tau(\mathcal{N}\mathfrak{p}-1) \tag{6.23}$$

valid for arbitrary $\gamma \in \mathbb{N}$ and $\kappa \in \mathbb{R}_+$. Now assume $\kappa = \gamma$. The asserted upper bound easily follows by a famous result due to Linnik (cf. [67]):

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \operatorname{Ind}_\gamma^\gamma(\mathfrak{p}) \ll_{\mathbb{K}} \sum_{\substack{\mathcal{N}\mathfrak{p} \le x \\ \mathfrak{p} \text{ linear}}} \tau(\mathcal{N}\mathfrak{p}-1) + x^{2/3} \ll_{\mathbb{K}} \sum_{p \le x} \tau(p-1) + x^{2/3} \ll x.$$

Invoking (6.11), we find

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \operatorname{Ind}_\gamma^\gamma(\mathfrak{p}) = \sum_{d \le x} \frac{\varphi_\gamma(d)}{d} \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ d \mid \mathcal{N}\mathfrak{p}-1}} 1 \ge \sum_{d \le x} \frac{\varphi(d)}{d} \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ d \mid \mathcal{N}\mathfrak{p}-1}} 1.$$

We attend the inner sum by Proposition 4.9, the number field analogue of the Bombieri-Vinogradov theorem. To this end, we need to restrict the range for the moduli d a little further. Any $d \in \mathbb{N}$ for which $(d, \Delta_{\mathbb{L}}) = 1$ holds also satisfies $(\Delta_{\mathbb{Q}(\zeta_d)}, \Delta_{\mathbb{L}}) = 1$ (cf. Posposition 2.7 of [103]). Hence, $[\mathbb{L}(\zeta_d) : \mathbb{L}] = \varphi(d)$ and $\mathbb{L} \cap \mathbb{Q}(\zeta_d) = \mathbb{Q}$ hold whenever $(d, \Delta_{\mathbb{L}}) = 1$ (cf. [40, p. 98]). Since primes dividing $\Delta_{\mathbb{K}}$ must divide $\Delta_{\mathbb{L}}$ the same holds for $\mathbb{K}(\zeta_d)/\mathbb{K}$. Thus, we deduce $\mathbb{L} \cap \mathbb{K}(\zeta_d) = \mathbb{K}$ (cf. [46, p. 153]) and hence $|C(d)| = |C|$ by Lemma 6.10. For $0 < \alpha < 1/2$ small enough we finally obtain

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \operatorname{Ind}_\gamma^\gamma(\mathfrak{p}) \ge \sum_{\substack{d \le x^\alpha \\ (d, \Delta_{\mathbb{L}}) = 1}} \frac{\varphi(d)}{d} \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ d \mid \mathcal{N}\mathfrak{p}-1}} 1 \gg_{\mathbb{L}} \pi(x) \sum_{\substack{d \le x^\alpha \\ (d, \Delta_{\mathbb{L}}) = 1}} \frac{1}{d} \gg_{\mathbb{L}} x$$

by Proposition 4.9 and Möbius inversion. □

6.3.3. Proof of Theorem 6.2. Let us now consider the case where $\mathbb{L}/\mathbb{Q}$ and $\mathbb{K}/\mathbb{Q}$ are both Galois. The advantage here is the additional action of $\operatorname{Gal}(\mathbb{K}/\mathbb{Q})$ and $\operatorname{Gal}(\mathbb{L}/\mathbb{Q})$ on prime ideals of $\mathbb{K}$ and $\mathbb{L}$, respectively. By the same arguments as in Section 6.3.1, we may without loss of generality assume $\gamma \ge \kappa$. To begin with, we note that non-linear prime ideals of $\mathbb{K}$ are negligible, since there are only $O(\sqrt{x})$ such prime ideals $\mathfrak{p}$ with $\mathcal{N}\mathfrak{p} \le x$. Hence

$$\sum_{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K})} \operatorname{Ind}_\gamma^\kappa(\mathfrak{p}) = \sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ \mathfrak{p} \text{ linear}}} \operatorname{Ind}_\gamma^\kappa(\mathfrak{p}) + O_{\mathbb{K}}(x^{2/3})$$

by (6.23) and a trivial estimate for the divisor function (cf. [100, p. 81f]).

Now let $\sigma \in C$ and let $\mathcal{C}$ be the conjugacy class of σ in $\operatorname{Gal}(\mathbb{L}/\mathbb{Q})$. Clearly, we have $C \subset \mathcal{C} \subset \operatorname{Gal}(\mathbb{L}/\mathbb{K})$ because $\mathbb{K}/\mathbb{Q}$ is Galois. If $\mathcal{Z}(\sigma)$ denotes the centralizer of σ in $\operatorname{Gal}(\mathbb{L}/\mathbb{Q})$, let $\mathcal{R}$ be a set of representatives of right cosets of the subgroup $\mathcal{Z}(\sigma)\operatorname{Gal}(\mathbb{L}/\mathbb{K})$ in $\operatorname{Gal}(\mathbb{L}/\mathbb{Q})$. Then $\mathcal{C}$ is the disjoint union

$$\mathcal{C} = \bigcup_{\nu \in \mathcal{R}} C_\nu, \tag{6.24}$$

where C_ν shall denote the conjugacy class of $\nu\sigma\nu^{-1}$ in $\operatorname{Gal}(\mathbb{L}/\mathbb{K})$. If $\mathfrak{p}_1, \dots, \mathfrak{p}_{[\mathbb{K}:\mathbb{Q}]}$ are linear prime ideals of $\mathbb{K}$ lying over the same prime p, unramified in $\mathbb{L}$, one can easily verify (see e.g. [68, p. 126f]) the equivalence

$$\exists i : \left[\frac{\mathbb{L} \mid \mathbb{K}}{\mathfrak{p}_i}\right] = C \iff \left[\frac{\mathbb{L} \mid \mathbb{Q}}{p}\right] = \mathcal{C}.$$

In this case we deduce from (6.24) that the number of such prime ideals is exactly $\frac{|C|\cdot[\mathbb{K}:\mathbb{Q}]}{|\mathcal{C}|}$. Thus, we obtain

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) = \frac{|C|\cdot[\mathbb{K}:\mathbb{Q}]}{|\mathcal{C}|} \sum_{p\in\mathcal{P}_\mathcal{C}(x,\mathbb{L}/\mathbb{Q})} \mathrm{Ind}_\gamma^\kappa(p) + O_\mathbb{K}(x^{2/3}). \tag{6.25}$$

If $\gamma > \kappa$, (6.25) and the observation (6.22) from the end of Section 6.3.1 yield

$$\sum_{\mathfrak{p}\in\mathcal{P}_C(x,\mathbb{L}/\mathbb{K})} \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}) = \mathrm{li}(x)[\mathbb{K}:\mathbb{Q}] \sum_{n\geq 1} \frac{c_C(n)\varphi_\kappa(n)}{n^{\gamma-\kappa+1}[\mathbb{L}(\zeta_n):\mathbb{Q}]} + O\left(\frac{\mathrm{li}(x)}{(\log x)^{\frac{\gamma(\gamma-\kappa)}{6\gamma-3\kappa}-\varepsilon}}\right), \tag{6.26}$$

since $c_\mathcal{C}(n) = \frac{|\mathcal{C}|}{|C|}\cdot c_C(n)$, as one can easily derive from Lemma 6.10. The implied constant in (6.26) depends on γ, κ, $\mathbb{L}$ and ε.

Let us now consider the case $\gamma = \kappa$ and postpone the computation of the sum in (6.26). In this case (6.11) yields

$$\sum_{p\in\mathcal{P}_\mathcal{C}(x,\mathbb{L}/\mathbb{Q})} \mathrm{Ind}_\gamma^\gamma(p) = \sum_{p\in\mathcal{P}_\mathcal{C}(x,\mathbb{L}/\mathbb{Q})} \sum_{d\mid p-1} \sum_{f\mid(p-1)/d} \frac{\mu(f)}{f^\gamma}.$$

Here the terms for large d cannot be neglected any more. Set $y := \log^2 x$, and recall that $\gamma \geq 1$. Rearranging summation we obtain

$$\begin{aligned}\sum_{p\in\mathcal{P}_\mathcal{C}(x,\mathbb{L}/\mathbb{Q})} \mathrm{Ind}_\gamma^\gamma(p) &= \sum_{f\leq x} \frac{\mu(f)}{f^\gamma} \sum_{\substack{p\in\mathcal{P}_\mathcal{C}(x,\mathbb{L}/\mathbb{Q})\\ f\mid p-1}} \sum_{d\mid\frac{p-1}{f}} 1 \\ &= \sum_{f\leq y} \frac{\mu(f)}{f^\gamma} \sum_{\substack{p\in\mathcal{P}_\mathcal{C}(x,\mathbb{L}/\mathbb{Q})\\ f\mid p-1}} \sum_{d\mid\frac{p-1}{f}} 1 + O\left(\frac{x}{\log x}\right)\end{aligned}$$

by Lemma 4.5 and the same arguments used in the proof of Lemma 6.9. By the obvious estimate

$$\sum_{d\mid n} 1 = 2 \sum_{\substack{d\mid n\\ d<\sqrt{n}}} 1 + O(1)$$

and the Brun-Titchmarsh inequality, we get

$$\sum_{p\in\mathcal{P}_\mathcal{C}(x,\mathbb{L}/\mathbb{Q})} \mathrm{Ind}_\gamma^\gamma(p) = 2\sum_{f\leq y} \frac{\mu(f)}{f^\gamma} \sum_{\substack{p\in\mathcal{P}_\mathcal{C}(x,\mathbb{L}/\mathbb{Q})\\ f\mid p-1}} \sum_{\substack{d\mid\frac{p-1}{f}\\ d<\sqrt{\frac{p-1}{f}}}} 1 + O\left(\frac{x}{\log x}\right).$$

The above error term could be improved for $\gamma > 1$, but since there occur larger error terms in the sequel, we neglect this precision. Now we rearrange the sum again and get

$$\sum_{p\in\mathcal{P}_\mathcal{C}(x,\mathbb{L}/\mathbb{Q})} \mathrm{Ind}_\gamma^\gamma(p) = 2\sum_{f\leq y} \frac{\mu(f)}{f^\gamma} \sum_{d<\sqrt{\frac{x}{f}}} \sum_{\substack{p\in\mathcal{P}_\mathcal{C}(x,\mathbb{L}/\mathbb{Q})\\ p>d^2f+1\\ df\mid(p-1)}} 1 + O\left(\frac{x}{\log x}\right).$$

By the Brun-Titchmarsh inequality and Lemma 4.5, one easily deduces

$$\sum_{f\leq y} \frac{\mu(f)}{f^\gamma} \sum_{d<\sqrt{\frac{x}{f}}} \sum_{\substack{p\in\mathcal{P}_\mathcal{C}(d^2f,\mathbb{L}/\mathbb{Q})\\ df\mid(p-1)}} 1 = O\left(\frac{x}{\log x}\right).$$

Let B be a positive parameter. Proceeding as before, we get rid of the terms with $\sqrt{x}/\log^B x \le df < \sqrt{xf}$ and obtain

$$\sum_{p\in\mathcal{P}_{\mathcal{C}}(x,\mathbb{L}/\mathbb{Q})} \mathrm{Ind}_\gamma^{\mathcal{C}}(p) = 2\sum_{f\le y}\frac{\mu(f)}{f^\gamma}\sum_{df<\frac{\sqrt{x}}{\log^B x}}\sum_{\substack{p\in\mathcal{P}_{\mathcal{C}}(x,\mathbb{L}/\mathbb{Q})\\ df\mid(p-1)}} 1 + O\left(\frac{x\log\log x}{\log x}\right). \tag{6.27}$$

Due to the large moduli df in (6.27), the unconditional effective Čebotarev density theorem (Proposition 4.8) is not applicable to estimate the right side of (6.27) and the number field analogue of the Bombieri-Vinogradov theorem (Proposition 4.9) is not strong enough in general. Thus, by the effective Čebotarev density theorem under GRH (Proposition 4.7), if we assume GRH for the fields $\mathbb{L}(\zeta_{df})$, or by Proposition 4.9, if applicable, we find

$$\sum_{p\in\mathcal{P}_{\mathcal{C}}(x,\mathbb{L}/\mathbb{Q})} \mathrm{Ind}_\gamma^{\mathcal{C}}(p) = \frac{2|\mathcal{C}|}{|C|}\,\mathrm{li}(x)\sum_{f\le y}\frac{\mu(f)}{f^\gamma}\sum_{df<\frac{\sqrt{x}}{\log^B x}}\frac{c_C(df)}{[\mathbb{L}(\zeta_{df}):\mathbb{Q}]} + E' + O\left(\frac{x\log\log x}{\log x}\right)$$

with

$$\begin{aligned} E' &\ll \sum_{f\le y}\frac{1}{f^\gamma}\sum_{e<\frac{\sqrt{x}}{\log^B x}}\left[\frac{c_C(e)}{[\mathbb{L}(\zeta_e):\mathbb{Q}]}\cdot x^{\frac12}\log\left(\Delta_{\mathbb{L}(\zeta_e)}x^{[\mathbb{L}(\zeta_e):\mathbb{Q}]}\right) + \log(\Delta_{\mathbb{L}(\zeta_e)})\right]\\ &\ll \log\log x\sum_{e<\frac{\sqrt{x}}{\log^B x}}\left[x^{\frac12}\log(x) + [\mathbb{L}(\zeta_e):\mathbb{Q}]\log(x)\right] \ll \frac{x\log\log x}{(\log x)^{B-1}} \end{aligned}$$

by Lemma 4.12. Choosing $B \ge 2$, we finally arrive at

$$\begin{aligned} \sum_{p\in\mathcal{P}_{\mathcal{C}}(x,\mathbb{L}/\mathbb{Q})} \mathrm{Ind}_\gamma^{\mathcal{C}}(p) &= \frac{2|\mathcal{C}|}{|C|}\,\mathrm{li}(x)\sum_{f\le y}\frac{\mu(f)}{f^\gamma}\sum_{df<\frac{\sqrt{x}}{\log^B x}}\frac{c_C(df)}{[\mathbb{L}(\zeta_{df}):\mathbb{Q}]} + O_{\mathbb{L}}\left(\frac{x\log\log x}{\log x}\right)\\ &= \frac{2|\mathcal{C}|}{|C|}\,\mathrm{li}(x)\sum_{f\ge1}\frac{\mu(f)}{f^\gamma}\sum_{df<\frac{\sqrt{x}}{\log^B x}}\frac{c_C(df)}{[\mathbb{L}(\zeta_{df}):\mathbb{Q}]} + O_{\mathbb{L}}\left(\frac{x\log\log x}{\log x}\right)\\ &= \frac{2|\mathcal{C}|}{|C|}\,\mathrm{li}(x)\sum_{n\le\frac{\sqrt{x}}{\log^B x}}\frac{c_C(n)\varphi_\gamma(n)}{n[\mathbb{L}(\zeta_n):\mathbb{Q}]} + O_{\mathbb{L}}\left(\frac{x\log\log x}{\log x}\right)\\ &= \frac{2|\mathcal{C}|}{|C|}\,\mathrm{li}(x)\sum_{n\le\sqrt{x}}\frac{c_C(n)\varphi_\gamma(n)}{n[\mathbb{L}(\zeta_n):\mathbb{Q}]} + O_{\mathbb{L}}\left(\frac{x\log\log x}{\log x}\right). \end{aligned} \tag{6.28}$$

In light of (6.26) and (6.28), it suffices to compute an asymptotic formula for

$$\sum_{n\le\sqrt{x}}\frac{c_C(n)\varphi_\kappa(n)}{n^{\gamma-\kappa+1}[\mathbb{L}(\zeta_n):\mathbb{Q}]},$$

with arbitrary $\gamma \ge \kappa$ to prove both Theorem 6.2 (i) and (ii). Choosing $m \in \mathbb{N}$ such that $\mathbb{L}^{ab} \subset \mathbb{Q}(\zeta_m)$ (this is possible by the Kronecker-Weber theorem [68, p. 273]), we obtain

$$\sum_{n\le\sqrt{x}}\frac{c_C(n)\varphi_\kappa(n)}{n^{\gamma-\kappa+1}[\mathbb{L}(\zeta_n):\mathbb{Q}]}=\sum_{d\mid m}\sum_{\substack{n\le\sqrt{x}\\(n,m)=d}}\frac{c_C(n)\varphi_\kappa(n)[\mathbb{L}\cap\mathbb{Q}(\zeta_n):\mathbb{Q}]}{n^{\gamma-\kappa+1}\varphi(n)[\mathbb{L}:\mathbb{Q}]}$$
$$=\frac{|C|}{[\mathbb{L}:\mathbb{Q}]}\sum_{\substack{d\mid m\\c_C(d)\neq0}}[\mathbb{L}\cap\mathbb{Q}(\zeta_d):\mathbb{Q}]\sum_{\substack{n\le\sqrt{x}\\(n,m)=d}}\frac{\varphi_\kappa(n)}{n^{\gamma-\kappa+1}\varphi(n)}$$

since $\mathbb{Q}(\zeta_k)\cap\mathbb{Q}(\zeta_l)=\mathbb{Q}(\zeta_{(k,l)})$ holds for any $k,l\in\mathbb{N}$. The subsequent lemma eventually completes the proof in case $\gamma\ge\kappa$ if one observes that the above sum on d is positive, for all summands are non-negative, and the term associated to $d=1$ is not zero. As in Section 6.3.1, the case $\gamma<\kappa$ again follows by swapping γ and κ and applying a simple partial summation argument. □

LEMMA 6.11. *Let $\gamma,\kappa\in\mathbb{R}_+$ satisfy*[21] *$\gamma\ge\kappa$. For any two positive integers m, d with $d\mid m$ we define $a_\gamma^{(\kappa)}(m,d)$ to be the product*

$$\prod_{p\nmid m}\left(1+\frac{1-p^{1-\kappa}}{(p-1)p^{\gamma-\kappa+1}}\right)\prod_{p\mid d}\left(1+\frac{1-p^{1-\kappa}}{(p-1)p^{\gamma-\kappa}}\right)\prod_{\substack{p\mid\frac{m}{d}\\p\nmid d}}\left(1+\frac{(1-p^{1-\kappa})(p^{\gamma-\kappa}-1)}{(p-1)p^{\gamma-\kappa}(p^{\gamma-\kappa+1}-1)}\right).$$

This product is absolutely convergent and positive. If $\gamma=\kappa$, we have

$$\sum_{\substack{n\le x\\(n,m)=d}}\frac{\varphi_\kappa(n)}{n^{\gamma-\kappa+1}\varphi(n)}=\frac{\varphi_{\gamma-\kappa+1}(\frac{m}{d})a(m,d)}{md^{\gamma-\kappa}}\cdot\log x+O_m(1),$$

and if $\gamma>\kappa$, we have

$$\sum_{\substack{n\le x\\(n,m)=d}}\frac{\varphi_\kappa(n)}{n^{\gamma-\kappa+1}\varphi(n)}=\frac{\varphi_{\gamma-\kappa+1}(\frac{m}{d})a(m,d)\zeta(\gamma-\kappa+1)}{md^{\gamma-\kappa}}+O_m(x^{\kappa-\gamma}).$$

PROOF. By Möbius inversion we initially obtain

$$\sum_{\substack{n\le x\\(n,m)=d}}\frac{\varphi_\kappa(n)}{n^{\gamma-\kappa+1}\varphi(n)}=\sum_{e\mid\frac{m}{d}}\mu(e)\sum_{\substack{n\le x\\ed\mid n}}\frac{\varphi_\kappa(n)}{n^{\gamma-\kappa+1}\varphi(n)}.\tag{6.29}$$

The function $\varphi_\kappa(n)/\varphi(n)$ is clearly multiplicative and may be written as

$$\frac{\varphi_\kappa(n)}{\varphi(n)}=\sum_{s\mid n}\mu^2(s)\xi_\kappa(s),\tag{6.30}$$

with a multiplicative function $\xi_\kappa(s)$ which fulfils

$$\xi_\kappa(p)=\frac{1-p^{1-\kappa}}{p-1}\qquad\text{and}\qquad|\xi_\kappa(p)|\le\begin{cases}\frac{1}{\varphi(p)}, & \text{if }\kappa\ge1,\\ 1, & \text{otherwise}\end{cases}\tag{6.31}$$

for any prime p. By (6.30), the right side of (6.29) equals

$$\frac{1}{d^{\gamma-\kappa+1}}\sum_{e\mid\frac{m}{d}}\frac{\mu(e)}{e^{\gamma-\kappa+1}}\sum_{s\le x}\frac{\mu^2(s)\xi_\kappa(s)(s,ed)}{s^{\gamma-\kappa+1}}\sum_{n\le\frac{x}{[s,ed]}}\frac{1}{n^{\gamma-\kappa+1}}.$$

[21] For the term $A_{\kappa,C}^{(\gamma)}$ in Theorem 6.2 to make sense, we allow real values for γ.

As one can easily verify using (6.31), the sum on n may be extended to all $n \in \mathbb{N}$ if $\gamma > \kappa$, and to $n \leq x$ if $\kappa = \gamma$, which effects the asserted error terms. In both cases the sum on n thereby becomes independent of the other terms and yields the respective factors $\zeta(\gamma - \kappa + 1)$ and $\log x$ in the assertion. By analogue arguments one may extend the sum on s to all $s \in \mathbb{N}$. Thus it remains to compute

$$\sum_{e \mid \frac{m}{d}} \frac{\mu(e)}{e^{\gamma-\kappa+1}} \sum_{s \geq 1} \frac{\mu^2(s)\xi_\kappa(s)(s, ed)}{s^{\gamma-\kappa+1}}. \tag{6.32}$$

The sum on s can be expressed as an Euler product, so that (6.32) becomes

$$\begin{aligned} &\sum_{e \mid \frac{m}{d}} \frac{\mu(e)}{e^{\gamma-\kappa+1}} \prod_{p \mid ed} \left(1 + \frac{\xi_\kappa(p)}{p^{\gamma-\kappa}}\right) \prod_{p \nmid ed} \left(1 + \frac{\xi_\kappa(p)}{p^{\gamma-\kappa+1}}\right) \\ &= \prod_{p \nmid d} \left(1 + \frac{\xi_\kappa(p)}{p^{\gamma-\kappa+1}}\right) \prod_{p \mid d} \left(1 + \frac{\xi_\kappa(p)}{p^{\gamma-\kappa}}\right) \sum_{e \mid \frac{m}{d}} \frac{\mu(e)}{e^{\gamma-\kappa+1}} \prod_{\substack{p \mid e \\ p \nmid d}} \left(\frac{1 + \frac{\xi_\kappa(p)}{p^{\gamma-\kappa}}}{1 + \frac{\xi_\kappa(p)}{p^{\gamma-\kappa+1}}}\right). \end{aligned} \tag{6.33}$$

The sum on e is clearly multiplicative, and equals

$$\prod_{\substack{p \mid \frac{m}{d} \\ p \mid d}} \left(1 - \frac{1}{p^{\gamma-\kappa+1}}\right) \prod_{\substack{p \mid \frac{m}{d} \\ p \nmid d}} \left(1 - \frac{1 + \frac{\xi_\kappa(p)}{p^{\gamma-\kappa}}}{p^{\gamma-\kappa+1} + \xi_\kappa(p)}\right). \tag{6.34}$$

Combining (6.33) and (6.34), one easily checks that (6.32) equals

$$\prod_{p \nmid m} \left(1 + \frac{\xi_\kappa(p)}{p^{\gamma-\kappa+1}}\right) \prod_{p \mid d} \left(1 + \frac{\xi_\kappa(p)}{p^{\gamma-\kappa}}\right) \prod_{p \mid \frac{m}{d}} \left(1 - \frac{1}{p^{\gamma-\kappa+1}}\right) \prod_{\substack{p \mid \frac{m}{d} \\ p \nmid d}} \left(1 + \frac{\xi_\kappa(p)(p^{\gamma-\kappa} - 1)}{p^{\gamma-\kappa}(p^{\gamma-\kappa+1} - 1)}\right).$$

By (6.31), this product is positive and the assertion follows. □

6.4. Generalizing a work of Luca

The preceding sections of this chapter naturally raise the question, whether the analogue idea of double averaging is amenable to the easier case of the residual order instead of the residual index. Letting

$$\operatorname{Ord}_\gamma^\kappa(\mathfrak{p}) := \sum_{a_1, \ldots, a_\gamma \in (\mathcal{O}_\mathbb{K} / \mathfrak{p})^*} \frac{\operatorname{ord}_{\langle a_1, \ldots, a_\gamma \rangle}(\mathfrak{p})^\kappa}{(\mathcal{N}\mathfrak{p} - 1)^\gamma}, \tag{6.35}$$

one would then ask for asymptotic formulae for the average order of $\operatorname{Ord}_\gamma^\kappa(\mathfrak{p})$ over prime ideals $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L} / \mathbb{K})$. We have already proved corresponding results for $\operatorname{ord}_\Gamma(\mathfrak{p})$ under GRH without an additional averaging process in Chapter 5. Hence, this task is only worth investigating if one could relax the GRH condition. Luca [69] has addressed this problem in case $\mathbb{L} = \mathbb{K} = \mathbb{Q}$ and $\gamma = \kappa = 1$ and successfully managed to prove the following unconditional result:

Proposition 6.12 (Luca, 2005). *For any constant $A > 0$, one has*

$$\sum_{p \leq x} \operatorname{Ord}_1^1(p) = c_{Stephens} \cdot \operatorname{li}(x^2) + O_A\left(\frac{x^2}{(\log x)^{A+1}}\right),$$

where $c_{Stephens}$ is the Stephens' constant defined in Remark 5.2.

The proof uses methods similar to those presented in Section 6.3. Its key ingredients are the Brun-Titchmarsh inequality and the Siegel-Walfisz theorem to estimate primes in arithmetic progression. Even though not executed here, this proof admits a straightforward generalization to number fields, and yields corresponding asymptotic formulae for the average order of $\mathrm{Ord}_\gamma^\kappa(\mathfrak{p})$ which agree with Theorem 5.3. The Siegel-Walfisz theorem then needs to be replaced by Proposition 4.8, the unconditional effective Čebotarev density theorem. Different to the corresponding results for $\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$, the asymptotic formulae hold unconditionally, even if $\gamma = \kappa$. This is due to the fact that the residual order is large in general, so that terms corresponding to small residual order may be neglected and Proposition 4.8 becomes applicable (cf. [69]). This did not work for $\mathrm{Ind}_\gamma^\gamma(\mathfrak{p})$, where the necessary prime ideal estimates were not within the scope of Proposition 4.8, and one had to resort to the effective Čebotarev density theorem under GRH (or number field analogues of the Bombieri-Vinogradov theorem if applicable) instead.

6.5. Reduction of the summation range via Poisson summation

Let κ, $\mathbb{K}$, Γ and γ be as above and fix $\mathfrak{p} \in \mathcal{P}(\mathbb{K})$. In light of (4.2) one has to confront the question how good $\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$ and $\mathrm{Ord}_\gamma^\kappa(\mathfrak{p})$ resemble $\mathrm{ind}_\Gamma(\mathfrak{p})^\kappa$ and $\mathrm{ord}_\Gamma(\mathfrak{p})^\kappa$, respectively. As a matter of fact, one might obtain more appropriate approximations to $\mathrm{ind}_\Gamma(\mathfrak{p})^\kappa$ and $\mathrm{ord}_\Gamma(\mathfrak{p})^\kappa$ if one reduces the summation ranges in (6.1) and (6.35) and, instead of averaging over all elements of $(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*$, only averages over a sufficiently small portion of these. In case of the rational numbers it would be standard procedure to consider

$$\frac{1}{y^\gamma} \sum_{\substack{1 \le a_1,\dots,a_\gamma \le y \\ \forall i:\ p \nmid a_i}} \mathrm{ind}_{\langle a_1,\dots,a_\gamma\rangle}(p)^\kappa \quad \text{and} \quad \frac{1}{y^\gamma} \sum_{\substack{1 \le a_1,\dots,a_\gamma \le y \\ \forall i:\ p \nmid a_i}} \mathrm{ord}_{\langle a_1,\dots,a_\gamma\rangle}(p)^\kappa \tag{6.36}$$

instead of $\mathrm{Ind}_\gamma^\kappa(p)$ and $\mathrm{Ord}_\gamma^\kappa(p)$ for some $y \le p$ which one desires to choose as small as possible. However, choosing it too small might prevent the establishment of appropriate asymptotic formulae such as in Theorem 6.1. In case $\gamma = 1$, Felix [27] showed how to reduce the summation range on average over $p \le x$ to any y which satisfies $x/\log x = o(y)$. In this section we consider "smoothened" number field analogues of (6.36).

6.5.1. Introduction and statement. For the remainder of this section we set $N := [\mathbb{K} : \mathbb{Q}]$, and observe that the integers $\mathcal{O}_\mathbb{K}$ of $\mathbb{K}$ naturally define a complete lattice in the N-space $V := \mathbb{K} \otimes_\mathbb{Q} \mathbb{R}$. For convenience, we fix an integral basis $\mathcal{B} = (\alpha_1, \dots, \alpha_N)$ of $\mathbb{K}$ and identify V with $\mathbb{R}^N$, i.e. we identify vectors of V by their coordinate vector according to $\mathcal{B}$. Moreover, we may as well regard each integer in $\mathcal{O}_\mathbb{K}$ as a tupel in $\mathbb{Z}^N$ and any ideal of $\mathcal{O}_\mathbb{K}$, in particular the prime ideal $\mathfrak{p}$ itself, as a complete sublattice therein (cf. [86, p. 16]). Henceforth, we will interchangeably write $\mathbb{R}^N$ or V and $\mathbb{Z}^N$ or $\mathcal{O}_\mathbb{K}$, respectively.

Following standard notation, $\boldsymbol{\lambda}$ shall denote the Lebesgue measure in $\mathbb{R}^N$, the standard scalar product on $\mathbb{R}^N$ is denoted by $\langle \cdot, \cdot \rangle$ and the associated euclidean norm by $\|\cdot\|_2$. For any linear automorphism A of $\mathbb{R}^N$, its Hermitian adjoint is denoted by A^*. As inverting and adjoining are commuting operations on A, we write A^{-*} for $(A^*)^{-1} = (A^{-1})^*$. Further, we let $\rho_{\min}(A)$ be the square-root of the smallest eigenvalue of A^*A, or equivalently

$$\rho_{\min}(A) := \sup\left\{ t \in \mathbb{R}_+ : \|Ax\|_2 \ge t\|x\|_2 \text{ holds for all } x \in \mathbb{R}^N \right\} \tag{6.37}$$

(cf. [91, p. 52f]). Since eigenvalues of A^*A and AA^* coincide (cf. [91, p. 65f]), we have

$$\rho_{\min}(A) = \rho_{\min}(A^*). \tag{6.38}$$

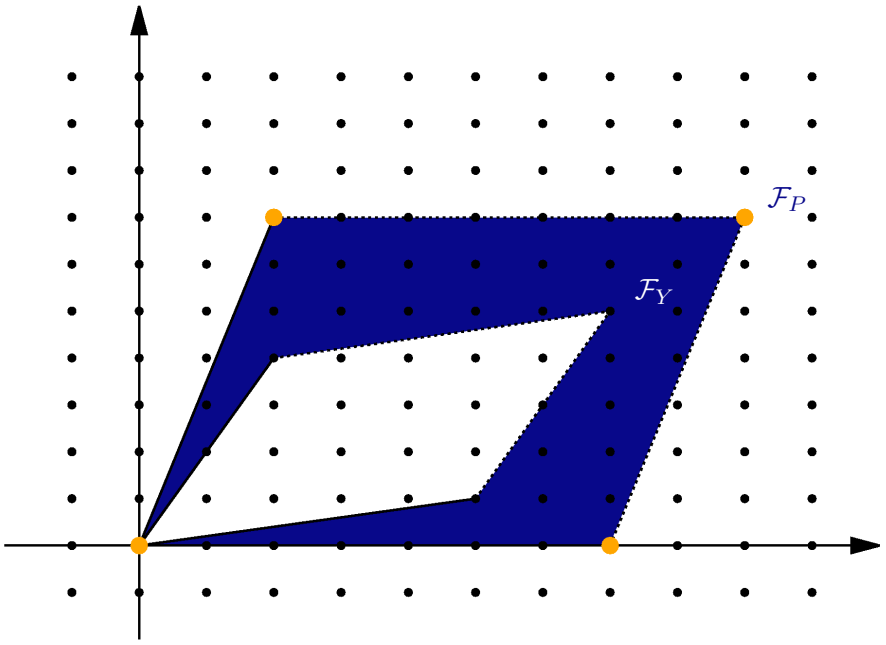


FIGURE 6.1. A reduced summation range for an inert prime ideal $\mathfrak{p} \mid 7$ of a quadratic field $\mathbb{K}$. Integers $\mathcal{O}_\mathbb{K}$ are represented as $\mathbb{Z}^2$ with sublattice $\mathfrak{p}$ (orange). $\mathcal{F}_P$ (blue rhomboid) and $\mathcal{F}_Y$ (white rhomboid) are images of the two-dimensional standard hyper cube under P and Y as in Theorem 6.13.

Let us turn to number field analogues of (6.36). To this end, let P and Y be linear automorphisms of $\mathbb{R}^N$, where P ought to map $\mathbb{Z}^N$ onto $\mathfrak{p}$ and Y shall take the place of the parameter y in (6.36). Then $Y\,\mathbb{Z}^N$ is a complete lattice in $\mathbb{R}^N$ of volume[22] $|\det(Y)|$ and we denote the fundamental domain in $\mathbb{R}^N$ associated to the image of $\mathcal{B}$ under Y by $\mathcal{F}_Y$. In the same way we define $\mathcal{F}_P$. If the number of points in $\mathcal{F}_Y \cap \mathbb{Z}^N$ is approximated by $|\det(Y)|$ sufficiently well, appropriate generalizations to number fields of (6.36) are provided by

$$\frac{1}{|\det(Y)|^\gamma} \sum_{\substack{a_1,\dots,a_\gamma \in \mathcal{F}_Y \cap \mathbb{Z}^N \\ \forall i\colon\ a_i \notin \mathfrak{p}}} \operatorname{ind}_{\langle a_1,\dots,a_\gamma\rangle}(\mathfrak{p})^\kappa, \tag{6.39}$$

and

$$\frac{1}{|\det(Y)|^\gamma} \sum_{\substack{a_1,\dots,a_\gamma \in \mathcal{F}_Y \cap \mathbb{Z}^N \\ \forall i\colon\ a_i \notin \mathfrak{p}}} \operatorname{ord}_{\langle a_1,\dots,a_\gamma\rangle}(\mathfrak{p})^\kappa, \tag{6.40}$$

in which one wishes to choose Y such that $|\det(Y)|$ is small compared to $\mathcal{N}\mathfrak{p} = |\det(P)|$ (see Figure 6.1).

Instead, however, we follow a slightly different approach and insert an appropriate "smoothing weight" into (6.39) and (6.40) to allow for the application of powerful methods from Fourier analysis. To this end, we choose γ "sufficiently smooth" *weight functions* $\omega_1, \dots, \omega_\gamma : \mathbb{R}^N \to \mathbb{R}$. What exactly is meant by "sufficiently smooth" will become clear

[22] Volume is always understood with respect to $\boldsymbol{\lambda}$.

in Theorem 6.13. We require the ω_i to be *normalized*, i.e.

$$\hat{\omega}_i(0) = \int_{\mathbb{R}^N} \omega_i(t)\, d\boldsymbol{\lambda}(t) = 1, \qquad i = 1, \dots, \gamma,$$

and to appropriately approximate the characteristic function on the fundamental domain associated to the standard basis of $\mathbb{R}^N$, referred to as the *standard hyper cube* of $\mathbb{R}^N$. Here, the *Fourier transforms* of the ω_i are defined as the functions $\hat{\omega}_i : \mathbb{R}^N \to \mathbb{R}$ given by

$$\hat{\omega}_i(u) := \int_{\mathbb{R}^N} \omega(t) e(-\langle u, t\rangle)\, d\boldsymbol{\lambda}(t).$$

Moreover, we define $\boldsymbol{\omega} : \mathbb{R}^{N\times\gamma} \to \mathbb{R}$ by

$$\boldsymbol{\omega}(x_1, \dots, x_\gamma) := \omega_1(x_1) \cdots \omega_\gamma(x_\gamma).$$

For any γ-tupel $\boldsymbol{a} = (a_1, \dots, a_\gamma) \in \mathbb{Z}^{N\times\gamma}$, $a_i \notin \mathfrak{p}$, we write $\mathrm{ind}_{\boldsymbol{a}}(\mathfrak{p})$ and $\mathrm{ord}_{\boldsymbol{a}}(\mathfrak{p})$ instead of $\mathrm{ind}_{\langle a_1,\dots,a_\gamma\rangle}(\mathfrak{p})$ and $\mathrm{ord}_{\langle a_1,\dots,a_\gamma\rangle}(\mathfrak{p})$, respectively, and for any two γ-tupels $\boldsymbol{x} = (x_1, \dots, x_\gamma)$ and $\boldsymbol{y} = (y_1, \dots, y_\gamma) \in \mathbb{R}^{N\times\gamma}$ and any linear automorphism A of $\mathbb{R}^N$, we set $A\,\boldsymbol{x} := (Ax_1, \dots, Ax_\gamma)$ and $\boldsymbol{x} + \boldsymbol{y} := (x_1 + y_1, \dots, x_\gamma + y_\gamma)$. On the basis of these notations define

$$\mathrm{Ind}_\gamma^\kappa(\mathfrak{p}; \boldsymbol{\omega}, Y) := \frac{1}{|\det(Y)|^\gamma} \sum_{\substack{\boldsymbol{a}\in\mathbb{R}^{N\times\gamma} \\ \forall i:\ a_i\notin\mathfrak{p}}} \mathrm{ind}_{\boldsymbol{a}}(\mathfrak{p})^\kappa\, \boldsymbol{\omega}(Y^{-1}\,\boldsymbol{a}), \tag{6.41}$$

and

$$\mathrm{Ord}_\gamma^\kappa(\mathfrak{p}; \boldsymbol{\omega}, Y) := \frac{1}{|\det(Y)|^\gamma} \sum_{\substack{\boldsymbol{a}\in\mathbb{R}^{N\times\gamma} \\ \forall i:\ a_i\notin\mathfrak{p}}} \mathrm{ord}_{\boldsymbol{a}}(\mathfrak{p})^\kappa\, \boldsymbol{\omega}(Y^{-1}\,\boldsymbol{a}). \tag{6.42}$$

Clearly, (6.41) and (6.42) yield "smoothened approximations" to (6.39) and (6.40), since these would arise from (6.41) and (6.42) if each of the ω_i was the characteristic function on the standard hyper cube. We prove the following theorem which provides information on how well (6.41) and (6.42) approximate $\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$ and $\mathrm{Ord}_\gamma^\kappa(\mathfrak{p})$, respectively.

THEOREM 6.13. *Let $\kappa \in \mathbb{R}_+$, $\gamma \in \mathbb{N}$ and $\mathfrak{p} \in \mathcal{P}(\mathbb{K})$. Let Y and P be linear automorphisms of $\mathbb{R}^N$ such that $P\,\mathbb{Z}^N = \mathfrak{p}$, $\rho_{\min}(Y) = \mathcal{N}\mathfrak{p}^\alpha$ with $\alpha \geq 0$ and $\rho_{\min}(P^{-1}Y) = \mathcal{N}\mathfrak{p}^{-\beta}$ with $\beta \geq 0$. Let $\omega_1, \dots, \omega_\gamma : \mathbb{R}^N \to \mathbb{R}$ be continuous and normalized with*

$$\omega_i(t) \ll (1 + \|t\|_2)^{-N-\delta} \qquad \text{and} \qquad \hat{\omega}_i(u) \ll (1 + \|u\|_2)^{-N-\delta}$$

for any $t, u \in \mathbb{R}^N$ and some $\delta > 0$. Then, for any $\varepsilon > 0$ and $0 < \delta' < \delta$ we have

$$\begin{aligned}\mathrm{Ord}_\gamma^\kappa(\mathfrak{p}; \boldsymbol{\omega}, Y) = {} & \mathrm{Ord}_\gamma^\kappa(\mathfrak{p})\Big(1 + O_\gamma(\mathcal{N}\mathfrak{p}^{-1})\Big) \\ & + O\left(\frac{\mathcal{N}\mathfrak{p}^\kappa}{\mathcal{N}\mathfrak{p}^{\alpha(N+\delta)}} + \frac{\mathcal{N}\mathfrak{p}^{\kappa+\varepsilon}}{\mathcal{N}\mathfrak{p}^{\gamma\left(\frac{1}{2}-\beta(N+\delta')\right)}} + \frac{\mathcal{N}\mathfrak{p}^{\kappa+\varepsilon}}{\mathcal{N}\mathfrak{p}^{\frac{1}{2}-\beta(N+\delta')}}\right)\end{aligned}$$

and

$$\begin{aligned}\mathrm{Ind}_\gamma^\kappa(\mathfrak{p}; \boldsymbol{\omega}, Y) = {} & \mathrm{Ind}_\gamma^\kappa(\mathfrak{p})\Big(1 + O_\gamma(\mathcal{N}\mathfrak{p}^{-1})\Big) \\ & + O\left(\frac{\mathcal{N}\mathfrak{p}^{\max\{\kappa-\gamma,0\}+\varepsilon}}{\mathcal{N}\mathfrak{p}^{\alpha(N+\delta)}} + \frac{\mathcal{N}\mathfrak{p}^{\kappa+\varepsilon}}{\mathcal{N}\mathfrak{p}^{\gamma\left(\frac{1}{2}-\beta(N+\delta')\right)}} + \frac{\mathcal{N}\mathfrak{p}^{\max\{\kappa-\gamma+1,0\}+\varepsilon}}{\mathcal{N}\mathfrak{p}^{\frac{1}{2}-\beta(N+\delta')}}\right),\end{aligned}$$

where each of the implied constants in the second O-terms depend on γ, ε, N, δ and δ'.

REMARK 6.14. To illustrate the condition $\rho_{\min}(P^{-1}Y) = \mathcal{N}\mathfrak{p}^{-\beta}$ with $\beta > 0$, assume that P and Y are given by symmetric matrices which share a basis of eigenvectors of $\mathbb{R}^N$, for convenience. Then, $\rho_{\min}(P^{-1}Y) = \mathcal{N}\mathfrak{p}^{-\beta}$, with $\beta > 0$, ensures that the fundamental domain $\mathcal{F}_Y$ is properly contained in $\mathcal{F}_P$ (see Figure 6.1 and Example 6.20).

We now proceed with the proof of Theorem 6.13 and postpone a more detailed discussion to Section 6.5.4. As mentioned above, the main ingredient of this proof is a higher dimensional Poisson summation formula. To utilize this to our benefit, we need some basic results concerning Gauß sums in number fields which we provide subsequently.

6.5.2. Preliminaries on Gauß sums. As in the classical theory of Dirichlet characters, any character χ of $(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*$ may be extended to a *Dirichlet character modulo* $\mathfrak{p}$ on $\mathcal{O}_{\mathbb{K}}$ via $\chi(a) := \chi(a \bmod \mathfrak{p})$, if $a \notin \mathfrak{p}$ and $\chi(a) := 0$, for $a \in \mathfrak{p}$. Now recall the identification of $\mathcal{O}_{\mathbb{K}}$ with $\mathbb{Z}^N$ introduced above and let P be an automorphism of $\mathbb{R}^N$ which maps $\mathbb{Z}^N$ onto the sublattice $\mathfrak{p}$. For a fixed vector $n \in P^{-*}\mathbb{Z}^N$, and any $x \in \mathbb{Z}^N$ we define the *Gauß sum* $\tau_{\mathfrak{p},n}(\chi, x)$ of a character χ of $(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*$ by

$$\tau_{\mathfrak{p},n}(\chi, x) := \sum_{a \bmod \mathfrak{p}} \chi(a) e(\langle n, xa\rangle),$$

where a runs through a set of representatives of $\mathbb{Z}^N/\mathfrak{p}$ and xa is understood to be the vector in $\mathbb{Z}^N$ corresponding to the product of x and a in $\mathcal{O}_{\mathbb{K}}$. The following generalization of a result concerning classical Gauß sums (cf. [13, p. 67ff]) is crucial for our method.

LEMMA 6.15. *Let $n \in P^{-*}\mathbb{Z}^N \setminus \mathbb{Z}^N$ and $x \in \mathbb{Z}^N \setminus \mathfrak{p}$. For any Dirichlet character χ modulo $\mathfrak{p}$, we have*

$$|\tau_{\mathfrak{p},n}(\chi, x)| = \begin{cases} \sqrt{\mathcal{N}\mathfrak{p}}, & \text{if } \chi \neq \chi_0, \\ 1, & \text{if } \chi = \chi_0. \end{cases}$$

Here χ_0 denotes the principal character modulo $\mathfrak{p}$, *i.e. $\chi_0(a) = 1$ for all $a \in \mathcal{O}_{\mathbb{K}} \setminus \mathfrak{p}$.*

PROOF. As in the classical case (see [13, p. 67ff]) we initially write

$$\begin{aligned} \sum_{x \bmod \mathfrak{p}} |\tau_{\mathfrak{p},n}(\chi, x)|^2 &= \sum_{x \bmod \mathfrak{p}} \sum_{a \bmod \mathfrak{p}} \sum_{b \bmod \mathfrak{p}} \chi(a)\overline{\chi(b)} e(\langle n, x(a-b)\rangle) \\ &= \sum_{a \bmod \mathfrak{p}} \sum_{b \bmod \mathfrak{p}} \chi(a)\overline{\chi(b)} \sum_{x \bmod \mathfrak{p}} e(\langle n, x(a-b)\rangle). \end{aligned}$$

In case $a - b \in \mathfrak{p}$, the sum on x clearly equals $\mathcal{N}\mathfrak{p}$ since $n \in P^{-*}\mathbb{Z}^N$. If $a - b \notin \mathfrak{p}$, then the sum on x vanishes. To see this, let $c \in \mathbb{Z}^N \setminus \mathfrak{p}$, and choose $y \in \mathbb{Z}^N$ with $\langle n, y\rangle \notin \mathbb{Z}$, whence $e(\langle n, y\rangle) \neq 1$. This is possible because $n \notin \mathbb{Z}^N$. Since

$$e(\langle n, y\rangle) \sum_{x \bmod \mathfrak{p}} e(\langle n, xc\rangle) = \sum_{x \bmod \mathfrak{p}} e(\langle n, y + xc\rangle) = \sum_{x \bmod \mathfrak{p}} e(\langle n, xc\rangle),$$

we indeed obtain

$$\sum_{x \bmod \mathfrak{p}} e(\langle n, xc\rangle) = 0, \qquad \text{for all } c \in \mathbb{Z}^N \setminus \mathfrak{p}. \tag{6.43}$$

Thus we get

$$\sum_{x \bmod \mathfrak{p}} |\tau_{\mathfrak{p},n}(\chi, x)|^2 = \mathcal{N}\mathfrak{p} \cdot (\mathcal{N}\mathfrak{p} - 1). \tag{6.44}$$

Further, we have

$$\tau_{\mathfrak{p},n}(\chi,x)=\sum_{a \bmod \mathfrak{p}}\chi(a)e(\langle n,xa\rangle)=\overline{\chi}(x)\sum_{b \bmod \mathfrak{p}}\chi(b)e(\langle n,b\rangle)=\overline{\chi(x)}\cdot\tau_{\mathfrak{p},n}(\chi,1) \tag{6.45}$$

for any $x\in\mathbb{Z}^N\setminus\mathfrak{p}$, as the map $a\mapsto xa$ is a bijection on $(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*$ in this case. If $\chi\neq\chi_0$, we have $\tau_{\mathfrak{p},n}(\chi,x)=0$ for $x\in\mathfrak{p}$ by character orthogonality (cf. [45, p. 43f]), and the assertion follows by (6.44) and (6.45). If $\chi=\chi_0$, the assertion already follows by (6.43). □

6.5.3. Proof of Theorem 6.13 by Poisson summation. For convenience we let $\vartheta\in\mathbb{R}^*$ and extend our definitions to $\mathrm{ord}_{\boldsymbol{a}}(\mathfrak{p})^\vartheta$, $\mathrm{Ord}^\vartheta_\gamma(\mathfrak{p})$ and $\mathrm{Ord}^\vartheta_\gamma(\mathfrak{p};\boldsymbol{\omega},Y)$ in the natural way. This allows us to only treat the quantities $\mathrm{Ord}^\vartheta_\gamma(\mathfrak{p};\boldsymbol{\omega},Y)$ which for $\vartheta\in\mathbb{R}_+$ clearly yields the desired results for $\mathrm{Ord}^\kappa_\gamma(\mathfrak{p};\boldsymbol{\omega},Y)$ with $\kappa=\vartheta$, and for $\vartheta\in\mathbb{R}_-$ it yields the corresponding results for $\mathrm{Ind}^\kappa_\gamma(\mathfrak{p};\boldsymbol{\omega},Y)$ with $\kappa=-\vartheta$ by the identity

$$\mathrm{Ind}^\kappa_\gamma(\mathfrak{p};\boldsymbol{\omega},Y)=(\mathcal{N}\mathfrak{p}-1)^\kappa\cdot\mathrm{Ord}^\vartheta_\gamma(\mathfrak{p};\boldsymbol{\omega},Y). \tag{6.46}$$

By the conditions on the weight functions ω_i we may write

$$\begin{aligned}\mathrm{Ord}^\vartheta_\gamma(\mathfrak{p};\boldsymbol{\omega},Y)&=\frac{1}{|\det(Y)|^\gamma}\sum_{\substack{\boldsymbol{a}\in\mathbb{Z}^{N\times\gamma}\\ \forall i:\ a_i\notin\mathfrak{p}}}\mathrm{ord}_{\boldsymbol{a}}(\mathfrak{p})^\vartheta\,\boldsymbol{\omega}(Y^{-1}\boldsymbol{a})\\&=\frac{1}{|\det(Y)|^\gamma}\sideset{}{^*}\sum_{\boldsymbol{a} \bmod \mathfrak{p}}\mathrm{ord}_{\boldsymbol{a}}(\mathfrak{p})^\vartheta\sum_{\boldsymbol{m}\in\mathbb{Z}^{N\times\gamma}}\boldsymbol{\omega}\big(Y^{-1}P(P^{-1}\boldsymbol{a}+\boldsymbol{m})\big).\end{aligned} \tag{6.47}$$

Here, the outer sum runs over a set of representatives $\boldsymbol{a}$ of $(\mathbb{Z}^N/\mathfrak{p})^\gamma$ such that each component a_i of $\boldsymbol{a}$ satisfies $a_i\notin\mathfrak{p}$. As for the inner sum, we quote the following higher dimensional *Poisson summation formula* [98, p. 252] which clearly applies to our case.

Proposition 6.16 (Poisson summation formula). *Let $f:\mathbb{R}^N\to\mathbb{R}$ be a continuous function with continuous Fourier transform $\hat{f}$ and assume*

$$f(t)\ll(1+\|t\|_2)^{-N-\delta}\qquad\text{and}\qquad\hat{f}(u)\ll(1+\|u\|_2)^{-N-\delta},$$

for any $t,u\in\mathbb{R}^N$ and some $\delta>0$. Then we have

$$\sum_{m\in\mathbb{Z}^N}f(x+m)=\sum_{m\in\mathbb{Z}^N}\hat{f}(m)e(\langle m,x\rangle),$$

for any $x\in\mathbb{R}^N$, and the sums on both sides are absolutely convergent.

The Poisson summation formula transforms the right side of (6.47) into

$$\begin{aligned}&\frac{1}{|\det(P)|^\gamma}\sideset{}{^*}\sum_{\boldsymbol{a} \bmod \mathfrak{p}}\mathrm{ord}_{\boldsymbol{a}}(\mathfrak{p})^\vartheta\sum_{\boldsymbol{n}\in\mathbb{Z}^{N\times\gamma}}\hat{\boldsymbol{\omega}}\left((P^{-1}Y)^*\boldsymbol{n}\right)\boldsymbol{e}\left(\langle\boldsymbol{n},P^{-1}\boldsymbol{a}\rangle\right)\\&=\frac{1}{\mathcal{N}\mathfrak{p}^\gamma}\sum_{\boldsymbol{n}\in\mathbb{Z}^{N\times\gamma}}\hat{\boldsymbol{\omega}}\left(Y^*P^{-*}\boldsymbol{n}\right)\sideset{}{^*}\sum_{\boldsymbol{a} \bmod \mathfrak{p}}\mathrm{ord}_{\boldsymbol{a}}(\mathfrak{p})^\vartheta\,\boldsymbol{e}\left(\langle\boldsymbol{n},P^{-1}\boldsymbol{a}\rangle\right).\end{aligned} \tag{6.48}$$

Here, for convenience, we set

$$\boldsymbol{e}\left(\langle\boldsymbol{x},\boldsymbol{y}\rangle\right):=e(\langle x_1,y_1\rangle)\cdots e(\langle x_\gamma,y_\gamma\rangle),$$

for γ-tupels $\boldsymbol{x}=(x_1,\dots,x_\gamma),\boldsymbol{y}=(y_1,\dots,y_\gamma)\in\mathbb{R}^{N\times\gamma}$. Since each ω_i is normalized, we have $\hat{\omega}_i(0)=1$ and the term corresponding to $\boldsymbol{n}=\boldsymbol{0}:=(0,\dots,0)$ in (6.48) equals

$$\frac{(\mathcal{N}\mathfrak{p}-1)^\gamma}{\mathcal{N}\mathfrak{p}^\gamma}\cdot\mathrm{Ord}^\vartheta_\gamma(\mathfrak{p})=\mathrm{Ord}^\vartheta_\gamma(\mathfrak{p})\left(1+O_\gamma\left(\frac{1}{\mathcal{N}\mathfrak{p}}\right)\right), \tag{6.49}$$

which already yields the main term in Theorem 6.13. Next we bound the remaining sum

$$E := \frac{1}{\mathcal{N}\mathfrak{p}^{\gamma}} \sum_{\boldsymbol{n}\in\mathbb{Z}^{N\times\gamma}\setminus\{\mathbf{0}\}} \hat{\boldsymbol{\omega}}\left(Y^{*}P^{-*}\boldsymbol{n}\right) \sideset{}{^{*}}\sum_{\boldsymbol{a} \bmod \mathfrak{p}} \operatorname{ord}_{\boldsymbol{a}}(\mathfrak{p})^{\vartheta}\, \boldsymbol{e}\left(\langle \boldsymbol{n}, P^{-1}\boldsymbol{a}\rangle\right)$$

from above. To this end, we define

$$E_k := \frac{1}{\mathcal{N}\mathfrak{p}^{\gamma}} \sum_{\substack{\boldsymbol{n}\in\mathbb{Z}^{N\times\gamma}\setminus\{\mathbf{0}\}\\ n_1,\dots,n_k\in P^{*}\mathbb{Z}^{N}\\ n_{k+1},\dots,n_\gamma\notin P^{*}\mathbb{Z}^{N}}} \hat{\boldsymbol{\omega}}\left(Y^{*}P^{-*}\boldsymbol{n}\right) \sideset{}{^{*}}\sum_{\boldsymbol{a} \bmod \mathfrak{p}} \operatorname{ord}_{\boldsymbol{a}}(\mathfrak{p})^{\vartheta}\, \boldsymbol{e}\left(\langle \boldsymbol{n}, P^{-1}\boldsymbol{a}\rangle\right) \tag{6.50}$$

for $k = 0, 1, \dots, \gamma$ which clearly yields

$$E = \sum_{k=0}^{\gamma} \binom{\gamma}{k} E_k \tag{6.51}$$

for symmetry reasons. Here, as usual, the $\binom{\gamma}{k}$ denote the familiar binomial coefficients. To estimate the terms E_k, the following lemma proves useful.

LEMMA 6.17. *Let $\vartheta \in \mathbb{R}^{*}$, $k \in \{0, 1, \dots, \gamma\}$ and $\boldsymbol{n} = (n_1, \dots, n_\gamma) \in \mathbb{Z}^{N\times\gamma}$ and assume $n_1, \dots, n_k \in P^{*}\mathbb{Z}^{N}$ and $n_{k+1}, \dots, n_\gamma \notin P^{*}\mathbb{Z}^{N}$.*

(i) *If $k = \gamma$, we have*

$$\sideset{}{^{*}}\sum_{\boldsymbol{a} \bmod \mathfrak{p}} \operatorname{ord}_{\boldsymbol{a}}(\mathfrak{p})^{\vartheta}\, \boldsymbol{e}\left(\langle \boldsymbol{n}, P^{-1}\boldsymbol{a}\rangle\right) \begin{cases} \leq \mathcal{N}\mathfrak{p}^{\gamma+\vartheta}, & \text{if } \vartheta > 0,\\ \ll_{\varepsilon} \max\{\mathcal{N}\mathfrak{p}^{\gamma-|\vartheta|+\varepsilon}, \mathcal{N}\mathfrak{p}^{\varepsilon}\}, & \text{if } \vartheta < 0. \end{cases}$$

(ii) *If $k < \gamma$, we have*

$$\sideset{}{^{*}}\sum_{\boldsymbol{a} \bmod \mathfrak{p}} \operatorname{ord}_{\boldsymbol{a}}(\mathfrak{p})^{\vartheta}\, \boldsymbol{e}\left(\langle \boldsymbol{n}, P^{-1}\boldsymbol{a}\rangle\right) \ll_{\varepsilon} \mathcal{N}\mathfrak{p}^{\frac{\gamma-k}{2}+\varepsilon} \max\{1, \mathcal{N}\mathfrak{p}^{\vartheta+k}\}.$$

PROOF. First assume $k = \gamma$. In this case we have $\langle n_i, P^{-1}a_i\rangle \in \mathbb{Z}$ for all i, whence

$$\sideset{}{^{*}}\sum_{\boldsymbol{a} \bmod \mathfrak{p}} \operatorname{ord}_{\boldsymbol{a}}(\mathfrak{p})^{\vartheta}\, \boldsymbol{e}\left(\langle \boldsymbol{n}, P^{-1}\boldsymbol{a}\rangle\right) \leq \mathcal{N}\mathfrak{p}^{\vartheta} \sum_{\boldsymbol{a} \bmod \mathfrak{p}} 1 \leq \mathcal{N}\mathfrak{p}^{\gamma+\vartheta}$$

if $\vartheta > 0$. If $\vartheta < 0$, then (6.23) yields

$$\begin{aligned} \sideset{}{^{*}}\sum_{\boldsymbol{a} \bmod \mathfrak{p}} \operatorname{ord}_{\boldsymbol{a}}(\mathfrak{p})^{\vartheta}\, \boldsymbol{e}\left(\langle \boldsymbol{n}, P^{-1}\boldsymbol{a}\rangle\right) &= (\mathcal{N}\mathfrak{p}-1)^{\vartheta} \sideset{}{^{*}}\sum_{\boldsymbol{a} \bmod \mathfrak{p}} \frac{(\mathcal{N}\mathfrak{p}-1)^{|\vartheta|}}{\operatorname{ord}_{\boldsymbol{a}}(\mathfrak{p})^{|\vartheta|}}\\ &= (\mathcal{N}\mathfrak{p}-1)^{\gamma-|\vartheta|} \operatorname{Ind}_{\gamma}^{|\vartheta|}(\mathfrak{p})\\ &\ll_{\varepsilon} \max\{\mathcal{N}\mathfrak{p}^{\gamma-|\vartheta|+\varepsilon}, \mathcal{N}\mathfrak{p}^{\varepsilon}\}. \end{aligned}$$

Now assume $k < \gamma$ and write

$$\sideset{}{^{*}}\sum_{\boldsymbol{a} \bmod \mathfrak{p}} \operatorname{ord}_{\boldsymbol{a}}(\mathfrak{p})^{\vartheta}\, \boldsymbol{e}\left(\langle \boldsymbol{n}, \boldsymbol{a}\rangle\right) = \sum_{d \mid \mathcal{N}\mathfrak{p}-1} d^{\vartheta} \sideset{}{^{*}}\sum_{\substack{\boldsymbol{a} \bmod \mathfrak{p}\\ \operatorname{ord}_{\boldsymbol{a}}(\mathfrak{p})=d}} \boldsymbol{e}\left(\langle \boldsymbol{n}, P^{-1}\boldsymbol{a}\rangle\right). \tag{6.52}$$

By Möbius inversion, the inner sum becomes

$$\sum_{f \mid d} \mu\left(\frac{d}{f}\right) \sideset{}{^{*}}\sum_{\substack{\boldsymbol{a} \bmod \mathfrak{p}\\ \operatorname{ord}_{\boldsymbol{a}}(\mathfrak{p}) \mid f}} \boldsymbol{e}\left(\langle \boldsymbol{n}, P^{-1}\boldsymbol{a}\rangle\right). \tag{6.53}$$

Now observe that $(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*$ is cyclic and set $H_f := \{a \in (\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^* : a^f \equiv 1 \bmod \mathfrak{p}\}$ for any divisor f of $\mathcal{N}\mathfrak{p}-1$. Then (6.53) becomes

$$\sum_{f|d} \mu\left(\frac{d}{f}\right) \prod_{i=1}^{\gamma} \sum_{a\in H_f} e\left(\langle P^{-*} n_i, a\rangle\right) = \sum_{f|d} \mu\left(\frac{d}{f}\right) f^k \prod_{i=k+1}^{\gamma} \sum_{a\in H_f} e\left(\langle P^{-*} n_i, a\rangle\right), \tag{6.54}$$

since H_f is a cyclic group with exactly f elements. Let now $j \in \{k+1,\dots,\gamma\}$. The characters χ of $(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*$ evidently form a cyclic group isomorphic to $(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*$ with identity χ_0 (or rather its restriction to $(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*$). By character orthogonality (cf. [45, p. 43f]) and Lemma 6.15, we thus obtain

$$\begin{aligned}\left|\sum_{a\in H_f} e\left(\langle P^{-*} n_j, a\rangle\right)\right| &= \left|\sum_{a\in(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*} e\left(\langle P^{-*} n_j, a\rangle\right) \frac{1}{\frac{\mathcal{N}\mathfrak{p}-1}{f}} \sum_{\chi:\chi^{\frac{\mathcal{N}\mathfrak{p}-1}{f}}=\chi_0} \chi(a)\right| \\ &= \frac{f}{\mathcal{N}\mathfrak{p}-1}\left|\sum_{\chi:\chi^{\frac{\mathcal{N}\mathfrak{p}-1}{f}}=\chi_0} \sum_{a\in(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*} \chi(a) e\left(\langle P^{-*} n_j, a\rangle\right)\right| \\ &\le \sqrt{\mathcal{N}\mathfrak{p}}.\end{aligned} \tag{6.55}$$

Combining (6.52)–(6.55), we eventually get

$$\begin{aligned}\left|\sideset{}{^*}\sum_{\boldsymbol{a} \bmod \mathfrak{p}} \operatorname{ord}_{\boldsymbol{a}}(\mathfrak{p})^{\vartheta}\, \boldsymbol{e}\left(\langle \boldsymbol{n}, P^{-1}\,\boldsymbol{a}\rangle\right)\right| &\le \mathcal{N}\mathfrak{p}^{(\gamma-k)/2} \sum_{d|\mathcal{N}\mathfrak{p}-1} d^{\vartheta} \sum_{f|d} \mu^2\left(\frac{d}{f}\right) f^k \\ &\ll_{\varepsilon} \mathcal{N}\mathfrak{p}^{\frac{\gamma-k}{2}+\varepsilon}\, \sigma_{\vartheta+k}(\mathcal{N}\mathfrak{p}-1) \\ &\ll_{\varepsilon} \mathcal{N}\mathfrak{p}^{\frac{\gamma-k}{2}+\varepsilon} \max\{1, \mathcal{N}\mathfrak{p}^{\vartheta+k}\},\end{aligned}$$

by standard divisor sum estimates (cf. Chapter I.5 of [100]). This proves the assertion. □

Now we apply Lemma 6.17 to bound the terms E_k defined in (6.50). If $k=\gamma$, we find

$$|E_\gamma| \le \mathcal{N}\mathfrak{p}^{\vartheta} \sum_{\substack{\boldsymbol{n}\in\mathbb{Z}^{N\times\gamma}\setminus\{\boldsymbol{0}\} \\ n_1,\dots,n_\gamma\in P^*\,\mathbb{Z}^N}} \left|\hat{\boldsymbol{\omega}}(Y^* P^{-*}\,\boldsymbol{n})\right| \tag{6.56}$$

if $\vartheta > 0$, and if $\vartheta < 0$, we have

$$|E_\gamma| \ll_{\varepsilon} \frac{1}{\mathcal{N}\mathfrak{p}^{\min\{|\vartheta|,\gamma\}-\varepsilon}} \sum_{\substack{\boldsymbol{n}\in\mathbb{Z}^{N\times\gamma}\setminus\{\boldsymbol{0}\} \\ n_1,\dots,n_\gamma\in P^*\,\mathbb{Z}^N}} \left|\hat{\boldsymbol{\omega}}(Y^* P^{-*}\,\boldsymbol{n})\right|. \tag{6.57}$$

In case $k<\gamma$ we similarly obtain

$$|E_k| \ll_{\varepsilon} \frac{\mathcal{N}\mathfrak{p}^{\max\{0,\vartheta+k\}}}{\mathcal{N}\mathfrak{p}^{\frac{\gamma+k}{2}-\varepsilon}} \sum_{\substack{\boldsymbol{n}\in\mathbb{Z}^{N\times\gamma}\setminus\{\boldsymbol{0}\} \\ n_1,\dots,n_k\in P^*\,\mathbb{Z}^N \\ n_{k+1},\dots,n_\gamma\notin P^*\,\mathbb{Z}^N}} \left|\hat{\boldsymbol{\omega}}(Y^* P^{-*}\,\boldsymbol{n})\right|.$$

Let us treat the case $k = \gamma$ first and estimate the sums occurring in (6.56) and (6.57). By (6.37), (6.38) and the prerequisites of Theorem 6.13, we have

$$\begin{aligned}\sum_{\substack{\boldsymbol{n}\in\mathbb{Z}^{N\times\gamma}\setminus\{\mathbf{0}\}\\ n_1,\dots,n_\gamma\in P^*\,\mathbb{Z}^N}} \big|\hat{\boldsymbol{\omega}}(Y^*P^{-*}\,\boldsymbol{n})\big| &= \sum_{\boldsymbol{n}\in\mathbb{Z}^{N\times\gamma}\setminus\{\mathbf{0}\}} |\hat{\boldsymbol{\omega}}(Y^*\,\boldsymbol{n})| \ll \sum_{\boldsymbol{n}\in\mathbb{Z}^{N\times\gamma}\setminus\{\mathbf{0}\}} \prod_{i=1}^{\gamma} \frac{1}{(1+\|Y^*n_i\|_2)^{N+\delta}}\\ &\le \sum_{n_1\in\mathbb{Z}^N\setminus\{0\}} \frac{\gamma}{(1+\|Y^*n_1\|_2)^{N+\delta}} \prod_{i=2}^{\gamma}\sum_{n_i\in\mathbb{Z}^N} \frac{1}{(1+\|Y^*n_i\|_2)^{N+\delta}}\\ &\ll_\gamma \sum_{n_1\in\mathbb{Z}^N\setminus\{0\}} \frac{1}{(1+\rho_{\min}(Y)\|n_1\|_2)^{N+\delta}}\\ &\le \frac{1}{\rho_{\min}(Y)^{N+\delta}} \sum_{n_1\in\mathbb{Z}^N\setminus\{0\}} \frac{1}{\|n_1\|_2^{N+\delta}} \ll_{N,\delta} \frac{1}{\rho_{\min}(Y)^{N+\delta}}.\end{aligned}$$

Hence, if $\vartheta > 0$ we obtain

$$E_\gamma \ll_{\gamma,N,\delta} \mathcal{N}\mathfrak{p}^{\vartheta-\alpha(N+\delta)}, \tag{6.58}$$

and if $\vartheta < 0$ we have

$$E_\gamma \ll_{\gamma,N,\delta,\varepsilon} \frac{\mathcal{N}\mathfrak{p}^{\varepsilon}}{\mathcal{N}\mathfrak{p}^{\min\{|\vartheta|,\gamma\}+\alpha(N+\delta)}}. \tag{6.59}$$

Now assume $k < \gamma$ and let $\delta' : 0 < \delta' \le \delta$ be some parameter. As before we deduce

$$\sum_{\substack{\boldsymbol{n}\in\mathbb{Z}^{N\times\gamma}\setminus\{\mathbf{0}\}\\ n_1,\dots,n_k\in P^*\,\mathbb{Z}^N\\ n_{k+1},\dots,n_\gamma\notin P^*\,\mathbb{Z}^N}} \big|\hat{\boldsymbol{\omega}}(Y^*P^{-*}\,\boldsymbol{n})\big| = R\cdot T,$$

where

$$\begin{aligned}R &= \sum_{n_1,\dots,n_k\in P^*\,\mathbb{Z}^N} \prod_{i=1}^{k} |\omega_i(Y * P^{-*}n_i)| \le \sum_{n_1,\dots,n_k\in P^*\,\mathbb{Z}^N} \prod_{i=1}^{k} \frac{1}{(1+\|Y^*P^{-*}n_i\|_2)^{N+\delta'}}\\ &\le \sum_{n_1,\dots,n_k\in\mathbb{Z}^N} \prod_{i=1}^{k} \frac{1}{(1+\|n_i\|_2)^{N+\delta'}} = O_{N,\delta'}(1),\end{aligned}$$

since $\rho_{\min}(Y) \ge 1$ by assumption, and

$$\begin{aligned}T &= \sum_{n_{k+1},\dots,n_\gamma\notin P^*\,\mathbb{Z}^N} \prod_{i=k+1}^{\gamma} \frac{1}{(1+\|Y^*P^{-*}n_i\|_2)^{N+\delta'}}\\ &\le \left(\sum_{n\in\mathbb{Z}^N} \frac{1}{(1+\rho_{\min}(P^{-1}Y)\|n\|_2)^{N+\delta'}}\right)^{\gamma-k}\\ &\le \frac{1}{\rho_{\min}(P^{-1}Y)^{(\gamma-k)(N+\delta')}} \left(\sum_{n\in\mathbb{Z}^N} \frac{1}{(1+\|n\|_2)^{N+\delta'}}\right)^{\gamma-k}\\ &\ll_{\gamma,k,N,\delta'} \frac{1}{\rho_{\min}(P^{-1}Y)^{(\gamma-k)(N+\delta')}},\end{aligned}$$

since $\rho_{\min}(P^{-1}Y) \le 1$. Summing up, we find

$$E_k \ll_{\gamma,N,\delta',\varepsilon} \frac{\mathcal{N}\mathfrak{p}^{\max\{0,\vartheta+k\}}\,\mathcal{N}\mathfrak{p}^{\beta(\gamma-k)(N+\delta')}}{\mathcal{N}\mathfrak{p}^{\frac{\gamma+k}{2}-\varepsilon}}, \tag{6.60}$$

where the k-dependency of the implied constant is included in the γ-dependency, for convenience. It is easy to check that the maximum of the error terms E_k, $k \in \{0,\dots,\gamma-1\}$, is attained either if k is 0 or $\gamma-1$, and hence equals either

$$\frac{\mathcal{N}\mathfrak{p}^{\max\{0,\vartheta\}+\varepsilon}}{\mathcal{N}\mathfrak{p}^{\gamma(\frac{1}{2}-\beta(N+\delta'))}} \qquad \text{or} \qquad \frac{\mathcal{N}\mathfrak{p}^{\max\{1-\gamma,\vartheta\}+\varepsilon}}{\mathcal{N}\mathfrak{p}^{\frac{1}{2}-\beta(N+\delta')}}.$$

Combining this with (6.46)–(6.51) and (6.58)–(6.60) finally proves Theorem 6.13. □

6.5.4. Applications. Let us take a closer look at Theorem 6.13. To rate its accuracy and determine whether or not it actually yields asymptotic formulae, we need estimates for $\mathrm{Ord}^\kappa_\gamma(\mathfrak{p})$ and $\mathrm{Ind}^\kappa_\gamma(\mathfrak{p})$ in the first place. For the first of these we have the rough estimates

$$\mathcal{N}\mathfrak{p}^{\kappa-\varepsilon} \ll_\varepsilon \mathrm{Ord}^\kappa_\gamma(\mathfrak{p}) \le \mathcal{N}\mathfrak{p}^\kappa,$$

where the upper bound is obvious and the lower bound can be seen from Lemma 6.6. As for $\mathrm{Ind}^\kappa_\gamma(\mathfrak{p})$, we have

$$\mathcal{N}\mathfrak{p}^{\max\{\kappa-\gamma,0\}} \ll \mathrm{Ind}^\kappa_\gamma(\mathfrak{p}) \ll_\varepsilon \mathcal{N}\mathfrak{p}^{\max\{\kappa-\gamma,0\}+\varepsilon}.$$

Here, the lower bound is trivial and the upper bound follows from (6.23). From these estimates we infer that the terms in Theorem 6.13 which involve α are negligible if we ensure $\alpha > 0$ and choose the weight functions ω_i such that δ is sufficiently large. Under these constraints, the accuracy of Theorem 6.13 only depends on β, i.e. on the size of $\rho_{\min}(P^{-1}Y)$, which determines whether or not the error terms in Theorem 6.13 are dominated by the respective main terms. To give a clearer account, we state the following weaker version of Theorem 6.13 which is more suitable for applications.

THEOREM 6.18. *Let $\varepsilon,\kappa \in \mathbb{R}_+$, $\gamma \in \mathbb{N}$ and $\mathfrak{p} \in \mathcal{P}(\mathbb{K})$. Let Y and P be linear automorphisms of $\mathbb{R}^N$ such that $P\,\mathbb{Z}^N = \mathfrak{p}$, $\rho_{\min}(Y) = \mathcal{N}\mathfrak{p}^\alpha$ with $\alpha > 0$ and $\rho_{\min}(P^{-1}Y) = \mathcal{N}\mathfrak{p}^{-\beta}$ with $\beta \ge 0$. Let $\omega_1,\dots,\omega_\gamma : \mathbb{R}^N \to \mathbb{R}$ be continuous and normalized with*

$$\omega_i(t) \ll (1+\|t\|_2)^{-N-\delta} \qquad \text{and} \qquad \hat{\omega}_i(u) \ll (1+\|u\|_2)^{-N-\delta}$$

for some $\delta > 0$.

(i) *If $\alpha(N+\delta) \ge 1$ and $\beta N < 1/2$, we have*

$$\mathrm{Ord}^\kappa_\gamma(\mathfrak{p};\boldsymbol{\omega},Y) = \mathrm{Ord}^\kappa_\gamma(\mathfrak{p}) + O\left(\frac{\mathcal{N}\mathfrak{p}^{\kappa+\varepsilon}}{\mathcal{N}\mathfrak{p}^{\frac{1}{2}-\beta N}}\right).$$

(ii) *Assume $\alpha(N+\delta) \ge 1$.*

a) *If $\kappa \ge (\gamma-1)(\frac{1}{2}-\beta N)$, we have*

$$\mathrm{Ind}^\kappa_\gamma(\mathfrak{p};\boldsymbol{\omega},Y) = \mathrm{Ind}^\kappa_\gamma(\mathfrak{p}) + O\left(\frac{\mathcal{N}\mathfrak{p}^{\kappa+\varepsilon}}{\mathcal{N}\mathfrak{p}^{\gamma(\frac{1}{2}-\beta N)}}\right).$$

b) *If $\kappa < (\gamma-1)(\frac{1}{2}-\beta N)$, we have*

$$\mathrm{Ind}^\kappa_\gamma(\mathfrak{p};\boldsymbol{\omega},Y) = \mathrm{Ind}^\kappa_\gamma(\mathfrak{p}) + O\left(\frac{\mathcal{N}\mathfrak{p}^{\varepsilon}}{\mathcal{N}\mathfrak{p}^{\frac{1}{2}-\beta N}}\right).$$

In all cases the implied constants may depend on γ, ε, β, N and δ.

From Theorems 6.13 and 6.18 we easily deduce the following:

COROLLARY 6.19. *With the notation being as in Theorem 6.18, assume that* $\alpha > 0$ *and* $\beta N < 1/2$. *Then, as* $\mathcal{N}\mathfrak{p} \to \infty$, *we have*

$$\mathrm{Ord}_\gamma^\kappa(\mathfrak{p}; \boldsymbol{\omega}, Y) \sim \mathrm{Ord}_\gamma^\kappa(\mathfrak{p})$$

and if $\kappa < \gamma(\frac{1}{2} - \beta N)$ *we also have*

$$\mathrm{Ind}_\gamma^\kappa(\mathfrak{p}; \boldsymbol{\omega}, Y) \sim \mathrm{Ind}_\gamma^\kappa(\mathfrak{p}).$$

We conclude this chapter with the following easy example to illustrate Corollary 6.19.

EXAMPLE 6.20. Let $\mathfrak{p} \in \mathcal{P}(\mathbb{K})$ with inertia degree f over the prime p. It is an easy exercise to show that there exists an integral basis $\mathcal{B} = (\alpha_1, \dots, \alpha_N)$ of $\mathbb{K}$ such that $\alpha_1 \bmod \mathfrak{p}, \dots, \alpha_f \bmod \mathfrak{p}$ form an $\mathbb{F}_p$-basis of $\mathcal{O}_\mathbb{K} / \mathfrak{p}$ and $\alpha_{f+1}, \dots, \alpha_N$ are contained in $\mathfrak{p}$. Identifying $\mathcal{O}_\mathbb{K}$ with $\mathbb{Z}^N$ via this basis, $\mathfrak{p}$ defines an N-dimensional cuboid in $\mathbb{R}^N$ with f edges of length p and $N - f$ edges of length 1. Accordingly, we define the $N \times N$-matrices

$$P = \left(\begin{array}{ccc|ccc} p & & & & & \\ & \ddots & & & 0 & \\ & & p & & & \\ \hline & & & 1 & & \\ & 0 & & & \ddots & \\ & & & & & 1 \end{array}\right) \quad \text{and} \quad Y = \left(\begin{array}{ccc|ccc} y & & & & & \\ & \ddots & & & 0 & \\ & & y & & & \\ \hline & & & 1 & & \\ & 0 & & & \ddots & \\ & & & & & 1 \end{array}\right),$$

where $y := p^\delta$ with $\delta \in (0, 1]$ is some parameter, and obtain $P\,\mathbb{Z}^N = \mathfrak{p}$ and $\rho_{\min}(P^{-1}Y) = y/p < 1$. Choosing appropriate weight functions ω_i, Corollary 6.19 yields

$$\mathrm{Ord}_\gamma^\kappa(\mathfrak{p}; \boldsymbol{\omega}, Y) \sim \mathrm{Ord}_\gamma^\kappa(\mathfrak{p}),$$

whenever $y > p^{1 - \frac{f}{2N}}$. Thus, at least in our smoothened setting, instead of averaging $\mathrm{ord}_{\langle a_1, \dots, a_\gamma \rangle}(\mathfrak{p})^\kappa$ over all a_i inside the cube of volume p^f defined by $\mathfrak{p}$, it suffices to restrict to a subcube of volume $p^{f(1 - \frac{f}{2N})}$ to gain the same asymptotic behaviour. Note that we made no assumptions on κ or γ. This, however, changes when we turn to the residual index. By Corollary 6.19, we have

$$\mathrm{Ind}_\gamma^\kappa(\mathfrak{p}; \boldsymbol{\omega}, Y) \sim \mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$$

if $\delta > \max\{1 - \frac{f}{2N}, 1 + \frac{\kappa - \gamma/2}{N}\}$. Thus, even though this result is much weaker than the one for the residual order, we at least save a bit of averaging range provided that γ is sufficiently large compared to κ.

REMARK 6.21. This example in particular reveals that our method for a reduction of the summation range has the biggest impact if $\mathfrak{p}$ is inert over $\mathbb{Q}$.

CHAPTER 7

Moments of the Residual Index over All Ideals

Up to now we were only concerned with the distribution of residual index and order over certain prime ideals of a given number field. In light of the work of Li, Pomerance and Kurlberg (cf. Section 2.3), it is inevitable to ask: What can one say about moments of residual index and order modulo all ideals of a given number field? In case of the rational numbers this question has been studied intensely for the residual order. In fact, Kurlberg and Pomerance [51] proved the existence of an explicitly computable positive constant B such that

$$\sum_{\substack{n\leq x\\(n,a)=1}} \operatorname{ord}_a(n) = \frac{x^2}{\log x}\exp\left(\frac{B\log\log x}{\log\log\log x}(1+o(1))\right)$$

holds under GRH, uniformly for any integer a in the range $1 < |a| \leq \log x$ and x large enough (in fact the upper bound holds unconditionally). This result clearly underlines our expectations concerning the typical size of $\operatorname{ord}_a(n)$. Further reading on this topic is provided in [25, 70].

In this chapter we address the problem of establishing lower bounds for moments of $\operatorname{ind}_\Gamma(\mathfrak{a})$ over all ideals $\mathfrak{a}$ of $\mathbb{K}$. To our knowledge this task has not been treated satisfactorily yet. We introduce the problem we are studying in Section 7.1, and in Section 7.2 we state the main results of this chapter which are proved in the subsequent section and will soon appear in [1]. We conclude this chapter with remarks concerning double averaging, as introduced Chapter 6, over all ideals of $\mathbb{K}$.

7.1. A problem of Rohrlich

As before, let $\mathbb{K}$ be a number field and Γ a finitely generated, not necessarily torsion-free, infinite subgroup of $\mathbb{K}^*$, say with rank $\gamma \in \mathbb{N}$. As $\mathfrak{a}$ runs through all ideals of $\mathbb{K}$, the quantity $\operatorname{ind}_\Gamma(\mathfrak{a})$ behaves even more erratically than over prime ideals, as a comparison of Figures 7.1 and 2.1 illustrates in case $\mathbb{K} = \mathbb{Q}$ and $\Gamma = \langle 5\rangle \subset \mathbb{Q}^*$. However, suitable generalizations of AC, such as the statements of Lenstra, Wagstaff, Moree and Kurlberg (cf. Chapter 2) and Theorem 6.1, still suggest that $\operatorname{ind}_\Gamma(\mathfrak{a})$ is typically small and in fact $\overline{\Gamma}$ should even generate $(\mathcal{O}_\mathbb{K}/\mathfrak{a})^*$ quite frequently. This is also in line with Figure 7.1. On the other hand, Rohrlich [88] has explicitly constructed a (very sparse) infinite family of ideals $\mathfrak{a}$ of $\mathbb{K}$ for which $\operatorname{ind}_{\mathcal{U}_\mathbb{K}}(\mathfrak{a})$ is as large as $(\mathcal{N}\mathfrak{a})^{1-\varepsilon}$, provided that $\mathcal{U}_\mathbb{K}$ is infinite. This construction was one of the key ingredients for strong bounds towards the Ramanujan conjecture for GL_n over number fields [72]. But at the same time the sparseness of this sequence prevented an extension of the Kim-Sarnak bound [48] for GL_2 over $\mathbb{Q}$ to general number fields. We refer to [9] and the recent survey article [10] of Blomer and Brumley for a detailed treatment of this problem.

In a recent paper of Rohrlich [89], the quantity $\operatorname{ind}_{\mathcal{U}_\mathbb{K}}(\mathfrak{a})$ appeared once again. This time its average order occupied an important position in connection with counting self-dual Artin representations over number fields (cf. [89]). In this regard, Zelinsky [107]

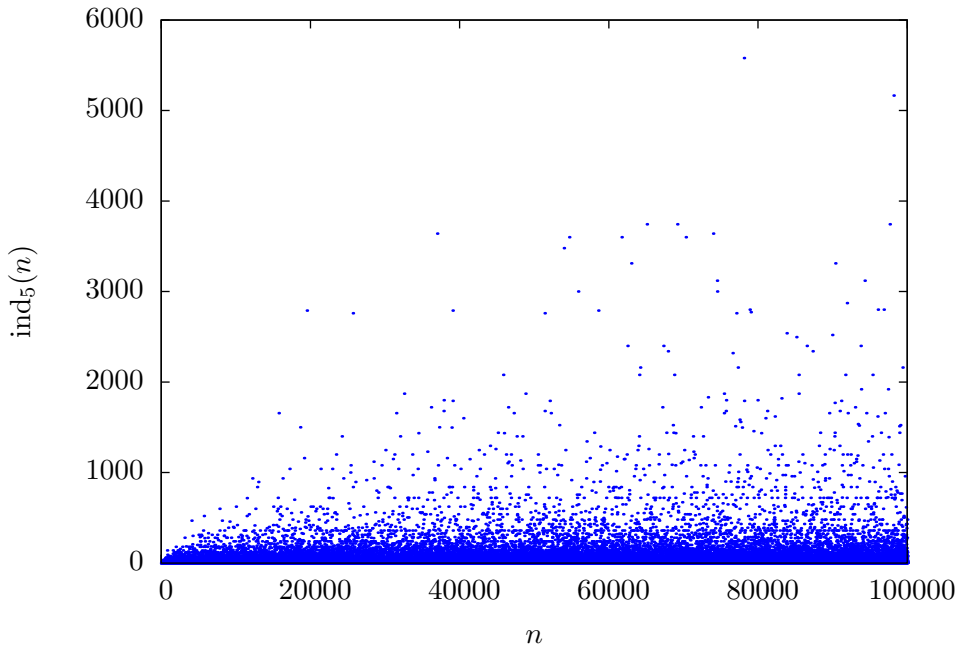


FIGURE 7.1. Chaotic Behaviour of $\mathrm{ind}_5(n)$ over $5 \nmid n \in \mathbb{N}$.

has recently proved

$$\sum_{\mathcal{N}\mathfrak{a}\leq x} \mathrm{ind}_{\mathcal{U}_{\mathbb{K}}}(\mathfrak{a}) \ll \frac{x^2}{\log^{3-\varepsilon} x},$$

for any $\varepsilon > 0$, if $\mathcal{U}_{\mathbb{K}}$ is infinite, thereby improving the trivial bounds

$$x \ll \sum_{\mathcal{N}\mathfrak{a}\leq x} \mathrm{ind}_{\mathcal{U}_{\mathbb{K}}}(\mathfrak{a}) \ll x^2. \tag{7.1}$$

Apart from this, surprisingly, little seems to be known.

In this chapter we shed further light on this problem, and, returning to our general setting, establish lower bounds for the κ-th moments of $\mathrm{ind}_\Gamma(\mathfrak{a})$ over all ideals of $\mathbb{K}$

$$\sum_{\substack{\mathcal{N}\mathfrak{a}\leq x \\ \overline{\Gamma}\subset(\mathcal{O}_{\mathbb{K}}/\mathfrak{a})^*}} \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa \tag{7.2}$$

which are in fact larger than expected. Indeed, Figure 7.2 for example suggests that (7.2) should for $\kappa = 1$ be at least $\gg x^{1.3}$. We even believe that the correct order of growth in this case is close to x^2, and we give evidence for this conjecture in general, by proving a conditional result which unexpectedly suggests that (7.2) is of size $x^{\kappa+1+o(1)}$.

7.2. Lower bounds for moments of $\mathrm{ind}_\Gamma(\mathfrak{a})$

We will now provide the announced statements concerning lower bounds for κ-th moments of $\mathrm{ind}_\Gamma(\mathfrak{a})$ over all ideals of $\mathbb{K}$. For a positive integer n we recall that $P^+(n)$ denotes the largest prime divisor of n, and 1 if $n = 1$, and for any $\delta, y \in \mathbb{R}_+$ we set

$$\mathcal{P}_{\delta,\mathbb{K}}(y) := \left\{\mathfrak{p} \in \mathcal{P}(y,\mathbb{K}) : P^+(\mathcal{N}\mathfrak{p}-1) < y^\delta\right\}.$$

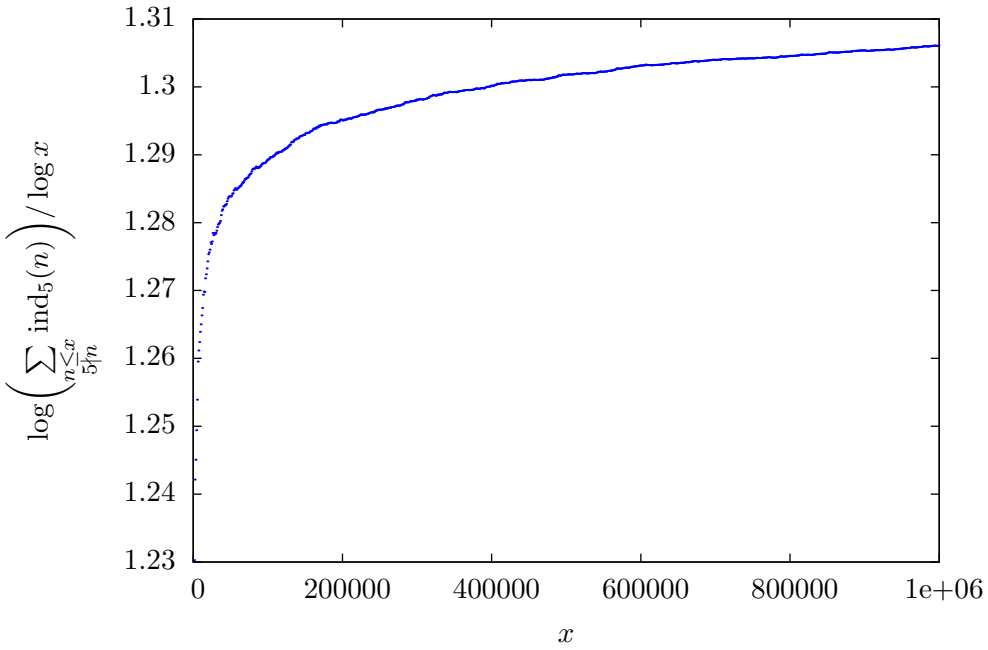


FIGURE 7.2. Unexpected growth of $\mathrm{ind}_5(n)$ on average over $5 \nmid n \in \mathbb{N}$.

We establish the following statement.

THEOREM 7.1. *Let $\mathbb{K}$ be a number field. Assume that $\delta \in \mathbb{R}_+$ is a positive constant such that there exist constants $K = K(\delta)$ and $y_0(\delta)$ for which the* smoothness condition

$$\sharp\, \mathcal{P}_{\delta,\mathbb{K}}(y) \gg \frac{y}{(\log y)^K} \tag{7.3}$$

holds, for all $y > y_0(\delta)$ with an implied constant possibly depending on $\mathbb{K}$. For any $\kappa \in \mathbb{R}_+$ and any subgroup Γ of $\mathbb{K}^*$ of arithmetic rank $\gamma \in \mathbb{N}$, we then have

$$\sum_{\substack{\mathcal{N}\mathfrak{a}\leq x\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{a})^*}} \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa \geq x^{1+\kappa-\delta+o(1)},$$

where the o-term depends on γ, κ and $\mathbb{K}$.

The accuracy of this lower bound depends on the quality of the smoothness condition (7.3). In case $\mathbb{K} = \mathbb{Q}$ one knows that (7.3) is satisfied for $\delta = 0.2961\ldots$ (cf. [5]). It is conjectured to hold, for all $\delta > 0$ with any $K > 1$ (cf. [70]). We believe that this is also true for a general number field and expect an asymptotic law like

$$\sum_{\substack{\mathcal{N}\mathfrak{a}\leq x\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{a})^*}} \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa = x^{1+\kappa+o(1)}.$$

ROHRLICH [88] proved that (7.3) holds with $K = 1$ and some δ sufficiently close to 1 and depending on $\mathbb{K}$, thereby improving the lower bound in (7.1) for any fixed number field. We establish, partly on GRH, admissible values for δ which are in fact smaller than $1/2$.

THEOREM 7.2. *Let $\mathbb{K}^{(n)}$ be a normal closure of $\mathbb{K}$. Then, the smoothness condition (7.3) is satisfied for $K = 2$ and every $\delta > \delta_0$, where δ_0 depends on $\mathbb{K}$ and may be chosen as follows:*

(i) *If $\mathbb{K}^{(n)} / \mathbb{Q}$ is abelian*[23]*, then $\delta_0 := \frac{1}{2\sqrt{e}} = 0.303265\ldots$.*

(ii) *If GRH holds for the fields $\mathbb{K}^{(n)}(\zeta_l)$, $l \in \mathbb{N}$, then $\delta_0 := \frac{1}{2}\exp\left(-\frac{1}{[\mathbb{K}^{(n)}:\mathbb{Q}]+1}\right)$.*

(iii) *If $\mathrm{Gal}(\mathbb{K}^{(n)} / \mathbb{Q})$ has an abelian subgroup of index ≤ 4, then $\delta_0 := \frac{1}{2} - \eta$ with some $\eta > 0$ depending on $\mathbb{K}$.*

REMARK 7.3. The value of δ_0 in (ii) can be slightly improved. For details and the exact value of η in (iii), we refer to Section 7.4.2.

Theorem 7.1 is very surprising. On the one hand, as we have already learned, the residual index averaged over prime ideals is typically small, which in view of AC and Wagstaff's heuristic is not an unexpected phenomenon. On the other hand, results of KURLBERG [50] and KURLBERG and POMERANCE [51] suggest that even within the set of all ideals the index is small with probability 1. Nevertheless it turns out that the number of (highly composite) ideals of $\mathbb{K}$ for which the index is exceptionally big is larger than expected (see also Figure 7.1). In fact, it is the core of the proof of Theorem 7.1 to construct sufficiently many such ideals.

7.3. Proof of Theorem 7.1

For an ideal $\mathfrak{a}$ of $\mathbb{K}$, let $\varphi(\mathfrak{a})$ and $\lambda(\mathfrak{a})$ denote order and exponent of $(\mathcal{O}_\mathbb{K} / \mathfrak{a})^*$, respectively. As in the classical case, $\varphi(\mathfrak{a})$ is multiplicative on ideals by the Chinese remainder theorem and satisfies

$$\varphi(\mathfrak{a}) = \mathcal{N}\mathfrak{a} \prod_{\mathfrak{p}\mid\mathfrak{a}} \left(1 - \frac{1}{\mathcal{N}\mathfrak{p}}\right). \tag{7.4}$$

As for $\lambda(\mathfrak{a})$, we have

$$\lambda(\mathfrak{a}) = \mathrm{lcm}(\varphi(\mathfrak{p}) : \mathfrak{p} \mid \mathfrak{a}) \tag{7.5}$$

if $\mathfrak{a}$ is composed of distinct prime ideals. For an ideal $\mathfrak{a}$ which is divisible by the square of some prime ideal, the situation is more complicated, for it depends on the inertia degree of $\mathfrak{p}$ over $\mathbb{Q}$ whether or not $(\mathcal{O}_\mathbb{K} / \mathfrak{p}^k)^*$ is cyclic for $k > 1$ (cf. [85, p. 268]).

The proof of Theorem 7.1 is initiated by the trivial lower bound

$$\mathrm{ind}_\Gamma(\mathfrak{a}) \gg_\mathbb{K} \frac{\varphi(\mathfrak{a})}{\lambda(\mathfrak{a})^\gamma}. \tag{7.6}$$

The implied constant accounts for the torsion part of Γ, and depends only on $\mathbb{K}$. Hence, to obtain a lower bound for κ-th moments of $\mathrm{ind}_\Gamma(\mathfrak{a})$, it suffices to establish one for the average order of $\frac{\varphi(\mathfrak{a})^\kappa}{\lambda(\mathfrak{a})^{\gamma\kappa}}$ over ideals $\mathfrak{a}$ which satisfy $\overline{\Gamma} \subset (\mathcal{O}_\mathbb{K} / \mathfrak{a})^*$. In this regard, we state the following number field analogue of a result of LUCA and SANKARANARAYANAN [70].

PROPOSITION 7.4. *Let $\mathbb{K}$ be a number field and Γ a finitely generated subgroup of $\mathbb{K}^*$ of arithmetic rank $\gamma \in \mathbb{N}$. For any $\kappa, r \in \mathbb{R}_+$ and any $\delta \in \mathbb{R}_+$ which is admissible in the*

[23] Note that $\mathbb{K}^{(n)} / \mathbb{Q}$ is abelian if and only if $\mathbb{K} / \mathbb{Q}$ is abelian.

sense of Theorem 7.1 we have

$$\sum_{\substack{\mathcal{N}\mathfrak{a}\le x\\ \overline{\Gamma}\subset(\mathcal{O}_{\mathbb{K}}/\mathfrak{a})^*}}\frac{\varphi(\mathfrak{a})^{\kappa}}{\lambda(\mathfrak{a})^{r}}\ge x^{1+\kappa-\delta+o(1)},$$

where the o-term depends on κ, γ, r and $\mathbb{K}$.

Proposition 7.4 is proved by a simple number field adaption of the original proof in [70]. In fact, it suffices to replace primes by prime ideals $\mathfrak{p}$ of $\mathbb{K}$ satisfying $\overline{\Gamma}\subset(\mathcal{O}_{\mathbb{K}}/\mathfrak{p})^*$ therein, and utilize the prime ideal theorem, the identities (7.4), (7.5) and the estimate $\varphi(\mathfrak{a})\ge\varphi(\mathcal{N}\mathfrak{a})\gg\frac{\mathcal{N}\mathfrak{a}}{\log\log\mathcal{N}\mathfrak{a}}$ (cf. [100, p. 84]). □

7.4. Proof of Theorem 7.2

We will now validate the admissible values for δ_0 asserted in Theorem 7.2. Our proof combines ideas of Balog [6] and Friedlander [34].

In the sequel, we set $\mathbb{L}:=\mathbb{Q}(\zeta_m)$ if $\mathbb{K}^{(n)}/\mathbb{Q}$ is abelian and contained[24] in $\mathbb{Q}(\zeta_m)$. Otherwise we set $\mathbb{L}:=\mathbb{K}^{(n)}$. A prime number which splits completely in $\mathbb{L}$ is necessarily lifted to linear prime ideals in $\mathbb{K}$. Hence

$$\begin{aligned}\sharp\,\mathcal{P}_{\delta,\mathbb{K}}(y)&\ge\sharp\left\{\mathfrak{p}\in\mathcal{P}(y,\mathbb{K})\ \text{ linear}: P^+(\mathcal{N}\mathfrak{p}-1)<y^{\delta}\right\}\\ &\ge\sharp\left\{p\le y: p\ \text{splits completely in }\ \mathbb{L}, P^+(p-1)<y^{\delta}\right\}.\end{aligned}\tag{7.7}$$

Proceeding as in the original work of Balog [6], we let $\varepsilon>0$ be sufficiently small and define

$$h(p):=\sharp\{p-1=kn: P^+(kn)\le y^{\delta}, N_1<n\le N_2\}\tag{7.8}$$

with

$$N_1:=y^{\frac12+\varepsilon}\qquad\text{and}\qquad N_2:=y^{\frac12+2\varepsilon}.\tag{7.9}$$

Then (7.7) and the Cauchy-Schwarz inequality yield

$$\sharp\,\mathcal{P}_{\delta,\mathbb{K}}(y)\ge\Bigg(\sum_{p\in\mathcal{P}_{C_0}(y,\mathbb{L}/\mathbb{Q})}h(p)\Bigg)^2\Bigg(\sum_{p\in\mathcal{P}_{C_0}(y,\mathbb{L}/\mathbb{Q})}h(p)^2\Bigg)^{-1},\tag{7.10}$$

where $C_0:=\{\mathrm{id}\}\subset\mathrm{Gal}(\mathbb{L}/\mathbb{Q})$. Thus we need a good lower and upper bound for the numerator and the denominator in (7.10), respectively.

For the denominator, a simple change of summation order and the Brun-Titchmarsh inequality yield

$$\begin{aligned}\sum_{p\in\mathcal{P}_{C_0}(y,\mathbb{L}/\mathbb{Q})}h(p)^2&\le\sum_{p\le y}\Bigg(\sum_{\substack{k\mid p-1\\ k\le(y-1)/N_1}}1\Bigg)^2\le\sum_{k_1,k_2\le\frac{y-1}{N_1}}\pi(y;1,[k_1,k_2])\\ &\ll\frac{y}{\log y}\sum_{k_1,k_2\le\frac{y-1}{N_1}}\frac{1}{\varphi([k_1,k_2])}.\end{aligned}$$

[24] This is again possible by the Kronecker-Weber theorem (cf. [68, p. 273]).

By Lemma 4.5 we obtain

$$\sum_{a,b\le z}\frac{1}{\varphi([a,b])}\le\sum_{\substack{a,b,c\le z\\(a,b)=c}}\frac{1}{\varphi\left(\frac{a}{c}\right)\varphi\left(\frac{b}{c}\right)\varphi(c)}\le\left(\sum_{n\le z}\frac{1}{\varphi(n)}\right)^3\ll\log^3 z$$

and hence

$$\sum_{p\in\mathcal{P}_{C_0}(y,\mathbb{L}/\mathbb{Q})}h(p)^2\ll y\log^2 y. \tag{7.11}$$

As for the numerator in (7.10), we clearly have

$$\begin{aligned}h(p)&=\sharp\{p-1=kn:P^+(k)\le y^\delta,N_1<n\le N_2\}\\&\quad-\sharp\{p-1=kn:P^+(k)\le y^\delta,P^+(n)>y^\delta,N_1<n\le N_2\}\\&\ge\sharp\{p-1=kn:P^+(k)\le y^\delta,N_1<n\le N_2\}\\&\quad-\sharp\{p-1=kql:y^\delta<q,N_1<ql\le N_2\},\end{aligned}$$

where the letter q is henceforth reserved for primes. Thus, we obtain

$$\sum_{p\in\mathcal{P}_{C_0}(y,\mathbb{L}/\mathbb{Q})}h(p)\ge S_1-S_2$$

with

$$S_1:=\sum_{\substack{k\le y\\P^+(k)\le y^\delta}}\sum_{\substack{p\in\mathcal{P}_{C_0}(y,\mathbb{L}/\mathbb{Q})\\k\mid p-1\\N_1<\frac{p-1}{k}\le N_2}}1\qquad\text{and}\qquad S_2:=\sum_{y^\delta<q}\sum_{N_1<ql\le N_2}\sum_{\substack{p\in\mathcal{P}_{C_0}(y,\mathbb{L}/\mathbb{Q})\\ql\mid p-1}}1.$$

7.4.1. Estimating S_1 from below. We must establish a lower bound for S_1. We do so in detail for part (i) and (ii) of Theorem 7.2 and briefly discuss the case (iii) at the end of Section 7.4.2. To start with, we observe that

$$S_1\ge\sum_{\substack{\frac{y}{N_2}<k\le\frac{y}{N_1}\\P^+(k)\le y^\delta}}\sum_{\substack{p\in\mathcal{P}_{C_0}(y,\mathbb{L}/\mathbb{Q})\\p>N_1k+1\\k\mid p-1}}1=\sum_{\substack{\frac{y}{N_2}<k\le\frac{y}{N_1}\\P^+(k)\le y^\delta}}\sum_{\substack{p\in\mathcal{P}_{C_0}(y,\mathbb{L}/\mathbb{Q})\\k\mid p-1}}1+O\left(\frac{y}{\log y}\right)$$

holds by the Brun-Titchmarsh inequality, since

$$\sum_{\substack{\frac{y}{N_2}<k\le\frac{y}{N_1}\\P^+(k)\le y^\delta}}\sum_{\substack{p\in\mathcal{P}_{C_0}(y,\mathbb{L}/\mathbb{Q})\\p\le N_1k+1\\k\mid p-1}}1\le\sum_{k\le\frac{y}{N_1}}\pi(N_1k+1;1,k)\ll\frac{N_1}{\log y}\sum_{k\le\frac{y}{N_1}}\frac{k}{\varphi(k)}\ll\frac{y}{\log y}.$$

Invoking the effective Čebotarev density theorem under GRH (Proposition 4.7), we find

$$S_1\ge\mathrm{li}(y)\sum_{\substack{\frac{y}{N_2}<k\le\frac{y}{N_1}\\P^+(k)\le y^\delta}}\frac{1}{[\mathbb{L}(\zeta_k):\mathbb{Q}]}+O_{\mathbb{K}}\left(\frac{y}{\log y}\right). \tag{7.12}$$

If $\mathbb{L} = \mathbb{Q}(\zeta_m)$, the same follows by the Bombieri-Vinogradov theorem, since we have $\pi_{C_0}(y, \mathbb{L}/\mathbb{Q}) = \pi(y; 1, m)$ in this case. Letting $m' \in \mathbb{N}$ satisfy $\mathbb{L}^{ab} \subset \mathbb{Q}(\zeta'_m)$, we deduce

$$S_1 \geq \mathrm{li}(y) \sum_{d|m'} \frac{1}{[\mathbb{L} : \mathbb{L} \cap \mathbb{Q}(\zeta_d)]} \sum_{\substack{\frac{y}{N_2} < k \leq \frac{y}{N_1} \\ (k,m')=d \\ P^+(k) \leq y^\delta}} \frac{1}{\varphi(k)} + O_{\mathbb{K}}\left(\frac{y}{\log y}\right) \tag{7.13}$$

by the same arguments as in Section 6.3 (see the paragraph before Lemma 6.11). The sum over k is bounded from below by

$$\sum_{\substack{\frac{y}{N_2} < k \leq \frac{y}{N_1} \\ (k,m')=d}} \frac{1}{\varphi(k)} - \sum_{y^\delta < q \leq y^{1/2}} \frac{1}{\varphi(q)} \sum_{\substack{\frac{y}{qN_2} < l \leq \frac{y}{qN_1} \\ (l,m')=d}} \frac{1}{\varphi(l)}, \tag{7.14}$$

if we choose y big enough so that (ql, m') becomes (l, m'). To treat sums of this type we prove the following elementary result:

LEMMA 7.5. *For positive integers $b \mid a$, let*

$$B(a,b) := \frac{\varphi(\frac{a}{b})b}{\varphi(b)a} \prod_{p \nmid a} \left(1 + \frac{1}{p(p-1)}\right).$$

Then we have

$$\sum_{\substack{n \leq x \\ (a,n)=b}} \frac{1}{\varphi(n)} = B(a,b) \cdot \log x + O_a(1).$$

PROOF. First we observe that

$$\sum_{\substack{n \leq x \\ (a,n)=b}} \frac{1}{\varphi(n)} = \sum_{\substack{n \leq \frac{x}{b} \\ (\frac{a}{b},n)=1}} \frac{1}{\varphi(bn)} = \sum_{e | \frac{a}{b}} \mu(e) \sum_{\substack{n \leq \frac{x}{b} \\ e|n}} \frac{1}{\varphi(bn)} = \sum_{e | \frac{a}{b}} \mu(e) \sum_{\substack{n \leq x \\ eb|n}} \frac{1}{\varphi(n)}$$

holds by the inclusion-exclusion principle. Applying the formula $\frac{1}{\varphi(n)} = \frac{1}{n} \sum_{s|n} \frac{\mu^2(s)}{\varphi(s)}$, the inner sum becomes

$$\sum_{\substack{n \leq x \\ eb|n}} \frac{1}{n} \sum_{s|n} \frac{\mu^2(s)}{\varphi(s)} = \sum_{s \leq x} \frac{\mu^2(s)}{\varphi(s)[s, eb]} \sum_{n \leq \frac{x}{[s,eb]}} \frac{1}{n} = \log x \sum_{s \geq 1} \frac{\mu^2(s)}{\varphi(s)[s, eb]} + O_{e,b}(1).$$

Hence, we obtain

$$\sum_{\substack{n \leq x \\ (a,n)=b}} \frac{1}{\varphi(n)} = \log x \sum_{e | \frac{a}{b}} \mu(e) \sum_{s \geq 1} \frac{\mu^2(s)}{\varphi(s)[s, eb]} + O_a(1).$$

To treat the double sum, we express the inner sum as an Euler product:

$$\begin{aligned}\sum_{e|\frac{a}{b}}\mu(e)\sum_{s\geq 1}\frac{\mu^2(s)}{\varphi(s)[s,eb]} &= \frac{1}{b}\sum_{e|\frac{a}{b}}\frac{\mu(e)}{e}\sum_{s\geq 1}\frac{\mu^2(s)(s,eb)}{s\varphi(s)}\\ &= \frac{1}{b}\sum_{e|\frac{a}{b}}\frac{\mu(e)}{e}\prod_{p|eb}\left(1+\frac{1}{p-1}\right)\prod_{p\nmid eb}\left(1+\frac{1}{p(p-1)}\right)\\ &= \frac{1}{b}\prod_{p\nmid b}\left(1+\frac{1}{p(p-1)}\right)\frac{b}{\varphi(b)}\sum_{e|\frac{a}{b}}\frac{\mu(e)}{e}\prod_{\substack{p|e\\ p\nmid b}}\frac{p^2}{p^2-p+1}.\end{aligned}$$

The sum over e is clearly multiplicative and can be easily verified to equal

$$\prod_{\substack{p|\frac{a}{b}\\ p|b}}\left(1-\frac{1}{p}\right)\prod_{\substack{p|\frac{a}{b}\\ p\nmid b}}\left(1-\frac{p}{p^2-p+1}\right)=\frac{\varphi(\frac{a}{b})b}{a}\prod_{\substack{p|\frac{a}{b}\\ p\nmid b}}\left(1+\frac{1}{p(p-1)}\right)^{-1}.$$

Hence, we obtain

$$\begin{aligned}\sum_{e|\frac{a}{b}}\mu(e)\sum_{s\geq 1}\frac{\mu^2(s)}{\varphi(s)[s,eb]} &= \frac{\varphi(\frac{a}{b})b}{\varphi(b)a}\prod_{p\nmid b}\left(1+\frac{1}{p(p-1)}\right)\prod_{\substack{p|\frac{a}{b}\\ p\nmid b}}\left(1+\frac{1}{p(p-1)}\right)^{-1}\\ &= \frac{\varphi(\frac{a}{b})b}{\varphi(b)a}\prod_{p\nmid a}\left(1+\frac{1}{p(p-1)}\right)\end{aligned}$$

and the assertion follows. □

Combining this result with (7.13), (7.14) and Mertens' formula, we finally infer

$$S_1 \geq \mathrm{li}(y)\log\left(\frac{N_2}{N_1}\right)\left(1-\log\left(\frac{1}{2\delta}\right)\right)\sum_{d|m'}\frac{B(m',d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}+O_{m'}\left(\frac{y\log\log y}{\log y}\right). \tag{7.15}$$

7.4.2. Estimating S_2 from above. To estimate S_2, we need to handle sums of $\pi(x;a,q)$ for moduli q slightly exceeding $x^{1/2}$. Here the Bombieri-Vinogradov theorem is not applicable and the Brun-Titchmarsh inequality is too imprecise for an accurate account, and we therefore utilize Proposition 4.4. It is convenient to treat the cases $\mathbb{L}=\mathbb{Q}(\zeta_m)$ and $\mathbb{L}=\mathbb{K}^{(n)}$ separately.

If $\mathbb{L}=\mathbb{Q}(\zeta_m)$, then S_2 becomes

$$\sum_{y^\delta<q}\sum_{N_1<ql\leq N_2}\sum_{\substack{p\leq y\\ [m,ql]|p-1}}1,$$

and for $\delta>\frac{1}{4}+\varepsilon$ Proposition 4.4 and Lemma 7.5 yield

$$\begin{aligned}S_2 &= \sum_{y^\delta<q\leq N_2}\sum_{\frac{N_1}{q}<l\leq\frac{N_2}{q}}\frac{\mathrm{li}(y)}{[\mathbb{L}(\zeta_{ql}):\mathbb{Q}]}+O(\varepsilon^2)\,\mathrm{li}(y)\sum_{N_1<k\leq N_2}\frac{1}{[\mathbb{L}(\zeta_k):\mathbb{Q}]}\\ &\leq \mathrm{li}(y)\Bigg(\sum_{y^\delta<q\leq N_2}\frac{1}{\varphi(q)}\sum_{\frac{N_1}{q}<l\leq\frac{N_2}{q}}\frac{1}{[\mathbb{L}(\zeta_l):\mathbb{Q}]}+\log(N_2/N_1)O\left(\varepsilon^2\right)\Bigg).\end{aligned}$$

Applying the same arguments as in the estimation of S_1, it is easily shown that

$$S_2 \leq \mathrm{li}(y)\log(N_2/N_1)\log\left(\frac{\frac{1}{2}+\varepsilon}{\delta}\right)\left(\sum_{d|m}\frac{B(m,d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}+O\left(\varepsilon^2\right)\right).$$

Now choose $m'=m$ in (7.15). Then, for $\delta>\frac{1}{2\sqrt{e}}$, we have $S_1-S_2\gg_{\mathbb{K}} y$, if y is large and ε small enough, respectively. In combination with (7.7), (7.10) and (7.11), this proves Theorem 7.2 (i).

Now assume that $\mathbb{L}$ equals $\mathbb{K}^{(n)}$. i.e. $\mathbb{K}$ is not contained in any cyclotomic field. Unfortunately, the splitting condition $p\in\mathcal{P}_{C_0}(\mathbb{L}\,/\,\mathbb{Q})$ cannot be translated into an arithmetic progression condition. Hence we omit this condition and start with the trivial estimate

$$S_2 \leq \sum_{y^\delta<q\leq N_2}\sum_{N_1<ql\leq N_2}\sum_{\substack{p\leq y\\ ql|p-1}}1,$$

probably loosing a lot. As in the first case, we invoke Proposition 4.4 and deduce

$$\begin{aligned} S_2 &\leq \mathrm{li}(y)\Bigg(\sum_{y^\delta<q\leq N_2}\frac{1}{\varphi(q)}\sum_{\frac{N_1}{q}<l\leq\frac{N_2}{q}}\frac{1}{\varphi(l)}+O(\varepsilon^2)\sum_{N_1<k\leq N_2}\frac{1}{\varphi(k)}\Bigg)\\ &\leq \mathrm{li}(y)\log(N_2/N_1)\log\left(\frac{\frac{1}{2}+\varepsilon}{\delta}\right)\left(B(1,1)+O\left(\varepsilon^2\right)\right), \end{aligned} \tag{7.16}$$

for $\delta>\frac{1}{4}+\varepsilon$. Finally, by (7.15) and (7.16), we obtain $S_1-S_2\gg_{\mathbb{K}} y$ if

$$\delta>\frac{1}{2}\exp\left(-\frac{\sum_{d|m'}\frac{B(m',d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}}{B(1,1)+\sum_{d|m'}\frac{B(m',d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}}\right)$$

and y and ε are chosen large and small enough, respectively. Since $[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]\leq[\mathbb{L}:\mathbb{Q}]$ and $\sum_{d|m'}B(m',d)=B(1,1)$, we clearly have

$$\frac{\sum_{d|m'}\frac{B(m',d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}}{B(1,1)+\sum_{d|m'}\frac{B(m',d)}{[\mathbb{L}:\mathbb{L}\cap\mathbb{Q}(\zeta_d)]}}\geq\frac{1}{[\mathbb{L}:\mathbb{Q}]+1}$$

and Theorem 7.2 (ii) follows.

As for Theorem 7.2 (iii), we first observe that, (7.12) remains true by Proposition 4.9, the number field analogue of the Bombieri-Vinogradov theorem, if we restrict to those k for which $\mathbb{Q}(\zeta_k)\cap\mathbb{L}=\mathbb{Q}$. If $(m',k)=d$ for some divisor d of m', we clearly have $\mathbb{Q}(\zeta_k)\cap\mathbb{L}=\mathbb{Q}(\zeta_d)\cap\mathbb{L}$. Hence, (7.13) holds if one restricts to divisors d of m' which satisfy $\mathbb{Q}(\zeta_d)\cap\mathbb{L}=\mathbb{Q}$. Proceeding as before in the cases (ii) and (iii), finally yields the choice

$$\delta_0=\frac{1}{2}\exp\left(-\frac{\sum^*_{d|m'}B(m',d)}{B(1,1)[\mathbb{L}:\mathbb{Q}]+\sum^*_{d|m'}B(m',d)}\right),$$

where * indicates the restriction to those d for which $\mathbb{Q}(\zeta_d)\cap\mathbb{L}=\mathbb{Q}$. □

7.5. A note on double averaging modulo all ideals

In Chapter 6 we discovered that averaging $\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$ instead of $\mathrm{ind}_\Gamma(\mathfrak{p})^\kappa$ over prime ideals effects much stronger results. Setting

$$\mathrm{Ind}_\gamma^\kappa(\mathfrak{a}) := \sum_{a_1,\dots,a_\gamma \in (\mathcal{O}_\mathbb{K}/\mathfrak{a})^*} \frac{\mathrm{ind}_{\langle a_1,\dots,a_\gamma\rangle}(\mathfrak{a})^\kappa}{\varphi(\mathfrak{a})^\gamma}$$

for an arbitrary ideal $\mathfrak{a}$ of $\mathbb{K}$, it is natural to ask whether similar improvements are expectable, if we average $\mathrm{Ind}_\gamma^\kappa(\mathfrak{a})$ instead of $\mathrm{ind}_\Gamma(\mathfrak{a})^\kappa$ over all ideals of $\mathbb{K}$. On the one hand, we certainly have

$$\mathrm{Ind}_\gamma^\kappa(\mathfrak{a}) \geq \frac{\varphi(\mathfrak{a})^\kappa}{\lambda(\mathfrak{a})^{\gamma\kappa}},$$

whence Theorem 7.1 remains true if one replaces $\mathrm{ind}_\Gamma(\mathfrak{a})^\kappa$ by $\mathrm{Ind}_\gamma^\kappa(\mathfrak{a})$. This is not very surprising. Different to the prime ideal case, however, we did not manage to improve on this result.

On the other hand, $\mathrm{Ind}_\gamma^\kappa(\mathfrak{a})$ admits a very nice feature in case $\kappa = 1$ which might help to illuminate Rohrlich's original interest, the average order of $\mathrm{ind}_{\mathcal{U}_\mathbb{K}}(\mathfrak{a})$ if $\mathcal{U}_\mathbb{K}$ is infinite. Keeping in mind that $\mathrm{Ind}_\gamma^\kappa(\mathfrak{a})$ is nothing but $\mathrm{Ind}_\gamma^\kappa((\mathcal{O}_\mathbb{K}/\mathfrak{a})^*)$, in the sense of Section 6.2, one has the following estimates, as $\lambda(G)^\gamma \geq \lambda_\gamma(G)$ holds for any finite abelian group G.

Theorem 7.6. *Let $\gamma \in \mathbb{N}$ and $\mathbb{K}$ a number field. For any ideal $\mathfrak{a}$ of $\mathbb{K}$ we have*

$$\frac{\varphi(\mathfrak{a})}{\lambda(\mathfrak{a})} \leq \mathrm{Ind}_1^1(\mathfrak{a}) \leq \tau(\lambda(\mathfrak{a})) \cdot \frac{\varphi(\mathfrak{a})}{\lambda(\mathfrak{a})},$$

and if $\gamma > 1$ we have

$$\frac{\varphi(\mathfrak{a})}{\lambda(\mathfrak{a})^\gamma} \leq \mathrm{Ind}_\gamma^1(\mathfrak{a}) \leq 2^{\omega(\varphi(\mathfrak{a}))} \cdot \frac{\varphi(\mathfrak{a})}{\lambda(\mathfrak{a})}.$$

From this result we learn that the average order of $\mathrm{Ind}_\gamma^1(\mathfrak{a})$ is (up to an ε-power of $\mathcal{N}\mathfrak{a}$) determined by the average order of the fractions $\frac{\varphi(\mathfrak{a})}{\lambda(\mathfrak{a})}$ and $\frac{\varphi(\mathfrak{a})}{\lambda(\mathfrak{a})^\gamma}$. On the contrary, as we have seen above, the average order of these fractions bound the average order of $\mathrm{ind}_\Gamma(\mathfrak{a})$ from below. In this way we obtain another approach towards Rohrlich's problem, for any improvement towards lower bounds for the average order of $\mathrm{Ind}_\gamma^1(\mathfrak{a})$ yields an improvement concerning lower bounds for the average order of $\mathrm{ind}_\Gamma(\mathfrak{a})$ by Theorem 7.6 and (7.6).

Part III

Residual Index and Residual Order on Elliptic Curves over Finite Fields

CHAPTER 8

Background on Elliptic Curves

Until now we have only studied properties of residue rings arising from reductions in number fields. In this last part of the thesis we deal with analogue questions provided by elliptic curves over finite fields. In this chapter we catch up on a brief introduction to the theory of ellitpic curves and provide basic notation and facts which are needed in the following two chapters. This introduction covers only basic properties and builds on the book [96] of SILVERMAN and the survey paper [17] of COJOCARU to which we refer for a more extensive treatment. In the subsequent chapters we go more into detail and also state some more specific results which are mostly taken from the papers [17, 19] of COJOCARU and the paper [92] of SCHOOF.

8.1. Basic facts about elliptic curves

Let $\mathbb{F}$ be an arbitrary field and let $\overline{\mathbb{F}}$ be an algebraic closure thereof. We denote by $\mathbb{P}^2 := \mathbb{P}^2(\overline{\mathbb{F}})$ the projective plane over $\overline{\mathbb{F}}$. An *elliptic curve* (E, O), or simply E, is a non-singular curve E of genus one in $\mathbb{P}^2$ containing a specified *point at infinity* denoted by O. If E is given by a non-singular polynomial with coefficients in $\mathbb{F}$, and O may be given by coordinates in $\mathbb{F}$, we say that E is *defined over* $\mathbb{F}$ and express this by writing $\mathrm{E}/\mathbb{F}$. An elliptic curve which is defined over $\mathbb{Q}$ is called a *rational elliptic curve*.

In case $\mathrm{char}(\mathbb{F}) \neq 2, 3$, it can be shown (cf. [96, p. 44f]) that for any elliptic curve $\mathrm{E}/\mathbb{F}$, there exists an $\mathbb{F}$-isomorphism (see below) which transforms E into an elliptic curve $\mathrm{E}_{a,b}$ given by the projective closure of a so called *Weierstraß equation*

$$\mathrm{E}_{a,b}: \quad y^2 = x^3 + ax + b, \tag{8.1}$$

with $a, b \in \mathbb{F}$ such that the *discriminant* $\Delta_{\mathrm{E}_{a,b}} := -16(4a^3 + 27b^2)$ of $\mathrm{E}_{a,b}$ is non-zero. Note that, under this transformation, the point O is mapped to the projective point $[0:1:0]$ which explains the term "point at infinity".

The set of points on an elliptic curve $\mathrm{E}/\mathbb{F}$ forms an abelian group, with O as identity, in virtue of a simple geometric construction, illustrated in Figure 8.1 (see [96] for details). We write $P + Q$ for the result of two points of E under this operation and note that the coordinates of $P + Q$ are given by rational expressions involving the coordinates of P and Q. The set of $\mathbb{F}$-*rational points* $\mathrm{E}(\mathbb{F})$ of E (or simply *rational points* if $\mathbb{F} = \mathbb{Q}$) are defined as the set containing all points of E which may be given by coordinates in $\mathbb{F}$. In particular we have $O \in \mathrm{E}(\mathbb{F})$, since E is defined over $\mathbb{F}$. It is easily seen that $E(\mathbb{F})$ is a subgroup of E, and, if $\mathbb{K}$ is a number field, then $\mathrm{E}(\mathbb{K})$ is finitely generated by the *Mordell-Weil theorem* (cf. [96, p. 239]). For any $k \in \mathbb{N}$, we denote by $\mathrm{E}[k]$, the k-*torsion points* of E, i.e. the set of points of E which are annihilated by k-fold addition. If k is prime to $\mathrm{char}(\mathbb{F})$, the only case we shall consider, then the structure of $\mathrm{E}[k]$ is determined by (cf. [96, p. 86])

$$\mathrm{E}[k] \cong \mathbb{Z}/k\mathbb{Z} \oplus \mathbb{Z}/k\mathbb{Z}\,. \tag{8.2}$$

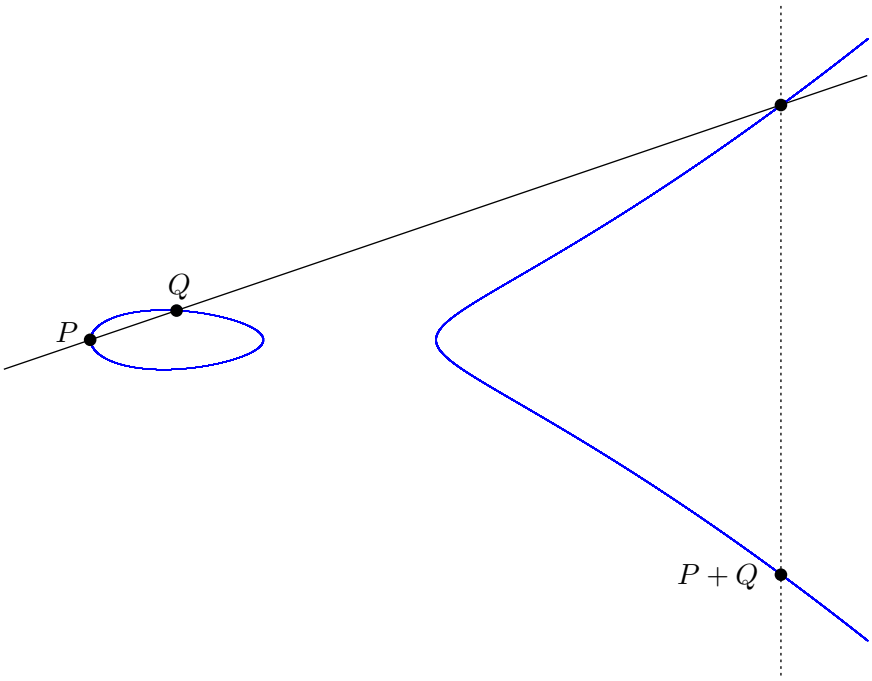


FIGURE 8.1. Addition of points on the elliptic curve $y^2 = x^3 - x$.

The field $\mathbb{F}(\mathrm{E}[k])$ which is obtained by adjoining all coordinates[25] of points of $\mathrm{E}[k]$ to $\mathbb{F}$ is called the *k-division field of* E. It can be shown that $\mathbb{F}(\mathrm{E}[k])$ is a finite Galois extension of $\mathbb{F}$ which contains the k-th roots of unity (cf. [96, p. 96]). The k-division fields of rational elliptic curves will appear very often in Chapter 9 as they, in some sense, are the elliptic curve analogues to cyclotomic fields. We make this precise in Section 8.2.

Given two elliptic curves (E_1, O_1) and (E_2, O_2) defined over $\mathbb{F}$, an *$\mathbb{F}$-isogeny* from E_1 to E_2 is a morphism $\phi : \mathrm{E}_1 \to \mathrm{E}_2$ defined over $\mathbb{F}$ which satisfies $\phi(O_1) = O_2$ (cf. [96, p. 66]). It turns out that every such $\mathbb{F}$-isogeny also yields a group homomorphism between the corresponding elliptic curves (cf. [96, p. 71]). If there exists another $\mathbb{F}$-isogeny $\psi : \mathrm{E}_2 \to \mathrm{E}_1$ such that $\psi \circ \phi$ and $\phi \circ \psi$ yield the identity maps on E_1 and E_2, respectively, then ϕ is called an *$\mathbb{F}$-isomorphism*, and E_1 and E_2 are said to be *isomorphic over* $\mathbb{F}$. In case $\mathbb{F} = \overline{\mathbb{F}}$ we simply speak of *isogenies*, *isomorphisms* and *isomorphic* elliptic curves. An isogeny ($\mathbb{F}$-isogeny) from an elliptic curve $\mathrm{E} / \mathbb{F}$ to itself is called an *endomorphism* (*$\mathbb{F}$-endomorphism*) of E, and the set of all endomorphisms ($\mathbb{F}$-endomorphisms) of E forms a ring of characteristic 0 with no zero divisors, the so called *endomorphism ring* $\mathrm{End}(\mathrm{E})$ (*$\mathbb{F}$-endomorphism ring* $\mathrm{End}_{\mathbb{F}}(\mathrm{E})$) of E (cf. [96, p. 68]). The invertible elements of this ring are called *automorphisms* (*$\mathbb{F}$-automorphisms*) of E, and form the *automorphism group* $\mathrm{Aut}(\mathrm{E})$ (*$\mathbb{F}$-automorphism group* $\mathrm{Aut}_{\mathbb{F}}(\mathrm{E})$) of E. It can be shown that, for any elliptic curve E, there exists a characteristic number j_{E}, the so called *j-invariant* of E, such that any other elliptic curve is isomorphic to E if and only if it has the same j-invariant (cf. [96, p. 45]). If E is given by a Weierstraß equation, $\mathrm{E} = \mathrm{E}_{a,b}$ say, then one has $j_{\mathrm{E}} = -1728(4a)^3/\Delta_{\mathrm{E}_{a,b}}$. Note that curves $\mathrm{E}_1 / \mathbb{F}$ and $\mathrm{E}_2 / \mathbb{F}$ with the same j-invariant need not be isomorphic over $\mathbb{F}$, if $\mathbb{F}$ is not algebraically closed.

[25] Of course, before adjoining the coordinates of a point $P = [x : y : z]$ one has to normalize the coordinates so that one of x, y or z equals 1.

Clearly, k-fold addition defines an endomorphism for any elliptic curve E, so that End(E) always contains a copy of $\mathbb{Z}$ as a subring. Whenever End(E) is strictly larger than $\mathbb{Z}$, one says that E has *complex multiplication*, or simply *CM*, and calls E a *CM curve*. Otherwise, E is called a *non-CM curve*. If E is a rational CM curve, then End(E) is an order in an imaginary quadratic field $\mathbb{Q}(\sqrt{-d})$ of class number 1, i.e. $d \in \{1, 2, 3, 7, 11, 19, 43, 67, 163\}$ (cf. [17]), and the field $\mathbb{Q}(\sqrt{-d})$ is referred to as the *CM field* associated to E. Due to the additional structure on E provided by complex multiplication, rational CM curves are usually easier to handle, as we have already noticed in Section 2.4 in connection with the Lang-Trotter conjecture. We will encounter this phenomenon again in Chapter 9. Unfortunately, most rational elliptic curves are non-CM curves, so complex multiplication is rather the exception in this case. This changes if one considers elliptic curves defined over $\mathbb{F}_p$ instead. In fact, every elliptic curve is a CM curve in this case, and the associated endomorphism ring is either an order in an imaginary quadratic field or, which is rather seldom, an order in a quaternion algebra (cf. [96, p. 144f]). More information about this distinction and other facts concerning elliptic curves defined over $\mathbb{F}_p$ are provided in the subsequent section.

8.2. Elliptic curves defined over $\mathbb{F}_p$ and reduction modulo p

Let us start with an arbitrary elliptic curve $\mathrm{E}/\mathbb{F}_p$, for some prime $p > 3$, and consider its $\mathbb{F}_p$-rational points $\mathrm{E}(\mathbb{F}_p)$. By elementary arguments one would suggest that $\mathrm{E}(\mathbb{F}_p)$ contains roughly about $p + 1$ points (see [96, p. 137]). Indeed, writing

$$a := \sharp\,\mathrm{E}(\mathbb{F}_p) - p - 1,$$

Hasse proved the following estimate in the 1930s, to which we refer as *Hasse's theorem*, which was conjectured by Artin in his thesis (cf. [96, p. 138]).

Proposition 8.1 (Hasse's theorem). *For any prime p, and any elliptic curve $\mathrm{E}/\mathbb{F}_p$ we have*

$$|a| \leq 2\sqrt{p}.$$

This result is a special case of the so called Weil conjectures, proposed by Weil in 1949 and proved in 1974 by Deligne (see Chapter V.2 of [96]). The number a plays a crucial role in determining the structure of End(E). If $a \neq 0$, then End(E) is an order in an imaginary quadratic field, and E is called an *ordinary* curve. If a happens to be zero, then End(E) is an order in a quaternion algebra and E is called *supersingular* (cf. [17]). As for the structure of $\mathrm{E}(\mathbb{F}_p)$, the isomorphism (8.2) yields that $\mathrm{E}(\mathbb{F}_p)$ is a subgroup of $\mathbb{Z}/k\mathbb{Z} \oplus \mathbb{Z}/k\mathbb{Z}$, for some k which is divisible by $\sharp\,\mathrm{E}(\mathbb{F}_p)$. Hence, we obtain a decomposition[26]

$$\mathrm{E}(\mathbb{F}_p) \cong \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/de\,\mathbb{Z}, \tag{8.3}$$

for appropriate $d, e \in \mathbb{N}$ to which we refer as the *structure constants* of $\mathrm{E}(\mathbb{F}_p)$. Any $\mathbb{F}_p$-rational point Q of E generates a cyclic group inside $\mathrm{E}(\mathbb{F}_p)$ and, just as in the number field setting, we define *residual index* $\mathrm{ind}_Q(\mathrm{E})$ and *residual order* $\mathrm{ord}_Q(\mathrm{E})$ *of Q in* $\mathrm{E}(\mathbb{F}_p)$ as the index and order of this cyclic group, respectively. As in Part II, these two quantities will be the centre of interest in the subsequent investigations.

In the next chapter we will deal with elliptic curves defined over $\mathbb{F}_p$ which arise from a rational elliptic curve in a canonical way: If E is an arbitrary rational elliptic curve, given by a Weierstraß equation (8.1) say, then for any prime $p > 3$ one obtains a curve $\mathrm{E}_p/\mathbb{F}_p$,

[26] In the literature the integers d and e are sometimes defined by $\mathrm{E}(\mathbb{F}_p) \cong \mathbb{Z}/d\mathbb{Z} \oplus \mathbb{Z}/e\,\mathbb{Z}$ with $d \mid e$.

the so called *reduction of* E *modulo* p, by reducing the defining equation modulo p. It turns out that this is again an elliptic curve defined over $\mathbb{F}_p$ if and only if p does not divide the *conductor* N_{E} of E, an important invariant of E which we not specify any further (see [96, p. 256] for details). Such primes are called *primes of good reduction* for E, the divisors of N_{E} are said to have *bad reduction* for E. The reduction of a rational point Q of E modulo a prime p of good reduction is denoted by $\overline{Q}$, and for notational convenience we write $\mathrm{ind}_Q(\mathrm{E}_p)$ and $\mathrm{ord}_Q(\mathrm{E}_p)$ instead of $\mathrm{ind}_{\overline{Q}}(\mathrm{E}_p)$ and $\mathrm{ord}_{\overline{Q}}(\mathrm{E}_p)$, respectively. For any prime p of good reduction for E, we write a_p, d_p and e_p for the integers a, d and e introduced above. A prime p of good reduction for E is called *of supersingular reduction* if $a_p = 0$, and *of ordinary reduction*, otherwise.

We close this section with a preparation for Chapter 9. Here, we will study the distribution of $\mathrm{ord}_Q(\mathrm{E}_p)$ (or rather its average over Q) over primes p of good reduction for E. During this investigation we will frequently need criteria for a positive integer k to divide the numbers d_p and $\sharp\,\mathrm{E}_p(\mathbb{F}_p)$, respectively. These properties turn out to be encoded in the k-division field $\mathbb{Q}(\mathrm{E}[k])$. In fact, the first property is easily translated into a splitting condition for p [17].

LEMMA 8.2. *Let* E *be a rational elliptic curve of conductor* N_{E}*,* $k \in \mathbb{N}$ *and* p *a prime such that* $p \nmid kN_{\mathrm{E}}$*. Then,* k *divides* d_p *if and only if* p *splits completely in* $\mathbb{Q}(\mathrm{E}[k])$*.*

To deal with the second question, we recall that the k-division field $\mathbb{Q}(\mathrm{E}[k])$ is Galois over $\mathbb{Q}$. In view of (8.2), one then has a natural representation

$$\phi_k : \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[k])/\,\mathbb{Q}) \to \mathrm{GL}_2(\mathbb{Z}\,/k\,\mathbb{Z}),$$

called the *Galois representation associated to* $\mathrm{E}[k]$ which is easily seen to be injective (see Lemma 9.3 for more details about ϕ_k). The subsequent lemma expresses the condition that k divides $\sharp\,\mathrm{E}_p(\mathbb{F}_p)$ in terms of ϕ_k and also characterizes primes which ramify in $\mathbb{Q}(\mathrm{E}[k])$ (cf. [17]).

LEMMA 8.3. *Let* E *be a rational elliptic curve of conductor* N_{E} *and* $k \in \mathbb{N}$*. The primes which ramify in* $\mathbb{Q}(\mathrm{E}[k])$ *divide* kN_{E}*, and for primes* $p \nmid kN_{\mathrm{E}}$ *we have*

$$k \mid \sharp\,\mathrm{E}_p(\mathbb{F}_p) \iff \left[\frac{\mathbb{Q}(\mathrm{E}[k]) \mid \mathbb{Q}}{p}\right] \subset D_k,$$

where D_k *is given by*

$$D_k := \big\{\sigma \in \mathrm{Gal}(\mathbb{Q}(\mathrm{E}[k])/\,\mathbb{Q}) : \det \phi_k(\sigma) + 1 - \mathrm{tr}\,\phi_k(\sigma) \equiv 0 \ (k)\big\}$$

which is clearly closed under conjugation in $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[k])/\,\mathbb{Q})$*.*

CHAPTER 9

Moments of the Residual Order of Rational Points modulo Primes

In Part II we investigated the distribution of residual index and residual order of algebraic integers modulo ideals of a given number field. One way to transfer this problem to the field of elliptic curves is the following: Let E be a rational elliptic curve and Q a fixed rational point of infinite order in $\mathrm{E}(\mathbb{Q})$. Similar to the number field case, one may ask for the distribution of $\mathrm{ind}_Q(\mathrm{E}_p)$ and $\mathrm{ord}_Q(\mathrm{E}_p)$, as p varies over primes of good reduction for E. Due to the non-cyclicity of $\mathrm{E}_p(\mathbb{F}_p)$ and other obstructions, this problem proves to be harder than in the number field case.

In this chapter we adapt methods from Chapter 6 to attack the analogue of Luca's problem presented in Section 6.4 to elliptic curves. In particular we only deal with the case of the residual order which is much easier to handle and, partly on GRH, admits asymptotic formulae. A precise formulation of the problem we are interested in and the main results we established are provided in Section 9.1. In Section 9.2 we quote some preliminary results, and the proof of our main theorem is executed in Section 9.3.

9.1. Introduction and statement

Let E be a rational elliptic curve and Q a rational point on E which we assume to be of infinite order in $\mathrm{E}(\mathbb{Q})$. We are interested in the asymptotic behaviour of

$$\sum_{p \le x, p \nmid N_{\mathrm{E}}} \mathrm{ord}_Q(\mathrm{E}_p)^\kappa,$$

the *κ-th moments of* $\mathrm{ord}_Q(\mathrm{E}_p)$ *over primes p of good reduction for* E. By the Lang-Trotter conjecture and the corresponding results over number fields (cf. Theorem 5.3) it is self-evident that $\mathrm{ord}_Q(\mathbb{F}_p)$ should be typically large and, in view of Hasse's theorem, we expect

$$\frac{1}{\pi(x)} \sum_{p \le x, p \nmid N_{\mathrm{E}}} \mathrm{ord}_Q(\mathrm{E}_p)^\kappa \sim c_{\mathrm{E},Q}^{(\kappa)} \cdot x^\kappa, \tag{9.1}$$

for any $\kappa \in \mathbb{R}_+$, with a positive constant $c_{\mathrm{E},Q}^{(\kappa)}$ depending on E, Q and κ. While we established the corresponding result in number fields under GRH, this problem is still open for elliptic curves. Its complexity may be ascribed to the non-cyclicity of $\mathrm{E}_p(\mathrm{E}_p)$ and the absence of strong prime number estimates especially in the non-CM case, the same obstacles which prevented a proof of the Lang-Trotter conjecture even under GRH. It is therefore reasonable to first study related problems which appear less involved but more promising.

In a recent paper Freiberg and Kurlberg [32] have investigated the average behaviour of the exponent $e_p d_p$ of $\mathrm{E}_p(\mathbb{F}_p)$, clearly an upper bound for $\mathrm{ord}_Q(\mathrm{E}_p)$, over primes

of good reduction for E. They proved

$$\sum_{p\le x, p\nmid N_{\mathrm{E}}} e_p d_p = b_{\mathrm{E}}\cdot \mathrm{li}(x^2) + O_{\mathrm{E}}\left(x^{19/10}(\log x)^{6/5}\right)$$

under GRH, and

$$\sum_{p\le x, p\nmid N_{\mathrm{E}}} e_p d_p = b_{\mathrm{E}}\cdot \mathrm{li}(x^2) + O_{\mathrm{E}}\left(x^2\frac{\log\log x}{(\log x)^{9/8}}\right)$$

unconditionally if E has CM, with a positive constant $b_{\mathrm{E}}\in(0,1)$ given by

$$b_{\mathrm{E}} := \sum_{k=1}^{\infty}\frac{(-1)^{\omega(k)}\varphi(\mathrm{rad}(k))}{[\mathbb{Q}(\mathrm{E}[k]):\mathbb{Q}]}.$$

In both cases the error terms have been improved later on by Kim [49] and Wu [106]. These results immediately yield an upper bound for the left side of (9.1) in case $\kappa = 1$. But even though we expect $\mathrm{ord}_Q(\mathrm{E}_p)$ to be close to $e_p d_p$ most of the time, the constant b_E may not be the best approximation to the expected constant $c^{(1)}_{\mathrm{E},Q}$.

In this chapter we therefore follow a different approach. Instead of comparing $\mathrm{ord}_Q(\mathrm{E}_p)$ to the exponent of $\mathrm{E}_p(\mathbb{F}_p)$, we compare it to the average of $\mathrm{ord}_Q(\mathrm{E}_p)$, as Q runs through the $\mathbb{F}_p$-rational points of E_p. More precisely, we are interested in the average behaviour of

$$\mathrm{Ord}^{\kappa}(\mathrm{E}_p) := \frac{1}{\sharp\,\mathrm{E}_p(\mathbb{F}_p)}\sum_{Q\in\mathrm{E}_p(\mathbb{F}_p)}\mathrm{ord}_Q(\mathrm{E}_p)^{\kappa}$$

as p ranges over primes of good reduction for E. Just as in Chapter 6 one may hope that this quantity yields a reasonable approximation to $\mathrm{ord}_Q(\mathrm{E}_p)^{\kappa}$ and possibly a more appropriate predictor for $\mathrm{ord}_Q(p)^{\kappa}$ than $(e_p d_p)^{\kappa}$. Adapting the methods introduced in Chapter 6 we establish the following asymptotic formulae for the average order of $\mathrm{Ord}^{\kappa}(\mathrm{E}_p)$.

Theorem 9.1. *Let* E *be a rational elliptic curve of conductor* N_{E} *and let* $\kappa\in\mathbb{R}_+$. *For any two integers* $m,n\in\mathbb{N}$ *we set*[27]

$$D(m,n) := \left\{\sigma\in\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[[m,n]])/\mathbb{Q}) : \sigma|_{\mathbb{Q}(\mathrm{E}[m])}\in D_m \text{ and } \sigma|_{\mathbb{Q}(\mathrm{E}[n])} = \mathrm{id}\right\},$$

with D_m *as defined in Lemma 8.3, and we define*

$$c^{(\kappa)}_{\mathrm{E}} := \sum_{f,n,d,e\ge 1}\frac{\mu(n)\mu(e)}{n(fd)^{1+\kappa}}\sum_{mk\mid d} m\mu(k)\cdot\frac{\sharp D(mkdnf,de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf,de]]):\mathbb{Q}]}.$$

This sum converges absolutely and we have the following asymptotic formulae:

(i) *If* E *is a non-CM curve and we assume GRH for the fields* $\mathbb{Q}(\mathrm{E}[n])$, $n\in\mathbb{N}$, *the constant* $c^{(\kappa)}_{\mathrm{E}}$ *is positive and we have*

$$\sum_{\substack{p\le x\\ p\nmid N_{\mathrm{E}}}}\mathrm{Ord}^{\kappa}(\mathrm{E}_p) = c^{(\kappa)}_{\mathrm{E}}\cdot\mathrm{li}(x^{1+\kappa}) + O\left(\frac{x^{1+\kappa}}{x^{\xi(k)-\varepsilon}}\right),$$

[27] By $\mathrm{E}[[m,n]]$ we mean the $[m,n]$-division field of E, where $[m,n]$ denotes the least common multiple of m and n. This notation will appear frequently throughout this chapter.

where the implied constant depends on κ, ε, N_{E} and a certain constant $B(\mathrm{E})$ (cf. Lemma 9.3), and the saving $\xi(\kappa)$ is given by

$$\xi(\kappa) := \begin{cases} 1/11, & \text{if } 11 < \kappa, \\ \kappa/(10\kappa+11), & \text{if } 5 < \kappa \leq 11, \\ \kappa/(9\kappa+16), & \text{if } 4/3 < \kappa \leq 5, \\ \kappa/(6\kappa+20), & \text{if } 0 < \kappa \leq 4/3. \end{cases}$$

(ii) *If E has CM by the ring of integers of an imaginary quadratic field $\mathbb{K}$, then $c_{\mathrm{E}}^{(\kappa)}$ is positive and we have*

$$\sum_{\substack{p \leq x \\ p \nmid N_{\mathrm{E}}}} \mathrm{Ord}^{\kappa}(\mathrm{E}_p) = c_{\mathrm{E}}^{(\kappa)} \cdot \mathrm{li}(x^{1+\kappa}) + O\left(\frac{x^{1+\kappa}}{(\log x)^{1+\eta(\kappa)-\varepsilon}}\right),$$

where the implied constant depends on κ, ε, N_{E} and a certain ideal $\mathfrak{f}$ of $\mathbb{K}$ (cf. Proposition 9.6), and the saving $\eta(\kappa)$ is given by

$$\eta(\kappa) := \frac{1}{8 + \frac{12\kappa+8}{\kappa^2+\kappa}}.$$

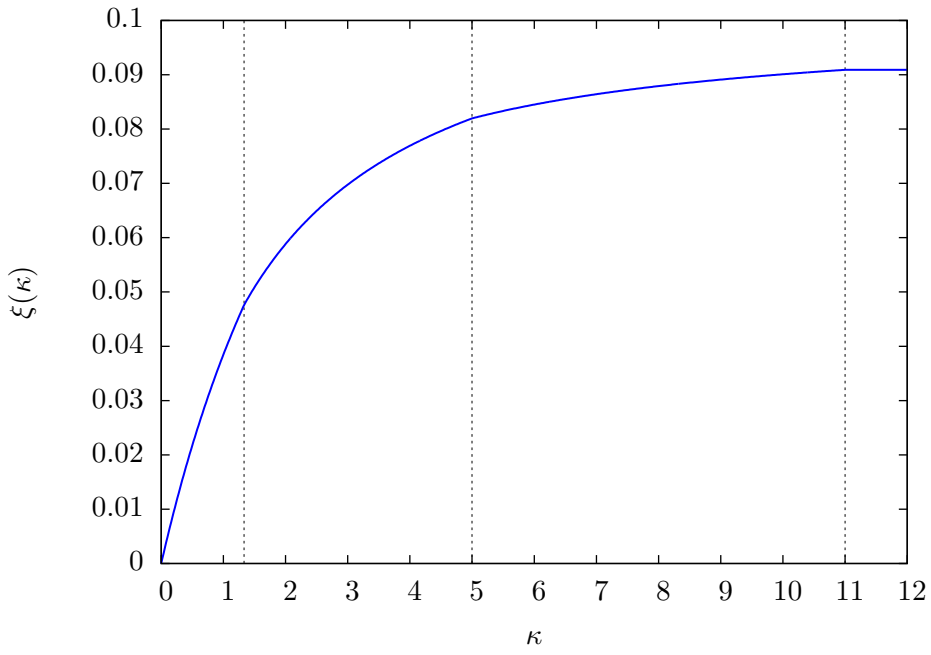


FIGURE 9.1. Plot of the saving $\xi(\kappa)$ from Theorem 9.1 (i).

REMARK 9.2. In both cases we were not able to prove the positivity of $c_{\mathrm{E}}^{(\kappa)}$ straight from its definition. This is due to the alternating nature of the defining sum and lack of information concerning the involved field degrees, a problem we did not manage to overcome. Nevertheless, we circumvented this problem and proved the positivity of $c_{\mathrm{E}}^{(\kappa)}$ in the respective cases by methods that are similar to those which enabled us to establish the positivity of $c_{\Gamma,C}^{(\kappa)}$ under GRH in Chapter 5. We come back to this in Section 9.3.3.

Theorem 9.1 nicely illustrates the phenomenon which we already encountered in Section 2.4: While we need to assume the GRH in the non-CM case, the asymptotic formula asserted in Theorem 9.1 holds unconditionally, if E has CM by the ring of integers of an imaginary quadratic field. This is due to number field analogues of the Brun-Titchmarsh inequality for the sizes of certain families of primes which are only available in the non-CM case. We present the corresponding statements in the subsequent section. These estimates allow for an application of the unconditional effective Čebotarev density theorem.

Moreover, it is notable that the GRH in Theorem 9.1 (i) may be replaced by a quasi δ-GRH (see Section 2.4) for any $\delta \in [1/2, 1)$ which in turn results in a larger error term. Also, it is possible to improve the aforesaid error term if one even assumes the GRH for Artin L-functions, for this, as first observed by Serre, results in sharper error terms for effective versions of the Čebotarev density theorem. For details, we refer to [19].

9.2. Tools for prime number estimates

Before proceeding with the proof of Theorem 9.1, it is necessary to provide additional information concerning rational elliptic curves and their reductions modulo p. Let E be a rational elliptic curve of conductor N_{E}. We will frequently need to count primes $p \leq x$ of good reduction for E for which d_p or $\sharp \mathrm{E}_p(\mathbb{F}_p)$ are divisible by a given integer $k \in \mathbb{N}$. In Section 8.2 (cf. Lemmas 8.2 and 8.3) we learned that these primes are exactly the ones counted by $\pi_{\mathrm{id}}(x, \mathbb{Q}(\mathrm{E}[k])/\mathbb{Q})$ and $\pi_{D_k}(x, \mathbb{Q}(\mathrm{E}[k])/\mathbb{Q})$, respectively. Hence, questions of this kind may be handled by effective version of the Čebotarev density theorem and therefore, we need estimates for the corresponding prime densities $1/[\mathbb{Q}(\mathrm{E}[k]) : \mathbb{Q}]$ and $\sharp D_k/[\mathbb{Q}(\mathrm{E}[k]) : \mathbb{Q}]$. To deal with the first problem one may utilize the Galois representation ϕ_k associated to $\mathrm{E}[k]$. Since ϕ_k is injective, asking for the size of $[\mathbb{Q}(\mathrm{E}[k]) : \mathbb{Q}]$ amounts to estimating the size of the image of ϕ_k. The following lemma (cf. [17, 32]) gives a precise account of this question.

Lemma 9.3. *Let* E *be a rational elliptic curve.*

(i) *If* E *has CM by the ring of integers of an imaginary quadratic field, and* $k > 2$*, then* ϕ_k *is not surjective, and we have*

$$\varphi(k)^2 \leq [\mathbb{Q}(\mathrm{E}[k]) : \mathbb{Q}] \leq k^2.$$

(ii) *If* E *is without CM, then there exists a positive integer* $A(\mathrm{E})$ *depending on* E *such that* ϕ_k *is surjective for all* $k \in \mathbb{N}$ *coprime to* $A(\mathrm{E})$ *in which case we have*

$$[\mathbb{Q}(\mathrm{E}[k]) : \mathbb{Q}] = \sharp \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}) = k^4 \prod_{q \mid k} \left(1 - \frac{1}{q}\right)\left(1 - \frac{1}{q^2}\right),$$

where the product runs over prime divisors of k*. For arbitrary* $k \in \mathbb{N}$*, there exists a constant* $B(\mathrm{E}) \geq 1$ *depending on* E*, such that*

$$\sharp \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z})/B(\mathrm{E}) \leq [\mathbb{Q}(\mathrm{E}[k]) : \mathbb{Q}] \leq \sharp \mathrm{GL}_2(\mathbb{Z}/k\mathbb{Z}).$$

Estimates for $\sharp D_k$ and $\sharp D_k/[\mathbb{Q}(\mathrm{E}[k]) : \mathbb{Q}]$ are given by the following lemma. These estimates are not as precise as they could be, but suffice for our purposes. To obtain sharp upper bounds, one needs to count matrices in $\mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z})$ with eigenvalue 1.

Lemma 9.4. *Let* E *be a rational elliptic curve and* $k \in \mathbb{N}$*. Then we have*

$$\frac{\sharp D_k}{[\mathbb{Q}(\mathrm{E}[k]) : \mathbb{Q}]} \ll_\varepsilon \frac{1}{k^{1-\varepsilon}}.$$

If E *is a non-CM curve, then*

$$\sharp D_k \ll_\varepsilon m^{3+\varepsilon},$$

and if E *has CM by the ring of integers of an imaginary quadratic field, then*

$$\sharp D_k \ll_\varepsilon m^{1+\varepsilon}.$$

PROOF. In the non-CM case, the estimate for $\frac{\sharp D_k}{[\mathbb{Q}(\mathrm{E}[k]):\mathbb{Q}]}$ is an immediate consequence of Proposition 10 of [19], Lemma 9.3 and Mertens' formula. In the CM case, the estimate follows by the same arguments, and the fact that the density of primes p of supersingular reduction for E for which $k \mid \mathrm{E}_p(\mathbb{F}_p)$ holds is bounded from above by $1/\varphi(k)$ by DIRICHLET's prime number theorem for primes in arithmetic progression. The estimates for $\sharp D_k$ then follow immediately from Lemma 9.3. □

Finally, we provide some results which are quite useful to estimate $\pi_{\mathrm{id}}(x, \mathbb{Q}(\mathrm{E}[k])/\mathbb{Q})$ and $\pi_{D_k}(x, \mathbb{Q}(\mathrm{E}[k])/\mathbb{Q})$, if the (unconditional) effective Čebotarev density theorem does not apply. The following two statements deal with upper bounds for $\pi_{\mathrm{id}}(x, \mathbb{Q}(\mathrm{E}[k])/\mathbb{Q})$. The first of these was proved by COJOCARU using a sieve argument and may be found in [49]. The second estimate applies only in the CM case and is based on a number field analogue of the Brun-Titchmarsh inequality due to HINZ and LODEMANN [41]. We omit the details concerning class field theory and simply state the form in which we apply it.

PROPOSITION 9.5. *Let* E *be a rational elliptic curve of conductor* N_{E}*. Then, for any* $2 \le k \le 2\sqrt{x}$ *we have*

$$\pi_{\mathrm{id}}(x, \mathbb{Q}(\mathrm{E}[k])/\mathbb{Q}) \ll \frac{x}{k^2},$$

where the implied constant is absolute.

PROPOSITION 9.6. *Let* E *be a rational elliptic curve of conductor* N_{E} *with CM by the ring of integers of an imaginary quadratic field* $\mathbb{K}$*. Then there exists an ideal* $\mathfrak{f}$ *of* $\mathcal{O}_{\mathbb{K}}$*, such that*

$$\pi_{\mathrm{id}}(x, \mathbb{Q}(\mathrm{E}[k])/\mathbb{Q}) \ll_{N_{\mathrm{E}}} \frac{x}{[\mathbb{Q}(\mathrm{E}[k]):\mathbb{Q}] \log\left(\frac{x}{\mathrm{N}_{\mathbb{K}/\mathbb{Q}}(k\mathfrak{f})}\right)}$$

holds, whenever $1 \le k < x^{1/4}$.

PROOF. The estimate immediately follows from equations (13) and (19), and Lemmas 2.4 and 2.5 of [49]. □

As for an upper bound for $\pi_{D_k}(x, \mathbb{Q}(\mathrm{E}[k])/\mathbb{Q})$, a convenient estimate is given by Proposition 9.7. Again this statement only applies if E has CM by the ring of integers of an imaginary quadratic field $\mathbb{K}$, for in this case one can translate the property $k \mid \sharp \mathrm{E}_p(\mathbb{F}_p)$ into an appropriate splitting condition for p in $\mathbb{K}$. It builds on a number field analogue of the Brun-Titchmarsh inequality due to SCHAAL (cf. Proposition 18 of [19]).

PROPOSITION 9.7. *Let* E *be a rational elliptic curve with CM by the ring of integers of an imaginary quadratic field. For any* $k \le (x/\log x)^{1/2}$*, we then have*

$$\pi_{D_k}(x, \mathbb{Q}(\mathrm{E}[k])/\mathbb{Q}) \ll \frac{\tau(k)}{\varphi(k)} \cdot \frac{x}{\log x},$$

where the implied constant is absolute.

PROOF. The result may be obtained by extending Proposition 19 in [19]. Even though this result only deals with primes of ordinary reduction for E, it remains true for all primes, since the primes p of supersingular reduction for E for which $k \mid \mathrm{E}_p(\mathbb{F}_p)$ holds satisfy $p \equiv -1 \ (k)$, and may be treated by the Brun-Titchmarsh inequality. □

9.3. Proof of Theorem 9.1

We proceed with the proof of Theorem 9.1 which we divide into three parts. We start with a proof of the asymptotic formulae in Sections 9.3.1 and 9.3.2, first in the non-CM case and afterwards in the case where E has CM by the ring of integers of an imaginary quadratic field. Finally, in Section 9.3.3 we establish the positivity of the asymptotic constant $c_{\mathrm{E}}^{(\kappa)}$ in the respective cases.

9.3.1. Proof of the asymptotic formula - the non-CM case. Assume that E is a non-CM curve. Without any further notice, the letter p will always refer to a prime of good reduction for E, for notational convenience. By Hasse's theorem, (8.3), Lemma 6.7 and a simple change of summation order, we obtain

$$\sum_{p\le x}\frac{\mathrm{Ord}^{\kappa}(\mathrm{E}_p)}{(\sharp\,\mathrm{E}_p(\mathbb{F}_p))^{\kappa}}=\sum_{f\le 2x}\frac{1}{f^{1+\kappa}}\sum_{\substack{p\le x\\ f\mid d_pe_p}}\frac{1}{d_p^{1+\kappa}}\sum_{n\mid \frac{d_pe_p}{f}}\frac{\mu(n)}{n}\left(\frac{d_pe_p}{nf},d_p\right). \tag{9.2}$$

Next we eliminate terms with large values of f and n, respectively. To this end, let $0<y_1,y_2\le x^{1/4}$ be some parameters which will be specified later. Swapping the roles of n and $\frac{d_pe_p}{nf}$ in the inner sum of (9.2), the contribution of terms in (9.2) with $f>y_1$ is clearly bounded from above by

$$\begin{aligned}\sum_{y_1<f}\frac{1}{f^{\kappa}}\sum_{\substack{p\le x\\ f\mid d_pe_p}}\frac{1}{d_p^{2+\kappa}e_p}\sum_{n\mid\frac{d_pe_p}{f}}n\,(n,d_p)&\le\sum_{y_1<f}\frac{1}{f^{\kappa}}\sum_{p\le x}\frac{1}{d_p^{1+\kappa}e_p}\sigma\left(\frac{d_pe_p}{f}\right)\\&\ll\log\log x\sum_{y_1<f}\frac{1}{f^{1+\kappa}}\sum_{p\le x}\frac{1}{d_p^{\kappa}}\ll_{\kappa}\frac{x\log\log x}{y_1^{\kappa}\log x}\end{aligned}$$

by the prime number theorem, Hasse's theorem, and well-known estimates for the divisor sum function (cf. [100, p. 85f]). Again by Hasse's theorem and common estimates for the divisor function (cf. [100, p. 81f]), the contribution of the terms with $n>y_2$ in (9.2) is less than

$$\frac{1}{y_2}\sum_{f\ge 1}\frac{1}{f^{1+\kappa}}\sum_{p\le x}\frac{\tau(e_pd_p)}{d_p^{\kappa}}\ll_{\kappa}\frac{1}{y_2}\sum_{p\le x}\tau(e_p)\ll_{\varepsilon}\frac{x^{1+\varepsilon}}{y_2}.$$

Hence we obtain

$$\sum_{p\le x}\frac{\mathrm{Ord}^{\kappa}(\mathrm{E}_p)}{(\sharp\,\mathrm{E}_p(\mathbb{F}_p))^{\kappa}}=\sum_{f\le y_1}\frac{1}{f^{1+\kappa}}\sum_{n\le y_2}\frac{\mu(n)}{n}\sum_{\substack{p\le x\\ nf\mid d_pe_p}}\frac{\left(\frac{d_pe_p}{nf},d_p\right)}{d_p^{1+\kappa}}+O_{\kappa,\varepsilon}\left(\frac{x\log\log x}{y_1^{\kappa}\log x}+\frac{x^{1+\varepsilon}}{y_2}\right). \tag{9.3}$$

As a next step we collect primes which give rise to the same value for d_p. By Hasse's theorem and (8.3), the main part of the right side of (9.3) then becomes

$$\sum_{f\le y_1}\frac{1}{f^{1+\kappa}}\sum_{n\le y_2}\frac{\mu(n)}{n}\sum_{d\le 2\sqrt{x}}\frac{1}{d^{1+\kappa}}\sum_{\substack{p\le x\\ dnf\mid\sharp\,\mathrm{E}_p(\mathbb{F}_p)\\ d_p=d}}\left(\frac{\sharp\,\mathrm{E}_p(\mathbb{F}_p)}{dnf},d\right).$$

The terms with large d in this expression are negligible, too. To see this, we recall that the d-division field $\mathbb{Q}(\mathrm{E}[d])$ always contains the d-th roots of unity. Hence, the condition $d\mid d_p$ implies that $p-1$ is divisible by d. Thus, by Lemma 8.2, the Brun-Titchmarsh

inequality and Lemma 4.5, the contribution of terms with $d > y_3$, where $0 < y_3 \le x^{1/4}$ is another parameter, is bounded from above by

$$\begin{aligned}(9.4)\qquad \sum_{f\le y_1}\frac{1}{f^{1+\kappa}}\sum_{n\le y_2}\frac{1}{n}\sum_{2\sqrt{x}\ge d>y_3}\frac{1}{d^\kappa}\sum_{\substack{p\le x\\ dnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ d=d_p}} 1 &\ll_\kappa \sum_{n\le y_2}\frac{1}{n}\sum_{2\sqrt{x}\ge d>y_3}\frac{1}{d^\kappa}\sum_{\substack{p\le x\\ d\mid d_p}}1\\ &\ll \frac{x}{\log x}\sum_{n\le y_2}\frac{1}{n}\sum_{d>y_3}\frac{1}{d^\kappa\varphi(d)}\\ &\ll_\kappa \frac{x\log y_2}{y_3^\kappa\log x}.\end{aligned}$$

From the inclusion-exclusion principle and Hasse's theorem we now infer the identity

$$\sum_{d\le y_3}\frac{1}{d^{1+\kappa}}\sum_{\substack{p\le x\\ dnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ d_p=d}}\left(\frac{\sharp \mathrm{E}_p(\mathbb{F}_p)}{dnf},d\right)=\sum_{d\le y_3}\frac{1}{d^{1+\kappa}}\sum_{e\le 2\sqrt{x}}\mu(e)\sum_{\substack{p\le x\\ dnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ de\mid d_p}}\left(\frac{\sharp \mathrm{E}_p(\mathbb{F}_p)}{dnf},d\right).$$

To enable an application of Lemmas 8.2 and 8.3 combined with the effective Čebotarev density theorem under GRH (Proposition 4.7), we must eliminate terms with large e as well. Let therefore $0 < y_4 < x^{1/4}$ be yet another parameter. Then Proposition 9.5 yields

$$\sum_{d\le y_3}\frac{1}{d^{1+\kappa}}\sum_{y_4<e\le 2\sqrt{x}}\mu(e)\sum_{\substack{p\le x\\ dnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ de\mid d_p}}\left(\frac{\sharp \mathrm{E}_p(\mathbb{F}_p)}{dnf},d\right)\ll x\sum_{d\le y_3}\frac{1}{d^{2+\kappa}}\sum_{e>y_4}\frac{1}{e^2}\ll\frac{x}{y_4},$$

and hence

$$(9.5)\qquad \sum_{f\le y_1}\frac{1}{f^{1+\kappa}}\sum_{n\le y_2}\frac{1}{n}\sum_{d\le y_3}\frac{1}{d^{1+\kappa}}\sum_{y_4<e\le 2\sqrt{x}}\mu(e)\sum_{\substack{p\le x\\ dnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ de\mid d_p}}\left(\frac{\sharp \mathrm{E}_p(\mathbb{F}_p)}{dnf},d\right)\ll_\kappa\frac{x\log y_2}{y_4}.$$

To get rid of the gcd-term inside the p-summation, we utilize the Möbius inversion formula to obtain

$$(9.6)\qquad \sum_{\substack{p\le x\\ dnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ de\mid d_p}}\left(\frac{\sharp \mathrm{E}_p(\mathbb{F}_p)}{dnf},d\right)=\sum_{m\mid d}m\sum_{\substack{p\le x\\ dnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ de\mid d_p\\ m=\left(\frac{\sharp \mathrm{E}_p(\mathbb{F}_p)}{dnf},d\right)}}1=\sum_{m\mid d}m\sum_{k\mid\frac{d}{m}}\mu(k)\sum_{\substack{p\le x\\ kmdnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ de\mid d_p}}1.$$

Eventually, combining (9.3) with (9.4), (9.5) and (9.6), we obtain

$$\begin{aligned}(9.7)\qquad \sum_{p\le x}\frac{\mathrm{Ord}^\kappa(\mathrm{E}_p)}{(\sharp \mathrm{E}_p(\mathbb{F}_p))^\kappa} &= \sum_{\substack{f\le y_1,n\le y_2\\ d\le y_3,e\le y_4}}\frac{\mu(n)\mu(e)}{n(fd)^{1+\kappa}}\sum_{mk\mid d}m\mu(k)\sum_{\substack{p\le x\\ mkdnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ de\mid d_p}}1\\ &\quad+O_{\varepsilon,\kappa}\left(\frac{x\log\log x}{y_1^\kappa\log x}+\frac{x^{1+\varepsilon}}{y_2}+\frac{x\log y_2}{y_3^\kappa\log x}+\frac{x\log y_2}{y_4}\right).\end{aligned}$$

To be in the position of evaluating the sum over p in (9.7), we need to translate the summation conditions in a way to make effective versions of the Čebotarev density theorem

applicable. In this regard we prove the following lemma beforehand which also applies to CM curves.

LEMMA 9.8. *Let* E *be a rational elliptic curve and* $r, s \in \mathbb{N}$. *Then we have*

$$\mathbb{Q}(\mathrm{E}[[r,s]]) = \mathbb{Q}(\mathrm{E}[r]) \cdot \mathbb{Q}(\mathrm{E}[s]).$$

Further, $D(r,s)$ *is a union of conjugacy classes in* $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[[r,s]])/\mathbb{Q})$, *and we have:*

(i) *Recall that* $\|D_r\|$ *denotes the number of conjugacy classes inside* D_r. *Then*[28]

$$\|D_r\| \leq 2r$$

if E *is without CM, and*

$$\|D_r\| \ll_\varepsilon r^{1+\varepsilon}$$

if E *has CM by the ring of integers of an imaginary quadratic field.*

(ii) $\sharp D(r,s) \leq \sharp D_r$ *and* $\|D(r,s)\| \leq \|D_r\|$.

(iii) *For any prime* $p \nmid rs$ *of good reduction for* E, *we have the equivalence*

$$\left[\frac{\mathbb{Q}(\mathrm{E}[r]) \mid \mathbb{Q}}{p}\right] \subset D_r \text{ and } \left[\frac{\mathbb{Q}(\mathrm{E}[s]) \mid \mathbb{Q}}{p}\right] = \mathrm{id} \Longleftrightarrow \left[\frac{\mathbb{Q}(\mathrm{E}[[r,s]]) \mid \mathbb{Q}}{p}\right] \subset D(r,s).$$

(iv) *For any divisors* k *and* l *of* r *and* s, *respectively, we have*

$$\frac{\sharp D(k,l)}{[Q(\mathrm{E}[[k,l]]) : \mathbb{Q}]} \geq \frac{\sharp D(r,s)}{[Q(\mathrm{E}[[r,s]]) : \mathbb{Q}]}.$$

PROOF. Clearly, $D(r,s)$ is a union of conjugacy classes and $\mathbb{Q}(\mathrm{E}[[r,s]])$ contains the composite field $\mathbb{Q}(\mathrm{E}[r]) \cdot \mathbb{Q}(\mathrm{E}[s])$. As for the other inclusion, it obviously suffices to show $\mathbb{Q}(\mathrm{E}[rs]) \subset \mathbb{Q}(\mathrm{E}[r]) \cdot \mathbb{Q}(\mathrm{E}[s])$ if r and s are coprime. In this case we have $\mathrm{E}[rs] = \mathrm{E}[r] \oplus \mathrm{E}[s]$. Hence, any point $P \in \mathrm{E}[rs]$ may be written as $P = P_r + P_s$ with $P_r \in \mathrm{E}[r]$ and $P_s \in \mathrm{E}[s]$. Since the coordinates of P are given by rational functions in the coordinates of P_r and P_s, P must be contained in the composite field $\mathbb{Q}(\mathrm{E}[r]) \cdot \mathbb{Q}(\mathrm{E}[s])$.

Let us turn to (i). By the trivial estimate $\|D_r\| \leq \sharp D_r$ we obtain $\|D_r\| \ll_\varepsilon r^{1+\varepsilon}$ in the CM case by Lemma 9.4. Since in this case $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[r])/\mathbb{Q})$ is abelian for $(r, 6N_{\mathrm{E}}) = 1$ (cf. Proposition 9 of [19]) it is hard to improve on this estimate. Now assume that E is without CM. Then we may identify $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[r])/\mathbb{Q})$ with a subgroup of $\mathrm{GL}_2(\mathbb{Z}/r\mathbb{Z})$ and it suffices to consider matrices in $\mathrm{GL}_2(\mathbb{Z}/r\mathbb{Z})$ which have 1 as an eigenvalue (cf. Lemma 8.3). If A is such a matrix, then the characteristic polynomial of A factors into linear polynomials over $\mathbb{Z}/r\mathbb{Z}$ and we denote the second eigenvalue of A by λ. Note that $\lambda \in (\mathbb{Z}/r\mathbb{Z})^*$ because A is invertible. If $\lambda \not\equiv 1 \ (r)$, then A is conjugated to the diagonal matrix with diagonal entries 1 and λ (cf. Section 29 of [102]). If $\lambda \equiv 1 \ (r)$, then A is conjugated to a matrix $\begin{pmatrix} 1 & x \\ 0 & 1 \end{pmatrix}$ for some $x \in \mathbb{Z}/r\mathbb{Z}$ (cf. Section 29 of [102]). Hence, we find $\|D_r\| \leq \varphi(r) + r \leq 2r$.

To prove (ii), one essentially proceeds as in the proof of Lemma 5.5. If $D(r,s)$ is empty, we are done. If $D(r,s)$ contains a conjugacy class of some isomorphism σ, then $\tau\sigma\tau^{-1}|_{\mathbb{Q}(\mathrm{E}[r])}$ runs through the conjugacy class of $\sigma|_{\mathbb{Q}(\mathrm{E}[r])}$ inside D_r as τ runs through $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[[r,s]])/\mathbb{Q})$. On the other hand, the restriction map $D(r,s) \to D_r$ is injective because $\mathbb{Q}(\mathrm{E}[[r,s]])$ is the composite field of $\mathbb{Q}(\mathrm{E}[r])$ and $\mathbb{Q}(\mathrm{E}[s])$. Hence, the respective conjugacy classes of σ and $\sigma|_{\mathbb{Q}(\mathrm{E}[r])}$ are of the same size. In this way we obtain an injective mapping between the conjugacy classes of $D(r,s)$ and the ones inside D_r which preserves cardinality and thereby proves (ii).

[28] Again, the upper bounds for $\|D_r\|$ are not sharp, but we don't need the precision.

Statement (iii) easily follows by elementary properties of Frobenius symbols (cf. e.g. Chapter 7 in [68]).

Assertion (iv) follows by the Čebotarev density theorem. Indeed, for any two divisors k of r and l of s we have $k \mid \mathrm{E}_p(\mathbb{F}_p)$ and $l \mid d_p$, whenever $r \mid \mathrm{E}_p(\mathbb{F}_p)$ and $s \mid d_p$. The set of primes with the latter property is therefore contained in the set of primes with the first property. The assertion then follows by (iii), the Čebotarev density theorem and Lemmas 8.2 and 8.3. □

Let us now assume GRH[29] for the fields $\mathbb{Q}(\mathrm{E}[n])$, $n \in \mathbb{N}$, and apply the effective Čebotarev density theorem (Proposition 4.7) to the sum over p in (9.7). By Lemma 8.3, Proposition 4.11, and 9.3, the estimate

$$\log \Delta_{\mathbb{Q}(\mathrm{E}[k])} \le [\mathbb{Q}(\mathrm{E}[k]) : \mathbb{Q}] \Big(\log(k^4) + \sum_{p \mid k N_{\mathrm{E}}} \log p \Big) \le [\mathbb{Q}(\mathrm{E}[k]) : \mathbb{Q}] \log(k^5 N_{\mathrm{E}})$$

holds for any positive integer k. Thus, for any $r, s \in \mathbb{N}$, Proposition 4.7, Hasse's theorem and Lemma 9.8 yield

$$\begin{aligned} (9.8) \qquad & \Big(\sum_{\substack{p \le x, s \mid d_p \\ r \mid \sharp \mathrm{E}_p(\mathbb{F}_p)}} 1 \Big) - \frac{\sharp D(r,s)}{[\mathbb{Q}(\mathrm{E}[[r,s]]) : \mathbb{Q}]} \cdot \mathrm{li}(x) \\ & \ll \sharp D_r \cdot x^{1/2} \log\left([r,s] N_{\mathrm{E}} x\right) + \|D_r\| [r,s]^4 \log([r,s] N_{\mathrm{E}}) \\ & \ll_{\varepsilon, N_{\mathrm{E}}} r^3 x^{\frac{1}{2}+\varepsilon} + x^{\varepsilon} r [r,s]^4. \end{aligned}$$

Inserting (9.8) into (9.7), the main term in (9.7) becomes

$$(9.9) \qquad \mathrm{li}(x) \sum_{\substack{f \le y_1, n \le y_2 \\ d \le y_3, e \le y_4}} \frac{\mu(n)\mu(e)}{n (df)^{1+\kappa}} \sum_{mk \mid d} m \mu(k) \cdot \frac{\sharp D(mkdnf, de)}{[\mathbb{Q}(\mathrm{E}[mkdnf, de]) : \mathbb{Q}]} + E_1 + E_2,$$

with error terms E_1 and E_2 corresponding to the two summands in the last line of (9.8). These error terms satisfy[30]

$$\begin{aligned} E_1 &\ll_{\varepsilon, N_{\mathrm{E}}} x^{\frac{1}{2}+\varepsilon} \sum_{f \le y_1} f^{2-\kappa} \sum_{n \le y_2} n^2 \sum_{d \le y_3} d^{2-\kappa} \sum_{e \le y_4} \sum_{m \mid d} m^4 \sum_{k \mid \frac{d}{m}} k^3 \\ &\ll_{\varepsilon, N_{\mathrm{E}}} x^{\frac{1}{2}+\varepsilon} \max\{y_1^{3-\kappa}, 1\} y_2^3 y_4 \max\{y_3^{7-\kappa}, 1\} \end{aligned}$$

and

$$\begin{aligned} E_2 &\ll_{\varepsilon, N_{\mathrm{E}}} x^{\varepsilon} \sum_{f \le y_1} f^{4-\kappa} \sum_{n \le y_2} n^4 \sum_{d \le y_3} d^{4-\kappa} \sum_{e \le y_4} e^4 \sum_{m \mid d} m^6 \sum_{k \mid \frac{d}{m}} k^5 \\ &\ll_{\varepsilon, N_{\mathrm{E}}} x^{\varepsilon} \max\{y_1^{5-\kappa}, 1\} y_2^5 y_4^5 \max\{y_3^{11-\kappa}, 1\}. \end{aligned}$$

by common estimates for divisor sum functions (cf. [100, p. 85f]).

To complete the proof of the asserted asymptotic formula in Theorem 9.1 (i) it remains to show that the summation ranges for f, d, e and n in (9.9) may be extended to all positive integers, respectively, and estimate the corresponding error terms which are

[29] The necessity to assume GRH comes from the large error terms in (9.7) which prevent us from choosing the y_i small powers of $\log x$ to enable an application of the unconditional Proposition 4.8. In the CM case we will see how to overcome this problem by Propositions 9.6 and 9.7.

[30] All occurring log-terms are absorbed by the x^{ε}.

caused. Hereby, we also prove the absolute convergence of the sum in (9.9). To deal with large f, d and e we note the estimate

$$\frac{\sharp D(r,s)}{\mathbb{Q}(\mathrm{E}[[r,s]]):\mathbb{Q}]} \leq \frac{1}{[\mathbb{Q}(\mathrm{E}[s]):\mathbb{Q}]} \ll_{B(\mathrm{E})} \frac{\log s}{s^4},$$

which may easily be deduced from Lemma 9.3, Mertens' formula, and by choosing $k=1$ and $l=s$ in Lemma 9.8 (iv). The constant $B(\mathrm{E})$ is as defined in Lemma 9.3. An invocation of this estimate and estimates for divisor functions (cf. [100, p. 81f]) yields

$$\begin{aligned}&\sum_{f>y_1}\frac{1}{f^{1+\kappa}}\sum_{n\leq y_2}\frac{\mu(n)}{n}\sum_{d\leq y_3}\frac{1}{d^{1+\kappa}}\sum_{e\leq y_4}\mu(e)\sum_{mk|d}m\mu(k)\cdot\frac{\sharp D(mkdnf,de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf,de]]):\mathbb{Q}]}\\ \ll_{B(\mathrm{E})}&\sum_{f>y_1}\frac{1}{f^{1+\kappa}}\sum_{n\leq y_2}\frac{1}{n}\sum_{d\leq y_3}\frac{1}{d^{1+\kappa}}\sum_{e\leq y_4}1\sum_{mk|d}m\cdot\frac{\log(de)}{(de)^4}\ll_\kappa\frac{\log y_2}{y_1^\kappa},\end{aligned}$$

and

$$\begin{aligned}&\sum_{f\geq 1}\frac{1}{f^{1+\kappa}}\sum_{n\leq y_2}\frac{\mu(n)}{n}\sum_{d>y_3}\frac{1}{d^{1+\kappa}}\sum_{e\leq y_4}\mu(e)\sum_{mk|d}m\mu(k)\cdot\frac{\sharp D(mkdnf,de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf,de]]):\mathbb{Q}]}\\ \ll_{B(\mathrm{E})}&\sum_{f\geq 1}\frac{1}{f^{1+\kappa}}\sum_{n\leq y_2}\frac{1}{n}\sum_{d>y_3}\frac{1}{d^{1+\kappa}}\sum_{e\leq y_4}1\sum_{mk|d}m\cdot\frac{\log(de)}{(de)^4}\ll_{\kappa,\varepsilon}\frac{\log y_2}{y_3^{3+\kappa-\varepsilon}},\end{aligned}$$

and

$$\begin{aligned}&\sum_{f\geq 1}\frac{1}{f^{1+\kappa}}\sum_{n\leq y_2}\frac{\mu(n)}{n}\sum_{d\geq 1}\frac{1}{d^{1+\kappa}}\sum_{e>y_4}\mu(e)\sum_{mk|d}m\mu(k)\cdot\frac{\sharp D(mkdnf,de)}{[\mathbb{Q}([[mkdnf,de]]):\mathbb{Q}]}\\ \ll_{B(\mathrm{E})}&\sum_{f\geq 1}\frac{1}{f^{1+\kappa}}\sum_{n\leq y_2}\frac{1}{n}\sum_{d\geq 1}\frac{1}{d^{1+\kappa}}\sum_{e>y_4}1\sum_{mk|d}m\cdot\frac{\log(de)}{(de)^4}\ll_{\kappa,\varepsilon}\frac{\log y_2}{y_4^{3-\varepsilon}}.\end{aligned}$$

Finally, to extend the summation range of n to $\mathbb{N}$, we observe

$$\frac{\sharp D(r,s)}{[\mathbb{Q}(\mathrm{E}[[r,s]]):\mathbb{Q}]}\leq\frac{\sharp D_r}{[\mathbb{Q}(\mathrm{E}[[r,s]]):\mathbb{Q}]}\ll_{\varepsilon,B(\mathrm{E})}\frac{r^3}{[r,s]^{4-\varepsilon}},$$

again by Lemma 9.3 and Lemma 9.8 (ii). Hence, by Lemma 9.8 (iv) we obtain

$$\begin{aligned}&\sum_{f\geq 1}\frac{1}{f^{1+\kappa}}\sum_{n>y_2}\frac{\mu(n)}{n}\sum_{d\geq 1}\frac{1}{d^{1+\kappa}}\sum_{e\geq 1}\mu(e)\sum_{mk|d}m\mu(k)\cdot\frac{\sharp D(mkdnf,de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf,de]]):\mathbb{Q}]}\\ &\ll_{\kappa,\varepsilon,B(\mathrm{E})}\sum_{n>y_2}n^2\sum_{d\geq 1}\frac{1}{d^{\kappa-\varepsilon}}\sum_{e\geq 1}\frac{1}{[n,de]^{4-\varepsilon}}\\ &\ll_{\kappa,\varepsilon}\sum_{n>y_2}\frac{1}{n^{2-\varepsilon}}\sum_{c|n}c^{4-\varepsilon}\sum_{\substack{d,e\geq 1\\ c|de}}\frac{1}{(de)^{4-\varepsilon}}=\sum_{n>y_2}\frac{1}{n^{2-\varepsilon}}\sum_{c|n}c^{4-\varepsilon}\sum_{\substack{m\geq 1\\ c|m}}\frac{\tau(m)}{m^{4-\varepsilon}}\\ &\ll_\varepsilon\sum_{n>y_2}\frac{1}{n^{2-\varepsilon}}\sum_{c|n}c^\varepsilon\ll_\varepsilon\frac{1}{y_2^{1-\varepsilon}}.\end{aligned}$$

Collecting error terms, we eventually find

$$\sum_{p\leq x}\frac{\mathrm{Ord}^\kappa(\mathrm{E}_p)}{(\sharp\,\mathrm{E}_p(\mathbb{F}_p))^\kappa}=c_{\mathrm{E}}^{(\kappa)}\cdot\mathrm{li}(x)+E,$$

where the constant $c_{\mathrm{E}}^{(\kappa)}$ is given by

$$c_{\mathrm{E}}^{(\kappa)} := \sum_{f,n,d,e\geq 1} \frac{\mu(n)\mu(e)}{n(fd)^{1+\kappa}} \sum_{mk|d} m\mu(k) \cdot \frac{\sharp D(mkdnf, de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf, de]]) : \mathbb{Q}]}$$

and

(9.10)

$$\begin{aligned} E \ll{}& \frac{x\log\log x}{y_1^{\kappa}\log x} + \frac{x^{1+\varepsilon}}{y_2} + \frac{x\log y_2}{y_3^{\kappa}\log x} + \frac{x\log y_2}{y_4} \\ &+ x^{\frac{1}{2}+\varepsilon}\max\{y_1^{3-\kappa},1\}y_2^3y_4\max\{y_3^{7-\kappa},1\} + x^{\varepsilon}\max\{y_1^{5-\kappa},1\}y_2^5y_4^5\max\{y_3^{11-\kappa},1\} \\ &+ \frac{x\log y_2}{y_1^{\kappa}\log x} + \frac{x\log y_2}{y_3^{3+\kappa-\varepsilon}\log x} + \frac{x\log y_2}{y_4^{3-\varepsilon}\log x} + \frac{x}{y_2^{1-\varepsilon}\log x} \end{aligned}$$

with an implied constant depending on ε, κ, N_{E} and $B(\mathrm{E})$. Numerical data suggests that E becomes as small as possible if y_1^{κ}, y_2, y_3^{κ} and y_4 are, up to a factor $O(x^{\varepsilon})$, chosen identical powers of x, say $y_2 = x^{\xi(\kappa)-\varepsilon}$. An easy exercise then provides the choice

$$\xi(\kappa) := \begin{cases} 1/11, & \text{if } 11 < \kappa, \\ \kappa/(10\kappa+11), & \text{if } 5 < \kappa \leq 11, \\ \kappa/(9\kappa+16), & \text{if } 4/3 < \kappa \leq 5, \\ \kappa/(6\kappa+20), & \text{if } 0 < \kappa \leq 4/3. \end{cases}$$

The asserted asymptotic formula of Theorem 9.1 (i) follows by partial summation and Hasse's theorem. □

9.3.2. Proof of the asymptotic formula - the CM case. Let us now assume that E has CM by the ring of integers of an imaginary quadratic field $\mathbb{K}$. To prove the asymptotic formula of Theorem 9.1 (ii), we basically proceed as in Section 9.3.1. However, Propositions 9.6 and 9.7 enable us to choose the parameters y_i from Section 9.3.1 substantially smaller so that Proposition 4.8, the unconditional effective Čebotarev density theorem, becomes applicable and we no longer need to rely on the GRH.

By (9.3) and (9.4), estimates which we established without any assumptions on E, we clearly have

$$\sum_{p\leq x} \frac{\mathrm{Ord}^{\kappa}(\mathrm{E}_p)}{(\sharp\,\mathrm{E}_p(\mathbb{F}_p))^{\kappa}} = \sum_{f,n,d\leq x^{1/8}} \frac{\mu(n)}{n(df)^{1+\kappa}} \sum_{\substack{p\leq x \\ dnf\mid \sharp\,\mathrm{E}_p(\mathbb{F}_p) \\ d_p = d}} \left(\frac{\sharp\,\mathrm{E}_p(\mathbb{F}_p)}{dnf}, d\right) + O_{\kappa}\left(\frac{x}{x^{\kappa/16}} + \frac{x}{x^{1/16}}\right),$$

if we choose $y_1 = y_2 = y_3 = x^{1/8}$. Let now $0 < z_1, z_2, z_3 \leq x^{1/16}$ be parameters. Applying Proposition 9.7 we may eliminate the terms with $z_1 < f \leq x^{1/8}$, $z_2 < n \leq x^{1/8}$ and $z_3 < d \leq x^{1/8}$, and obtain

$$\begin{aligned} \sum_{p\leq x} \frac{\mathrm{Ord}^{\kappa}(\mathrm{E}_p)}{(\sharp\,\mathrm{E}_p(\mathbb{F}_p))^{\kappa}} = {}& \sum_{\substack{f\leq z_1 \\ n\leq z_2 \\ d\leq z_3}} \frac{\mu(n)}{n(df)^{1+\kappa}} \sum_{\substack{p\leq x \\ dnf\mid \sharp\,\mathrm{E}_p(\mathbb{F}_p) \\ d_p = d}} \left(\frac{\sharp\,\mathrm{E}_p(\mathbb{F}_p)}{dnf}, d\right) \\ &+ O_{\kappa,\varepsilon}\left(\frac{x}{x^{\kappa/16}} + \frac{x}{\log x}\left(z_1^{-1-\kappa+\varepsilon} + z_2^{-1+\varepsilon} + z_3^{-\kappa+\varepsilon}\right)\right). \end{aligned}$$

As in the preceding section, we invoke Möbius inversion to translate the condition $d_p = d$ into a convenient divisibility criterion for d_p. By Proposition 9.5, we easily find

$$\sum_{d\le z_3}\frac{1}{d^{1+\kappa}}\sum_{\substack{p\le x\\ dnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ d_p=d}}\left(\frac{\sharp \mathrm{E}_p(\mathbb{F}_p)}{dnf},d\right)$$
$$=\sum_{d\le z_3}\frac{1}{d^{1+\kappa}}\sum_{e\le x^{1/8}}\mu(e)\sum_{\substack{p\le x\\ dnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ de\mid d_p}}\left(\frac{\sharp \mathrm{E}_p(\mathbb{F}_p)}{dnf},d\right)+O\left(x^{7/8}\right).$$

Choosing another parameter $0 < z_4 \le x^{1/16}$, we may then apply Proposition 9.6 which in connection with Lemmas 9.3 and 4.5 yields

$$\sum_{d\le z_3}\frac{1}{d^{1+\kappa}}\sum_{\substack{p\le x\\ dnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ d_p=d}}\left(\frac{\sharp \mathrm{E}_p(\mathbb{F}_p)}{dnf},d\right)$$
$$=\sum_{d\le z_3}\frac{1}{d^{1+\kappa}}\sum_{e\le z_4}\mu(e)\sum_{\substack{p\le x\\ dnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ de\mid d_p}}\left(\frac{\sharp \mathrm{E}_p(\mathbb{F}_p)}{dnf},d\right)+O_{N_{\mathrm{E}},\mathfrak{f}}\left(\frac{x}{z_4\log x}\right).$$

Here, $\mathfrak{f}$ is an ideal of $\mathbb{K}$ as in Proposition 9.6. Combining this estimate with the preceding ones and invoking another Möbius inversion, we thus obtain

$$\sum_{p\le x}\frac{\mathrm{Ord}^{\kappa}(\mathrm{E}_p)}{(\sharp \mathrm{E}_p(\mathbb{F}_p))^{\kappa}}=\sum_{\substack{f\le z_1,n\le z_2\\ d\le z_3,e\le z_4}}\frac{\mu(n)\mu(e)}{n(df)^{1+\kappa}}\sum_{mk\mid d}m\mu(k)\sum_{\substack{p\le x\\ kmdnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ de\mid d_p}}1$$
$$+O\left(\frac{x}{x^{\kappa/16}}+\frac{x}{\log x}\left(z_1^{-1-\kappa+\varepsilon}+z_2^{-1+\varepsilon}+z_3^{-\kappa+\varepsilon}+\frac{\log z_2}{z_4}\right)\right),\tag{9.11}$$

with an implied constant depending on κ, ε, N_{E} and $\mathfrak{f}$. Now we are in the position to estimate the sum over p by Proposition 4.8, the unconditional effective Čebotarev density theorem, provided that the z_i are chosen sufficiently small. By Lemma 8.3, Proposition 4.11 and 9.3 we derive the estimate

$$\log \Delta_{\mathbb{Q}(\mathrm{E}[k])}\le [\mathbb{Q}(\mathrm{E}[k]):\mathbb{Q}]\log(k^3N_{\mathrm{E}}),\tag{9.12}$$

valid for any $k\in\mathbb{N}$. In view of Proposition 4.8 we thus choose the z_i according to

$$\log x\ge 10(z_1z_2z_3^2z_4)^4\log\left((z_1z_2z_3^2z_4)^3N_{\mathrm{E}}\right).\tag{9.13}$$

By Proposition 4.10 and (9.12) there exists an absolute constant $c>0$ such that

$$\beta_0(\mathbb{Q}(\mathrm{E}[k]))\le 1-\frac{1}{ck^3N_{\mathrm{E}}}\tag{9.14}$$

holds for all $k \in \mathbb{N}$, since $\mathbb{Q}(\mathrm{E}[k])/\mathbb{Q}$ is Galois. Analogous to the non-CM case, Proposition 4.8 then yields

(9.15)
$$\sum_{\substack{f\le z_1, n\le z_2\\ d\le z_3, e\le z_4}} \frac{\mu(n)\mu(e)}{n(df)^{1+\kappa}} \sum_{mk\mid d} m\mu(k) \sum_{\substack{p\le x\\ kmdnf\mid \sharp \mathrm{E}_p(\mathbb{F}_p)\\ de\mid d_p}} 1$$
$$= \mathrm{li}(x) \sum_{\substack{f\le z_1, n\le z_2\\ d\le z_3, e\le z_4}} \frac{\mu(n)\mu(e)}{n(df)^{1+\kappa}} \sum_{mk\mid d} m\mu(k)\cdot \frac{\sharp D(mkdnf, de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf, de]]):\mathbb{Q}]} + E_1' + E_2',$$

with

$$E_1' \ll \sum_{\substack{f\le z_1, n\le z_2\\ d\le z_3, e\le z_4}} \frac{1}{n(df)^{1+\kappa}} \sum_{mk\mid d} \frac{m\sharp D(mkdnf, de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf, de]]):\mathbb{Q}]} \cdot \mathrm{li}\left(x^{\beta_0(\mathbb{Q}(\mathrm{E}[[mkdnf, de]]))}\right)$$

and

$$E_2' \ll \sum_{\substack{f\le z_1, n\le z_2\\ d\le z_3, e\le z_4}} \frac{x}{n(df)^{1+\kappa}} \sum_{mk\mid d} m\|D(mkdnf, de)\| \exp\left(-c_2\left(\frac{\log x}{[\mathbb{Q}(\mathrm{E}[[mkdnf, de]]):\mathbb{Q}]}\right)^{1/2}\right).$$

By (9.14), Lemmas 9.3 and 9.8 and (9.13) one easily deduces

$$E_1', E_2' \ll_{A,\kappa,N_{\mathrm{E}}} \frac{x}{\log^A x}, \tag{9.16}$$

for any $A > 0$. It thus remains to extend the summation range of f, n, d and e in (9.11) to all positive integers. To do so, we note the estimates

$$\frac{\sharp D(m,n)}{[\mathbb{Q}(\mathrm{E}[[m,n]]):\mathbb{Q}]} \le \frac{1}{\varphi(n)^2} \quad \text{and} \quad \frac{\sharp D(m,n)}{[\mathbb{Q}(\mathrm{E}[[m,n]]):\mathbb{Q}]} \ll_\varepsilon \frac{m}{[m,n]^{2-\varepsilon}} \tag{9.17}$$

which follow easily from Lemma 9.8 (iv) and Lemma 9.3. We use the second of these estimates in combination with Lemmas 9.8 and 9.3 to eliminate large f, in the same way as we eliminated large n in the non-CM case:

$$\sum_{\substack{f> z_1, n\le z_2\\ d\le z_3, e\le z_4}} \frac{\mu(n)\mu(e)}{n(df)^{1+\kappa}} \sum_{mk\mid d} m\mu(k)\cdot \frac{\sharp D(mkdnf, de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf, de]]):\mathbb{Q}]}$$
$$\ll \sum_{\substack{f> z_1, n\le z_2\\ d\le z_3, e\le z_4}} \frac{1}{n(df)^{1+\kappa}} \sum_{mk\mid d} m\cdot \frac{\sharp D(f, de)}{[\mathbb{Q}(\mathrm{E}[[f, de]]):\mathbb{Q}]}$$
$$\ll_\varepsilon \log z_2 \sum_{f> z_1} \frac{1}{f^\kappa} \sum_{d\le z_3} \frac{1}{d^{\kappa-\varepsilon}} \sum_{e\le z_4} \frac{1}{[f, de]^{2-\varepsilon}}$$
$$\ll_\varepsilon \log z_2 \sum_{f> z_1} \frac{1}{f^{2+\kappa-\varepsilon}} \sum_{c\mid f} c^{2-\varepsilon} \sum_{\substack{d,e\ge 1\\ c\mid de}} \frac{1}{(de)^{2-\varepsilon}} \ll_\varepsilon \frac{\log z_2}{z_1^{1+\kappa-\varepsilon}}.$$

To get rid of large d and e, we invoke the first estimate in (9.17) in combination with Lemma 4.5 and elementary estimates for divisor sum functions (cf. [100, p. 85f]), and find

$$\sum_{\substack{f\geq 1,n\leq z_2\\ d>z_3,e\leq z_4}} \frac{\mu(n)\mu(e)}{n(df)^{1+\kappa}} \sum_{mk|d} m\mu(k)\cdot \frac{\sharp D(mkdnf,de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf,de]]):\mathbb{Q}]} \ll \sum_{\substack{f\geq 1,n\leq z_2\\ d>z_3,e\leq z_4}} \frac{1}{n(df)^{1+\kappa}} \sum_{mk|d} \frac{m}{\varphi(de)^2} \ll_{\kappa,\varepsilon} \frac{\log z_2}{z_3^{1+\kappa-\varepsilon}}$$

and

$$\sum_{\substack{f\geq 1,n\leq z_2\\ d\geq 1,e>z_4}} \frac{\mu(n)\mu(e)}{n(df)^{1+\kappa}} \sum_{mk|d} m\mu(k)\cdot \frac{\sharp D(mkdnf,de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf,de]]):\mathbb{Q}]} \ll \sum_{\substack{f\geq 1,n\leq z_2\\ d\geq 1,e>z_4}} \frac{1}{n(df)^{1+\kappa}} \sum_{mk|d} \frac{m}{\varphi(de)^2} \ll_{\kappa,\varepsilon} \frac{\log z_2}{z_4}.$$

Finally, we eliminate large n just as we eliminated large f before:

$$\begin{aligned}\sum_{\substack{f\geq 1,n>z_2\\ d\geq 1,e\geq 1}} \frac{\mu(n)\mu(e)}{n(df)^{1+\kappa}} \sum_{mk|d} m\mu(k)\cdot \frac{\sharp D(mkdnf,de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf,de]]):\mathbb{Q}]} &\ll \sum_{\substack{f\geq 1,n>z_2\\ d\geq 1,e\geq 1}} \frac{1}{n(df)^{1+\kappa}} \sum_{mk|d} m\cdot \frac{\sharp D(n,de)}{[\mathbb{Q}(\mathrm{E}[[n,de]]):\mathbb{Q}]}\\ &\ll_{\kappa,\varepsilon} \sum_{n>z_2}\sum_{d\geq 1}\frac{1}{d^{\kappa-\varepsilon}}\sum_{e\geq 1}\frac{1}{[n,de]^{2-\varepsilon}}\\ &\ll_{\varepsilon} \sum_{n>z_2}\frac{1}{n^{2-\varepsilon}}\sum_{c|n}c^{2-\varepsilon}\sum_{\substack{d,e\geq 1\\ c|de}}\frac{1}{(de)^{2-\varepsilon}} \ll_{\varepsilon} \frac{1}{z_2^{1-\varepsilon}}.\end{aligned}$$

Summing up, we find

$$\sum_{\substack{f\leq z_1,n\leq z_2\\ d\leq z_3,e\leq z_4}} \frac{\mu(n)\mu(e)}{n(df)^{1+\kappa}} \sum_{mk|d} m\mu(k)\cdot \frac{\sharp D(mkdnf,de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf,de]]):\mathbb{Q}]} = c_{\mathrm{E}}^{(\kappa)} + O_{\kappa,\varepsilon}\left(\frac{\log z_2}{z_1^{1+\kappa-\varepsilon}} + \frac{\log z_2}{z_3^{1+\kappa-\varepsilon}} + \frac{\log z_2}{z_4} + \frac{1}{z_2^{1-\varepsilon}}\right). \tag{9.18}$$

Combining (9.11), (9.13), (9.15), (9.16) and (9.18), we finally arrive at

$$\sum_{p\leq x} \frac{\mathrm{Ord}^{\kappa}(\mathrm{E}_p)}{(\sharp\,\mathrm{E}_p(\mathbb{F}_p))^{\kappa}} = c_{\mathrm{E}}^{(\kappa)}\cdot \mathrm{li}(x) + O\left(\frac{x}{\log x}\left(\frac{\log z_2}{z_1^{1+\kappa-\varepsilon}} + \frac{1}{z_2^{1-\varepsilon}} + \frac{\log z_2}{z_3^{\kappa-\varepsilon}} + \frac{\log z_2}{z_4}\right)\right).$$

In light of (9.13), we choose $z_1^{1+\kappa} = z_2 = z_3^{\kappa} = z_4 = (\log x)^{\eta(\kappa)-\varepsilon}$, with

$$\eta(\kappa) := \frac{1}{8+\frac{12\kappa+8}{\kappa^2+\kappa}}$$

and obtain

$$\sum_{p\le x}\frac{\mathrm{Ord}^{\kappa}(\mathrm{E}_p)}{(\sharp\,\mathrm{E}_p(\mathbb{F}_p))^{\kappa}}=c_{\mathrm{E}}^{(\kappa)}\cdot\mathrm{li}(x)+O\left(\frac{x}{(\log x)^{1+\eta(\kappa)-\varepsilon}}\right),\tag{9.19}$$

with an implied constant depending on κ, ε, N_{E} and $\mathfrak{f}$. A partial summation argument completes the proof of the asymptotic formula in Theorem 9.1 (ii). □

9.3.3. The positivity of $c_{\mathrm{E}}^{(\kappa)}$. It remains to establish the positivity of $c_{\mathrm{E}}^{(\kappa)}$ under the prerequisites of Theorem 9.1. To do so, we proceed similarly to Section 5.2.3, i.e. we prove a lower bound for

$$\sum_{p\le x}\frac{\mathrm{Ord}^{\kappa}(\mathrm{E}_p)}{(\sharp\,\mathrm{E}_p(\mathbb{F}_p))^{\kappa}}$$

which dominates the respective error terms in (9.10) and (9.19). To this end, we recall Lemma 6.7 which gives us the estimate

$$\mathrm{Ord}^{\kappa}(\mathrm{E}_p)\ge(e_pd_p)^{\kappa}\prod_{q\mid\sharp\,\mathrm{E}_p(\mathbb{F}_p)}\left(1-\frac{1}{q}-\frac{1}{q^2}\right),\tag{9.20}$$

for any prime p of good reduction for E. Here the product runs over primes q which divide $\sharp\,\mathrm{E}_p(\mathbb{F}_p)$ and may be estimated as follows:

$$\prod_{q\mid\sharp\,\mathrm{E}_p(\mathbb{F}_p)}\left(1-\frac{1}{q}-\frac{1}{q^2}\right)\ge\frac{1}{4}\prod_{\substack{q\mid\sharp\,\mathrm{E}_p(\mathbb{F}_p)\\ q>2}}\left(1-\frac{1}{q-1}\right)\gg\prod_{i=1}^{\omega(\sharp\,\mathrm{E}_p(\mathbb{F}_p))}\left(1-\frac{1}{p_i}\right).\tag{9.21}$$

Here, $p_1<p_2<p_3<\dots$ is a numbering of the primes. To bound this product from below, we note the following estimate.

Lemma 9.9. *For any $n\in\mathbb{N}$ we have*

$$\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)\gg\frac{1}{\log 2n}.$$

Proof. For the n-th prime p_n we have the rough upper bound

$$p_n\le 2n^2$$

which is an immediate consequence of the estimate

$$\frac{p_n}{n}<\log n+\log\log n,$$

valid for any $n\ge 6$ (cf. [4, p. 233]). Hence, by Mertens' formula we obtain

$$\prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)\ge\prod_{q\le 2n^2}\left(1-\frac{1}{q}\right)\gg\frac{1}{\log 2n}.$$

□

Combining Lemma 9.9 with (9.21), standard estimates for $\omega(n)$ (cf. [100, p. 83f]) and Hasse's theorem, we obtain

$$\prod_{q\mid\sharp\,\mathrm{E}_p(\mathbb{F}_p)}\left(1-\frac{1}{q}-\frac{1}{q^2}\right)\gg\frac{1}{\log\log p}.\tag{9.22}$$

Inserting (9.22) into (9.20), Hasse's theorem yields

$$\sum_{p\le x}\frac{\mathrm{Ord}^{\kappa}(\mathrm{E}_p)}{(\sharp\,\mathrm{E}_p(\mathbb{F}_p))^{\kappa}}\gg_{\kappa}\frac{1}{x^{\kappa}\log\log x}\sum_{p\le x}(e_pd_p)^{\kappa}.$$

To treat the sum over p, we quote the following result of Duke [22] which suggests that the exponent e_pd_p of $\mathrm{E}_p(\mathbb{F}_p)$ is very large for almost all primes p of good reduction for E.

Proposition 9.10 (Duke, 2003). *Let* E *be a rational elliptic curve. If* E *does not have CM, then assume GRH for the fields* $\mathbb{Q}(\mathrm{E}[n])$, $n\in\mathbb{N}$. *For any function* $f(x)$ *on* $[2,\infty)$, *which tends to infinity as* $x\to\infty$, *we have*

$$e_pd_p\le\frac{p}{f(p)}$$

for $o(x/\log x)$ *primes* p *of good reduction for* E.

Applying this result with $f(x)=\log\log(x)$ eventually yields

$$\sum_{p\le x}\frac{\mathrm{Ord}^{\kappa}(\mathrm{E}_p)}{(\sharp\,\mathrm{E}_p(\mathbb{F}_p))^{\kappa}}\gg_{\kappa}\frac{x}{\log x(\log\log x)^2}$$

which in view of (9.10) and (9.19) proves the positivity of $c_{\mathrm{E}}^{(\kappa)}$ under the prerequisites of Theorem 9.1. □

CHAPTER 10

Moments of the Residual Index and Residual Order for Elliptic Curves defined over $\mathbb{F}_p$

In both, the number field and the elliptic curve setting, we have been studying the distribution of residual index and order over reductions of a fixed number field and rational elliptic curve, respectively. There is a nice aspect of the elliptic curve setting which allows for a different point of view. Instead of averaging over primes, as in the preceding chapter, one may fix some prime p and ask for the distribution of "typical" values for residual index and order of points taken from a family of elliptic curves defined over $\mathbb{F}_p$. In this chapter we address this question for a two-parameter family of elliptic curves $\mathrm{E}_{a,b}$ given by a Weierstraß equation with a and b in some range $|a| \leq A$ and $|b| \leq B$.

A precise specification of the problem and the established main results are provided in Section 10.1. In Section 10.2 we quote necessary tools from the literature. The proofs of the aforementioned main results are then executed in Sections 10.3 and 10.4.

10.1. Introduction and statements

Let p be a prime and $\kappa \in \mathbb{R}_+$. Throughout this chapter we assume $p > 3$, for convenience. For an arbitrary elliptic curve $\mathrm{E} / \mathbb{F}_p$ we recall the definition

$$\mathrm{Ord}^{\kappa}(\mathrm{E}) := \frac{1}{\sharp\, \mathrm{E}(\mathbb{F}_p)} \sum_{Q \in \mathrm{E}(\mathbb{F}_p)} \mathrm{ord}_Q(\mathrm{E})^{\kappa}.$$

In a similar way we define an analogue for the residual index by

$$\mathrm{Ind}^{\kappa}(\mathrm{E}) := \frac{1}{\sharp\, \mathrm{E}(\mathbb{F}_p)} \sum_{Q \in \mathrm{E}(\mathbb{F}_p)} \mathrm{ind}_Q(\mathrm{E})^{\kappa}.$$

In a way, these quantities resemble "typical" values for $\mathrm{ord}_Q(\mathrm{E})^{\kappa}$ and $\mathrm{ind}_Q(\mathrm{E})^{\kappa}$, $Q \in \mathrm{E}(\mathbb{F}_p)$, and allow for a comparison of residual index and order of $\mathbb{F}_p$-rational points from different elliptic curves $\mathrm{E} / \mathbb{F}_p$ and study their distribution, as E ranges over families of such curves.

The sizes of $\mathrm{Ord}^{\kappa}(\mathrm{E})$ and $\mathrm{Ind}^{\kappa}(\mathrm{E})$, with respect to p, only depend on the structure of $\mathrm{E}(\mathbb{F}_p) = \mathbb{Z} / d\mathbb{Z} \oplus \mathbb{Z} / de\mathbb{Z}$. If e is close to 1, then $\mathrm{ind}_Q(\mathrm{E})$ and $\mathrm{ord}_Q(\mathrm{E})$ of any $Q \in \mathrm{E}(\mathbb{F}_p)$, and hence $\mathrm{Ind}^1(\mathrm{E})$ and $\mathrm{Ord}^1(\mathrm{E})$ as well, are roughly bounded by $\sqrt{p}$ from below and above, respectively. If, on the other hand, d is close to 1, it is easy to show that $\mathrm{Ord}^1(\mathrm{E})$ is roughly of size p and $\mathrm{Ind}^1(\mathrm{E})$ is of size $O_{\varepsilon}(p^{\varepsilon})$ (see also Lemmas 6.6 and 6.7).

In this chapter we study the average behaviour of $\mathrm{Ind}^{\kappa}(\mathrm{E})$ and $\mathrm{Ord}^{\kappa}(\mathrm{E})$ as E varies over a two-parameter family of elliptic curves $\mathrm{E}_{a,b} / \mathbb{F}_p$ given by Weierstraß equations

$$\mathrm{E}_{a,b} : \quad y^2 \equiv x^3 + ax + b \ (p),$$

where a and b are integers chosen according to $4a^3 + 27b^2 \not\equiv 0 \ (p)$ and $|a| \leq A$ and $|b| \leq B$ for some positive parameters $A, B \leq (p-1)/2$. Our aim is to find asymptotic laws for the average orders of $\mathrm{Ord}^k(\mathrm{E}_{a,b})$ and $\mathrm{Ind}^k(\mathrm{E}_{a,b})$, and simultaneously choose A and B as small as possible without effecting these asymptotic formulae. In fact, using techniques of

Banks and Shparlinski [7] and Schoof [92], we prove the following statements which connect the average orders of $\mathrm{Ord}^\kappa(\mathrm{E}_{a,b})$ and $\mathrm{Ind}^\kappa(\mathrm{E}_{a,b})$ to certain sums of class numbers of binary quadratic forms.

Theorem 10.1. *Let $p>3$ be a prime, $\kappa\in\mathbb{R}_+$ and $0<A,B\leq(p-1)/2$. Further, set*

$$M_{\mathrm{Ord}}(p,\kappa):=p^{\kappa-1}\sum_{de\mid p-1}\frac{\mu(e)}{d^{\kappa+1}}\sum_{\substack{N\in I_p\\(de)^2\mid N}}H\left(\frac{(p+1-N)^2-4p}{(de)^2}\right)\sum_{m\mid\frac{N}{d}}\frac{\psi_\kappa(m)\left(d,\frac{N}{dm}\right)}{m^{\kappa+1}},$$

where I_p denotes the interval $[p+1-\sqrt{p},p+1+\sqrt{p}]$ and $\psi_\kappa(n)=\sum_{d\mid n}d^\kappa\mu(d)$ as defined in Theorem 5.3. Let further $H(\Delta)$ denote the Kronecker class number of discriminant Δ (see Section 10.2.1). Then, for any $\varepsilon'>0$ there exists some $\delta=\delta(\varepsilon')>0$, such that

$$\frac{1}{4AB}\sum_{\substack{|a|\leq A,|b|\leq B\\p\nmid 4a^3+27b^2}}\mathrm{Ord}^\kappa(\mathrm{E}_{a,b})=M_{\mathrm{Ord}}(p,\kappa)+O_{\kappa,\varepsilon,\varepsilon'}\left(p^{\kappa+\varepsilon-\min\{\delta,1/2\}}\right)$$

holds, whenever $\min(A,B)\geq p^{\frac{1}{4}+\varepsilon'}$ and $AB\geq p^{1+\varepsilon'}$.

Theorem 10.2. *Let $p>3$ be a prime, $\kappa\in\mathbb{R}_+$ and $0<A,B\leq(p-1)/2$. Further, set*

$$M_{\mathrm{Ind}}(p,\kappa):=p^{\kappa-2}\sum_{de\mid p-1}\mu(e)\sum_{\substack{N\in I_p\\(de)^2\mid N}}H\left(\frac{(p+1-N)^2-4p}{(de)^2}\right)\sum_{n\mid\frac{N}{d}}\frac{(n,d)}{n^{\kappa-1}}\cdot\theta_\kappa\left(\frac{N}{dn}\right)$$

with $\theta_\kappa(n):=\sum_{d\mid n}\mu(d)/d^\kappa$.

(i) *If $\kappa\geq 3$, and $\varepsilon'>0$, there exists $\delta=\delta(\varepsilon')>0$, such that*

$$\frac{1}{4AB}\sum_{\substack{|a|\leq A,|b|\leq B\\p\nmid 4a^3+27b^2}}\mathrm{Ind}^\kappa(\mathrm{E}_{a,b})=M_{\mathrm{Ind}}(p,\kappa)+O_{\kappa,\varepsilon,\varepsilon'}\left(p^{\max\{\kappa-\frac{3}{2},\kappa-1-\delta\}+\varepsilon}\right)$$

holds, whenever $\min(A,B)\geq p^{\frac{1}{4}+\varepsilon'}$ and $AB\geq p^{1+\varepsilon'}$.

(ii) *If $1<\kappa<3$, and $\varepsilon'>0$, there exists $\delta=\delta(\varepsilon')>0$, such that*

$$\frac{1}{4AB}\sum_{\substack{|a|\leq A,|b|\leq B\\p\nmid 4a^3+27b^2}}\mathrm{Ind}^\kappa(\mathrm{E}_{a,b})=M_{\mathrm{Ind}}(p,\kappa)+O_{\varepsilon,\varepsilon',\kappa}\left(p^{\kappa-1}\left(\frac{p^{2+\delta-2\frac{\delta-\varepsilon}{3-\kappa}}}{AB}\right)^{\frac{3-\kappa}{2}}\right),$$

holds, whenever $\min(A,B)\geq p^{\frac{1}{4}+\varepsilon'}$, and $AB\geq\max\left\{p^{2+\delta-2\frac{\delta-\varepsilon}{3-\kappa}},p^{1+\varepsilon'}\right\}$.

(iii) *If $0<\kappa\leq 1$, then*

$$\frac{1}{p^2}\sum_{\substack{a,b\in\mathbb{F}_p\\p\nmid 4a^3+27b^2}}\mathrm{Ind}^\kappa(\mathrm{E}_{a,b})=M_{\mathrm{Ind}}(p,\kappa)+O_{\kappa,\varepsilon}\left(p^{\kappa-\frac{3}{2}+\varepsilon}\right).$$

To make these formulae meaningful, it is necessary to bound $M_{\mathrm{Ord}}(p,\kappa)$ and $M_{\mathrm{Ind}}(p,\kappa)$ from below. Unfortunately the alternating behaviour of the respective summands makes it hard to establish such estimates directly from the definitions. However, this problem may be circumvented by the definitions of $\mathrm{Ord}^\kappa(\mathrm{E})$ and $\mathrm{Ind}^\kappa(\mathrm{E})$ and their properties which we disclosed in Section 6.2. In fact, observing that "many" elliptic curves $\mathrm{E}_{a,b}/\mathbb{F}_p$ have $\mathrm{E}_{a,b}(\mathbb{F}_p)$ cyclic by a result due to Vlăduţ (see Proposition 10.11), we can prove the

following estimates for $M_{\mathrm{Ord}}(p,\kappa)$ which confirm that $M_{\mathrm{Ord}}(p,\kappa)$ is indeed the main term in Theorem 10.1.

THEOREM 10.3. *Let $p>3$ be a prime and $\kappa\in\mathbb{R}_+$. Then*

$$\frac{p^\kappa}{\log\log p}\ll_\kappa M_{\mathrm{Ord}}(p,\kappa)\ll_\kappa p^\kappa.$$

As for $M_{\mathrm{Ind}}(p,\kappa)$, it is rather easy to obtain appropriate lower bounds which disclose that the main terms in Theorem 10.2 deserve this name. Moreover, the theory of class numbers of binary quadratic forms provides upper bounds for $M_{\mathrm{Ind}}(p,\kappa)$ which up to a p^ε-factor agree with these lower bounds.

THEOREM 10.4. *Let $p>3$ be a prime. For any $\kappa\geq 1$ we have*

$$p^{\kappa-1}\ll_\kappa M_{\mathrm{Ind}}(p,\kappa)=\begin{cases}O_\kappa\left(p^{\kappa-1}\log p(\log\log p)^2\right), & \text{if } \kappa>2,\\ O\left(p\log p(\log\log p)^3\right), & \text{if } \kappa=2,\\ O_\varepsilon\left(p^{\kappa-1+\varepsilon}\right), & \text{if } 1<\kappa<2,\end{cases}$$

and in case $0<\kappa\leq 1$ we have $1\leq M_{\mathrm{Ind}}(p,\kappa)=O_\varepsilon(p^\varepsilon)$.

Both results agree with corresponding estimates from the preceding chapter and analogues in the number field setting. Moreover, Theorems 10.1 and 10.2 again confirm that on average the residual index is harder to handle than the residual order which this time manifests in the shorter admissible summation range for the residual order for small κ. We prove Theorems 10.1 and 10.2 in Section 10.3 and in Section 10.4 we turn to the proofs of Theorems 10.3 and 10.4. To prepare for these proofs we introduce some auxiliary tools in the subsequent section.

10.2. Counting elliptic curves defined over $\mathbb{F}_p$

During the proofs of the above-stated theorems we will be confronted with counting elliptic curves $\mathrm{E}_{a,b}/\mathbb{F}_p$ with $|a|\leq A$ and $|b|\leq B$ for which the group $\mathrm{E}_{a,b}(\mathbb{F}_p)$ has a prescribed structure. In this section we provide tools to overcome these problems. Many attributes of the structure of an elliptic curve are encoded in its endomorphism ring which, since we are working over $\mathbb{F}_p$, is an order in an imaginary quadratic field most of the time. Such orders, as we will see, may be counted using class numbers of binary quadratic forms and we start to summarize some properties thereof.

10.2.1. Binary quadratic forms and class numbers. In this subsection we follow the brief exposition given by LENSTRA in [59]. For more details we refer to this paper or the standard literature.

Let Δ be a negative integer which satisfies $\Delta\equiv 0,1\ (4)$. A *(positive definite) binary quadratic form* of *discriminant* Δ, or briefly a *form*, is a polynomial $F:=F(X,Y):=aX^2+bXY+cY^2$ with $a,b,c\in\mathbb{Z}$, $a>0$ and $b^2-4ac=\Delta$. Such a form is called *primitive* if $\gcd(a,b,c)=1$. It is well known that the group $\mathrm{SL}_2(\mathbb{Z})$ acts on the set of binary quadratic and primitive binary quadratic forms of discriminant Δ, respectively, by

$$F(X,Y)\circ\begin{pmatrix}\alpha & \beta\\ \gamma & \delta\end{pmatrix}:=F(\alpha X+\beta Y,\gamma X+\delta Y).$$

Two forms F and F' which lie in the same orbit are called *equivalent*, a feature which clearly defines an equivalence relation. A matrix which transforms F into F' is called an *isomorphism* from F to F'. An isomorphism from F to itself is called an *automorphism* of

F and the group of such automorphisms is denoted by $\mathrm{Aut}(F)$. This group can be shown to be a cyclic subgroup of $\mathrm{SL}_2(\mathbb{Z})$, with cardinality given by

$$\sharp\,\mathrm{Aut}(F) = \begin{cases} 6, & \text{if } F \text{ is equivalent to } aX^2 + aXY + aY^2, \\ 4, & \text{if } F \text{ is equivalent to } aX^2 + aY^2, \\ 2, & \text{otherwise.} \end{cases} \tag{10.1}$$

For a fixed discriminant Δ the sets of equivalence classes of forms and primitive forms of discriminant Δ are both finite. The *Kronecker class number* $H(\Delta)$ and the *(ordinary) class number* $h(\Delta)$ of Δ are defined by the weighted cardinalities[31] of the sets of equivalence classes of binary quadratic forms and primitive binary quadratic forms of discriminant Δ, respectively. By weighted cardinality we mean that the equivalence class of a form F of discriminant Δ only contributes $1/\sharp\,\mathrm{Aut}(F)$ to $H(\Delta)$ and $h(\Delta)$, respectively. $H(\Delta)$ and $h(\Delta)$ are related by the formula

$$H(\Delta) = \sum_{\substack{d^2 \mid \Delta \\ \frac{\Delta}{d^2} \equiv 0,1 \ (4)}} h\left(\frac{\Delta}{d^2}\right), \tag{10.2}$$

and the class number $h(\Delta)$ may be estimated by the *analytic class number formula*

$$h(\Delta) = \frac{\sqrt{-\Delta}}{2\pi} \cdot L(1, \chi).$$

Here, $L(s, \chi)$ is the L-function of the quadratic character associated to Δ (see [59] for details). Combining this formula and (10.2) with standard estimates for L-functions, one can derive the following estimates for $H(\Delta)$. For a proof and more details we refer to [59].

LEMMA 10.5. *For each $n \in \mathbb{N}$ there exists $\Delta^* = \Delta^*(n) < -4$, such that*

$$\frac{\sqrt{-\Delta}}{\log n} \ll H(\Delta) \ll \sqrt{-\Delta} \cdot \log|\Delta| \cdot (\log\log|\Delta|)^2$$

holds uniformly for all $\Delta \equiv 0, 1 \ (4)$ with $-n \leq \Delta < 0$, except that the left inequality may fail for $\Delta = \Delta^* f^2$, where f, the conductor *of Δ, is the largest integer d in the summation range of (10.2).*

10.2.2. Equivalence classes of elliptic curves $\mathrm{E}/\mathbb{F}_p$ with given structure. Most of the following content is taken from SCHOOF's paper [92] and partially builds on previous work of DEURING [21] and WATERHOUSE [104].

Henceforth, the term *complex quadratic order* refers to an order in an imaginary quadratic field $\mathbb{K}$, i.e. a subring of $\mathcal{O}_{\mathbb{K}}$ of finite index. Such orders are denoted by $\mathcal{O}$ in the sequel. A complex quadratic order $\mathcal{O}$ is uniquely determined by its *discriminant* $\Delta = \Delta(\mathcal{O})$ and we write $\mathcal{O}(\Delta)$ for the unique complex quadratic order of discriminant Δ. If $\mathcal{O}' \subset \mathcal{O}$ are two complex quadratic orders, we have $\Delta(\mathcal{O}) = \Delta(\mathcal{O}')/[\mathcal{O} : \mathcal{O}']^2$, i.e. the respective discriminants differ by the square of an integer.

Let $t \in \mathbb{Z}$. Following SCHOOF [92], we denote by $I(t)$ the set of elliptic curves $\mathrm{E}/\mathbb{F}_p$ for which $\mathrm{E}(\mathbb{F}_p)$ contains exactly $p + 1 - t$ points. Note that $I(t)$ is closed under $\mathbb{F}_p$-isomorphisms, and it is empty when $|t| > 2\sqrt{p}$ by Hasse's theorem. As already mentioned in Section 8.2, the endomorphism ring $\mathrm{End}(\mathrm{E})$ is either a complex quadratic order or an

[31] In the literature, e.g. in [92], $H(\Delta)$ and $h(\Delta)$ are often defined without weights. We meant this definition in the paragraph subsequent to Theorem 3.1. The way we defined it here, however, is more convenient for future arguments.

order in a quaternion algebra. The ring of $\mathbb{F}_p$-endomorphisms $\mathrm{End}_{\mathbb{F}_p}(\mathrm{E})$, however, can only be a complex quadratic order (cf. Theorem 4.2 of [92]), and the following result due to Schoof (cf. Theorem 4.3 of [92]) determines which orders may occur as $\mathbb{F}_p$-endomorphism rings for curves $\mathrm{E} \in I(t)$.

Proposition 10.6. *Let $-2\sqrt{p} \leq t \leq 2\sqrt{p}$ be an integer. Then $I(t)$ is not empty and the complex quadratic orders which occur as rings of $\mathbb{F}_p$-endomorphisms of some elliptic curve $\mathrm{E} \in I(t)$ are precisely those which contain $\mathcal{O}(t^2 - 4p)$.*

For upcoming computations, it is useful to know how many $\mathbb{F}_p$-isomorphism classes of elliptic curves $\mathrm{E} / \mathbb{F}_p$ there are inside $I(t)$, for which $\mathrm{E}(\mathbb{F}_p)$ contains the n-torsion points $\mathrm{E}[n]$ of E for a fixed $n \in \mathbb{N}$. By the following result (cf. Prop. 3.7 in [92]) one can again utilize complex quadratic orders to clear this question.

Proposition 10.7 (Schoof, 1987). *Let $\mathrm{E} / \mathbb{F}_p$ be an elliptic curve and $n \in \mathbb{N}$ with $p \nmid n$. Then we have $\mathrm{E}[n] \subset \mathrm{E}(\mathbb{F}_p)$ if and only if $n \mid p - 1$, $n^2 \mid p + 1 - t$ and*[32]

$$\mathcal{O}\left(\frac{t^2 - 4p}{n^2}\right) \subset \mathrm{End}_{\mathbb{F}_p}(\mathrm{E}),$$

where $t = p + 1 - \sharp\,\mathrm{E}(\mathbb{F}_p)$.

To apply Proposition 10.7 for counting purposes we need to know about the number of $\mathbb{F}_p$-isomorphism classes in $I(t)$ whose $\mathbb{F}_p$-endomorphism rings equal a prescribed complex quadratic order. An answer to this is provided by the following result which basically coincides with Theorem 4.5 (i) of [92]. The distinction of cases comes from the different way in which Schoof defined the class number of a form, and takes (10.1) into account.

Proposition 10.8. *Let $\mathcal{O} = \mathcal{O}(\Delta)$ be a complex quadratic order that occurs as the $\mathbb{F}_p$-endomorphism ring $\mathrm{End}_{\mathbb{F}_p}(\mathrm{E})$ of some elliptic curve in $I(t)$. Let f denote the inertia degree of p in $\mathcal{O}$. Then the number of $\mathbb{F}_p$-isomorphism classes of elliptic curves $\mathrm{E} / \mathbb{F}_p \in I(t)$ with $\mathrm{End}_{\mathbb{F}_p}(\mathrm{E}) = \mathcal{O}$ equals $f \cdot h(\Delta) \cdot \alpha$ with*

$$\alpha = \begin{cases} 6, & \text{if } \Delta = -3, \\ 4, & \text{if } \Delta = -4, \\ 2, & \text{otherwise.} \end{cases}$$

If we start with an elliptic curve defined over $\mathbb{F}_p$ rather than with a complex quadratic order, we easily obtain the following variation of the preceding statement.

Proposition 10.9. *Let $\mathrm{E} / \mathbb{F}_p \in I(t)$ be an elliptic curve with j-invariant j_{E} and $\mathrm{End}_{\mathbb{F}_p}(\mathrm{E}) = \mathcal{O}$, a complex quadratic order. Let f denote the inertia degree of p in $\mathcal{O}$. Then the number of $\mathbb{F}_p$-isomorphism classes inside $I(t)$ with $\mathbb{F}_p$-endomorphism ring equal to $\mathcal{O}$ is $f \cdot h(\Delta(\mathcal{O})) \cdot \beta$ with*

$$\beta = \begin{cases} 6, & \text{if } p \equiv 1 \ (3) \text{ and } j_{\mathrm{E}} = 0, \\ 4, & \text{if } p \equiv 1 \ (4) \text{ and } j_{\mathrm{E}} = 1728, \\ 2, & \text{otherwise.} \end{cases}$$

Proof. It is easily seen that $\Delta(\mathbb{Z}[\zeta_3]) = -3$ and $\Delta(\mathbb{Z}[i]) = -4$. As described on pages 190f in [92], the respective orders occur as $\mathbb{F}_p$-endomorphism ring of E if and only if $p \equiv 1 \ (3)$ and $j_{\mathrm{E}} = 0$, and $p \equiv 1 \ (4)$ and $j_{\mathrm{E}} = 1728$, respectively. The assertion then follows by Proposition 10.8. □

[32] Note that the divisibility conditions for n particularly ensure $(t^2 - 4p)/n^2 \in \mathbb{Z}$.

10.2.3. Counting Weierstraß equations over $\mathbb{F}_p$. To make the above results applicable to our original problem, we will now explain how they enable us to count elliptic curves $\mathrm{E}_{a,b}/\mathbb{F}_p$ which are furnished with a certain structure. Let $\mathrm{E}_{a,b}$ and $\mathrm{E}_{r,s}$ be two elliptic curves defined over $\mathbb{F}_p$ given by Weierstraß equations. These curves are isomorphic over $\mathbb{F}_p$ (cf. [96, p. 45]) if and only if there exists $u \in \mathbb{F}_p^*$ such that

$$r = u^4 a \quad \text{and} \quad s = u^6 b. \tag{10.3}$$

In particular, $\mathrm{Aut}_{\mathbb{F}_p}(\mathrm{E}_{a,b})$ is always cyclic and its order depends on p, a and b in the following way:

$$\sharp\,\mathrm{Aut}_{\mathbb{F}_p}(\mathrm{E}_{a,b}) = \begin{cases} 6, & \text{if } a = 0 \text{ and } p \equiv 1 \ (3), \\ 4, & \text{if } b = 0 \text{ and } p \equiv 1 \ (4), \\ 2, & \text{otherwise.} \end{cases} \tag{10.4}$$

Note that the cases $a = 0$ and $b = 0$ yield exactly those curves $\mathrm{E}_{a,b}/\mathbb{F}_p$ with j-invariant equal to 0 and 1728, respectively.

For any subset $\mathcal{S}$ of $\mathbb{F}_p^2$ and positive parameters $1 \le A, B \le (p-1)/2$, we define

$$\mathcal{M}_p(\mathcal{S}; A, B) := \{\mathrm{E}_{a,b}/\mathbb{F}_p : |a| \le A, |b| \le B, (a \bmod p, b \bmod p) \in \mathcal{S}\}.$$

Now assume that $\mathcal{S}$ has the property that if $(a,b) \in \mathcal{S}$ and $\mathrm{E}_{a,b}$ is isomorphic to $\mathrm{E}_{r,s}$ over $\mathbb{F}_p$ then (r,s) also belongs to $\mathcal{S}$. We call such a set *closed under $\mathbb{F}_p$-isomorphism*. Using (10.3) and effective bounds on character sums, Banks and Shparlinski have proved the following equidistribution result for $\mathcal{M}_p(\mathcal{S}; A, B)$, applicable if $\mathcal{S}$ is closed under $\mathbb{F}_p$-isomorphism (cf. Corollary 16 of [7]).

Proposition 10.10 (Banks–Shparlinski, 2009). *Let $\mathcal{S} \subset \mathbb{F}_p^2$ be closed under $\mathbb{F}_p$-isomorphism and $1 \le A, B \le (p-1)/2$. For any $\varepsilon > 0$ there exists $\delta > 0$ such that*

$$\mathcal{M}_p(\mathcal{S}; A, B) - \frac{4AB}{p^2} \cdot \sharp\,\mathcal{S} \ll_\varepsilon ABp^{-\delta}$$

holds, whenever

$$\min(A, B) \ge p^{\frac{1}{4}+\varepsilon} \quad \text{and} \quad AB \ge p^{1+\varepsilon}.$$

Examples for sets which are closed under $\mathbb{F}_p$-isomorphism and turn out to be of great importance in upcoming situations, are given by

$$\mathcal{S}_{p,cyclic} := \{(a,b) \in \mathbb{F}_p^2 : \mathrm{E}_{a,b}(\mathbb{F}_p) \text{ is cyclic}\}$$

and

$$\mathcal{S}_p(n, N) := \{(a,b) \in \mathbb{F}_p^2 : \sharp\,\mathrm{E}_{a,b}(\mathbb{F}_p) = N,\ \mathrm{E}_{a,b}[n] \subset \mathrm{E}_{a,b}(\mathbb{F}_p)\}$$

for arbitrary $n, N \in \mathbb{N}$. In both definitions we tacitly assumed $4a^3 + 27b^2 \not\equiv 0 \ (p)$. Vlăduţ has proved the following useful estimate for $\mathcal{S}_{p,cyclic}$ (cf. Lemma 10 of [7]):

Proposition 10.11 (Vlăduţ, 1999). *Define*

$$\vartheta_p := \prod_{q \mid p-1} \left(1 - \frac{1}{q(q^2-1)}\right),$$

where the product runs over prime divisors of $p-1$. Then, as $p \to \infty$, we have

$$\left|\sharp\,\mathcal{S}_{p,cyclic} - \vartheta_p p^2\right| \le p^{\frac{3}{2}+o(1)}.$$

As for $\mathcal{S}_p(n,N)$, we first observe that $\mathcal{S}_p(n,N)$ is empty if n does not divide $p-1$, since $\mathrm{E}_{a,b}[n] \subset \mathrm{E}_{a,b}(\mathbb{F}_p)$ implies that p splits completely in $\mathbb{Q}(\zeta_n)$, i.e. $p \equiv 1\ (n)$. Moreover, $\mathcal{S}_p(n,N)$ is empty, if one of $N \notin I_p$ or $n^2 \nmid N$ is fulfilled. In all other cases we are able to determine $\sharp\,\mathcal{S}_p(n,N)$ in terms of Kronecker class numbers.

PROPOSITION 10.12. *Let $N, n \in \mathbb{N}$ and assume $N \in I_p$, $n \mid p-1$ and $n^2 \mid N$. Then we have*

$$\sharp\,\mathcal{S}_p(n,N) = (p-1) \cdot H\left(\frac{(p+1-N)^2-4p}{n^2}\right).$$

PROOF. Write $t = p+1-N$, and let $[\mathrm{E}]$ denote the $\mathbb{F}_p$-isomorphism class of an elliptic curve $\mathrm{E}/\mathbb{F}_p$. For any curve $\mathrm{E}' \in [\mathrm{E}]$ we write $\mathrm{E} \sim \mathrm{E}'$. Then, by (10.3) and Proposition 10.7, we obtain

$$\begin{aligned}\sharp\,\mathcal{S}_p(n,N) &= \sum_{\substack{[\mathrm{E}]\in I(t)\\ \mathcal{O}\left(\frac{t^2-4p}{n^2}\right)\subset \mathrm{End}_{\mathbb{F}_p}(\mathrm{E})}} \sharp\{\mathrm{E}_{a,b}/\mathbb{F}_p : \mathrm{E}_{a,b} \sim \mathrm{E}\} \\ &= (p-1) \sum_{\mathcal{O}\left(\frac{t^2-4p}{n^2}\right)\subset\mathcal{O}} \sum_{\substack{[\mathrm{E}]\in I(t)\\ \mathrm{End}_{\mathbb{F}_p}(\mathrm{E})=\mathcal{O}}} \frac{1}{\sharp\,\mathrm{Aut}_{\mathbb{F}_p}(\mathrm{E})}.\end{aligned}$$

Now observe that the inertia degree of p in a complex quadratic order $\mathcal{O}$ is 2 if the Legendre symbol $\left(\frac{\Delta(\mathcal{O})}{p}\right)$ equals -1, and it is 1 otherwise (cf. Theorem 4.5 of [92]). Since the discriminant of an order $\mathcal{O} \supset \mathcal{O}\left(\frac{t^2-4p}{n^2}\right)$ only differs from t^2-4p by a square, we clearly have $\left(\frac{\Delta(\mathcal{O})}{p}\right) \neq -1$. Note that this also holds for $t=0$. Combining Proposition 10.9, (10.4) and (10.2), we finally arrive at

$$\sharp\,\mathcal{S}_p(n,N) = (p-1) \sum_{\mathcal{O}\left(\frac{t^2-4p}{n^2}\right)\subset\mathcal{O}} h(\Delta(\mathcal{O})) = (p-1)\cdot H\left(\frac{t^2-4p}{n^2}\right),$$

since all complex quadratic orders which contain $\mathcal{O}\left(\frac{t^2-4p}{n^2}\right)$ have discriminants $\frac{t^2-4p}{d^2n^2}$ for some $d \in \mathbb{N}$ which fulfils $d^2 \mid \frac{t^2-4p}{n^2}$ and $\frac{t^2-4p}{d^2n^2} \equiv 0, 1\ (4)$. □

10.3. Proofs of the asymptotic formulae

Let us return to our original problem and prove Theorems 10.1 and 10.2.

10.3.1. Proof of Theorem 10.1. We start with the easier residual order case, i.e. we compute an asymptotic formula for

$$\frac{1}{4AB} \sum_{\substack{|a|\le A, b\le B\\ p\nmid 4a^3+27b^2}} \mathrm{Ord}^{\kappa}(\mathrm{E}_{a,b}).$$

For the remainder of this section we omit the summation condition $|a| \le A$, $|b| \le B$, and tacitly assume $4a^3+27b^2 \not\equiv 0\ (p)$, too, for notational convenience. Also, we write $d_{a,b}$ and $e_{a,b}$ for the structure constants of $\mathrm{E}_{a,b}(\mathbb{F}_p)$ as defined in (8.3), $N_{a,b}$ instead of $\sharp\,\mathrm{E}_{a,b}(\mathbb{F}_p)$,

and recall that $N_{a,b} = e_{a,b}\, d_{a,b}^2$. We start with some elementary calculations. By Lemma 6.7, we deduce

$$\begin{aligned}\sum_{a,b} \mathrm{Ord}^\kappa(\mathrm{E}_{a,b}) &= \sum_{a,b} \frac{1}{N_{a,b}} \sum_{Q \in \mathrm{E}_{a,b}(\mathbb{F}_p)} \mathrm{ord}_Q(\mathrm{E}_{a,b})^\kappa \\ &= \sum_{a,b} \frac{1}{N_{a,b}} \sum_{n \mid d_{a,b}\, e_{a,b}} \frac{(e_{a,b}\, d_{a,b})^{\kappa+1}}{n^{\kappa+1}} \sum_{l \mid e_{a,b}\, d_{a,b}\, /n} \frac{\mu(l)}{l} \left(\frac{e_{a,b}\, d_{a,b}}{nl}, d_{a,b} \right) \\ &= \sum_{a,b} \sum_{n \mid d_{a,b}\, e_{a,b}} \frac{N_{a,b}^\kappa}{(n d_{a,b})^{\kappa+1}} \sum_{l \mid e_{a,b}\, d_{a,b}\, /n} \frac{\mu(l)}{l} \left(\frac{e_{a,b}\, d_{a,b}}{nl}, d_{a,b} \right).\end{aligned}$$

Next we note $N_{a,b} = p + O(\sqrt{p})$ by Hasse's theorem, whence, by Taylor's formula, we may replace $N_{a,b}^\kappa$ by $p^\kappa + O_\kappa(p^{\kappa - \frac{1}{2}})$. We obtain[33]

$$\begin{aligned}&\sum_{a,b} \mathrm{Ord}^\kappa(\mathrm{E}_{a,b}) \\ &\quad= \left(p^\kappa + O_\kappa\left(p^{\kappa-\frac{1}{2}}\right)\right) \sum_{a,b} \sum_{n \mid d_{a,b}\, e_{a,b}} \frac{1}{(n\, d_{a,b})^{\kappa+1}} \sum_{l \mid e_{a,b}\, d_{a,b}\, /n} \frac{\mu(l)}{l} \left(\frac{e_{a,b}\, d_{a,b}}{nl}, d_{a,b} \right) \\ &\quad= \left(p^\kappa + O_\kappa\left(p^{\kappa-\frac{1}{2}}\right)\right) \sum_{n \le 2p} \frac{1}{n^{\kappa+1}} \sum_{l \le 2p/n} \frac{\mu(l)}{l} \sum_{\substack{d \le 2\sqrt{p} \\ d \mid p-1}} \frac{1}{d^{\kappa+1}} \sum_{\substack{a,b \\ d_{a,b} = d \\ dnl \mid N_{a,b}}} \left(\frac{N_{a,b}}{dnl}, d_{a,b} \right) \\ &\quad= \left(p^\kappa + O_\kappa\left(p^{\kappa-\frac{1}{2}}\right)\right) \sum_{nl \le 2p} \frac{\mu(l)}{l n^{\kappa+1}} \sum_{\substack{d \le 2\sqrt{p} \\ d \mid p-1}} \frac{1}{d^{\kappa+1}} \sum_{m \mid d} m\, \mathcal{M}_p(\mathcal{S}(d, mdnl, m); A, B),\end{aligned}$$

where, for $m, d, k \in \mathbb{N}$ with $m \mid d$,

$$\mathcal{S}(d,k,m) := \left\{ (a,b) \in \mathbb{F}_p^2 : d_{a,b} = d, k \mid N_{a,b}, \left(\frac{N_{a,b}}{k}, \frac{d}{m} \right) = 1 \right\}$$

is clearly closed under $\mathbb{F}_p$-isomorphism, and $\mathcal{M}_p(\mathcal{S}(d, mdnl, m); A, B)$ is defined as in Section 10.2.3. Let us now fix some $\varepsilon' > 0$ and choose $\delta = \delta(\varepsilon')$, A and B according to Proposition 10.10. By the same proposition, we have

$$\mathcal{M}_p(\mathcal{S}(d, mdnl, m); A, B) = \frac{4AB}{p^2} \cdot \sharp\, \mathcal{S}(d, mdnl, m) + O_{\varepsilon'}\left(AB p^{-\delta}\right)$$

which gives us

$$\begin{aligned}(10.5)\quad &\frac{1}{4AB} \sum_{a,b} \mathrm{Ord}^\kappa(\mathrm{E}_{a,b}) \\ &\qquad = p^{\kappa-2} \sum_{nl \le 2p} \frac{\mu(l)}{l n^{\kappa+1}} \sum_{\substack{d \le 2\sqrt{p} \\ d \mid p-1}} \frac{1}{d^{\kappa+1}} \sum_{m \mid d} m \cdot \sharp\, \mathcal{S}(d, mdnl, m) + E_1 + E_2,\end{aligned}$$

[33]Even though it might be dangerous in general to extract the error term in this way from an alternating sum, this procedure is legitimate here, because no cancellation takes place and the Möbius function is estimated by its absolute value 1 during later error estimates.

with error terms[34]

$$E_1 \ll_\kappa p^{\kappa-\frac{5}{2}} \sum_{nl\le 2p} \frac{1}{ln^{\kappa+1}} \sum_{\substack{d\le 2\sqrt{p}\\ d|p-1}} \frac{1}{d^{\kappa+1}} \sum_{m|d} m \cdot \sharp\mathcal{S}(d, mdnl, m)$$
$$\ll_\kappa p^{\kappa-\frac{1}{2}} \sum_{l\le 2p} \frac{1}{l} \sum_{\substack{d\le 2\sqrt{p}\\ d|p-1}} \frac{1}{d^{\kappa+1}} \sum_{m|d} m \ll_\varepsilon p^{\kappa-\frac{1}{2}+\varepsilon}$$

and

$$E_2 \ll_{\varepsilon'} p^{\kappa-\delta} \sum_{n\le 2p} \frac{1}{n^{\kappa+1}} \sum_{l\le 2p/n} \frac{\mu(l)}{l} \sum_{\substack{d\le 2\sqrt{p}\\ d|p-1}} \frac{1}{d^{\kappa+1}} \sum_{m|d} m \ll_{\kappa,\varepsilon} p^{\kappa-\delta+\varepsilon}.$$

Let us now turn to the main term in (10.5). As a first step, we express $\sharp\mathcal{S}(d, mdnl, m)$ in terms of the cardinalities of $\mathcal{S}_p(k, N)$, as defined in Section 10.2.3. For that purpose, we collect pairs (a, b) which yield the same value $N \in I_p = [p+1-2\sqrt{p}, p+1+2\sqrt{p}]$ for $N_{a,b}$. By Proposition 10.12 and the inclusion-exclusion principle, we obtain

$$\begin{aligned}\sharp\mathcal{S}(d, mdnl, m) &= \sum_{f|\frac{d}{m}} \mu(f) \sum_{\substack{e\le \frac{2\sqrt{p}}{d}\\ de|p-1}} \mu(e) \sum_{\substack{N\in I_p\\ fmdnl|N\\ (de)^2|N}} \mathcal{S}_p(de, N)\\ &= (p-1)\sum_{f|\frac{d}{m}} \mu(f) \sum_{\substack{e\le \frac{2\sqrt{p}}{d}\\ de|p-1}} \mu(e) \sum_{\substack{N\in I_p\\ fmdnl|N\\ (de)^2|N}} H\left(\frac{(p+1-N)^2-4p}{(de)^2}\right).\end{aligned}$$

Hence, the main part in (10.5) equals

$$p^{\kappa-1}\left(1-\frac{1}{p}\right) \sum_{nl\le 2p} \frac{\mu(l)}{ln^{\kappa+1}} \sum_{\substack{de\le 2\sqrt{p}\\ de|p-1}} \frac{\mu(e)}{d^{\kappa+1}} \sum_{mf|d} m\mu(f) \sum_{\substack{N\in I_p\\ fmdnl|N\\ (de)^2|N}} H\left(\frac{(p+1-N)^2-4p}{(de)^2}\right),$$

where the factor $(1-1/p)$ may be neglected, as $p\to\infty$, by the same arguments as above. Applying some changes of the summation order, and recalling basic facts of the Möbius function, the sum expression becomes

$$\begin{aligned}&\sum_{de|p-1} \frac{\mu(e)}{d^{\kappa+1}} \sum_{\substack{N\in I_p\\ (de)^2|N}} H\left(\frac{(p+1-N)^2-4p}{(de)^2}\right) \sum_{nl|\frac{N}{d}} \frac{\mu(l)}{ln^{\kappa+1}} \sum_{m|d,\frac{N}{dnl}} m \sum_{f|\frac{d}{m},\frac{N}{mdnl}} \mu(f)\\ &= \sum_{de|p-1} \frac{\mu(e)}{d^{\kappa+1}} \sum_{\substack{N\in I_p\\ (de)^2|N}} H\left(\frac{(p+1-N)^2-4p}{(de)^2}\right) \sum_{nl|\frac{N}{d}} \frac{\mu(l)\left(d, \frac{N}{dnl}\right)}{ln^{\kappa+1}}\\ &= \sum_{de|p-1} \frac{\mu(e)}{d^{\kappa+1}} \sum_{\substack{N\in I_p\\ (de)^2|N}} H\left(\frac{(p+1-N)^2-4p}{(de)^2}\right) \sum_{m|\frac{N}{d}} \frac{\psi_\kappa(m)\left(d, \frac{N}{dm}\right)}{m^{\kappa+1}}.\end{aligned}$$

This proves Theorem 10.1. □

[34] Error term E_1 might be improved to $O_\kappa\left(ABp^{\kappa-\frac{1}{2}}\right)$ using results of Howe [43] and Lenstra [59]. Since E_2 usually dominates E_1, we abstain from this precision.

10.3.2. Proof of Theorem 10.2. Let us now turn to the analogue problem for the residual index, and prove Theorem 10.2, i.e. establish an asymptotic formula for

$$\sum_{a,b} \mathrm{Ind}^{\kappa}(\mathrm{E}_{a,b}) = \sum_{a,b} \frac{1}{N_{a,b}} \sum_{Q \in \mathrm{E}_{a,b}(\mathbb{F}_p)} \mathrm{ind}_Q(\mathrm{E}_{a,b})^{\kappa}. \tag{10.6}$$

We prove Theorem 10.2 for $\kappa > 1$ in detail and give a sketch for the case $0 < \kappa \leq 1$ afterwards.

Assume $\kappa > 1$. Inserting Lemma 6.7 into (10.6), and utilizing Hasse's theorem in combination with Taylor's formula, we obtain[35]

$$\begin{aligned} \sum_{a,b} \mathrm{Ind}^{\kappa}(\mathrm{E}_{a,b}) &= \sum_{a,b} N_{a,b}^{\kappa-1} \sum_{n \mid d_{a,b}\, e_{a,b}} \frac{1}{n^{\kappa-1}} \sum_{l \mid n} \frac{\mu(l)}{l} \left(\frac{n}{l}, d_{a,b}\right) \\ &= \left(p^{\kappa-1} + O_{\kappa}\left(p^{\kappa-\frac{3}{2}}\right)\right) \sum_{a,b} \sum_{l \mid d_{a,b}\, e_{a,b}} \frac{\mu(l)}{l} \sum_{\substack{n \mid d_{a,b}\, e_{a,b} \\ l \mid n}} \frac{1}{n^{\kappa-1}} \left(\frac{n}{l}, d_{a,b}\right) \\ &= \left(p^{\kappa-1} + O_{\kappa}\left(p^{\kappa-\frac{3}{2}}\right)\right) \sum_{l \leq 2p} \frac{\mu(l)}{l^{\kappa}} \sum_{n \leq 2p/l} \frac{1}{n^{\kappa-1}} \sum_{\substack{a,b \\ nl \mid d_{a,b}\, e_{a,b}}} (n, d_{a,b}). \end{aligned} \tag{10.7}$$

To treat the sum over a and b, we collect those pairs (a,b) which yield the same value $d_{a,b}$, and obtain

$$\sum_{\substack{a,b \\ nl \mid d_{a,b}\, e_{a,b}}} (n, d_{a,b}) = \sum_{\substack{d \leq 2\sqrt{p} \\ d \mid p-1}} (n,d)\, \mathcal{M}_p(\mathcal{T}(d, dnl); A, B), \tag{10.8}$$

where for $d, k \in \mathbb{N}$

$$\mathcal{T}(d,k) := \{(a,b) \in \mathbb{F}_p^2 : d_{a,b} = d, k \mid N_{a,b}\}$$

is clearly closed under $\mathbb{F}_p$-isomorphism. To make Proposition 10.10 applicable, we need to get rid of terms for large n. To do so, we recall that A and B are both bounded by $(p-1)/2$ which clearly yields

$$\mathcal{M}_p(\mathcal{T}(d, dnl); A, B) \leq \sharp\, \mathcal{T}(d, dnl). \tag{10.9}$$

Using the inclusion-exclusion principle and Proposition 10.12, we then obtain

$$\begin{aligned} \sharp\, \mathcal{T}(d, dnl) &= \sum_{\substack{e \leq \frac{2\sqrt{p}}{d} \\ de \mid p-1}} \mu(e) \sum_{\substack{N \in I_p \\ (de)^2 \mid N \\ dnl \mid N}} \sharp\, \mathcal{S}_p(de, N) \\ &= (p-1) \sum_{\substack{e \leq \frac{2\sqrt{p}}{d} \\ de \mid p-1}} \mu(e) \sum_{\substack{N \in I_p \\ (de)^2 \mid N \\ dnl \mid N}} H\left(\frac{(p+1-N)^2 - 4p}{(de)^2}\right), \end{aligned} \tag{10.10}$$

where I_p still denotes the interval $[p+1-\sqrt{p}, p+1+\sqrt{p}]$. Now let $0 < y \leq p$ be some power of p which we specify later. By (10.8), (10.9), (10.10) and Lemma 10.5, we then

[35] As in Section 10.3.1, extracting the error term from the alternating sum is uncritical here.

obtain[36]

$$\sum_{l\le 2p}\frac{\mu(l)}{l^\kappa}\sum_{y<n\le 2p/l}\frac{1}{n^{\kappa-1}}\sum_{\substack{a,b\\ nl\mid d_{a,b}\ e_{a,b}}}(n,d_{a,b}) \tag{10.11}$$

$$\ll_\varepsilon p^{\frac{3}{2}+\varepsilon}\sum_{l\le 2p}\frac{1}{l^\kappa}\sum_{y<n\le 2p/l}\frac{1}{n^{\kappa-1}}\sum_{\substack{d\le 2\sqrt{p}\\ d\mid p-1}}(n,d)\sum_{\substack{e\le\frac{2\sqrt{p}}{d}\\ de\mid p-1}}\sum_{\substack{N\in I_p\\ (de)^2\mid N\\ dnl\mid N}}\frac{1}{de}$$

$$\ll p^{2+\varepsilon}\sum_{l\le 2p}\frac{1}{l^{\kappa+1}}\sum_{y<n\le 2p/l}\frac{1}{n^\kappa}\ll_\kappa\frac{p^{2+\varepsilon}}{y^{\kappa-1}},$$

since $\kappa>1$.

Remark 10.13. Note that we may not neglect the terms with large n in case $\kappa\le 1$ which is exactly the reason why our method fails in that case and we may not choose A and B any smaller than $(p-1)/2$.

Now fix some $\varepsilon'>0$ and choose $\delta=\delta(\varepsilon')>0$, A and B according to Proposition 10.10. From this proposition and the displays (10.7) and (10.11) we infer

$$\frac{1}{4AB}\sum_{a,b}\mathrm{Ind}^\kappa(\mathrm{E}_{a,b})=p^{\kappa-3}\sum_{l\le 2p}\frac{\mu(l)}{l^\kappa}\sum_{n\le y}\frac{1}{n^{\kappa-1}}\sum_{\substack{d\le 2\sqrt{p}\\ d\mid p-1}}(n,d)\cdot\sharp\mathcal{T}(d,dnl) \tag{10.12}$$

$$+E_1'+E_2'+O_{\varepsilon,\kappa}\left(\frac{p^{\kappa+1+\varepsilon}}{ABy^{\kappa-1}}\right)$$

with

$$E_1'\ll_\kappa p^{\kappa-\frac{7}{2}}\sum_{l\le 2p}\frac{1}{l^\kappa}\sum_{n\le y}\frac{1}{n^{\kappa-1}}\sum_{\substack{d\le 2\sqrt{p}\\ d\mid p-1}}(n,d)\cdot\sharp\mathcal{T}(d,dnl)$$

and

$$E_2'\ll_{\varepsilon'}p^{\kappa-1-\delta}\sum_{l\le 2p}\frac{1}{l^\kappa}\sum_{n\le y}\frac{1}{n^{\kappa-1}}\sum_{\substack{d\le 2\sqrt{p}\\ d\mid p-1}}(n,d)\ll_{\varepsilon,\kappa}p^{\kappa-1-\delta+\varepsilon}\max\{1,y^{3-\kappa}\}.$$

Here, a possible $\log y$ factor which occurs in case $\kappa=3$ is absorbed by the p^ε-term. As for E_1', we invoke (10.9), (10.10) and Lemma 10.5, to obtain

$$E_1'\ll_\kappa p^{\kappa-\frac{7}{2}}\sum_{l\le 2p}\frac{\mu(l)}{l^\kappa}\sum_{n\le y}\frac{1}{n^{\kappa-1}}\sum_{\substack{d\le 2\sqrt{p}\\ d\mid p-1}}(n,d)\sum_{\substack{e\le\frac{2\sqrt{p}}{d}\\ de\mid p-1}}\sum_{\substack{N\in I_p\\ (de)^2\mid N\\ dnl\mid N}}\sharp\mathcal{S}_p(de,N)$$

$$\ll_\varepsilon p^{\kappa-2+\varepsilon}\sum_{l\le 2p}\frac{\mu(l)}{l^\kappa}\sum_{n\le y}\frac{1}{n^{\kappa-1}}\sum_{\substack{d\le 2\sqrt{p}\\ d\mid p-1}}(n,d)\sum_{\substack{e\le\frac{2\sqrt{p}}{d}\\ de\mid p-1}}\sum_{\substack{N\in I_p\\ (de)^2\mid N\\ dnl\mid N}}\frac{1}{de}$$

$$\ll_{\kappa,\varepsilon}p^{\kappa-\frac{3}{2}+\varepsilon}.$$

[36]The factor p^ε in the following display can be improved to a logarithm power of p, but we disregard this precision.

Hence, the sum E' of the three error terms in (10.12) satisfies

$$E' \ll_{\varepsilon,\varepsilon',\kappa} p^{\kappa-\frac{3}{2}+\varepsilon} + p^{\kappa-1-\delta+\varepsilon}\max\{1, y^{3-\kappa}\} + \frac{p^{\kappa+1+\varepsilon}}{ABy^{\kappa-1}}. \tag{10.13}$$

In view of Theorem 10.4, we aim to choose y and AB in a way such that $E' = o_\kappa(p^{\kappa-1})$ holds. To this end, we distinguish the cases $\kappa \geq 3$ and $1 < \kappa < 3$.

If $\kappa \geq 3$, we may choose y as large as possible, $y := p$ say. Then, for any A and B in the range given by Proposition 10.10 we obtain

$$\mathrm{E}' \ll_{\kappa,\varepsilon,\varepsilon'} p^{\max\{\kappa-\frac{3}{2},\kappa-1-\delta\}+\varepsilon},$$

since $AB \geq p$.

Now assume $1 < \kappa < 3$. To control the second term in (10.13), it is necessary to choose $y = O\big(p^{\frac{\delta-\varepsilon}{3-k}}\big)$. To adjust the second and third term in (10.13), we choose y and the product AB such that $y^2 = p^{2+\delta}/(AB)$ which eventually suggests the choice

$$y := \frac{p^{1+\frac{\delta}{2}}}{\sqrt{AB}} \qquad \text{and} \qquad AB \geq \max\left\{p^{2+\delta-2\frac{\delta-\varepsilon}{3-k}}, p^{1+\varepsilon'}\right\},$$

and effects the asserted error term

$$E' \ll_{\varepsilon,\varepsilon',\kappa} p^{\kappa-1}\left(\frac{p^{2+\delta-2\frac{\delta-\varepsilon}{3-\kappa}}}{AB}\right)^{\frac{3-\kappa}{2}}.$$

We are left with the treatment of the main term in (10.12). By (10.10), we may write

$$\begin{aligned}\sum_{l\leq 2p}\frac{\mu(l)}{l^\kappa}\sum_{n\leq y}\frac{1}{n^{\kappa-1}}\sum_{\substack{d\leq 2\sqrt{p}\\ d\mid p-1}}(n,d)\cdot\sharp\mathcal{T}(d,dnl)\\ \sim p\sum_{l\leq 2p}\frac{\mu(l)}{l^\kappa}\sum_{n\leq\frac{2p}{l}}\frac{1}{n^{\kappa-1}}\sum_{d\mid p-1}(n,d)\sum_{de\mid p-1}\mu(e)\sum_{\substack{N\in I_p\\ (de)^2\mid N\\ dnl\mid N}}H\left(\frac{(p+1-N)^2-4p}{(de)^2}\right),\end{aligned}$$

as $p\to\infty$, where the error term may be neglected by the same arguments as above. After some changes of the summation order, the sum over l in the above expression equals

$$\sum_{de\mid p-1}\mu(e)\sum_{\substack{N\in I_p\\ (de)^2\mid N}}H\left(\frac{(p+1-N)^2-4p}{(de)^2}\right)\sum_{n\mid\frac{N}{d}}\frac{(n,d)}{n^{\kappa-1}}\sum_{l\mid\frac{N}{dn}}\frac{\mu(l)}{l^\kappa}$$

which proves Theorem 10.2 (i) and (ii).

To conclude the treatment of Theorem 10.2, let us briefly discuss the case $0 < \kappa \leq 1$ which, by what we have already seen above, is a rather easy task. Choosing $A := B := \frac{p-1}{2}$, we clearly have

$$\mathcal{M}_p(\mathcal{T}(d,dnl);A,B) = \sharp\mathcal{T}(d,dnl),$$

and don't need to rely on Proposition 10.10. Theorem 10.2 then easily follows from (10.7), (10.8) and (10.10). □

10.4. Estimates for $M_{\mathrm{Ord}}(p,\kappa)$ and $M_{\mathrm{Ind}}(p,\kappa)$

It remains to estimate the terms $M_{\mathrm{Ord}}(p,\kappa)$ and $M_{\mathrm{Ind}}(p,\kappa)$.

10.4.1. Proof of Theorem 10.3. Let $A := B := \frac{p-1}{2}$. By Theorem 10.1, we have

$$M_{\mathrm{Ord}}(p,\kappa) = \frac{1}{p^2} \sum_{\substack{a,b\in\mathbb{F}_p^2 \\ 4a^3+27b^2\not\equiv 0 \ (p)}} \mathrm{Ord}^\kappa(\mathrm{E}_{a,b}) + O_{\kappa,\delta}\left(p^{\kappa-\delta}\right),$$

for appropriate $\delta > 0$. By Hasse's theorem, the upper bound of Theorem 10.3 follows easily. As for the lower bound, recall that $\mathcal{S}_{p,cyclic}$ denotes the set of tupels $(a,b) \in \mathbb{F}_p^2$ such that $4a^3+27b^2 \not\equiv 0 \ (p)$ and $\mathrm{E}_{a,b}(\mathbb{F}_p)$ is cyclic. Hence, by Lemma 6.6 we obtain

$$\begin{aligned}\sum_{\substack{a,b\in\mathbb{F}_p^2 \\ 4a^3+27b^2\not\equiv 0 \ (p)}} \mathrm{Ord}^\kappa(\mathrm{E}_{a,b}) &\geq \sum_{(a,b)\in\mathcal{S}_{cyclic}} \mathrm{Ord}^\kappa(\mathrm{E}_{a,b}) \\ &\geq \sum_{(a,b)\in\mathcal{S}_{cyclic}} N_{a,b}^\kappa \prod_{q\mid N_{a,b}} \left(1-\frac{q^\kappa-1}{q^{\kappa+1}-1}\right) \\ &\geq \sum_{(a,b)\in\mathcal{S}_{cyclic}} N_{a,b}^\kappa \prod_{q\mid N_{a,b}} \left(1-\frac{1}{q}\right),\end{aligned}$$

where the products run over prime divisors of $N_{a,b}$. Proceeding as in Section 9.3.3, Lemma 9.9, standard estimates for $\omega(n)$ (cf. [100, p. 83f]) and Hasse's theorem yield

$$\sum_{\substack{a,b\in\mathbb{F}_p^2 \\ 4a^3+27b^2\not\equiv 0 \ (p)}} \mathrm{Ord}^\kappa(\mathrm{E}_{a,b}) \gg \sum_{(a,b)\in\mathcal{S}_{cyclic}} \frac{N_{a,b}^\kappa}{\log\log p} \gg_\kappa \frac{p^\kappa}{\log\log p} \cdot \sharp\,\mathcal{S}_{p,cyclic}\,.$$

Combining this with Proposition 10.11, we finally find

$$M_{\mathrm{Ord}}(p,\kappa) \gg_\kappa \frac{p^\kappa}{\log\log p} \prod_{q\mid p-1}\left(1-\frac{1}{q(q^2-1)}\right) \gg \frac{p^\kappa}{\log\log p}$$

which proves Theorem 10.3. □

10.4.2. Proof of Theorem 10.4. We start with the lower bound. Since the lower bound is trivial in case $0 < \kappa \leq 1$, let us assume $\kappa > 1$, and note that $\mathrm{ind}_O(\mathrm{E}_{a,b}) = N_{a,b} \gg p$ by Hasse's theorem, whence

$$\mathrm{Ind}^\kappa(\mathrm{E}_{a,b}) = \frac{1}{N_{a,b}} \sum_{Q\in\mathrm{E}_{a,b}(\mathbb{F}_p)} \mathrm{ind}_Q(\mathrm{E}_{a,b})^\kappa \geq \frac{\mathrm{ind}_O(\mathrm{E}_{a,b})^\kappa}{N_{a,b}} \gg_\kappa p^{\kappa-1}.$$

Let us now turn to the upper bounds in Theorem 10.4. By Lemma 10.5, we clearly have

$$\begin{aligned}M_{\mathrm{Ind}}(p,\kappa) &= p^{\kappa-2} \sum_{de\mid p-1} \mu(e) \sum_{\substack{N\in I_p \\ (de)^2\mid N}} H\left(\frac{(p+1-N)^2-4p}{(de)^2}\right) \sum_{n\mid\frac{N}{d}} \frac{(n,d)}{n^{\kappa-1}} \theta_\kappa\left(\frac{N}{dn}\right) \\ &\ll p^{\kappa-2} \sum_{de\mid p-1} d \sum_{\substack{N\in I_p \\ (de)^2\mid N}} H\left(\frac{(p+1-N)^2-4p}{(de)^2}\right) \sum_{n\mid\frac{N}{d}} \frac{1}{n^{\kappa-1}} \\ &\ll p^{\kappa-\frac{3}{2}} \log p(\log\log p)^2 \sum_{de\mid p-1} \frac{1}{e} \sum_{\substack{N\in I_p \\ (de)^2\mid N}} \sum_{n\mid\frac{N}{d}} \frac{1}{n^{\kappa-1}}. \qquad (10.14)\end{aligned}$$

If $\kappa > 2$, the sum on n in (10.14) is $O_\kappa(1)$, and we obtain

$$M_{\mathrm{Ind}}(p,\kappa) \ll_\kappa p^{\kappa-1}\log p(\log\log p)^2 \sum_{de\mid p-1}\frac{1}{d^2e^3} \ll p^{\kappa-1}\log p(\log\log p)^2.$$

If $1 < \kappa < 2$, then the sum on n in (10.14) is $O_\varepsilon(p^\varepsilon)$ which gives us

$$M_{\mathrm{Ind}}(p,\kappa) \ll_\varepsilon p^{\kappa-1+\varepsilon} \sum_{de\mid p-1}\frac{1}{d^2e^3} \ll p^{\kappa-1+\varepsilon}.$$

If $0 < \kappa \leq 1$, then the sum on n in (10.14) is $O_\varepsilon(p^{1-\kappa+\varepsilon})$, whence

$$M_{\mathrm{Ind}}(p,\kappa) \ll_\varepsilon p^{\varepsilon} \sum_{de\mid p-1}\frac{1}{d^2e^3} \ll p^{\varepsilon}.$$

To treat the case $\kappa = 2$, we note the estimate

$$\sum_{f\mid m}\frac{1}{f} \leq \prod_{p\mid m}\left(1-\frac{1}{p}\right)^{-1} \ll \log\log m$$

which follows easily by Lemma 9.9 and standard estimates for $\omega(n)$ (cf. [100, p. 83f]). From this, we eventually infer

$$M_{\mathrm{Ind}}(p,2) \ll p\log p(\log\log p)^3 \sum_{de\mid p-1}\frac{1}{d^2e^3} \ll p\log p(\log\log p)^3$$

which proves Theorem 10.4 and concludes this chapter. □

Conclusion and Outlook

We conclude with a brief account of ideas for further research which arose in connection with the presented problems and were not addressed here. We group this discussion according to the division of this thesis into parts.

Primitive and λ-roots. In Chapter 3 we proved that, for arbitrary $n \in \mathbb{N}$, the least λ-root expressible as a sum of two squares $s^*(n)$ satisfies

$$s^*(n) \ll_\varepsilon n_c^{\frac{1}{2}+\varepsilon},$$

for any $\varepsilon > 0$ (cf. Theorem 3.1). However, similar to the least (prime) primitive root case, we expect the actual magnitude of $s^*(n)$ to be much smaller. In fact, we believe that

$$s^*(n) \ll \log^A n \tag{8}$$

should hold for sufficiently large $A > 0$. In view of Shoup's [95] and Martin's [73] results mentioned in Section 3.1, one might attempt to prove (8) under GRH or unconditionally on a density 1 subset of $\mathbb{N}$. Another natural approach would be to consider the average order of $s^*(n)$ and try to establish (8) on average. For further inspiration we refer to Paragraph 27 of Section 9.7 of Moree's survey article [75].

Residual index and order in number fields. In Part II, we considered a number field $\mathbb{K}$ and a finitely generated infinite subgroup Γ of $\mathbb{K}^*$ of arithmetic rank γ, and, for $\kappa \in \mathbb{R}_+$, investigated κ-th moments of the residual index and residual order of Γ over certain families of prime ideals and all ideals of $\mathbb{K}$, respectively.

Prime ideals. In Chapter 5, we proved, conditionally on GRH, the asymptotic formula

$$\sum_{\substack{\mathfrak{p} \in \mathcal{P}_C(x, \mathbb{L}/\mathbb{K}) \\ \overline{\Gamma} \subset (\mathcal{O}_\mathbb{K}/\mathfrak{p})^*}} \operatorname{ord}_\Gamma(\mathfrak{p})^\kappa \sim c_{\Gamma,C}^{(\kappa)} \cdot \operatorname{li}(x^{\kappa+1}), \tag{9}$$

as $x \to \infty$, where $\mathbb{L}$ is a finite Galois extension of $\mathbb{K}$, C denotes a conjugacy class in $\operatorname{Gal}(\mathbb{L}/\mathbb{K})$ and

$$c_{\Gamma,C}^{(\kappa)} := \sum_{n \geq 1} \frac{\psi_\kappa(n) |C(\Gamma, n)|}{n^\kappa [\mathbb{L}_{\Gamma,n} : \mathbb{K}]}$$

is a constant which we, at least under GRH, proved to be positive (cf. Theorem 5.3). Clearly, this result leaves room for further research: For example, it is desirable to remove the GRH condition and establish an unconditional asymptotic formula like (9). But similar to AC, this would, at least for our approach, require sharper prime ideal estimates which are not within the scope of contemporary methods. Another interesting challenge is to derive an explicit formula for the constant $c_{\Gamma,C}^{(\kappa)}$ in terms of Euler products. Such an expression is worthwhile, as it should reveal its positivity without relying on the GRH. For this purpose, it would be useful to factorise the involved field degrees appropriately, a task which we, however, not managed to solve in general.

Above all, any improvement on Wagstaff's heuristic would be desirable, as it would have an impact on AC as well (see Chapter 4). As illustrated in Chapter 4, however, such a result seems out of reach at the moment. In Chapter 6 we considered number field analogues of Wagstaff's heuristic on average (cf. Theorems 6.1 and 6.2). Our approach dealt with the average orders of the quantities $\mathrm{Ind}_\gamma^\kappa(\mathfrak{p})$ over prime ideals $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}/\mathbb{K})$ for which we established asymptotic formulae in case $\gamma \neq \kappa$. For the harder case $\gamma = \kappa$, we proved appropriate upper and lower bounds which we managed to turn into an asymptotic formula under GRH[37], if we additionally assumed both $\mathbb{K}$ and $\mathbb{L}$ to be Galois over $\mathbb{Q}$. Both results were in the spirit of Wagstaff's heuristic. It would be satisfactory, if one could extend the latter statement and unconditionally prove an asymptotic formula in case $\gamma = \kappa$, valid for all choices of $\mathbb{L}$ and $\mathbb{K}$. To this end, it would be convenient to have better estimates for the number of certain prime ideals, at least on average, to avoid an application of the effective Čebotarev density theorem under GRH. Indeed, as we have seen in Section 6.3, a number field analogue of the Bombieri-Vinogradov theorem (see Proposition 4.9) of full strength for any choice of $\mathbb{L}$ and $\mathbb{K}$ would suffice to solve the problem.

The above-mentioned problems are certainly pertinent for analogues concerning matrices, function fields and many others. Inspired by a work of Roskam [90], another interesting variation of the above problems would be to investigate moments of $\mathrm{ind}_\Gamma(p\,\mathcal{O}_\mathbb{K})$ and $\mathrm{ord}_\Gamma(p\,\mathcal{O}_\mathbb{K})$, over appropriate rational primes p which are unramified in $\mathbb{K}$. This problem differs from the consideration of prime ideals of $\mathbb{K}$ in many aspects. If we assume that $\mathbb{K}/\mathbb{Q}$ is Galois, for convenience, then the group $(\mathcal{O}_\mathbb{K}/p\,\mathcal{O}_\mathbb{K})^*$ is isomorphic to the direct product $\prod_{\mathfrak{p}|p}(\mathcal{O}_\mathbb{K}/\mathfrak{p})^*$ which has order $(p^{f_p}-1)^{[\mathbb{K}:\mathbb{Q}]/f_p}$ and exponent $p^{f_p}-1$, if we denote the inertia degree of p in $\mathbb{K}$ by f_p. In particular, it is only cyclic if p is inert in $\mathbb{K}$. Moreover, primes of any given inertia degree in $\mathbb{K}$ have a positive density, so that primes which do not split completely in $\mathbb{K}$ may not be neglected. By what we have encountered so far, one would thus guess that the reduction of Γ modulo p typically generates a subgroup of approximately $p^{f_p\cdot\min\{\gamma,[\mathbb{K}:\mathbb{Q}]/f_p\}}$ elements in $(\mathcal{O}_\mathbb{K}/p\,\mathcal{O}_\mathbb{K})^*$. This, however, already fails in rather elementary settings. Indeed, if $\mathbb{K}$ is a real quadratic field and ε a fundamental unit of $\mathbb{K}$, it can be easily shown that, for any inert prime p, $\mathrm{ord}_\varepsilon(p\,\mathcal{O}_\mathbb{K})$ is always a divisor of $2(p+1)$, even though $(\mathcal{O}_\mathbb{K}/p\,\mathcal{O}_\mathbb{K})^*$ contains p^2-1 elements (cf. [90]). Hence, this problem appears more sophisticated, and one might try to consider it on average and adapt the methods provided in Chapter 6 in the first place.

All ideals. Our study of $\mathrm{ind}_\Gamma(\mathfrak{a})$ over all ideals $\mathfrak{a}$ of $\mathbb{K}$ revealed some surprising insights. Motivated by a problem of Rohrlich, we obtained lower bounds for κ-th moments of $\mathrm{ind}_\Gamma(\mathfrak{a})$ over all ideals of $\mathbb{K}$ of the form

$$\sum_{\substack{\mathcal{N}\mathfrak{a}\leq x\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{a})^*}} \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa \geq x^{1+\kappa-\delta+o(1)},$$

as $x\to\infty$, where the o-term depends on $\mathbb{K}$, γ and κ, and the parameter δ may be chosen to be any positive real number which satisfies the smoothness condition for prime ideals of $\mathbb{K}$ introduced in Theorem 7.1. In fact, we proved (cf. Theorem 7.2) that δ can at least be chosen according to

$$\delta > \begin{cases} 0.303265\ldots, & \text{if } \mathbb{K} \text{ is abelian over } \mathbb{Q},\\ 0.5, & \text{under GRH.}\end{cases}$$

[37] In fact, we managed to remove the GRH assumption for suitable $\mathbb{L}$ (cf. Theorem 6.2).

Thus, unexpectedly, $\mathrm{ind}_\Gamma(\mathfrak{a})$ tends to be rather large on average. The aforementioned smoothness condition is widely assumed to hold for any $\delta > 0$, whence we even expect

$$\sum_{\substack{\mathcal{N}\mathfrak{a}\leq x\\ \overline{\Gamma}\subset(\mathcal{O}_\mathbb{K}/\mathfrak{a})^*}} \mathrm{ind}_\Gamma(\mathfrak{a})^\kappa = x^{1+\kappa+o(1)},$$

as $x \to \infty$. In view of Rohrlich's initial problem, any approach towards such a result would indeed be satisfying. One way to attend this problem is to refine our proof in Section 7.4 and find a way to enlarge the admissible values for δ, especially if $\mathbb{K}/\mathbb{Q}$ is not abelian. Note that we gave away some precision in this case, even under GRH, as we failed to transform splitting conditions for rational primes in $\mathbb{K}^{(n)}$ into appropriate arithmetic progression conditions. Another approach to tackle Rohrlich's problem was introduced in Section 7.5, where we described how lower bounds for the average order of $\mathrm{ind}_\Gamma(\mathfrak{a})$ may be traced back to lower bounds for the average order of $\mathrm{Ind}^1_\gamma(\mathfrak{a})$. Since, as we have frequently observed, the double averaging step usually eases a problem substantially, this approach has some appeal.

Residual index and order on elliptic curves defined over finite fields. In Part III, we studied the distribution of residual index and residual order of $\mathbb{F}_p$-rational points of certain elliptic curves defined over $\mathbb{F}_p$. The families under consideration were on the one hand given by the reductions modulo p of a fixed rational elliptic curve E, with p varying over primes of good reduction for E. On the other hand, we also considered specific families of elliptic curves defined over $\mathbb{F}_p$ for a fixed prime p.

Reductions of a rational elliptic curve modulo p. Let E be a rational elliptic curve and Q a fixed rational point thereon of infinite order. Average order, and moments in general, of $\mathrm{ind}_Q(\mathrm{E}_p)$ and $\mathrm{ord}_Q(\mathrm{E}_p)$ over primes p of good reduction for E seem difficult to track and have not been established yet, not even for CM-curves under GRH. Recalling the corresponding number field issues, this is certainly no surprise for $\mathrm{ind}_Q(\mathrm{E}_p)$. If we, however, oppose the state of AC to the state of the Lang-Trotter conjecture, and recall (9), then it makes sense to believe that asymptotic formulae like

$$\frac{1}{\pi(x)} \sum_{\substack{p\leq x\\ p\nmid N_\mathrm{E}}} \mathrm{ord}_Q(\mathrm{E}_p)^\kappa \sim c^{(\kappa)}_{\mathrm{E},Q} \cdot x^\kappa,$$

as $x \to \infty$, with $c^{(\kappa)}_{\mathrm{E},Q} > 0$, are achievable under GRH, at least in the CM case. To prove such a result, it might be reasonable to follow the approach of Kurlberg and Pomerance [51] which we extended to number fields in Chapter 5, and combine their ideas with arguments of Gupta's and Ram Murty's work [37] concerning the Lang-Trotter conjecture.

In Chapter 9, we tackled this problem on average and proved (cf. Theorem 9.1)

$$\sum_{\substack{p\leq x\\ p\nmid N_\mathrm{E}}} \mathrm{Ord}^\kappa(\mathrm{E}_p) \sim c^{(\kappa)}_\mathrm{E} \cdot \mathrm{li}(x^{1+\kappa}),$$

as $x \to \infty$, if E has CM by the ring of integers of an imaginary quadratic field, or under GRH otherwise, with the positive constant

$$c^{(\kappa)}_\mathrm{E} := \sum_{f,n,d,e\geq 1} \frac{\mu(n)\mu(e)}{n(fd)^{1+\kappa}} \sum_{mk\mid d} m\mu(k) \cdot \frac{\sharp D(mkdnf, de)}{[\mathbb{Q}(\mathrm{E}[[mkdnf, de]]) : \mathbb{Q}]}. \tag{10}$$

Similar to earlier discussions, the following questions arise naturally: Firstly, one might wonder, if the GRH condition for non-CM curves could be removed by a refinement of the arguments presented in Section 9.3.1. For that purpose it would suffice to have analogues of Propositions 9.6 and 9.7 for the non-CM case, as this would allow for an application of the unconditional effective Čebotarev density theorem and circumvent the GRH. Recall that the latter was not possible in our treatment, since we failed to get rid of primes with certain splitting behaviour in $\mathbb{Q}(\mathrm{E}[k])$ for k larger than a logarithm power. Further research is provided by the constant $c_{\mathrm{E}}^{(\kappa)}$. Although we believe in its positivity, the complicated representation (10) and the involved field degrees hindered us from giving a rigorous proof. To attend this problem, one might find the work of Freiberg and Kurlberg [32] inspiring. Eventually, one might wonder about analogue problems for the residual index which we expect to be rather small on average. While the establishment of asymptotic formulae for moments of $\mathrm{ind}_Q(\mathrm{E}_p)$ seems little promising, one might attempt to estimate the average order of $\mathrm{Ind}^{\kappa}(\mathrm{E}_p)$, instead. However, this task should prove to be more difficult than in the number field case, and it is questionable whether the same methods which we used to estimate the average order of $\mathrm{Ord}^{\kappa}(\mathrm{E}_p)$ also apply to this problem.

Families of elliptic curves defined over $\mathbb{F}_p$. In Chapter 10 we took a different point of view and, for a fixed prime $p > 3$, considered the average order of $\mathrm{Ind}^{\kappa}(\mathrm{E}_{a,b})$ and $\mathrm{Ord}^{\kappa}(\mathrm{E}_{a,b})$, respectively, over a two-parameter family of elliptic curves $\mathrm{E}_{a,b} \,/\, \mathbb{F}_p$ given by Weierstraß equations with $|a| \leq A$ and $|b| \leq B$. For sufficiently large A and B, we managed to prove the asymptotic equivalences

$$\sum_{\substack{|a|\leq A,|b|\leq B\\ p\nmid 4a^3+27b^2}} \frac{\mathrm{Ord}^{\kappa}(\mathrm{E}_{a,b})}{4AB} \sim M_{\mathrm{Ord}}(p,\kappa) \qquad \text{and} \qquad \sum_{\substack{|a|\leq A,|b|\leq B\\ p\nmid 4a^3+27b^2}} \frac{\mathrm{Ind}^{\kappa}(\mathrm{E}_{a,b})}{4AB} \sim M_{\mathrm{Ind}}(p,\kappa),$$

as $p \to \infty$, which expressed the respective average orders in terms of Kronecker class numbers and allowed to confirm the expected orders of growth (cf. Theorems 10.1–10.4). Again, this result leaves room for further research. One might for example try to reduce the respective admissible ranges for A and B or consider variations for other families of elliptic curves defined over $\mathbb{F}_p$ which are, for instance, given in Legendre form (cf. [96]). A last but not less interesting challenge is the investigation of the terms $M_{\mathrm{Ind}}(p,\kappa)$ and $M_{\mathrm{Ord}}(p,\kappa)$. To this end, one might try to express the involved Kronecker class numbers by the analytic class number formula, apply estimates for character sums and hope for appropriate cancellation. In this way one would hopefully improve our understanding of the residual index and order of $\mathbb{F}_p$-rational points of elliptic curves defined over $\mathbb{F}_p$.

Bibliography

[1] C. Ambrose, *Artin's primitive root conjecture and a problem of Rohrlich*, to appear in Math. Proc. Cambridge Philos. Soc.

[2] C. Ambrose, *On the least primitive root expressible as a sum of two squares*, Integers, 13 (2013), pp. Paper No. A55, 7.

[3] E. Artin, *Collected papers*, Springer-Verlag, New York, 1982. Edited by Serge Lang and John T. Tate, Reprint of the 1965 original.

[4] E. Bach and J. Shallit, *Algorithmic number theory. Vol. 1*, Foundations of Computing Series, MIT Press, Cambridge, MA, 1996. Efficient algorithms.

[5] R. C. Baker and G. Harman, *Shifted primes without large prime factors*, Acta Arith., 83 (1998), pp. 331–361.

[6] A. Balog, $p + a$ *without large prime factors*, in Seminar on number theory, 1983–1984 (Talence, 1983/1984), Univ. Bordeaux I, Talence, 1984, pp. Exp. No. 31, 5.

[7] W. D. Banks and I. E. Shparlinski, *Sato-Tate, cyclicity, and divisibility statistics on average for elliptic curves of small height*, Israel J. Math., 173 (2009), pp. 253–277.

[8] H. Bilharz, *Primdivisoren mit vorgegebener Primitivwurzel*, Math. Ann., 114 (1937), pp. 476–492.

[9] V. Blomer and F. Brumley, *On the Ramanujan conjecture over number fields*, Ann. of Math. (2), 174 (2011), pp. 581–605.

[10] ———, *The role of the Ramanujan conjecture in analytic number theory*, Bull. Amer. Math. Soc. (N.S.), 50 (2013), pp. 267–320.

[11] E. Bombieri, J. B. Friedlander, and H. Iwaniec, *Primes in arithmetic progressions to large moduli. III*, J. Amer. Math. Soc., 2 (1989), pp. 215–224.

[12] S. Bosch, *Algebra. 5., überarbeitete Aufl.*, Springer-Lehrbuch. Berlin: Springer. viii, 376 S., 2004.

[13] J. Brüdern, *Einführung in die analytische Zahlentheorie*, Berlin: Springer-Verlag, 1995.

[14] D. A. Burgess, *On character sums and primitive roots*, Proc. London Math. Soc. (3), 12 (1962), pp. 179–192.

[15] ———, *On character sums and L-series. II*, Proc. London Math. Soc. (3), 13 (1963), pp. 524–536.

[16] J. Cohen, *Primitive roots in quadratic fields*, Int. J. Number Theory, 2 (2006), pp. 7–23.

[17] A. C. Cojocaru, *Questions about the reductions modulo primes of an elliptic curve*, in Number theory, vol. 36 of CRM Proc. Lecture Notes, pp. 61–79.

[18] ———, *Cyclicity of CM elliptic curves modulo p*, Trans. Amer. Math. Soc., 355 (2003), pp. 2651–2662 (electronic).

[19] ———, *Reductions of an elliptic curve with almost prime orders*, Acta Arith., 119 (2005), pp. 265–289.

[20] G. Cooke and P. J. Weinberger, *On the construction of division chains in algebraic number rings, with applications to* SL_2, Comm. Algebra, 3 (1975), pp. 481–524.

[21] M. Deuring, *Die Typen der Multiplikatorenringe elliptischer Funktionenkörper*, Abh. Math. Sem. Univ. Hamburg, 14 (1941), pp. 197–272.

[22] W. Duke, *Almost all reductions modulo p of an elliptic curve have a large exponent*, C. R. Math. Acad. Sci. Paris, 337 (2003), pp. 689–692.

[23] P. D. T. A. Elliott, *The distribution of primitive roots*, Canad. J. Math., 21 (1969), pp. 822–841.

[24] P. Erdős and M. R. Murty, *On the order of a* (mod p), in Number theory (Ottawa, ON, 1996), vol. 19 of CRM Proc. Lecture Notes, Amer. Math. Soc., Providence, RI, 1999, pp. 87–97.

[25] P. Erdős, C. Pomerance, and E. Schmutz, *Carmichael's lambda function*, Acta Arith., 58 (1991), pp. 363–385.

[26] A. T. Felix, *Variations on Artin's Primitive Root Conjecture*, ProQuest LLC, Ann Arbor, MI, 2011. Thesis (Ph.D.)–Queen's University (Canada).

[27] ———, *Generalizing the Titchmarsh divisor problem*, Int. J. Number Theory, 8 (2012), pp. 613–629.

[28] A. T. Felix and M. R. Murty, *A problem of Fomenko's related to Artin's conjecture*, Int. J. Number Theory, 8 (2012), pp. 1687–1723.
[29] O. M. Fomenko, *On the class numbers of indefinite binary quadratic forms and the residual indices of integers modulo a prime p*, Zap. Nauchn. Sem. S.-Peterburg. Otdel. Mat. Inst. Steklov. (POMI), 286 (2002), pp. 179–199, 231–232.
[30] C. Franc and M. R. Murty, *On a generalization of Artin's conjecture*, Pure Appl. Math. Q., 4 (2008), pp. 1279–1290.
[31] G. Frei, F. Lemmermeyer, and R. P. J., *Emil Artin and Helmut Hasse. Die Korrespondenz 1923–1934*, Göttingen: Universitätsverlag Göttingen, 2008.
[32] T. Freiberg and P. Kurlberg, *On the average exponent of elliptic curves modulo p*, Int. Math. Res. Not. IMRN, (2013), p. 29.
[33] J. Friedlander and H. Iwaniec, *Opera de cribro*, vol. 57 of American Mathematical Society Colloquium Publications, American Mathematical Society, Providence, RI, 2010.
[34] J. B. Friedlander, *Shifted primes without large prime factors*, in Number theory and applications (Banff, AB, 1988), vol. 265 of NATO Adv. Sci. Inst. Ser. C Math. Phys. Sci., Kluwer Acad. Publ., Dordrecht, 1989, pp. 393–401.
[35] C. F. Gauss, *Disquisitiones arithmeticae*, Springer-Verlag, New York, 1986. Translated and with a preface by Arthur A. Clarke, Revised by William C. Waterhouse, Cornelius Greither and A. W. Grootendorst and with a preface by Waterhouse.
[36] R. Gupta and M. R. Murty, *A remark on Artin's conjecture*, Invent. Math., 78 (1984), pp. 127–130.
[37] ———, *Primitive points on elliptic curves*, Compositio Math., 58 (1986), pp. 13–44.
[38] ———, *Cyclicity and generation of points mod p on elliptic curves*, Invent. Math., 101 (1990), pp. 225–235.
[39] D. R. Heath-Brown, *Artin's conjecture for primitive roots*, Quart. J. Math. Oxford Ser. (2), 37 (1986), pp. 27–38.
[40] D. Hilbert, *The theory of algebraic number fields*, Springer-Verlag, Berlin, 1998.
[41] J. Hinz and M. Lodemann, *On Siegel zeros of Hecke-Landau zeta-functions*, Monatsh. Math., 118 (1994), pp. 231–248.
[42] C. Hooley, *On Artin's conjecture*, J. Reine Angew. Math., 225 (1967), pp. 209–220.
[43] E. W. Howe, *On the group orders of elliptic curves over finite fields*, Compositio Math., 85 (1993), pp. 229–247.
[44] D. Husemöller, *Elliptic curves*, vol. 111 of Graduate Texts in Mathematics, Springer-Verlag, New York, second ed., 2004. With appendices by Otto Forster, Ruth Lawrence and Stefan Theisen.
[45] H. Iwaniec and E. Kowalski, *Analytic number theory*, vol. 53 of American Mathematical Society Colloquium Publications, American Mathematical Society, Providence, RI, 2004.
[46] J. C. Jantzen and J. Schwermer, *Algebra*, Springer-Verlag, Berlin, 2009.
[47] N. Kataoka, *The distribution of prime ideals in a real quadratic field with units having a given index in the residue class field*, J. Number Theory, 101 (2003), pp. 349–375.
[48] H. H. Kim, *Functoriality for the exterior square of* GL_4 *and the symmetric fourth of* GL_2, J. Amer. Math. Soc., 16 (2003), pp. 139–183 (electronic). With appendix 1 by Dinakar Ramakrishnan and appendix 2 by Kim and Peter Sarnak.
[49] S. Kim, *On the average exponent of CM elliptic curves modulo p*, arXiv preprint arXiv:1207.6652, (2012).
[50] P. Kurlberg, *On the order of unimodular matrices modulo integers*, Acta Arith., 110 (2003), pp. 141–151.
[51] P. Kurlberg and C. Pomerance, *On a problem of Arnold: the average multiplicative order of a given integer*, Algebra Number Theory, 7 (2013), pp. 981–999.
[52] J. C. Lagarias and A. M. Odlyzko, *Effective versions of the Chebotarev density theorem*, in Algebraic number fields: L-functions and Galois properties (Proc. Sympos., Univ. Durham, Durham, 1975), Academic Press, London, 1977, pp. 409–464.
[53] E. Landau, *Neuer Beweis des Primzahlsatzes und Beweis des Primidealsatzes*, Math. Ann., 56 (1903), pp. 645–670.
[54] S. Lang, *Algebraic number theory*, vol. 110 of Graduate Texts in Mathematics, Springer-Verlag, New York, second ed., 1994.
[55] ———, *Algebra*, vol. 211 of Graduate Texts in Mathematics, Springer-Verlag, New York, third ed., 2002.

[56] S. Lang and H. Trotter, *Primitive points on elliptic curves*, Bull. Amer. Math. Soc., 83 (1977), pp. 289–292.
[57] F. Lemmermeyer and R. P. J., *Die mathematischen Tagebücher von Helmut Hasse 1923-1935*, Göttingen: Universitätsverlag Göttingen, 2012.
[58] H. W. Lenstra, Jr., *On Artin's conjecture and Euclid's algorithm in global fields*, Invent. Math., 42 (1977), pp. 201–224.
[59] ———, *Factoring integers with elliptic curves*, Ann. of Math. (2), 126 (1987), pp. 649–673.
[60] S. Li, *On the number of elements with maximal order in the multiplicative group modulo n*, Acta Arith., 86 (1998), pp. 113–132.
[61] ———, *On extending Artin's conjecture to composite moduli.*, Mathematika, 46 (1999), pp. 373–390.
[62] ———, *An improvement of Artin's conjecture on average for composite moduli*, Mathematika, 51 (2004), pp. 97–109 (2005).
[63] ———, *Artin's conjecture for composite moduli*, Int. J. Pure Appl. Math., 45 (2008), pp. 419–427.
[64] S. Li and C. Pomerance, *Primitive roots: a survey*, in Number theoretic methods (Iizuka, 2001), vol. 8 of Dev. Math., Kluwer Acad. Publ., Dordrecht, 2002, pp. 219–231.
[65] ———, *On generalizing Artin's conjecture on primitive roots to composite moduli*, J. Reine Angew. Math., 556 (2003), pp. 205–224.
[66] ———, *The Artin-Carmichael primitive root problem on average*, Mathematika, 55 (2009), pp. 167–176.
[67] J. V. Linnik, *The dispersion method in binary additive problems*, Translated by S. Schuur, American Mathematical Society, Providence, R.I., 1963.
[68] F. Lorenz, *Algebraische Zahlentheorie*, Bibliographisches Institut, Mannheim, 1993.
[69] F. Luca, *Some mean values related to average multiplicative orders of elements in finite fields*, Ramanujan J., 9 (2005), pp. 33–44.
[70] F. Luca and A. Sankaranarayanan, *On the moments of the Carmichael λ function*, Acta Arith., 123 (2006), pp. 389–398.
[71] F. Luca and I. E. Shparlinski, *Average multiplicative orders of elements modulo n*, Acta Arith., 109 (2003), pp. 387–411.
[72] W. Luo, Z. Rudnick, and P. Sarnak, *On the generalized Ramanujan conjecture for* GL(n), in Automorphic forms, automorphic representations, and arithmetic (Fort Worth, TX, 1996), vol. 66 of Proc. Sympos. Pure Math., Amer. Math. Soc., Providence, RI, 1999, pp. 301–310.
[73] G. Martin, *The least prime primitive root and the shifted sieve*, Acta Arith., 80 (1997), pp. 277–288.
[74] ———, *Uniform bounds for the least almost-prime primitive root*, Mathematika, 45 (1998), pp. 191–207.
[75] P. Moree, *Artin's primitive root conjecture—a survey*, Integers, 12 (2012), pp. 1305–1416.
[76] ———, *Near-primitive roots*, Funct. Approx. Comment. Math., 48 (2013), pp. 133–145.
[77] T. W. Müller and J.-C. Schlage-Puchta, *On the number of primitive λ-roots*, Acta Arith., 115 (2004), pp. 217–223.
[78] L. Murata, *A problem analogous to Artin's conjecture for primitive roots and its applications*, Arch. Math. (Basel), 57 (1991), pp. 555–565.
[79] M. R. Murty, *On Artin's conjecture*, J. Number Theory, 16 (1983), pp. 147–168.
[80] ———, *Artin's conjecture for primitive roots*, Math. Intelligencer, 10 (1988), pp. 59–67.
[81] M. R. Murty and V. K. Murty, *A variant of the Bombieri-Vinogradov theorem*, in Number theory (Montreal, Que., 1985), vol. 7 of CMS Conf. Proc., Amer. Math. Soc., Providence, RI, 1987, pp. 243–272.
[82] M. R. Murty and K. L. Petersen, *A Bombieri-Vinogradov theorem for all number fields*, Trans. Amer. Math. Soc., 365 (2013), pp. 4987–5032.
[83] M. R. Murty and S. Srinivasan, *Some remarks on Artin's conjecture*, Canad. Math. Bull., 30 (1987), pp. 80–85.
[84] W. Narkiewicz, *A note on Artin's conjecture in algebraic number fields*, J. Reine Angew. Math., 381 (1987), pp. 110–115.
[85] ———, *Elementary and analytic theory of algebraic numbers*, Springer Monographs in Mathematics, Springer-Verlag, Berlin, third ed., 2004.
[86] J. Neukirch, *Algebraische Zahlentheorie*, Springer-Verlag, Berlin, 2007.
[87] F. Pappalardi, *On Hooley's theorem with weights*, Rend. Sem. Mat. Univ. Politec. Torino, 53 (1995), pp. 375–388. Number theory, II (Rome, 1995).
[88] D. E. Rohrlich, *Nonvanishing of L-functions for* GL(2), Invent. Math., 97 (1989), pp. 381–403.

[89] ———, *Self-dual Artin representations*, in Automorphic Representations and L-functions, vol. 22, Tata Institute of Fundamental Research Studies in Mathematics, Mumbai, 2013, pp. 455–499.
[90] H. Roskam, *Erratum: "A quadratic analogue of Artin's conjecture on primitive roots" [J. Number Theory* **81** *(2000), no. 1, 93–109; MR1743503 (2000k:11128)]*, J. Number Theory, 85 (2000), p. 108.
[91] R. Schaback and H. Wendland, *Numerische Mathematik*, Berlin: Springer, 5th completely new revised ed., 2005.
[92] R. Schoof, *Nonsingular plane cubic curves over finite fields*, J. Combin. Theory Ser. A, 46 (1987), pp. 183–211.
[93] J. Serre, *Résumé des cours de 1977-1978*, Annuaire du Collège de France, (1978), pp. 67–70.
[94] ———, *Quelques applications du théorème de densité de Chebotarev*, Inst. Hautes Études Sci. Publ. Math., (1981), pp. 323–401.
[95] V. Shoup, *Searching for primitive roots in finite fields*, Math. Comp., 58 (1992), pp. 369–380.
[96] J. H. Silverman, *The arithmetic of elliptic curves*, vol. 106 of Graduate Texts in Mathematics, Springer, Dordrecht, second ed., 2009.
[97] H. M. Stark, *Some effective cases of the Brauer-Siegel theorem*, Invent. Math., 23 (1974), pp. 135–152.
[98] E. M. Stein and G. Weiss, *Introduction to Fourier analysis on Euclidean spaces*, Princeton University Press, Princeton, N.J., 1971. Princeton Mathematical Series, No. 32.
[99] P. Stevenhagen, *The correction factor in Artin's primitive root conjecture*, J. Théor. Nombres Bordeaux, 15 (2003), pp. 383–391. Les XXIIèmes Journées Arithmetiques (Lille, 2001).
[100] G. Tenenbaum, *Introduction to analytic and probabilistic number theory*, vol. 46 of Cambridge Studies in Advanced Mathematics, Cambridge University Press, Cambridge, 1995.
[101] S. S. Wagstaff, Jr., *Pseudoprimes and a generalization of Artin's conjecture*, Acta Arith., 41 (1982), pp. 141–150.
[102] S. Warner, *Modern algebra. Vols. I, II*, Prentice-Hall Inc., Englewood Cliffs, N.J., 1965.
[103] L. C. Washington, *Introduction to cyclotomic fields*, vol. 83 of Graduate Texts in Mathematics, Springer-Verlag, New York, second ed., 1997.
[104] W. C. Waterhouse, *Abelian varieties over finite fields*, Ann. Sci. École Norm. Sup. (4), 2 (1969), pp. 521–560.
[105] A. Weil, *Sur les courbes algébriques et les variétés qui s'en déduisent*, Actualités Sci. Ind., no. 1041 = Publ. Inst. Math. Univ. Strasbourg **7** (1945), Hermann et Cie., Paris, 1948.
[106] J. Wu, *The average exponent of elliptic curves modulo p*, J. Number Theory, 135 (2014), pp. 28–35.
[107] J. Zelinsky, *Upper bounds for the number of primitive ray class characters with conductor below a given bound*, arXiv preprint arXiv:1307.2319, (2013).

List of Figures

List of Tables

List of Notations

To provide a clear account of the commonly used notation in this thesis, we, without further notice, agree upon the following conventions: By G and G' we mean finite abelian groups, and $\mathcal{A}$ denotes a subset of the positive integers. $\mathbb{F}$, $\mathbb{F}'$ and $\mathbb{F}''$ are fields, R denotes an arbitrary commutative ring, and by r and $\mathcal{I}$ we mean an arbitrary element and an ideal of R, respectively. Further, $\mathbb{K}$ denotes a number field of degree N over $\mathbb{Q}$, Γ a finitely generated subgroup of $\mathbb{K}^*$, $\mathbb{L}$ a finite Galois extension of $\mathbb{K}$ and C is a union of conjugacy classes inside $\mathrm{Gal}(\mathbb{L}\,/\,\mathbb{K})$. By $\mathfrak{a}$ and $\mathfrak{a}'$ we denote ideals of $\mathbb{K}$ and $\mathfrak{p}$ and $\mathfrak{P}$ denote prime ideals of $\mathbb{K}$ and $\mathbb{L}$, respectively. The letter p always denotes a prime number, and γ and κ denote a positive integer and a positive real number, respectively. Further, $\boldsymbol{a} = (a_1, \ldots, a_\gamma)$, $\boldsymbol{x} = (x_1, \ldots, x_\gamma)$ and $\boldsymbol{y} = (y_1, \ldots, y_\gamma)$ denote vectors in $\mathbb{R}^{N\times\gamma}$, $\omega_1, \ldots, \omega_\gamma$ are functions on $\mathbb{R}^N$ and A and Y denote either square matrices or automorphisms of the linear space $\mathbb{R}^N$. By $\mathcal{O}$, we mean a complex quadratic order, and E denotes an elliptic curve which is defined over $\mathbb{F}$. In some cases we tacitly assume $\mathbb{F} = \mathbb{Q}$ or $\mathbb{F} = \mathbb{F}_p$. Finally d, e, m, k, n and q denote arbitrary positive integers and x, y and z represent complex or real numbers which are chosen according to the respective context.

$\langle \cdot, \cdot \rangle$	Standard scalar product on $\mathbb{R}^N$	69
$\left[\frac{\mathbb{L}\|\mathbb{K}}{\mathfrak{p}}\right]$	Frobenius symbol of $\mathfrak{p}$ in $\mathrm{Gal}(\mathbb{L}\,/\,\mathbb{K})$	xvii
(a, b), $[a, b]$	Greatest common divisor and least common multiple of $a, b \in \mathbb{N}$	xv
$\left(\frac{a}{b}\right)$	Legendre-Jacobi symbol associated to $a \in \mathbb{Z}$ and $b \in \mathbb{N}$	xv
$\langle a_1, \ldots, a_n \rangle$	Subgroup of G generated by $a_1, \ldots, a_n \in G$	xv
(r)	Principal ideal in R generated by r	xv
$\bigoplus_{i=1}^n G_i$	Direct sum of groups $G_1, \ldots, G_n$	xv
$\overline{\mathbb{F}}$	Algebraic closure of $\mathbb{F}$	xvi
$\overline{\Gamma}$	Reduction of Γ modulo an ideal of $\mathbb{K}$	xvi
$\overline{\Gamma} \subset (\mathcal{O}_\mathbb{K}\,/\,\mathfrak{a})^*$	$\mathfrak{p}$-adic valuation of a is zero for any $a \in \Gamma$ and any $\mathfrak{p} \supset \mathfrak{a}$	xvi
$\overline{Q}$	Reduction of $Q \in \mathrm{E}(\mathbb{Q})$ modulo a prime of good reduction for E	94
$\overline{x}$	Complex conjugate of x	xvii
$\|\cdot\|_2$	Euclidean norm	69
$\|D\|$	Number of conjugacy classes in a union of conjugacy classes D	xv
$\mid M \mid$, $\sharp M$	Cardinality of a set M	xv
$\mid x \mid$	Absolute value of x	xvii
$\mathbf{0}$	Null vector $(0, \ldots, 0) \in \mathbb{R}^{N\times\gamma}$	73
A^*, A^{-*}	Hermitian adjoint of A and its inverse	69
$\mathfrak{a} \mid a$	$\mathfrak{a}$ divides $a\,\mathcal{O}_\mathbb{K}$ with $a \in \mathcal{O}_\mathbb{K}$	xvi
$\mathfrak{a} \mid \mathfrak{a}'$	$\mathfrak{a}$ divides $\mathfrak{a}'$	xvi
$a \mid b$, $a \nmid b$	$a \in \mathbb{Z}$ does or does not divide $b \in \mathbb{Z}$	xv
$a \equiv b\ (r)$	$a \in R$ and $b \in R$ yield the same residue class modulo (r)	xvi
$a \equiv b \bmod I$	$a \in R$ and $b \in R$ yield the same residue class modulo $\mathcal{I}$	xvi
$\mathcal{A}_d$	Set of $a \in \mathcal{A}$ which are divisible by $d \in \mathbb{N}$	18
$A^{(\kappa)}_{\gamma,C}$	Asymptotic constant for average order of $\mathrm{Ind}^\kappa_\gamma(\mathfrak{p})$ over $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}\,/\,\mathbb{K})$	54
$\alpha_z(n)$	Arithmetic function defined in (5.9)	39
$a \bmod \mathcal{I}$	Residue class of $a \in R$ modulo $\mathcal{I}$	xvi
a_p	Difference $\sharp\,\mathrm{E}_p(\mathbb{F}_p) - (p+1)$	94

$\mathrm{Aut}(\mathrm{E})$	Automorphism group of E 92
$\mathrm{Aut}(F)$	Group of automorphisms of a form F 114
$\mathrm{Aut}_{\mathbb{F}}(\mathrm{E})$	$\mathbb{F}$-automorphism group of E 92
$A\boldsymbol{x}$	$(Ax_1, \dots, Ax_\gamma)$ 71
$\mathcal{B}$	Integral basis of $\mathbb{K}$ 69
$\beta_0(\mathbb{K})$	Possible Siegel zero of $\zeta_{\mathbb{K}}(s)$ 30
$\beta_a(k)$	Arithmetic function, defined in Lemma 5.15 48
$\mathbb{C}$	Complex numbers xv
$C(\Gamma, n)$	Set of $\sigma \in \mathrm{Gal}(\mathbb{L}_{\Gamma,n} / \mathbb{K})$ which satisfy $\sigma\,\vert_{\mathbb{L}} \in C$ and $\sigma\,\vert_{\mathbb{K}_{\Gamma,n}} = \mathrm{id}$ 34
$c^{(\kappa)}$	generalized Stephens' constant 44
C_0	Conjugacy class $\{\mathrm{id}\}$ in a Galois group of a Galois extension 83
c_0	Certain coefficient associated to the principal character χ_0 modulo n 20
c_a	Asymptotic constant for average order of $\mathrm{ord}_a(p)$ over primes p 33
$C_{b,q}$	Conjugacy class in $\mathrm{Gal}(\mathbb{Q}(\zeta_q)/\mathbb{Q})$ corresponding to b mod $q \in (\mathbb{Z}/q\mathbb{Z})^*$ 48
$c_C(n)$	Number of $\sigma \in \mathrm{Gal}(\mathbb{L}(\zeta_n)/\mathbb{K})$ with $\sigma\,\vert_{\mathbb{L}} \in C$ and $\sigma\,\vert_{\mathbb{K}(\zeta_n)} = \mathrm{id}$ 54
c_χ	Certain coefficients associated to Dirichlet characters χ modulo n 19
$c_{\mathrm{E}}^{(\kappa)}$	Asymptotic constant for average order of $\mathrm{Ord}^\kappa(\mathrm{E})$ over primes p 96
$c_{\Gamma,C}^{(\kappa)}$	Asymptotic constant for κ-th moments of $\mathrm{ord}_\Gamma(\mathfrak{p})$ over $\mathfrak{p} \in \mathcal{P}_C(\mathbb{L}/\mathbb{K})$ 34
$\mathrm{char}(\mathbb{F})$	Characteristic of $\mathbb{F}$ xvi
χ_0	Principal character 72
c_∞	Limit of $c^{(\kappa)}$ as $\kappa \to \infty$ 46
C_n	Cyclic group with n elements xv
$c_{Stephens}$	Stephens' constant 33
$D(m, n)$	Certain union of conjugacy classes in $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[[m, n]])/\mathbb{Q})$ 96
$d_{a,b}$	Structure constant of $\mathrm{E}_{a,b}$ given by $\mathrm{E}_{a,b}(\mathbb{F}_p) = \mathbb{Z}/\,d_{a,b}\,\mathbb{Z} \oplus \mathbb{Z}/\,e_{a,b}\,d_{a,b}\,\mathbb{Z}$ . . . 117
D, D^+, D^-	Integers associated to discriminants Δ, Δ^+ and Δ^- 44
$\delta(h)$	Originally conjectured density by Artin 4
$\Delta(\mathcal{O})$	Discriminant of $\mathcal{O}$ 114
$\boldsymbol{\delta}(S)$	Density of the set S in some set T xvii
Δ^+, Δ^-	Discriminants of $\mathbb{K}^+$ and $\mathbb{K}^-$ 41
δ_a	Density of primes p for which a is a primitive root modulo p 3
$\delta_{a,k}$	Density of primes $p \nmid a$ which satisfy $\mathrm{ind}_a(p) = k$ 9
δ_{Artin}	Artin's constant 4
$\delta_{\mathrm{E},Q}$	Density of primes p for which $Q \in \mathrm{E}(\mathbb{Q})$ is a primitive point of E modulo p . . 14
$\Delta_{\mathrm{E}_{a,b}}$	Discriminant of $\mathrm{E}_{a,b}$ 91
$\Delta_{\mathbb{K}}$	Discriminant of $\mathbb{K}$ xvi
$\delta_n(k)$	Characteristic function of λ-roots modulo n 19
$\det(A)$	Determinant of A xv
D_k	Certain union of conjugacy classes in $\mathrm{Gal}(\mathbb{Q}(\mathrm{E}[k])/\mathbb{Q})$ 94
d_p	Structure constant of $\mathrm{E}_p(\mathbb{F}_p)$ given by $\mathrm{E}_p(\mathbb{F}_p) = \mathbb{Z}/d_p\,\mathbb{Z} \oplus \mathbb{Z}/e_p d_p\,\mathbb{Z}$ 94
e	Euler's constant xvii
$\boldsymbol{e}(\langle \boldsymbol{x}, \boldsymbol{y} \rangle)$	$e(\langle x_1, y_1 \rangle) \cdots e(\langle x_\gamma, y_\gamma \rangle)$ 73
$\mathrm{E}(\mathbb{F})$	$\mathbb{F}$-rational points of E 91
$\mathrm{E}[k]$	k-torsion points of E 91
$e(x)$	Additive character on $\mathbb{R}$ defined by $\exp(2\pi i x)$ xvii
$\mathrm{E}/\mathbb{F}$	E is defined over $\mathbb{F}$ 91
$e_{a,b}$	Structure constant of $\mathrm{E}_{a,b}$ given by $\mathrm{E}_{a,b}(\mathbb{F}_p) = \mathbb{Z}/\,d_{a,b}\,\mathbb{Z} \oplus \mathbb{Z}/\,e_{a,b}\,d_{a,b}\,\mathbb{Z}$ . . . 117
$\mathrm{End}(\mathrm{E})$	Endomorphism ring of E 92
$\mathrm{End}_{\mathbb{F}}(\mathrm{E})$	$\mathbb{F}$-endomorphism ring of E 92
E_p	Reduction of E modulo p, if E is defined over $\mathbb{Q}$ 93
e_p	Structure constant of $\mathrm{E}_p(\mathbb{F}_p)$ given by $\mathrm{E}_p(\mathbb{F}_p) = \mathbb{Z}/d_p\,\mathbb{Z} \oplus \mathbb{Z}/e_p d_p\,\mathbb{Z}$ 94
$\eta_\kappa(d)$	Correction factor in Theorem 5.14 44

Index