Class Number Problems for Quadratic Fields

By
Kostadinka Lapkova

Submitted to
Central European University
Department of Mathematics and Its Applications

In partial fulfilment of the requirements
for the degree of Doctor of Philosophy

Supervisor: András Biró

Budapest, Hungary
2012

Abstract

The current thesis deals with class number questions for quadratic number fields. The main focus of interest is a special type of real quadratic fields with Richaud–Degert discriminants $d = (an)^2 + 4a$, which class number problem is similar to the one for imaginary quadratic fields.

The thesis contains the solution of the class number one problem for the two-parameter family of real quadratic fields $\mathbb{Q}(\sqrt{d})$ with square-free discriminant $d = (an)^2 + 4a$ for positive odd integers a and n, where n is divisible by $43 \cdot 181 \cdot 353$. More precisely, it is shown that there are no such fields with class number one. This is the first unconditional result on class number problem for Richaud–Degert discriminants depending on two parameters, extending a vast literature on one-parameter cases. The applied method follows results of A. Biró for computing a special value of a certain zeta function for the real quadratic field, but uses also new ideas relating our problem to the class number of some imaginary quadratic fields.

Further, the existence of infinitely many imaginary quadratic fields whose discriminant has exactly three distinct prime factors and whose class group has an element of a fixed large order is proven. The main tool used is solving an additive problem via the circle method. This result on divisibility of class numbers of imaginary quadratic fields is applied to generalize the first theorem: there is an infinite family of parameters $q = p_1p_2p_3$, where p_1, p_2, p_3 are distinct primes, and $q \equiv 3 \pmod 4$, with the following property. If $d = (an)^2 + 4a$ is square-free for odd positive integers a and n, and q divides n, then the class number of $\mathbb{Q}(\sqrt{d})$ is greater than one.

The third main result is establishing an effective lower bound for the class number of the family of real quadratic fields $\mathbb{Q}(\sqrt{d})$, where $d = n^2 + 4$ is a square-free positive integer with $n = m(m^2 - 306)$ for some odd m, with the extra condition $\left(\frac{d}{N}\right) = -1$ for $N = 2^3 \cdot 3^3 \cdot 103 \cdot 10303$. This result can be regarded as a corollary of a theorem of Goldfeld and some calculations involving elliptic curves and local heights. The lower bound tending to infinity for a subfamily of the real quadratic fields with discriminant $d = n^2 + 4$ could be interesting having in mind that even the class number two problem for these discriminants is still an open problem.

The upper three results are described in [35], [36] and [37] respectively. Finally, the thesis contains a chapter on a joint work in progress with A. Biró and K. Gyarmati, which tries to solve the class number one problem for the whole family $d = (an)^2 + 4a$.

Acknowledgments

First of all I would like to thank my supervisor András Biró for introducing me to the class number one problem, for his guidance, valuable ideas, proofreading and patient support during the writing of this thesis. He sacrificed a lot of his time for regular meetings after which I usually felt happier and aspired to continue pursuing my research.

I am thankful to Tamas Szamuely for being my first-year adviser, for his encouragement, erudition and excellent teaching. The other person I would like to mention specially is Gergely Harcos for his enthusiasm, inspiring knowledge and support. Antal Balog helped me to simplify the paper [36] and pointed out some inaccuracies in its exposition. I am indebted to Prof. Kumar Murty for discussions on Goldfeld's theorem while being a hospitable and encouraging advisor during my stay at University of Toronto. The idea for [37] was formed during these discussions.

I am very thankful to Central European University for its generous support and warm atmosphere during my PhD studies, and to Central European University Budapest Foundation for supporting my visit to Toronto. The experience of meeting people from all around the world which CEU provides is rare for this part of Europe and truly enriching.

I am very grateful for the opportunity to meet all the amazing mathematicians working at Rényi Institute of Mathematics. I acknowledge the thoughtfulness of the members of Számelmélet Szeminárium at Rényi Institute who did not embarrass me too much trying to talk to me in Hungarian. Despite my limited level of Hungarian though, I truly enjoyed the seminar meetings.

Last, but by no means least, I would like to thank my husband Vajk Szécsi. Without his companionship these last few years might not have been some of the most pleasant in my life.

To the memory of grandmother Elena

and to the child I am expecting

Contents

Chapter 1

Introduction

The beginning of the class number problem arises as early as works of Euler and Legendre who remarked that certain quadratic forms give prime values for many consecutive values of the argument. Stepping on ideas of Lagrange for classifying binary quadratic forms with a fixed discriminant, in *Disquisitiones Arithmeticae* from 1801 Gauss showed the group structure of these quadratic forms and stated conjectures about the order of these groups depending on the growth of the discriminant.

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field with a fundamental discriminant d and the class number $h(d)$ denotes the size of the class group of K, i.e. the quotient group of the fractional ideals by the principal fractional ideals in K. In modern terms Gauss conjectured that for negative discriminants we have $h(d) \to \infty$ with $|d| \to \infty$. For positive discriminants he predicted completely different behaviour of the class number, namely that there are infinitely many real quadratic fields with class number $h(d) = 1$. Whilst the first conjecture is known to be true, the second one is still an open problem.

The conjecture for imaginary quadratic fields was shown to be true in a series of papers by Hecke, and Deuring and Heilbronn in the 1930's. The intriguing argument first assumed that the generalized Riemann hypothesis was true and then that it was false, giving the right answer in both cases. However, the method was ineffective and despite knowing that the number of discriminants $d < 0$ for which $h(d) = 1$ is finite, they were not known explicitly, so different methods were required to solve the class number one problem. Something more, the Hecke–Deuring–Heilbronn argument showed that if the conjectured discriminants $d < 0$ with $h(d) = 1$ did not constitute a complete list of the class number one negative fundamental discriminants, then the generalized Riemann hypothesis could not be true. This explains the active research that followed on this topic. The first solution of the Gauss class number one problem was developed in 1952 by

Heegner [25] with some gaps in his proof that later Stark cleared out, presenting his own proof with ideas similar to the ones of Heegner. The result also follows by the theorem for logarithms of algebraic numbers of Baker [1].

The existence of only finitely many negative discriminants with class number one can be seen by the Dirichlet's class number formula and the ineffective theorem of Siegel giving a lower bound for the value of the Dirichlet L-function at 1. Indeed, let χ be the real primitive character associated to the quadratic field K. Recall the Dirichlet L-function

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

The Dirichlet's class number formula (§6 [16]) claims that if $d<0$ and ω denotes the number of roots of unity in K, then

$$h(d)=\frac{\omega|d|^{1/2}}{2\pi}L(1,\chi_d)\,.$$

On the other hand, for positive $d>0$ and the fundamental unit of K denoted by ϵ_d, we have

$$h(d)\log\epsilon_d=d^{1/2}L(1,\chi_d)\,. \tag{1.1}$$

The Dirichlet's class number formula can be regarded as a special case of a more general class number formula (Theorem 125 [24]) holding for any number field, according to which the product of the class number and a certain regulator can be expressed as the residue at $s=1$ of the Dedekind zeta-function for the field. Siegel's theorem (§21 [16]) says that for every $\epsilon>0$ there exists a positive constant c_ϵ such that if χ is a real primitive character modulo q, then

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

If we take $q=|d|$ it follows that for $d<0$ we have

$$h(d)\gg_\epsilon|d|^{1/2-\epsilon}\,. \tag{1.2}$$

If, however, we want to use the same facts for examining positive discriminants we cannot separate the class number from the fundamental unit of the field K. Thus we limit our research within quadratic fields with a small fundamental unit, more precisely such that $\log\epsilon_d\asymp\log d$. These cases would lead to an analogous problem as in the imaginary case, with finitely many $d>0$ of the considered type with $h(d)=1$ and class number satisfying

(1.2). Thus, from one point we exclude discriminants that do not satisfy the Gauss class number one conjecture for real quadratic fields, and from other point we try to determine explicitly the class number one cases.

Examples of real quadratic fields with small fundamental units are the fields with discriminants of Richaud–Degert type. Special cases of these are the square-free discriminants $d = n^2 + 4$ and $d = 4n^2 + 1$. Their class number one problems were conjectured by Yokoi and Chowla respectively and were solved by Biró in [4] and [5]. His methods were further extended in a joint work with Granville [7]. This thesis steps on ideas from these works and try to resolve some of the open problems stated by Biró in [6]. In a certain way Biró's idea is analogous to the Baker's proof of the class number one problem for imaginary quadratic fields. The difference is that Biró can avoid working with a linear form of logarithms of algebraic numbers by using elementary algebraic number theory. His method is mostly influenced by Beck's paper [3] where non-trivial residue classes for the Yokoi's conjecture were solved.

The main theorems of the thesis, already described in the Abstract, will be stated precisely in the following chapters. Chapter 2 plays a preparatory role for the next parts. Its main result, Claim 2.6, is extracted from the paper [35]. The chapter deals with some elements of Gauss genus theory, defines Richaud–Degert discriminants and investigates the splitting behaviour of the small primes in some of these real quadratic fields. Chapter 3 presents the rest of the content of [35]. This is a self-contained proof of a class number one problem for square-free discriminants $d = (an)^2 + 4a$ for odd a and n, where n is divisible by a certain fixed number, and is the first unconditional result on two-parameter Richaud–Degert discriminants. The proof applies a method on computing a special value of a zeta-function from [7] and new ideas relating the problem to the class number of certain imaginary quadratic fields.

The research on Chapter 4 was motivated by the aim to extend the main theorem of the previous chapter. However, it includes results on divisibility of class numbers on imaginary quadratic fields which are interesting on their own. We give generalization of a result from [15] and use the circle method application as used by Balog and Ono in [2]. The content of Chapter 4 is to be published in [36].

In Chapter 5 we give an effective lower bound tending to infinity for the class number of a subfamily of the Yokoi's fields. This is interesting having in mind that even the class

number two problem for these fields has not been solved yet. We apply Goldfeld's theorem, so in reality we do not compute exactly the constant in our estimate as Goldfeld himself does not, though this could be done. A nice explicit expression for the constant is known only for the imaginary quadratic field case [44]. In this chapter we use techniques from elliptic curves arithmetic and the biggest part, §5.4, is devoted to prove unconditionally that a certain elliptic curve has analytic rank not smaller than 3. This is done by combining classical methods of Buhler–Gross–Zagier [12] and Silverman [47]. These results are contained in the submitted paper [37].

The last part, Chapter 6, deals with the same discriminants as in Chapter 3. In some sense these two chapters are complementing each other. This part, and to some extent §5.4, depend on computation in SAGE. The code, however, is omitted from the exposition of the last chapter due to its bulk. We hope that combining the methods of Chapter 6 with those of Chapter 3 will lead us to a final solution of the class number one problem for the whole family of positive square-free discriminants $d = (an)^2 + 4a$. The work on this chapter is joint with A. Biró and K. Gyarmati.

Chapter 2

Small Inert Primes in Real Quadratic Fields

2.1 Some Results from Gauss Genus Theory

In this and in the next chapter we apply some facts from Gauss genus theory. It is developed for the first time by Gauss in his *Disquisitiones Arithmeticae* in connection with representations of integers by quadratic forms. We give a modern language formulation only of the basic facts we need.

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic field for a square-free d and denote by I the set of the fractional ideals of K, and by P the set of principal fractional ideals. Then the class group $H = I/P$ is also called the *wide class group* and its order, the class number, is denoted by h. We will also use the notation $Cl(d) := H$ and $h(d) := h$ when we stress on the dependence on the discriminant. Similarly to the setting in the wide class group where $\mathfrak{a}, \mathfrak{b} \in I$ are equivalent if there is an algebraic number $\alpha \in K$ such that $\mathfrak{a} = (\alpha)\mathfrak{b}$, we consider

$$\mathfrak{a} = (\alpha)\mathfrak{b} \text{ with } \alpha \in K,\, N(\alpha) > 0\,.$$

We say that ideals satisfying the latter relation are equivalent in the *narrow* sense. If both α and its Galois conjugate are positive and $d > 0$ we call α *totally positive* and denote this by $\alpha \gg 0$. Introduce the set

$$P^+ = \{(\alpha) \text{ for } \alpha \in K,\, N(\alpha) > 0\}\,.$$

Note that for $d < 0$ we have $P^+ = P$ as then the norm of an algebraic integer is always positive. Also $P^+ = P$ if $d > 0$ and the fundamental unit is with a negative norm. The

narrow class group is $H^+ = I/P^+$ and the narrow class number is the order of the narrow class group denoted by $h^+ = |H^+|$. If ϵ is the fundamental unit of K for $d > 0$ by §45 [24] we have the relation

$$h^+ = \begin{cases} 2h & \text{if } K \text{ is real and } N(\epsilon) = 1\,, \\ h & \text{otherwise.} \end{cases}$$

Also recall that the 2-rank for a finite abelian group G is the nonnegative integer $\mathrm{rk}_2(G) = r$ such that $(G : G^2) = 2^r$. It is easy to see that $\mathrm{rk}_2(G/G^2) = \mathrm{rk}_2(G)$. Let the discriminant of K be divisible by t distinct primes p_i, $1 \leq i \leq t$. Then a basic result of genus theory is Theorem 132 [24]:

$$\mathrm{rk}_2(H^+) = t - 1\,.$$

Another important result for us could be found for example as Corollary in [43]:

Lemma 2.1 (Nemenzo, Wada [43]). *For odd discriminants $d > 0$ we have $rk_2(H^+) = rk_2(H)$ if and only if $p_i \equiv 1 \pmod 4, 1 \leq i \leq t$.*

If $h(d) = 1$ for $d > 0$ then clearly $\mathrm{rk}_2(H) = 0$. If also $N(\epsilon) = N(\epsilon_d) = 1$, we have $h^+ = 2h = 2$ so $\mathrm{rk}_2(H^+) \neq \mathrm{rk}_2(H)$. By Lemma 2.1, if d is odd, the discriminant has a divisor which is congruent to 3 modulo 4.

2.2 Richaud–Degert Discriminants

Let $K = \mathbb{Q}(\sqrt{d})$ be a quadratic imaginary field with $d < 0$ and let $\mathcal{O}_K$ be its ring of integers. If $h(d) = 1$ and a rational prime p splits completely in K then $(p) = \mathfrak{p}\bar{\mathfrak{p}}$ and $\mathfrak{p} = (\alpha)$ for some $\alpha \in \mathcal{O}_K$. Then there are integers m, n such that we can write $\alpha = (m + n\sqrt{d})/2$. If N is the norm from K to $\mathbb{Q}$ then $p = N(\alpha) = (m^2 - n^2 d)/4 = (m^2 + n^2|d|)/4$. Therefore a prime p splits completely in $\mathbb{Q}(\sqrt{d})$ only if $p \geq (1 + |d|)/4$. It is clear that we cannot draw the similar conclusion for $d > 0$ with the same argument as the norm of p might happen to be negative. That is why with different techniques we are aiming to give the best possible similar lower bounds for the smallest split prime for certain real quadratic fields.

Definition 2.2. *If the square-free integer $d = (an)^2 + ka > 0$ for positive integers a and n satisfies $\pm k \in \{1, 2, 4\}$, $-n < k \leq n$ and $d \neq 5$, then $K = \mathbb{Q}(\sqrt{d})$ is called a real quadratic field of Richaud–Degert (R-D) type.*

One of the main reasons why R-D fields are interesting is the form of their fundamental

unit. They are with short period of their continued fraction expansion and they are of "small" size: $\log \epsilon_d \asymp \log d$. More precisely we have the following claim.

Lemma 2.3 (Degert [17]). *Let $K = \mathbb{Q}(\sqrt{d})$, $d = (an)^2 + ka > 0$, be a real quadratic field of R-D type. Then the fundamental unit ϵ_d and its norm $N(\epsilon_d)$ are given as follows:*

$$\epsilon_d = an + \sqrt{d},\ N(\epsilon_d) = -sgn(k) \text{ if } |ka| = 1,$$

$$\epsilon_d = \frac{an + \sqrt{d}}{2},\ N(\epsilon_d) = -sgn(k) \text{ if } |ka| = 4,$$

and

$$\epsilon_d = \frac{2an^2 + k}{|k|} + \frac{2n}{|k|}\sqrt{d},\ N(\epsilon_d) = 1 \text{ if } |ka| \neq 1, 4\,.$$

In a paper from 1988 about Chowla's class number one conjecture Mollin gives the following upper bound implying inert primes, i.e. primes which stay prime in the corresponding number field extension.

Lemma 2.4 (Mollin [39]). *Let d be a square-free positive integer, $\sigma = 2$ if $d \equiv 1 \pmod 4$ and $\sigma = 1$ otherwise. Suppose that $(A + B\sqrt{d})/\sigma$ is the fundamental unit of $K = \mathbb{Q}(\sqrt{d})$ and $N\left((A + B\sqrt{d})/\sigma\right) = \delta$. If $h(d) = 1$ then p is inert in K for all primes*

$$p < \frac{(2A/\sigma) - \delta - 1}{B^2}\,.$$

This lemma is one of the results toward a theorem that characterizes the Chowla's discriminants of class number one through prime-producing polynomials:

Lemma 2.5 (Mollin [39]). *Let $d = 4n^2 + 1$ be square-free and n is a positive integer. Then the following are equivalent.*

(i) h(d)=1.

(ii) p is inert in $K = \mathbb{Q}(\sqrt{d})$ for all primes $p < n$.

(iii) $f(x) = -x^2 + x + n^2 \not\equiv 0 \pmod p$ for all integers x and primes p satisfying $0 < x < p < n$.

(iv) $f(x)$ is equal to a prime for all integers x satisfying $1 < x < n$.

Note that while Fact B of Biró [4] gives the same bound for the inert primes in $\mathbb{Q}(\sqrt{d})$ with Yokoi's discriminant $d = n^2 + 4$ as Lemma 2.4 provides, the analogous Fact B in Biró [5] already provides better bound. For Chowla's discriminants $d = 4n^2 + 1$ instead of the bound n from Lemma 2.4 he gets bound $2n$. This suggests to follow Biró's techniques.

2.3 The Discriminant $d = (an)^2 + 4a$

For the R-D discriminant of our main interest which we explore in the next chapters we get

Claim 2.6. *If $h(d) = 1$ for the square-free discriminant $d = (an)^2 + 4a$, then a and $an^2 + 4$ are primes. Something more, for any prime $r \neq a$ such that $2 < r < an/2$ we have*

$$\left(\frac{d}{r}\right) = -1\,.$$

After Lemma 2.3 the fundamental unit of the quadratic field with the upper discriminant for $a > 1$ is $\epsilon_d = \dfrac{(an^2+2) + n\sqrt{d}}{2}$. When we apply Lemma 2.4 we get that every prime $p < a$ is inert. We prove much stronger statement in which both parameters in the discriminant are included.

We introduce α as the positive root of the equation

$$x^2 + (an)x - a = 0\,.$$

Let $\overline{\alpha} = -(an + \sqrt{d})/2$ be the algebraic conjugate of α. We note that $(1, \overline{\alpha})$ form a $\mathbb{Z}$-basis of $\mathcal{O}_K$ with

$$\begin{pmatrix} 1 \\ \overline{\alpha} \end{pmatrix} = \begin{pmatrix} 1 & 0 \\ \frac{-an+1}{2} & -1 \end{pmatrix} \begin{pmatrix} 1 \\ \frac{\sqrt{d}+1}{2} \end{pmatrix}\,.$$

For the fundamental unit $\epsilon_d > 1$ the system $(1, \overline{\epsilon}_d)$ was used in [4] but it forms a basis of the ring $\mathcal{O}_K$ over $\mathbb{Z}$ only when $n = 1$. That is why we need to use different base system. Since

$$\begin{pmatrix} \epsilon_d \\ \overline{\alpha} \end{pmatrix} = \begin{pmatrix} 1 & -n \\ 0 & 1 \end{pmatrix} \begin{pmatrix} 1 \\ \overline{\alpha} \end{pmatrix}$$

with determinant of transformation equal to 1, we can take $(\epsilon_d, \overline{\alpha})$ as a basis of the ring $\mathcal{O}_K$ over $\mathbb{Z}$.

We also have $\epsilon_d \overline{\epsilon}_d = 1$ and

$$\epsilon_d + \overline{\epsilon}_d = 1 - n\alpha + 1 - n\overline{\alpha} = 2 - n(\alpha + \overline{\alpha}) = 2 + an^2\,. \tag{2.1}$$

Here we will reveal some of the splitting behaviour of the primes in the field K.

Lemma 2.7. *If β is an algebraic integer in $K = \mathbb{Q}(\sqrt{d})$ for the square-free $d = (an)^2 + 4a$ such that $|\beta\overline{\beta}| < an/2$, then $|\beta\overline{\beta}|$ is either divisible by a square of a rational integer greater than 1, or equals 1, or equals a.*

Proof. It is enough to prove the claim for

$$1 < |\beta| < \epsilon_d \,. \tag{2.2}$$

Indeed, if $|\beta| = 1$ or $|\beta| = \epsilon_d$ we have $|\beta\overline{\beta}| = 1$ and the statement is true. If $0 < |\beta| < 1$ or $|\beta| > \epsilon_d$ there is an integer k such that $\epsilon_d^{k-1} \leq |\beta| < \epsilon_d^k$, $k < 0$ in the first case and $k > 0$ - in the second. Then $\gamma := \epsilon_d^{1-k}\beta$ is in the interval $[1, \epsilon_d)$ and still $|\gamma\bar{\gamma}| = |\beta\bar{\beta}|$.

So further we assume (2.2). Then we can write $\beta = e\epsilon_d + f\overline{\alpha}$. If $e = 0$ then $\beta = f\overline{\alpha}$, $|\beta\bar{\beta}| = f^2 a$ and the claim is true.

Assume that $e > 0$, the negative case being analogous. If $f = 0$ then $\beta = e\epsilon_d$, $|\beta\bar{\beta}| = e^2$ and this fulfills the lemma. If we assume that the coefficient f is negative, from $\overline{\alpha} < 0$ we get $\beta = e\epsilon_d + f\overline{\alpha} > e\epsilon_d \geq \epsilon_d$ which is out of our range of consideration. Therefore $f > 0$.

Also notice that

$$\beta\bar{\beta} = (e\epsilon_d + f\overline{\alpha})(e\bar{\epsilon}_d + f\alpha) = e^2 + ef(\alpha\epsilon_d + \bar{\alpha}\bar{\epsilon}_d) - af^2.$$

We see that $\alpha\epsilon_d + \bar{\alpha}\bar{\epsilon}_d = \alpha(1 - n\bar{\alpha}) + \bar{\alpha}(1 - n\alpha) = \alpha + \bar{\alpha} - 2n\alpha\bar{\alpha} = -an + 2an = an$. Therefore

$$\beta\bar{\beta} = Q(e, f) := e^2 + (an)ef - af^2 \,, \tag{2.3}$$

where $Q(e, f) = f_2(e, f)$ with f_2 defined later in (3.11).

We look at the quadratic form $Q(x, y)$. By (2.3) we have that

$$\left| \begin{array}{l} Q'_x = 2x + any \\ Q'_y = anx - 2ay \end{array} \right. \tag{2.4}$$

and this yields that the local extremum of the form is at $x = -any/2$ and $-(an)^2 y/2 = 2ay$. The latter is true only for $y = 0$ but this is out of the considered range where $x, y \geq 1$. That is why for any bounded region of interest in $\mathbb{R}^2$ the extrema would be at its borders. Also $Q'_x > 0$ and therefore for a fixed argument y the function $Q(x, \underline{y})$ is increasing. Here and hereafter by $\underline{x}, \underline{y}$ we mean that the variable is fixed. On the other hand $Q''_y = -2a < 0$.

Thus for fixed x the function $Q(\underline{x}, y)$ has its maximum at $y = nx/2$.

We will investigate the form $Q(x, y)$ according to its sign. We show that it depends on the size of the coefficient f. For example if $f = en$, then $Q(e, f) = e^2 + anfe - af^2 = e^2 + af^2 - af^2 = e^2$ and the lemma is fulfilled. Further we consider

Case I : $f < ne$ **.** Here we have $Q(e, f) = e^2 + anfe - af^2 = e^2 + af(ne - f) > e^2 > 0$. On the other hand from $\bar{\alpha} < 0$ it follows that $f\bar{\alpha} > ne\bar{\alpha}$ and

$$\beta = e\epsilon_d + f\bar{\alpha} > e\epsilon_d + ne\bar{\alpha} = e(1 - n\bar{\alpha}) + en\bar{\alpha} = e \geq 1$$

and $\beta = |\beta| < \epsilon_d$ yields

$$1 \leq e < \beta < \epsilon_d < 2 + an^2 \, .$$

The latter estimate follows from (2.1) and $0 < \overline{\epsilon_d} < 1$. Thus in the case we regard we are in a region R_1

$$R_1 : \left| \begin{array}{lll} 1 & \leq e \leq & 1 + an^2 \\ 1 & \leq f \leq & ne - 1 \end{array} \right. \tag{2.5}$$

First assume that $n \geq 3$.

We explained earlier that the maximum of $Q(\underline{x}, y)$ for a fixed argument x is at the line $y = nx/2$. Then $1 < n/2 < n - 1$ and $\min_{R_1} Q(x, y)$ could be at the lines $l_1 : y = 1$ or $l_2 : y = nx - 1$. We are interested in the behaviour of the quadratic form on the latter lines. Since $Q(x, \underline{y})$ is increasing for fixed positive y we have $\min_{l_1} Q(x, y) = Q(1, 1)$. On the other hand on l_2 we have

$$\begin{aligned} Q(x, nx - 1) &= x^2 + anx(nx - 1) - a(nx - 1)^2 \\ &= x^2 + a(nx)^2 - anx - a(nx)^2 + 2anx - a = x^2 + anx - a \, . \end{aligned} \tag{2.6}$$

The local extrmemum of this function is achieved when $Q'_x(x, nx - 1) = 2x + an = 0$ and $Q''_x(x, nx - 1) = 2 > 0$ so it is minimum at $x = -an/2$. This means that for positive x the function $Q(x, nx - 1)$ is increasing and thus by (2.6) $\min_{l_2} Q(x, y) = Q(1, n - 1) = 1 + an - a = Q(1, 1)$. Therefore $\min_{R_1} Q(x, y) = 1 + an - a$. By the condition of the Lemma we know that $an/2 > |\beta\bar{\beta}| = |Q(e, f)| = Q(e, f)$. This is true for the smallest value of the quadratic form in the regarded region as well, i.e. $an/2 > 1 + an - a$. Then we need $a - 1 > an/2$. But for $n \geq 3$ this gives $a - 1 > an/2 > a$

- a contradiction.

From the definition of the discriminant d we know that n is odd, so $n \neq 2$. Now assume that $n = 1$. We cannot have $e = 1$, otherwise $1 \leq f < en = 1$. Thus $e \geq 2$ and we take up the region R_1 with this correction. Then $1 \leq nx/2 \leq nx - 1$ holds since $1 \leq x/2 \leq x - 1$ for $x \geq 2$. Hence again the minimum is at the very left points of l_1 and l_2, i.e. $\min_{R_1} Q(x, y) = Q(2, 1)$. This after (2.6) equals $4 + 2a - a = 4 + a$. Clearly $a > a/2 > 4 + a$ again gives contradiction. We conclude that case I is not possible.

Case II: $f > ne$**,** in other words $ne - f \leq -1$. Suppose that $Q(e, f) > 0$. Then $0 < Q(e, f) = e^2 + anef - af^2 = e^2 + af(ne - f) \leq e^2 - af$. Consequently $e^2 > af > ane$ and $e > an$. On the other hand, using that $\alpha > 0$, we get $\bar{\beta} = e\bar{\epsilon}_d + f\alpha > e(1 - n\alpha) + en\alpha = e \geq 1$. So after (2.2)

$$an > an/2 > |\beta\bar{\beta}| = |\beta|.|\bar{\beta}| \geq |\bar{\beta}| = \bar{\beta} > e\,. \tag{2.7}$$

We got $an > e > an$ - a contradiction. Therefore always when $f > ne$ the form $Q(x, y)$ is negative and $e < an/2 \leq an - 1$. The last inequality is not fulfilled only when $an = 1$. But in this case $an/2 = 1/2 > |Q(e, f)| = |\beta\bar{\beta}|$ implies that $\beta = 0$ because β is algebraic integer and its norm is integer. Therefore $an > 2$ and we can regard the region

$$R_2 : \left| \begin{array}{rl} 1 & \leq e \leq \quad an - 1 \\ ne + 1 & \leq f \end{array} \right. \tag{2.8}$$

Clearly $|Q(x, y)| = -Q(x, y) = -x^2 - anxy + ay^2 > 0$ and after (2.4) it has extremum out of R_2. Notice that for a fixed x the derivatives $-Q'_y(\underline{x}, y) = -anx + 2ay$ and $-Q''_y(\underline{x}, y) = 2a > 0$, so at $y = nx/2 < nx + 1$ we have minimum of $-Q(\underline{x}, y)$. Therefore $-Q(\underline{x}, y)$ is increasing on the lines $x = const$ and we search for the minimum of $-Q(x, y)$ on the line $l_3 : y = xn + 1$.

On the line l_3 we have

$$\begin{aligned} -Q(x, nx + 1) &= -x^2 - anx(nx + 1) + a(nx + 1)^2 = \\ &= -x^2 - a(nx)^2 - anx + a(nx)^2 + 2anx + a = -x^2 + anx + a \end{aligned} \tag{2.9}$$

and at $x = an/2$ we have maximum. So

$$\min_{R_2} |Q(x,y)| = \min\left(-Q(1,n+1), -Q(an-1, n(an-1)+1)\right) .$$

From (2.9) we see that $-Q(1,n+1) = -1+an+a$ and $-Q(an-1, n(an-1)+1) = -(an-1)^2 + an(an-1) + a = an - 1 + a$, so $\min_{R_2} |Q(x,y)| = -1+a+an$. Here by the lemma condition $an > -1+a+an$ and $0 > -1+a$ or $1 > a$ which is impossible. □

Remark 2.8. If β is an algebraic integer in K such that $|\beta\overline{\beta}| < n\sqrt{a}$, then $|\beta\overline{\beta}|$ is either divisible by a square of a rational integer, or equals 1, or equals a.

This follows easily if we notice that the finer estimate $an/2 > |\beta\bar{\beta}|$ needed for R_1 with $n \geq 3$ could be substituted by

$$n\sqrt{a} > |\beta\bar{\beta}| > 1 + an - a\,.$$

Indeed $n\sqrt{a} > 1+an-a \Leftrightarrow a-1 > n\sqrt{a}(\sqrt{a}-1) \Leftrightarrow (\sqrt{a}-1)(\sqrt{a}+1) > n\sqrt{a}(\sqrt{a}-1)$. If $a = 1$ then $1.n > 1+1.n-1$ is not true. Then $a > 1$ and we get by dividing by $\sqrt{a}-1 > 0$ the inequality $\sqrt{a}+1 > n\sqrt{a}$. This yields $2 > 1 + 1/\sqrt{a} > n \geq 3$.

For the other cases we showed that the stronger $an > \min Q(e,f)$ is impossible, so if we assume the statement of the remark with $n\sqrt{a} > Q(e,f)$ it would yield $an > \min Q(e,f)$, again a contradiction.

Here we give

Proof of Claim 2.6. By Gauss genus theory it follows that $h(d) = 1$ only if the discriminant d is prime or a product of two primes because h^+ equals 1 or 2 depending on the sign of $N(\epsilon_d)$. Hence the first statement of the claim.

Now let r be a prime such that $2 < r < an/2$ and $r \neq a$. Assume $\left(\frac{d}{r}\right) = 0$. This means that the prime r ramifies in K and there is a prime ideal $\mathfrak{p} \subset \mathcal{O}_K$ for which $r\mathcal{O}_K = \mathfrak{p}^2$. But as the class number is 1, $\mathcal{O}_K$ is a PID and there is $\beta \in \mathcal{O}_K$ such that $\mathfrak{p} = (\beta)$. Then $|\beta\bar{\beta}| = N(\mathfrak{p}) = r < an/2$. By Lemma 2.7 there is a square of an integer dividing the prime r except for $|\beta\bar{\beta}| = 1$, but then β is a unit and $\mathfrak{p} = \mathcal{O}_K$, a contradiction.

Assume that $\left(\frac{d}{r}\right) = 1$. Then there exists $b \in \mathbb{Z}$ such that $b^2 \equiv d \pmod{r}$. We claim that

$$(r) = \left(r, b+\sqrt{d}\right)\left(r, b-\sqrt{d}\right). \tag{2.10}$$

Indeed,

$$\begin{aligned}\left(r, b+\sqrt{d}\right)\left(r, b-\sqrt{d}\right) &= \left(r^2, r(b+\sqrt{d}), r(b-\sqrt{d}), b^2-d\right) \\ &= (r)\left(r, b+\sqrt{d}, b-\sqrt{d}, \frac{b^2-d}{r}\right).\end{aligned}$$

Now the coprime rational integers $r, 2b$ are in the second ideal I. Therefore there exist $x, y \in \mathbb{Z}$ for which $xr + y2ba = 1$. As $1 \in I$ we have $I = \mathcal{O}_K$ and (2.10) follows.

Also we have that $\left(r, b+\sqrt{d}\right) \neq \left(r, b-\sqrt{d}\right)$. If the ideals are equal, again $r, 2b$ are in each of them, so each of them is the whole ring of integers, which contradicts (2.10) because $2 < r$ and r does not generate the whole $\mathcal{O}_K$.
Then there are two prime ideals $\mathfrak{p}_1 \neq \mathfrak{p}_2$ such that $(r) = \mathfrak{p}_1\mathfrak{p}_2$ and $N(\mathfrak{p}_1) = N(\mathfrak{p}_2) = r$. But $h(d) = 1$ and $\mathfrak{p}_1 = (\beta)$ for some nonzero $\beta \in \mathcal{O}_K$. Therefore $N(\mathfrak{p}_1) = |\beta\overline{\beta}| = r < an/2$ and by the upper lemma and $r \neq a$, $r > 2$, we have that $|\beta\bar{\beta}|$ is divided by a square of integer $z > 1$. This contradicts r being prime.

We got that it is impossible to have $\left(\frac{d}{r}\right) = 1$. □

Remark 2.9. When $a = 1$ we have $d = n^2 + 4$ and $h(d) = 1$ yields d to be prime and for any prime $2 < r < n$

$$\left(\frac{n^2+4}{r}\right) = -1\,.$$

Something more, n is also prime.

The first part of the claim can be seen after we apply the same argument as in the proof of Claim 2.6 but with Remark 2.8 instead of Lemma 2.7. Actually in this fashion we got Fact B from [4]. We see from Corollary 3.16 in [13] that n is prime if the class number is 1.

2.4 Other R-D Discriminants

Further we want to mention similar results on the inert primes in other R-D fields. Note that the following fields are always of class number greater than one.

Lemma 2.10 (Byeon, Kim [13]). *For the following R-D discriminants we always have $h(d) > 1$:*

(i) $d = 4n^2 - 1$, $n > 1$.

(ii) $d = (2n+1)^2 + 1$, $n > 1$.

(iii) $d = (2n+1)^2 + 2r$, $r \equiv 1, 3 \pmod 4$, $r \mid 2n+1$, $r \neq 1$.

(iv) $d = (2n+1)^2 - 2r$, $r \equiv 1, 3 \pmod 4$, $r \mid 2n+1$, $r > 1$.

(v) $d = 4n^2 + 2r$, $r \equiv 1, 3 \pmod 4$, $r \mid n$, $r \neq 1$.

(vi) $d = 4n^2 - 2r$, $r \equiv 1, 3 \pmod 4$, $r \mid n$, $r > 1$.

Therefore the only R-D discriminants $d = (an)^2 + ka$ with $a > 1$ and $h(d) = 1$ are the ones with $\pm k \in \{1, 4\}$. We state analogues of Lemma 2.7 which was independent on the class number of the field $\mathbb{Q}(\sqrt{d})$. Note that the proofs are also very similar to the proof of Lemma 2.7 presented in detail in the previous section, that is why here we only give their brief sketches.

First consider the discriminant $d = (an)^2 + a$.

Lemma 2.11. *Let $d = (an)^2 + a > 0$ be square-free for $a > 1$ and $d \equiv 2, 3 \pmod 4$. If β is an algebraic integer in $K = \mathbb{Q}(\sqrt{d})$ such that $|\beta\overline{\beta}| < an$, then $|\beta\overline{\beta}|$ is either divisible by a square of a rational integer greater than 1, or equals 1, or equals a.*

Sketch of Proof. We consider the equation

$$x^2 + 2anx - a = 0$$

and take its negative root $\alpha = -an - \sqrt{d}$. By Lemma 2.3 we have $\epsilon_d = 1 - 2n\alpha$. If $d \equiv 2, 3 \pmod 4$, then $\mathcal{O}_K = \mathbb{Z}[\epsilon_d, \alpha]$. In this case take, like in the proof of Lemma 2.7, $\beta = e\epsilon_d + f\alpha$ and then

$$\beta\bar{\beta} = Q(e, f) := e^2 + 2anef - af^2 \,.$$

We conclude the result by assuming that both $e, f \geq 1$ and by examining the extremal values of the quadratic form $Q(x, y)$.

□

Corollary 2.12. *If $h(d) = 1$ for the square-free discriminant $d = (an)^2 + a$ with $a > 1$, then a and $an^2 + 4$ are primes. Something more, for any prime $r \neq a$ such that $2 < r < an$ we have*

$$\left(\frac{d}{r}\right) = -1 \,.$$

The other discriminant for which we worked out analogous statement is $d = (an)^2 - 4a$.

Lemma 2.13. *Let $d = (an)^2 - 4a > 0$ be square-free with $a > 1$. If β is an algebraic integer in $K = \mathbb{Q}(\sqrt{d})$ such that $|\beta\overline{\beta}| < an/2$, then $|\beta\overline{\beta}|$ is either divisible by a square of a rational integer greater than 1, or equals 1, or equals a.*

Sketch of Proof. Here we are interested in the equation

$$x^2 + anx + a = 0$$

and we take $\alpha = -(an + \sqrt{d})/2$ be its negative root. Then the fundamental unit $\epsilon_d = -1 - n\alpha$ and $\mathcal{O}_K = \mathbb{Z}[\epsilon_d, \alpha]$. We consider some $\beta = e\epsilon_d + f\alpha$ and the quadratic form

$$\beta\bar{\beta} = Q(e, f) := e^2 - anef + af^2 \,.$$

The statement of the lemma is achieved by some (quite technical) examination of the local extrema of $Q(x, y)$ in different regions on the plane. □

Corollary 2.14. *If $h(d) = 1$ for the square-free discriminant $d = (an)^2 - 4a$ and $a > 1$, then a and $an^2 - 4$ are primes. Something more, for any prime $r \neq a$ such that $2 < r < an/2$ we have*

$$\left(\frac{d}{r}\right) = -1 \,.$$

Chapter 3

Class Number One Problem for Certain Real Quadratic Fields

3.1 Introduction

Let us consider the quadratic fields $K = \mathbb{Q}(\sqrt{d})$ with class group $Cl(d)$ and order of the class group denoted by $h(d)$. In this chapter we solve the class number one problem for a subset of the fields K where $d = (an)^2 + 4a$ is square-free and a and n are positive odd integers. It is known that there are only a finite number of these fields after Siegel's theorem but as the latter is ineffective it is not applicable to finding the specific fields. For this sake we apply the effective methods developed by Biró in [4] and in his joint work with Granville [7].

We remark that the class number one problem that we consider was already suggested by Biró in [6] as a possible generalization of his works. The discriminant we regard is of Richaud–Degert type with $k = 4$. The class number one problem for special cases of Richaud–Degert type is solved in [4],[5],[14] and [38] where the parameter $a = 1$. However we already cover a subset of Richaud–Degert type that is of positive density and our problem depends on two parameters.

Under the assumption of a generalized Riemann hypothesis there is a list of principal quadratic fields of Richaud–Degert type, see [40]. Here, however, our main result is unconditional:

Theorem 3.1. *If $d = (an)^2 + 4a$ is square-free for odd positive integers a and n such that $43 \cdot 181 \cdot 353 \mid n$, then $h(d) > 1$.*

In [7] Biró and Granville give a finite formula for a partial zeta function at 0 in the

case of a general real quadratic field and a general odd Dirichlet character. Basically we follow their method in a much simpler situation where the field has a specific form as in Theorem 3.1, the character is real and its conductor divides the parameter n. As it could be expected, to deduce a formula in this special case is much simpler than in the general case.

The idea of the proof of Theorem 3.1 is roughly speaking the following. We arrive to the identity

$$qh(-q)h(-qd) = n\left(a + \left(\frac{a}{q}\right)\right)\frac{1}{6}\prod_{p|q}(p^2-1)\,, \tag{3.1}$$

where $q \equiv 3 \pmod 4$ is square-free, $(q,a) = 1$ and $q \mid n$. We do this by computing a partial zeta function at 0 at the principal integral ideals for our specific discriminant, taking a real character modulo q and applying the condition $h(d) = 1$. When we use Claim 2.6 to determine the value of $\left(\frac{a}{q}\right)$ and see the factorization of q, we can deduce the exact power of 2 which divides the right-hand side of (3.1). Here comes the place to explain the limitation $43 \cdot 181 \cdot 353 \mid n$. In the analysis of (3.1) we see that we can get a contradiction if we choose q in such a way that the class number $h(-q)$ is divisible by a large power of 2. We choose $q = 43 \cdot 181 \cdot 353$ and use that $h(-43 \cdot 181 \cdot 353) = 2^9.3$ has indeed a large power of 2 as a factor, e.g. in [11] not only the order but also the group structure of $Cl(-43 \cdot 181 \cdot 353)$ is given. Then we show that different powers of two divide the two sides of (3.1) and eventually conclude the proof of Theorem 3.1.

3.2 Notations and Structure of the Chapter

Let χ be a Dirichlet character of conductor q. Consider the fractional ideal I and the zeta function corresponding to the ideal class of I

$$\zeta_I(s,\chi) := \sum_{\mathfrak{a}} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s} \tag{3.2}$$

where the summation is over all integral ideals $\mathfrak{a}$ equivalent to I in the ideal class group $Cl(d)$.

Let $f(x,y) \in \mathbb{Z}[x,y]$ be a quadratic form $f(x,y) = Ax^2 + Bxy + Cy^2$ with discriminant $D = B^2 - 4AC$.

Denote by $B_\ell(x)$ the Bernoulli polynomial defined by

$$\frac{Te^{Tx}}{e^T-1}=\sum_{n\geq 0}B_n(x)\frac{T^n}{n!}$$

and introduce the generalized Gauss sum

$$g(\chi,f,B_\ell):=\sum_{0\leq u,v\leq q-1}\chi\left(f(u,v)\right)B_\ell\left(\frac{v}{q}\right). \tag{3.3}$$

The symbol χ_q always denote the real primitive Dirichlet character with conductor q, i.e. $\chi_q(m)=\left(\dfrac{m}{q}\right)$. This way we are interested in square-free q. The notation $\lceil x\rceil$ signifies the least integer not smaller than x and $(x)_q$ – the least nonnegative residue of x (mod q). Throughout the thesis by (a,b) we denote the greatest common divisor of the integers a and b. For $m\in\mathbb{Z}$ and $(m,q)=1$ we use the notation $\overline{m}$ for the multiplicative inverse of m modulo q. The same over-lining for $\alpha\in K$ will denote its algebraic conjugate $\overline{\alpha}$ and the exact use should be clear by the context. As usual $\varphi(x)$ and $\mu(x)$ mean the Euler function and the Möbius function. Let us further denote by $p^\alpha\|l$ the fact that $p^\alpha\mid l$ but $p^{\alpha+1}\nmid l$. We also remind that $B_\ell:=B_\ell(0)$.

$\mathcal{O}_K$ represents the ring of integers of the quadratic field K ; $P(K)$ – the set of all nonzero principal ideals of $\mathcal{O}_K$ and $P_F(K)$ – the set of all nonzero principal fractional ideals of K. Let $I_F(K)$ be the set of nonzero fractional ideals of K. The norm of an integral ideal $\mathfrak{a}$ in $\mathcal{O}_K$ is the index $[\mathcal{O}_K:\mathfrak{a}]$. The trace of $\alpha\in K$ will be $Tr(\alpha)=\alpha+\overline{\alpha}$. For $\alpha,\beta\in K$ we write $\alpha\equiv\beta\pmod q$ when $(\alpha-\beta)/q\in\mathcal{O}_K$. When $I_1,I_2\in I_F(K)$ are represented as ratios of two integral ideals as $\mathfrak{a}_1\mathfrak{b}_1^{-1}$ and $\mathfrak{a}_2\mathfrak{b}_2^{-1}$ we say that the ideals I_1 and I_2 are relatively prime and write $(I_1,I_2)=1$ in the case when $(\mathfrak{a}_1\mathfrak{b}_1,\mathfrak{a}_2\mathfrak{b}_2)=1$. We recall that the element $\beta\in K$ is called *totally positive*, denoted by $\beta\gg 0$, if $\beta>0$ and its algebraic conjugate $\bar{\beta}>0$.

The structure of the chapter is the following: in the next section §3.3 we compute the generalized Gauss sum (3.3) for real character χ_q. We need it because in §3.4 we formulate and prove Lemma 3.5 for the value of $\zeta_{P(K)}(0,\chi)$ in terms of sum (3.3). The main result there is Corollary 3.7 for the value of $\zeta_{P(K)}(0,\chi_q)$. In Chapter 2 we developed Lemma 2.7 with the help of which Claim 2.6, the analogue of Fact B in [4], was proven and we apply it in §3.5 where we prove the main Theorem 3.1. In Appendix A of the thesis for the sake of completeness we give the proof of Corollary 4.2 from [7] which we state and use in section

§3.4 as it is in [7].

3.3 On a Generalized Gauss Sum

The main statement in this section is

Lemma 3.2. *For $(2A, q) = (D, q) = 1$ and even $\ell \geq 2$ we have*

$$g(\chi_q, f, B_\ell) = \chi_q(A) q B_\ell \prod_{p|q} (1 - p^{-\ell}) \,.$$

Remark 3.3. When ℓ is odd we have $B_\ell = 0$ for every $\ell \geq 3$. By the property of the Bernoulli polynomials $B_n(1-x) = (-1)^n B_n(x)$ one could easily see that $g(\chi, f, B_\ell)$ is divisible by B_ℓ and thus equals zero, unless when $\ell = 1$ and $\chi = \chi_q$.

Proof. Take the summation on v in (3.3) at the first place:

$$g(\chi_q, f, B_\ell) = \sum_{v=0}^{q-1} B_\ell\left(\frac{v}{q}\right) \sum_{u=0}^{q-1} \chi_q(f(u,v)) \,.$$

Introduce $r := 2Au + Bv$. Since $(2A, q) = 1$ the values of r cover a full residue system modulo q when u does. Also $r^2 = 4A(f(u,v) + Dv^2/4A)$ so we get $\chi_q(f(u,v)) = \bar{\chi}_q(4A)\chi_q(r^2 - Dv^2)$. As χ_q is of order 2, we have $\chi_q = \bar{\chi}_q$ and $\chi_q(4A) = \chi_q(A)$. Therefore $\chi_q(f(u,v)) = \chi_q(A)\chi_q(r^2 - Dv^2)$. Then

$$\begin{aligned} g(\chi_q, f, B_\ell) &= \chi_q(A) \sum_{v=0}^{q-1} B_\ell\left(\frac{v}{q}\right) \sum_{r=0}^{q-1} \chi_q(r^2 - Dv^2) \\ &= \chi_q(A) \sum_{v=0}^{q-1} B_\ell\left(\frac{v}{q}\right) R \,, \end{aligned} \tag{3.4}$$

where we abbreviated $R := \sum_{0 \leq r \leq q-1} \chi_q(r^2 - Dv^2)$. We will show that for $g = (v, q)$

$$R = \varphi(g)\mu(\frac{q}{g}) \,. \tag{3.5}$$

Let $q = \prod_i p_i$. Here there is no square of a prime dividing q because χ_q is a primitive character modulo q which is of second order and $\left(\frac{\cdot}{p^2}\right) = 1$. After the Chinese Remainder

Theorem for any polynomial $F(x,y) \in \mathbb{Z}[x,y]$ we have

$$\sum_{u=0}^{q-1} \chi_q(F(u,v)) = \prod_i \sum_{u_i=0}^{p_i-1} \chi_{p_i}(F(u_i,v))\,.$$

Therefore it is enough to consider the sum in the definition of R for every $p \mid q$. In this way let $R_p = \sum_{0\le r\le p-1} \chi_p(r^2 - Dv^2)$. Then $R = \prod_{p|q} R_p\,.$

If $p \mid q/g$, i.e. $(p,v)=1$, we have

$$\left(\frac{r^2-Dv^2}{p}\right) = \left(\frac{Dv^2}{p}\right)\left(\frac{\overline{Dv^2}r^2-1}{p}\right) = \left(\frac{D}{p}\right)\left(\frac{\overline{Dv^2}r^2-1}{p}\right)$$

because $(D,p)=1$ and then

$$R_p = \sum_{r=0}^{p-1} \chi_p(r^2 - Dv^2) = \left(\frac{D}{p}\right)\sum_{r=0}^{p-1} \chi_p(\overline{D}r^2-1)\,. \tag{3.6}$$

If $\left(\frac{\nu}{p}\right) = -1$, then $\{\nu r^2 - 1 : 0 \le r \le p-1\} \cup \{r^2-1 : 0 \le r \le p-1\}$ gives us two copies of the full residue system modulo p. Then $\sum_{0\le r\le p-1} \chi_p(\nu r^2-1) + \sum_{0\le r\le p-1} \chi_p(r^2-1) = 2\sum_{0\le r\le p-1} \chi_p(r) = 0$ and therefore

$$\sum_{r=0}^{p-1} \chi_p(\nu r^2-1) = -\sum_{r=0}^{p-1} \chi_p(r^2-1) = \left(\frac{\nu}{p}\right)\sum_{r=0}^{p-1} \chi_p(r^2-1)\,.$$

Clearly when $\left(\frac{\nu}{p}\right) = 1$ we have $\{\nu r^2 - 1 \pmod p : 0 \le r \le p-1\} \equiv \{r^2 - 1 \pmod p : 0 \le r \le p-1\}$. We conclude that

$$\sum_{r=0}^{p-1} \chi_p(\nu r^2-1) = \left(\frac{\nu}{p}\right)\sum_{r=0}^{p-1} \chi_p(r^2-1)$$

and for the sum on the right-hand side of (3.6) we can finally assume $\overline{D} = 1$. So

$$\begin{aligned} R_p &= \left(\frac{D}{p}\right)\left(\frac{\overline{D}}{p}\right)\sum_{r=0}^{p-1}\chi_p(r^2-1) = \sum_{r=0}^{p-1}\chi_p(r-1)\chi_p(r+1) \\ &= \sum_{\substack{r=0\\ r\neq 1}}^{p-1}\chi_p(\overline{r-1})\chi_p(r+1) = \sum_{\substack{r=0\\ r\neq 1}}^{p-1}\chi_p\left(\frac{r+1}{r-1}\right) \\ &= \sum_{\substack{r=0\\ r\neq 1}}^{p-1}\chi_p\left(1+\frac{2}{r-1}\right) = \sum_{r=1}^{p-1}\chi_p(1+2r) = -1\,. \end{aligned}$$

On the other hand, if $p \mid g$, i.e. $p \mid v$, we have $R_p = \sum_{0\le r\le p-1}\chi_p(r^2) = p-1 = \varphi(p)$ because χ_p is of second order. Combining the results $R_p = -1$ when p divides q/g and $R_p = \varphi(p)$ when $p \mid g$ we get $R = R_q = \mu(q/g)\varphi(g)$ which is exactly (3.5).

When we substitute the value of R in (3.4) we get

$$g(\chi_q, f, B_\ell) = \chi_q(A)\sum_{v=0}^{q-1}\mu(q/g)\varphi(g)B_\ell\left(\frac{v}{q}\right) = \chi_q(A)\Sigma_1\,, \tag{3.7}$$

where we write Σ_1 for the sum on the right-hand side of (3.7). Further on if $V := v/g$ and $Q := q/g$

$$\Sigma_1 = \sum_{g\mid q}\mu(q/g)\varphi(g)\sum_{\substack{v=0\\ g=(v,q)}}^{q-1}B_\ell\left(\frac{v}{q}\right) = \sum_{g\mid q}\mu(q/g)\varphi(g)\sum_{\substack{V=0\\ (V,Q)=1}}^{Q-1}B_\ell\left(\frac{V}{Q}\right)\,.$$

Denote

$$\Sigma_2 := \sum_{\substack{V=0\\ (V,Q)=1}}^{Q-1}B_\ell(\frac{V}{Q})\,.$$

Then

$$\Sigma_2 = \sum_{V=0}^{Q-1}B_\ell\left(\frac{V}{Q}\right)\sum_{d\mid(V,Q)}\mu(d) = \sum_{d\mid Q}\mu(d)\sum_{\substack{V=0\\ d\mid V}}^{Q-1}B_\ell\left(\frac{V}{Q}\right) = \sum_{d\mid Q}\mu(d)\sum_{V/d=0}^{Q/d-1}B_\ell\left(\frac{V/d}{Q/d}\right)\,.$$

We make use of the following property of the Bernoulli polynomials §4.1[52]

$$\sum_{N=0}^{k-1} B_\ell\left(t+\frac{N}{k}\right) = k^{-(\ell-1)} B_\ell(kt)\,. \tag{3.8}$$

Then

$$\sum_{V/d=0}^{Q/d-1} B_\ell\left(\frac{V/d}{Q/d}\right) = (Q/d)^{-(\ell-1)} B_\ell(0) = Q^{-(\ell-1)} B_\ell d^{\ell-1}$$

and

$$\Sigma_2 = Q^{-(\ell-1)} B_\ell \sum_{d|Q} \mu(d) d^{l-1} = Q^{-(\ell-1)} B_\ell \prod_{p|Q}(1-p^{\ell-1})\,.$$

Now

$$\begin{aligned}
\Sigma_1 &= \sum_{g|q} \mu(q/g)\varphi(g) B_\ell Q^{-(\ell-1)} \prod_{p|Q}(1-p^{\ell-1}) \\
&= B_\ell q^{-(\ell-1)} \sum_{g|q} \varphi(g) g^{\ell-1} \mu(q/g) \prod_{p|(q/g)} (1-p^{\ell-1}) \\
&= B_\ell q^{-(\ell-1)} \prod_{p|q} (\varphi(p)p^{\ell-1} - (1-p^{\ell-1})) = B_\ell q^{-(\ell-1)} \prod_{p|q}(p^\ell - 1) \\
&= B_\ell q \prod_{p|q}(1-p^{-\ell})\,.
\end{aligned}$$

Finally we substitute the value of Σ_1 in (3.7) and this proves the lemma. □

3.4 Computation of a Partial Zeta Function

A main tool used in this section will be the following (Corollary 4.2 from [7])

Lemma 3.4. *Let (e,f) be a $\mathbb{Z}$-basis of $I \in I_F(K)$ for any real quadratic field K, t be a positive integer, $e^* = e + tf$, and assume that $e, e^* \gg 0$. Furthermore, let $\omega = Ce + Df$ with some rational integers $0 \le C, D < q$, and write $c = C/q$, $d = D/q$, $\delta = (D - tC)_q/q$. Let*

$$Z_{I,\omega,q}(s) = Z(s) := \sum_{\beta \in H} (\beta\bar{\beta})^{-s}$$

with $H = \{\beta \in I : \beta \equiv \omega \pmod q, \beta = Xe + Ye^* \text{ with } (X,Y) \in \mathbb{Q}^2, X > 0, Y \ge 0\}$. Then

$$Z(0) = A(1-c) + \frac{t}{2}(c^2 - c - \frac{1}{6}) + \frac{d-\delta}{2} + Tr\left(\frac{-f}{4e^*}\right) B_2(\delta) + Tr\left(\frac{f}{4e}\right) B_2(d)\,,$$

where $A = \lceil tc - d \rceil$.

For the sake of our argument's completeness we give the lemma's proof in Appendix A.

We use that $d \equiv 1 \pmod 4$, so the ring of integers $\mathcal{O}_K$ of the field K is of the type $\mathcal{O}_K = \mathbb{Z}\left[1, (\sqrt{d}+1)/2\right]$. Introduce $\alpha := (\sqrt{d} - an)/2$ which is the positive root of

$$x^2 + (an)x - a = 0\,. \tag{3.9}$$

Then $\alpha + \bar{\alpha} = -an$ and $\alpha\bar{\alpha} = -a$.

We will also come across the quadratic forms

$$f_1(x, y) = ax^2 + anxy - y^2 \tag{3.10}$$

and

$$f_2(x, y) = x^2 + anxy - ay^2\,, \tag{3.11}$$

both of which with discriminant $d = (an)^2 + 4a$.

Recall that $P(K)$ is the set of all nonzero principal ideals in $\mathcal{O}_K$ and define the zeta function

$$\zeta_{P(K)}(s, \chi) = \sum_{\mathfrak{a} \in P(K)} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s}\,.$$

We have

Lemma 3.5. *Let* $d = (an)^2 + 4a$ *be square-free for odd positive integers* a *and* n *with* $a > 1$ *and* $K = \mathbb{Q}(\sqrt{d})$. *If* q *is such a positive integer that* $q \mid n$ *and* $(q, 2a) = 1$, *then for any odd Dirichlet character* $\chi \pmod q$ *we have*

$$\zeta_{P(K)}(0, \chi) = n.g(\chi, f_1, B_2) + an.g(\chi, f_2, B_2)\,.$$

Proof. We know that for $a > 1$ the fundamental unit of K is $\varepsilon_d = 1 - n\overline{\alpha} > 1$, see Lemma 2.3. Thus $\overline{\varepsilon}_d = \varepsilon_+ = 1 - n\alpha$ satisfies $0 < \varepsilon_+ < 1$.

Let us take $I \in I_F(K)$ with $(I, q) = 1$ and consider the zeta function

$$\zeta_I^+(s, \chi) = \zeta_{Cl(I)}^+(s, \chi) := \sum_{\mathfrak{a}} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s}$$

where the sum is over all integral ideals of K which are equivalent to I in the sense that $\mathfrak{a} = (\beta)I$ for some $\beta \gg 0$. We have $N(\varepsilon_d) = 1$ and then

$$\zeta_I(s,\chi) = \zeta_I^+(s,\chi) + \zeta_{(\alpha)I}^+(s,\chi)\,.$$

It is also clear that $\zeta_{Cl(I)}^+(s,\chi) = \zeta_{Cl(I^{-1})}^+(s,\chi)$ and for the latter

$$\zeta_{I^{-1}}^+(s,\chi) = \sum_{b\in P_I} \frac{\chi(N(bI^{-1}))}{(N(bI^{-1}))^s} = (NI^{-1})^{-s} \sum_{b\in P_I} \chi\left(\frac{Nb}{NI}\right)(Nb)^{-s}$$

where $P_I = \{b \in P_F(K) : b = (\beta) \text{ for some } \beta \in I\,, \beta \gg 0\}$. We also introduce $V = \{\nu \pmod q : \nu \in I \text{ and } (\nu, q) = 1\}$ and $P_{I,\nu,q} = \{b \in P_F(K) : b = (\beta) \text{ for some } \beta \in I\,, \beta \equiv \nu \pmod q \text{ and } \beta \gg 0\}$. Since $q \mid n$ we get $\varepsilon_d = 1 - n\bar{\alpha} \equiv 1 \pmod q$ and $\varepsilon_+ = 1 - n\alpha \equiv 1 \pmod q$. Thus every $b \in P_I$ given by $b = (\beta) = (\beta\varepsilon_+^j)$ belongs to exactly one residue class $\nu \in V$. Then we have

$$\zeta_I^+(s,\chi) = (NI^{-1})^{-s} \sum_{\nu\in V} \sum_{b\in P_{I,\nu,q}} \chi\left(\frac{Nb}{NI}\right)(Nb)^{-s}\,.$$

If we take into account that $(I, q) = 1$ and therefore $(NI, q) = 1$, also $Nb = \beta\overline{\beta}$, we get

$$\zeta_I^+(s,\chi) = (NI^{-1})^{-s} \sum_{\nu\in V} \chi\left(\frac{\nu\bar{\nu}}{NI}\right) \sum_{b\in P_{I,\nu,q}} (\beta\overline{\beta})^{-s}\,.$$

Now assume that the $\mathbb{Z}$-basis of the fractional ideal I is of the form (e, f) where $e > 0$ is a rational integer and $e^* = e\varepsilon_+ = e + tf \gg 0$. Then for every principal ideal $b \in P_{I,\nu,q}$ there is a unique β such that $b = (\beta) = (\beta\varepsilon_+^j)$ for any $j \in \mathbb{Z}$, and $\varepsilon_+^2 < \beta/\bar{\beta} \leq 1$. As ε_+ is irrational number for every $\beta \in K$ there is a unique pair $(X, Y) \in \mathbb{Q}^2$ such that $\beta = Xe + Ye\varepsilon_+ = e(X + Y\varepsilon_+)$. Then from $\bar{\beta}\varepsilon_+^2 < \beta \leq \bar{\beta}$ we get

$$(X + Y\varepsilon_d)\varepsilon_+^2 < X + Y\varepsilon_+ \leq X + Y\varepsilon_d\,.$$

Now it follows easily that $X > 0$ and $Y \geq 0$. Thus any $b \in P_{I,\nu,q}$ can be presented uniquely like $b = (\beta)$ for $\beta = e(X+Y\varepsilon_+)$ where X, Y are nonnegative rationals with $X > 0$.

Note also that for $0 \leq C, D \leq q - 1$ the elements $\nu = Ce + Df \in I$ give a complete

system of resdues $\nu \pmod q$. Then we have

$$\zeta_I^+(0,\chi) = \sum_{C,D=0}^{q-1} \chi\left(\frac{(Ce+Df)\overline{(Ce+Df)}}{NI}\right) Z_{I,\nu,q}(0)$$

where $Z_{I,\nu,q}(s)$ is defined in Lemma 3.4.

Observe that $\zeta_{P(K)}(s,\chi) = \zeta_{\mathcal{O}_K}(s,\chi)$ and take $I = \mathcal{O}_K = \mathbb{Z}[1,-\alpha]$. Clearly $(\mathcal{O}_K, q) = 1$. Apply Lemma 3.4 with $e^* = \varepsilon_+ = 1 + n(-\alpha)$ so $t = n$. Also $N\mathcal{O}_K = 1$ and $\nu\bar{\nu} = (C - D\alpha)(C - D\overline{\alpha}) = C^2 - (\alpha + \bar{\alpha})CD + \alpha\bar{\alpha}D = C^2 + anCD - aD^2 = f_2(C,D)$. Since $q \mid t$ we have $\delta = (D - tC)_q/q = D/q = d$ and $\lceil tc - d \rceil = tC/q = tc$. Here $Tr(\alpha/4\varepsilon_+) = Tr(-\alpha/4) = an/4$. Hence

$$\begin{aligned} Z_{\mathcal{O}_K,\nu,q}(0) &= nc(1-c) + \frac{n}{2}(c^2 - c - \frac{1}{6}) + \frac{an}{2}B_2(d) \\ &= -\frac{n}{2}c^2 + \frac{n}{2}c - \frac{n}{2}\frac{1}{6} + \frac{an}{2}B_2(d) \\ &= -\frac{n}{2}(c^2 - c + \frac{1}{6}) + \frac{an}{2}B_2(d) = -\frac{n}{2}B_2(c) + \frac{an}{2}B_2(d) \end{aligned}$$

and

$$\begin{aligned} \zeta_I^+(0,\chi) &= \sum_{C,D=0}^{q-1} \chi(C^2 - aD^2)\left(-\frac{n}{2}B_2(c) + \frac{an}{2}B_2(d)\right) \\ &= -\frac{n}{2}\sum_{C,D=0}^{q-1} \chi(C^2 - aD^2)B_2(c) + \frac{an}{2}\sum_{C,D=0}^{q-1} \chi(C^2 - aD^2)B_2(d)\,. \end{aligned}$$

Now in the first sum make the change of notation $C \leftrightarrow D$ and take into account that $\chi(-1) = -1$. Then

$$\begin{aligned} \zeta_I^+(0,\chi) &= \frac{n}{2}\sum_{C,D=0}^{q-1} \chi(-D^2 + aC^2)B_2(d) + \frac{an}{2}\sum_{C,D=0}^{q-1} \chi(C^2 - aD^2)B_2(d) \\ &= \frac{n}{2}\sum_{C,D=0}^{q-1} \chi(f_1(C,D))B_2(\frac{D}{q}) + \frac{an}{2}\sum_{C,D=0}^{q-1} \chi(f_2(C,D))B_2(\frac{D}{q}) \\ &= \frac{an}{2}g(\chi, f_2, B_2) + \frac{n}{2}g(\chi, f_1, B_2)\,. \end{aligned} \tag{3.12}$$

Next we find $\zeta_{(\alpha)I}^+(0,\chi)$ after we again apply Lemma 3.4 for $(\alpha)I$. Here again $((\alpha)\mathcal{O}_K, q) = 1$. Clearly this follows from $\alpha\overline{\alpha} = a \in (\alpha)\mathcal{O}_K$ and $(a,q) = 1$. We

can take $\mathcal{O}_K = \mathbb{Z}[-\overline{\alpha}, -1]$. Then $(\alpha)\mathcal{O}_K = \mathbb{Z}[-\alpha\overline{\alpha}, -\alpha] = \mathbb{Z}[a, -\alpha]$. In this case $\nu\bar{\nu} = (Ca + D(-\alpha))(Ca + D(-\overline{\alpha})) = \alpha\overline{\alpha}(C\bar{\alpha} + D)(C\alpha + D) = -a(-aC^2 - anCD + D^2) = af_1(C, D)$. Here $N((\alpha)\mathcal{O}_K) = |\alpha\bar{\alpha}| = a$ and $\chi\left(\nu\bar{\nu}/N((\alpha)I)\right) = \chi(f_1(C, D)) = \chi(aC^2 - D^2)$. Also $e^* = a\varepsilon_+ = a + an(-\alpha) = a(1 - n\alpha)$ so $t = an$. Note that again $q \mid t$. Here $Tr(\alpha/4a\varepsilon_+) = Tr(-\alpha/4a) = n/4$ and therefore

$$\begin{aligned} Z_{(\alpha)\mathcal{O}_K,\nu,q}(0) &= anc(1-c) + \frac{an}{2}(c^2 - c - \frac{1}{6}) + \frac{n}{2}B_2(d) \\ &= -\frac{an}{2}c^2 + \frac{an}{2}c - \frac{an}{2}\frac{1}{6} + \frac{n}{2}B_2(d) \\ &= -\frac{an}{2}(c^2 - c + \frac{1}{6}) + \frac{n}{2}B_2(d) = -\frac{an}{2}B_2(c) + \frac{n}{2}B_2(d)\,. \end{aligned}$$

Thus we get

$$\begin{aligned} \zeta^+_{(\alpha)I}(0, \chi) &= -\frac{an}{2}\sum_{C,D=0}^{q-1}\chi(aC^2 - D^2)B_2(c) + \frac{n}{2}\sum_{C,D=0}^{q-1}\chi(aC^2 - D^2)B_2(d) \\ &= \frac{n}{2}g(\chi, f_1, B_2) + \frac{an}{2}(-1)\sum_{C,D=0}^{q-1}\chi(aD^2 - C^2)B_2(d) \\ &= \frac{n}{2}g(\chi, f_1, B_2) + \frac{an}{2}g(\chi, f_2, B_2)\,. \end{aligned} \tag{3.13}$$

Note that we got the equality $\zeta^+_I(0, \chi) = \zeta^+_{(\alpha)I}(0, \chi)$, an equation that holds true in most general real quadratic fields with $N(\epsilon_d) = 1$ and an odd character χ. When we sum up the two zeta functions (3.12) and (3.13) we obtain the statement of the lemma. □

Remark 3.6. Here the result on the zeta function at the class of principal integral ideal is for any odd Dirichlet character modulo q. If $a = 1$ we have that $N(\varepsilon_d) = -1$. In this case $\zeta_I(s, \chi) = \zeta^+_I(s, \chi)$ because for any principal ideal there is a totally positive generator.

From q – odd square-free, $q \mid n$ and $(q, a) = 1$ it follows that $(q, d) = 1$. When we combine Lemma 3.2 with Lemma 3.5 with the remark $B_2 = 1/6$ we arrive at

Corollary 3.7. *Let $d = (an)^2 + 4a$ be a square-free discriminant for odd positive integers a, n with $a > 1$ and $K = \mathbb{Q}(\sqrt{d})$. If $q \equiv 3 \pmod 4$ is such a square-free positive integer that $q \mid n$ and $(q, 2a) = 1$, then*

$$\zeta_{P(K)}(0, \chi_q) = \frac{q}{6}n(a + \chi_q(a))\prod_{p|q}(1 - p^{-2})\,.$$

3.5 Proof of Theorem 3.1

Assume that we are in a field $K = \mathbb{Q}(\sqrt{d})$ with $d = (an)^2 + 4a$ with a, n – odd positive integers, $43 \cdot 181 \cdot 353$ divides n and the class number $h(d)$ equals 1. Then all integral ideals are principal and for the Dedekind zeta function

$$\zeta_K(s, \chi) = \sum_{\mathfrak{a} \subset \mathcal{O}_K} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s}$$

we have $\zeta_K(s, \chi) = \zeta_{P(K)}(s, \chi)$. We know from §4.3 of [52] that

$$\zeta_K(s, \chi) = L(s, \chi) L(s, \chi\chi_d) \, .$$

By the class number formula for imaginary quadratic fields /Theorem 152 in [24]/, again §4.3 of [52], and by $\chi_q(-1) = -1$ because $q \equiv 3 \pmod 4$, we get

$$-L(0, \chi_q) = \sum_{1 \le x \le q-1} \frac{x}{q} \left(\frac{x}{q}\right) = h(-q) \, . \tag{3.14}$$

For $d \equiv 1 \pmod 4$ we have $\left(\frac{-1}{d}\right) = (-1)^{(d-1)/2} = 1$ and thus χ_d is an even characater. Hence $\chi_q \chi_d$ is odd character and $L(0, \chi_q\chi_d) = -h(-qd)$. Therefore

$$\zeta_{P(K)}(0, \chi_q) = L(0, \chi_q) L(0, \chi_q\chi_d) = h(-q) h(-qd) \, . \tag{3.15}$$

First think of a general parameter $q \neq a$ that is a prime number, $q \mid n$ and $2 < q < an/2$. Then after Claim 2.6 we have $\left(\frac{d}{q}\right) = -1$. When $q \mid n$ we get

$$\left(\frac{an^2+4}{q}\right) = \left(\frac{4}{q}\right) = 1 \quad \text{and} \quad \left(\frac{d}{q}\right) = \left(\frac{a}{q}\right)\left(\frac{an^2+4}{q}\right) = \left(\frac{a}{q}\right) = -1 \, .$$

That is why the case $a = 1$ is not possible : clearly $\left(\frac{1}{q}\right) = \left(\frac{a}{q}\right) = \left(\frac{d}{q}\right) = 1$. So we have $a > 1$.

Now, assume that $43 \cdot 181 \cdot 353 \mid n$ and $353 < an/2$. Notice that above the prime $a = q$ was not considered because of Claim 2.6. However $\left(\frac{43}{181}\right) = 1$, thus $a = 43$ is not possible; $\left(\frac{181}{43}\right) = 1$ and $\left(\frac{353}{43}\right) = 1$, so $a = 181$ and $a = 353$ are also excluded from our

assumptions. Hence, if $353 < an/2$ and $43, 181, 353 \mid n$, the class number $h(d) = 1$ only if $\left(\frac{a}{43}\right) = \left(\frac{a}{181}\right) = \left(\frac{a}{353}\right) = -1$.

Now we take the parameter $q = 43 \cdot 181 \cdot 353$. Again consider the real primitive character $\chi_q(m) = \left(\frac{m}{q}\right)$ modulo q. As $43 \equiv 3 \pmod 4$, $181 \equiv 1 \pmod 4$ and $353 \equiv 1 \pmod 4$ we have $q \equiv 3 \pmod 4$ and $\chi_q(-1) = -1$. Also $a > 1$ and we can apply (3.15) and Corollary 3.7 and multiply both sides of its equation by q. This way we arrive at the promised equation (3.1)

$$qh(-q)h(-qd) = n\left(a + \left(\frac{a}{q}\right)\right)\frac{1}{6}\prod_{p|q}(p^2 - 1)\,.$$

In this case

$$B := \frac{1}{6}\prod_{p|q}(p^2 - 1) = \frac{1}{6}42 \cdot 44 \cdot 180 \cdot 182 \cdot 352 \cdot 354 = 2^{11}3^3 \ldots$$

and $2^{11} \| B$.

As $a > 1$ we have that $d = a(an^2 + 4)$ is a product of two different primes. Notice as well that $a \equiv an^2 + 4 \pmod 4$. By Gauss genus theory and Lemma 2.1, as d is odd, we know that if $a \equiv an^2 + 4 \equiv 1 \pmod 4$ for the real quadratic field $K = \mathbb{Q}(\sqrt{a(an^2 + 4)})$, then the 2-rank of the class group is the same as the 2-rank of the narrow class group, i.e. $2 - 1 = 1$. This contradicts $h(d) = 1$. Therefore $a \equiv 3 \pmod 4$. But in this case $a + \left(\frac{a}{q}\right) = a - 1$ and $a - 1 \equiv 2 \pmod 4$ so $2 \| \left(a + \left(\frac{a}{q}\right)\right)$. Here Claim 2.6 has a great importance, also q being a product of three primes, for then $\left(\frac{a}{q}\right) = -1$. The parameter n is odd by definition. It follows that for the right-hand side of (3.1) we have

$$2^{12} \| n\left(a + \left(\frac{a}{q}\right)\right)B\,. \tag{3.16}$$

We regard the left-hand side of (3.1). As we pointed out in §3.1 we have $h(-43 \cdot 181 \cdot 353) = 2^9.3$. Again by genus theory the 2-class group of $Cl(-qd)$ has a rank $5 - 1 = 4$ since qd has 5 distinct prime divisors. Indeed, we showed that $a \notin \{43, 181, 353\}$, also $an^2 + 4 > an/2 > 353$ and clearly $a \neq an^2 + 4$. Therefore $2^{9+4} = 2^{13} \mid qh(-q)h(-qd)$. This contradicts (3.16).

We conclude that $h(d) > 1$ for $an/2 > 353$. But then for discriminants $d = (an)^2 + 4a$ for positive odd a and n and $43 \cdot 181 \cdot 353 \mid n$ we cannot have class number 1. This concludes the proof of Theorem 3.1.

Remark 3.8. The main idea used in this section, a comparison of 2-parts in (3.1), can be utilized toward other results of this type. For example, if $d = a(an^2 + 4)$ for odd positive integers a and n where $5 \cdot 359 \cdot 541 \mid n$, then $h(d) > 1$. The exact divisors of n are chosen according to Table 12 in [11]: $h(-5 \cdot 359 \cdot 541) = 2^9$ and again we have a bigger power of 2 on the left-hand side of (3.1). Also $5 \cdot 359 \cdot 541 \equiv 3 \pmod 4$ so when we take up a real character we have formula (3.14). Also $a \in \{5, 359, 541\}$ are not covered by Claim 2.6 for each prime in the set, but these a's are excluded by a simple check of the Legendre symbols of each other.

In this sense if we know a result similar to [15] but for discriminant with three prime divisors, we would have our theorem extended for an infinite family of n such that $pqr \mid n$. This we achieve in the next chapter.

Chapter 4

Divisibility of Class Numbers of Imaginary Quadratic Fields

4.1 Introduction

In this chapter we establish the existence of infinitely many imaginary quadratic fields $\mathbb{Q}(\sqrt{-d})$ with a discriminant $-d$, such that d has only three distinct prime factors and in the class group $Cl(-d)$ there is an element of order 2ℓ for any integer $\ell \geq 2$ and $5, 3 \nmid \ell$. The result extends naturally the one in [15], where the same problem is considered for $d = pq$, a product of two distinct primes. We show without a proof how with the same techniques an analogous result can be stated for any fixed number of prime divisors of d and any $\ell \geq 2$. Whereas in [15] the infinite number of solutions of a certain additive problem is borrowed by a strong estimate in [10], we will derive a weaker asymptotic formula following closely the method of §5 in [2]. The idea of generating such imaginary quadratic fields comes from [2] and [48], as stated in [15].

The main motivation for considering the questions of the present chapter was Theorem 3.1 which solves class number one problem for a certain type of real quadratic fields. We recall that for the square-free $d = (an)^2 + 4a$ with odd positive integers a and n such that n is divisible by $43 \cdot 181 \cdot 353$, one has $h(d) > 1$. The particular parameter dividing n was chosen from a table of class numbers which showed that the 2-part of the class group $Cl(-43 \cdot 181 \cdot 353)$ has a high order. More specifically, $h(-43 \cdot 181 \cdot 353) = 2^9 \cdot 3$, and we also needed that $43 \cdot 181 \cdot 353 \equiv 3 \pmod 4$. We will show how the main result of this chapter implies existence of an infinite family of parameters $q = p_1 p_2 p_3$, where p_i are distinct primes, and $q \equiv 3 \pmod 4$, such that for square-free $d = (an)^2 + 4a$ with odd positive a and n, and q dividing n, we have $h(d) > 1$.

Let $\ell \geq 2$ be any integer. Consider the additive problem

$$4m^{\ell} = p_1 + p_2 p_3 \,, \tag{4.1}$$

where m is an odd integer and the primes p_1, p_2, p_3 are different. Let Δ be a fixed positive integer such that $(15, \Delta) = 1$ and the variables in (4.1) satisfy

$$\begin{aligned} x^{1/8} < p_1 \leq x, \quad p_1 \equiv -5 \pmod{\Delta}\,; \\ x^{1/8} < p_2 \leq x^{1/4} < p_3, \ p_2 p_3 \leq x, \quad p_2, p_3 \equiv 3 \pmod{\Delta}\,. \end{aligned} \tag{4.2}$$

If we write

$$4m^{\ell} = U + V \tag{4.3}$$

for any positive integers U, V and assume that $U > V$, then for $n = (U - V)/2$ we have

$$4m^{2\ell} - n^2 = (2m^{\ell} - n)(2m^{\ell} + n) = \left(\frac{U+V}{2} - \frac{U-V}{2}\right)\left(\frac{U+V}{2} + \frac{U-V}{2}\right) = V \cdot U.$$

This way having infinitely many solutions of (4.1) we will find infinitely many corresponding discriminants $d = p_1 p_2 p_3 = 4m^{2\ell} - n^2$.

The following statement shows that under some conditions, which are satisfied from the solutions of (4.1), discriminants of the type $d = 4m^{2\ell} - n^2$ yield existence of an element of a large order in the class group $Cl(-d)$. The lemma is implicitly shown in the proof of the main result in [15].

Lemma 4.1. *For integer $\ell \geq 2$ let m and n be integers with $(n, 2) = 1$ and $2m^{\ell} - n > 1$. If d is a square-free integer for which*

$$d = 4m^{2\ell} - n^2 \,,$$

then $Cl(-d)$ contains an element of order 2ℓ.

With the notation $e(\alpha) = e^{2\pi i \alpha}$ we introduce the generating functions

$$f_1(\alpha) = \sum_{p_1} e(p_1 \alpha) = \sum_{n \leq x} b_n e(n\alpha), \tag{4.4}$$

$$f_2(\alpha) = \sum_{p_2, p_3} e(p_2 p_3 \alpha) = \sum_{n \leq x} c_n e(n\alpha), \tag{4.5}$$

$$g(\alpha) = \sum_{m} \ell m^{\ell-1} e(m^\ell \alpha) = \sum_{m \le M} \omega_m e(m^\ell \alpha), \tag{4.6}$$

where p_i satisfy (4.2) and

$$m \le M = \left(\frac{x}{2}\right)^{1/\ell} \quad \text{and} \quad (m, \Delta) = 1. \tag{4.7}$$

Remark that we will generally omit all the conditions on the parameters at which we make the summation in (4.4), (4.5), (4.6), but they will always satisfy (4.2) or (4.7), unless it is specified otherwise. We will use the circle method and in its setting it is sensible to consider

$$R(x) := \sum_{p_1 + p_2 p_3 = 4m^\ell} \ell m^{\ell-1} = \int_0^1 f_1(\alpha) f_2(\alpha) g(-4\alpha) d\alpha. \tag{4.8}$$

For this integral we state the following asymptotic formula whose proof will be the main focus of this chapter starting from section §4.3.

Theorem 4.2. *Suppose that Δ, ℓ are positive integers for which $16\ell^2 \mid \Delta$ and $(15, \Delta) = 1$. Then*

$$R(x) = 4\ell(2, \ell) \prod_{p \mid \Delta} (\ell, p-1) f_1(0) f_2(0) + \mathcal{O}\left(\frac{x^2}{\log^3 x}\right).$$

Note that the main term in the upper formula is larger than the error term. Indeed, the Prime Number Theorem for arithmetic progressions implies

$$\pi(x, q, b) = \frac{\pi(x)}{\varphi(q)} + \mathcal{O}\left(\frac{x}{\log^C x}\right) \tag{4.9}$$

for any fixed integers $C > 0$, b coprime to q. Here $\pi(x) \sim x/\log x$ is the usual prime counting function, and $\pi(x, q, b)$ counts the primes $p \le x$ in the residue class b modulo q. Therefore, taking $C = 2$,

$$f_1(0) = \sum_{\substack{x^{1/8} < p_1 \le x \\ p_1 \equiv -5 \pmod{\Delta}}} 1 = \pi(x, \Delta, -5) - \pi(x^{1/8}, \Delta, -5) = \frac{\pi(x)}{\varphi(\Delta)} + \mathcal{O}\left(\frac{x}{\log^2 x}\right),$$

hence

$$f_1(0) \asymp \frac{x}{\log x}. \tag{4.10}$$

We also have

$$f_2(0) = \sum_{p_2, p_3} 1 \asymp \frac{x}{\log x}. \tag{4.11}$$

This estimate follows from a more general result, Lemma 4.5, which is stated and proven

in the next section.

Estimates (4.10) and (4.11) show that the main term in Theorem 4.2 exceeds the error term. Note that the primes p_1, p_2, p_3, counted in $R(x)$, are growing to infinity with x.

In a similar way as in [2], taking into account that the weights in $g(\alpha)$ are $\ll M^{\ell-1} \ll x^{1-1/\ell}$, we can finally deduce

Corollary 4.3. *Let $\ell \geq 2$ and Δ be positive integers for which $16\ell^2 \mid \Delta$ and $(15, \Delta) = 1$. If $R^\sharp(X)$ denotes the number of positive integers $d \leq X$ of the form*

$$d = p_1 p_2 p_3 = 4m^{2\ell} - n^2 \,,$$

where p_1, p_2, p_3 are distinct primes which satisfy (4.2) with $x = \sqrt{X}$, then

$$R^\sharp(X) \gg \frac{X^{1/2+1/(2\ell)}}{\log^2 X} \,.$$

Now the result of Theorem 3.1 can be extended:

Corollary 4.4. *There is an infinite family of parameters $q = p_1 p_2 p_3$, where p_1, p_2, p_3 are distinct primes, and $q \equiv 3 \pmod 4$, with the following property. If $d = (an)^2 + 4a$ is square-free for odd positive integers a and n, and q divides n, then $h(d) > 1$.*

Proof. The main identity to prove Theorem 3.1 was

$$q.h(-q).h(-qd) = n\left(a + \left(\frac{a}{q}\right)\right)\frac{1}{6}\prod_{p\mid q}(p^2-1)\,, \tag{4.12}$$

which holds if we assume that $h(d) = 1$ and $q \equiv 3 \pmod 4$. According to Claim 2.6 if $h(d) = 1$ for the square-free discriminant $d = (an)^2 + 4a$, then a and $an^2 + 4$ are primes. Something more, for any prime $r \neq a$ such that $2 < r < an/2$ we have $\left(\frac{d}{r}\right) = -1$. Then by Lemma 2.1 it follows that $a \equiv 3 \pmod 4$. Also, if we further assume $an/2 > \max(p_1, p_2, p_3)$, we get $\left(\frac{a}{q}\right) = -1$, so $a + \left(\frac{a}{q}\right) = a - 1 \equiv 2 \pmod 4$. This is always true because $p_1 p_2 p_3$ divides n and therefore $n \geq p_1 p_2 p_3$.

Now consider $q = p_1 p_2 p_3$ from Corollary 4.3. Take ℓ such that $\ell = 2^g$ for $g \geq 9$. From conditions (4.2) and $16 \mid \Delta$ we see that $p_i \equiv 3 \pmod 8$, $q \equiv 3 \pmod 4$, and $2^9 \| \prod_{p_i}(p_i^2 - 1)$. Then the right-hand side of the above identity has 2-part exactly 2^9. The left-hand side,

on the other hand, is divisible by the class number $h(-p_1p_2p_3)$ and 2ℓ divides this class number. This is a contradiction. Therefore $h(d) > 1$. □

At this point it becomes clear why we solve the additive problem (4.1) with a factor 4 instead of the original equation

$$2m^\ell = AU + BV \tag{4.13}$$

from [2]. We need a discriminant d which is a product of exactly three primes, thus in our application we take $A = B = 1$. Something more, we want to control the 2-part in the right-hand side of (4.12). We do this by imposing $p_i \equiv 3 \pmod 8$. Then $p_1 + p_2p_3 \equiv 4 \pmod 8$ but $2m^\ell \not\equiv 4 \pmod 8$. So we need to change the coefficient 2 to 4 in (4.13). We can still keep the skeleton of the proof the same as in [2] and only work out slight modifications in the corresponding estimates.

4.2 Generalizations: Divisibility of Class Numbers

Let us fix any integers $\ell \geq 2$ and $k \geq 3$. Consider the additive problem

$$4m^\ell = p_1 + p_2 \dots p_k\,, \tag{4.14}$$

where m is an odd integer and the primes $p_1, p_2, \dots, p_k$ are different. Let Δ be an integer such that $(c_0(4 - c_0^{k-1}), \Delta) = 1$ and for the variables in (4.14) assume that $p_1 \equiv 4 - c_0^{k-1} \pmod \Delta$ and $p_2, \dots, p_k \equiv c_0 \pmod \Delta$. Denote $y = x^{1/2^{\ell+2}}$ and first assume that $y < p_1 \leq x$. Clearly there are positive real numbers $1 < \alpha_2 < \ldots < \alpha_{k-1}$ such that $\sum_{2\leq i\leq k-1} \alpha_i < 2^{\ell+2} - 1$ and letting them being fixed we further require

$$y < p_2 \leq y^{\alpha_2} < p_3 \leq y^{\alpha_3} < \ldots \leq y^{\alpha_{k-1}} < p_k \text{ and } p_2p_3 \dots p_k \leq x\,. \tag{4.15}$$

The latter guarantees that $p_2, \dots, p_k$ are different while the lower bound $x^{1/2^{\ell+2}}$ for each of them is applied during the proof of Theorem 4.2.

Here we show a statement we already used in the previous section:

Lemma 4.5. *Let $n \geq 2$ be an integer and $q_1, q_2, \dots, q_n$ be primes from the same arithmetic progression that also satisfy*

$$y < q_1 \leq y^{\alpha_1} < q_2 \leq y^{\alpha_2} < \ldots \leq y^{\alpha_{n-1}} < q_n \text{ and } q_1q_2 \dots q_n \leq x,$$

where $y = x^{1/\beta}$ *for some real* $\beta > 1$ *and* $\sum_{1\le i\le n-1}\alpha_i < \beta - 1$. *Then if* $f_n(\alpha) = \sum_{q_1,\dots,q_n} e(q_1\dots q_n\alpha)$, *we have*

$$f_n(0) = \sum_{q_1,\dots,q_n} 1 \asymp \frac{x}{\log x}\,.$$

Proof. We note that

$$x^{1-\frac{1}{\beta}(\alpha_1+\dots+\alpha_{n-1})} = \frac{x}{y^{\alpha_1+\dots+\alpha_{n-1}}} \le \frac{x}{q_1\dots q_{n-1}} \le \frac{x}{y^{1+\alpha_1+\dots+\alpha_{n-2}}} = x^{1-\frac{1}{\beta}(1+\alpha_1+\dots+\alpha_{n-2})}\,.$$

Then, since β and $\alpha_1,\dots,\alpha_{n-1}$ are fixed, we have $\log\dfrac{x}{q_1\dots q_{n-1}} \asymp \log x$. In that case after the Prime Number Theorem, similarly to (4.10), we get

$$f_n(0) \;=\; \sum_{q_1,\dots,q_{n-1}} \sum_{q_n > x^{\frac{\alpha_{n-1}}{\beta}}}^{x/(q_1\dots q_{n-1})} 1 \asymp \sum_{q_1,\dots,q_{n-1}} \frac{x/(q_1\dots q_{n-1})}{\log x}\,.$$

Obviously, with the notation $\alpha_0 = 1$,

$$\sum_{q_1,\dots,q_{n-1}} \frac{1}{q_1\dots q_{n-1}} = \prod_{i=1}^{n-1} \sum_{y^{\alpha_{i-1}} < q_i \le y^{\alpha_i}} \frac{1}{q_i}$$

and every interval $(y^{\alpha_{i-1}}, y^{\alpha_i}]$ can be divided into $\asymp \log x$ intervals of type $(A, 2A]$. If the primes p run over an arithmetic progression modulo some fixed q, then

$$\sum_{A<p\le 2A} \frac{1}{p} \asymp \frac{1}{\varphi(q)}\frac{1}{A}\frac{A}{\log A} \asymp \frac{1}{\log A}\,.$$

Therefore every factor $\sum_{q_i}\frac{1}{q_i} \asymp 1$ and

$$\sum_{q_1,\dots,q_{n-1}} \frac{1}{q_1\dots q_{n-1}} \asymp 1\,.$$

This finishes the proof of the lemma. □

From all these we can conclude that without much effort, following literally the method in this chapter for discriminants of only three prime factors, one can show an analogue of Corollary 4.3 for the solutions of (4.14). Then from Lemma 4.1 it follows

Lemma 4.6. *If for any fixed integers* $k \ge 3$ *and* $\ell \ge 2$ *there exist integers* c_0, Δ *with* $16\ell^2 \mid \Delta$ *and* $\big(c_0(4 - c_0^{k-1}), \Delta\big) = 1$, *then there are infinitely many discriminants* $d = p_1p_2\dots p_k$ *such that the group* $Cl(-d)$ *consists of an element of order* 2ℓ.

Observe that when $3 \mid \ell$ and $k-1$ is even, we always have $1 \equiv 4 \equiv c_0^{k-1} \pmod 3$ for any $(c_0, 3) = 1$. Therefore $(4 - c_0^{k-1}, \ell) > 1$ and we cannot use the same methods for (4.14). The situation can be remedied by considering

$$2m^\ell = p_1 + p_2 \dots p_k \,. \tag{4.16}$$

We require m to be an odd integer and the primes $p_1, \dots, p_k$ to be different elements of the same arithmetic progression with difference Δ and $p_i \equiv 1 \pmod \Delta$. Let the variables in (4.16) satisfy $x^{1/2^{\ell+1}} < p_1 \leq x$ and conditions (4.15), with the difference that $y = x^{1/2^{\ell+1}}$ and we demand in extra $2^{\ell+1} - 1 < 1 + \alpha_2 + \ldots + \alpha_{k-1} < 2^{\ell+1}$. This way we assure $d = p_1 \dots p_k \geq m^\ell$ and the different power in the definition of y comes from the difference between our Lemma 4.13 and the corresponding estimate in [2].

Proceeding exactly like in the paper of Balog and Ono we can show

Lemma 4.7. *For any fixed integers $k \geq 3$ and $\ell \geq 2$ there exists Δ with $4\ell^2 \mid \Delta$ such that there are infinitely many solutions of the equation (4.16).*

In order to apply the original lemmata from [2] we also need Proposition 1 [48]:

Lemma 4.8 (Soundararajan [48]). *Let $\ell \geq 2$ be an integer and let $d \geq 63$ be a square-free integer for which*

$$dt^2 = m^{2\ell} - n^2 \,,$$

where m and n are integers with $(m, 2n) = 1$ and $m^\ell \leq d$. Then $Cl(-d)$ contains an element of order 2ℓ.

We can conclude

Theorem 4.9. *Let $\ell \geq 2$ and $k \geq 3$ be integers. Then there are infinitely many imaginary quadratic fields whose ideal class group has an element of an order 2ℓ and whose discriminant has exactly k distinct prime divisors.*

On the one hand, in order to generalize Theorem 3.1 for real quadratic fields we have to solve equation (4.1) and modify some lemmata from [2]. On the other hand, to obtain Theorem 4.9 for imaginary quadratic fields we have to define the proper additive problem (4.13), which, however, we can solve after direct application of the statements from §5 of [2].

4.3 Preliminary Lemmata

For the integers $u\,, q$ we denote by $u(q)$ the fact that u runs through a whole system of residues modulo q. For integers $q \geq 1$ and a we require the Gaussian sum

$$G(q,a) = \sum_{\substack{u(q) \\ (u,q,\Delta)=1}} e\left(\frac{au^{\ell}}{q}\right)$$

and the auxiliary function

$$V(\eta) = \sum_{n \leq x/2} e(n\eta).$$

In this section we state the lemmata required for the estimate on the 'minor arcs' and more refined expressions of $g(\alpha)$ and $G(q,a)$. These are variants of Lemma 5.2 to Lemma 5.8 from §5 of [2] and some statements needed for the Hardy-Littlewood's circle method application taken from [51].

We start with the Dirichlet's approximation lemma

Lemma 4.10. *Let α denote a real number. Then for each real number $N \geq 1$ there exists a rational number a/q with $(a,q) = 1$, $1 \leq q \leq N$ and*

$$\left|\alpha - \frac{a}{q}\right| \leq \frac{1}{qN}\,.$$

Proof. This is Lemma 2.1 from [51]. □

Lemma 4.11 (Weyl). *Let α denote a real number and a/q is a rational number with $(a,q) = 1$ and $|\alpha - a/q| \leq 1/q^2$. Then for any positive ϵ we have*

$$\sum_{m \leq y} e(\alpha m^{\ell}) \ll y^{1+\epsilon}\left(\frac{1}{q} + \frac{1}{y} + \frac{q}{y^{\ell}}\right)^{2^{1-\ell}}\,.$$

Proof. This is Lemma 2.4 from [51]. □

Lemma 4.12. *If a and $q \geq 1$ are integers and η is a real number, then*

$$g\left(\frac{a}{q} + \eta\right) = \frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta} G(q,a)V(\eta) + \mathcal{O}\left(qM^{\ell-1}(1 + |\eta|M^{\ell})\right)$$

Here and afterwards in the chapter we mean $\varphi(a,b) := \varphi((a,b))$.

Proof. This is Lemma 5.2 from [2] without any modifications. □

Lemma 4.13. *Let $M^{1/2} < q \le N := M^{\ell-1/2}$, $(a,q)=1$ and $|\alpha - a/q| \le 1/qN$. Then we have*

$$g(4\alpha) \ll M^{\ell - 2^{-(\ell+2)}}$$

Proof. We give here modified version of the proof of Lemma 5.3 [2]. Note that we could only show the slightly weaker estimate $g(4\alpha) \ll M^{\ell-2^{-(\ell+2)}}$ than $g(2\alpha) \ll M^{\ell-2^{-(\ell+1)}}$ from [2]. Also there is a slight difference in the approximation we make below that comes from considering $g(4\alpha)$ in our case instead of $g(2\alpha)$. The inequality we want to prove is essentially Weyl's inequality from Lemma 4.11.

Recall that

$$g(4\alpha) = \sum_{\substack{m \le M \\ (m,\Delta)=1}} \ell m^{\ell-1} e(4\alpha m^\ell) = \sum_{d|\Delta} \mu(d) \ell d^{\ell-1} \sum_{m \le M/d} m^{\ell-1} e(4\alpha d^\ell m^\ell)$$

and applying summation by parts we get

$$g(4\alpha) = \sum_{d|\Delta} \mu(d) \ell d^{\ell-1} \left([M/d]^{\ell-1} \Sigma_{[M/d]} - \sum_{y=1}^{[M/d]-1} \left((y+1)^{\ell-1} - y^{\ell-1} \right) \Sigma_y \right), \tag{4.17}$$

where

$$\Sigma_y := \sum_{m \le y} e(4\alpha d^\ell m^\ell).$$

Notice that when $y \le M^{1-2^{-(\ell+1)}}$ trivially

$$|\Sigma_y| \le M^{1-2^{-(\ell+1)}} < M^{1-2^{-(\ell+2)}}.$$

Now assume that $y > M^{1-2^{-(\ell+1)}}$. To estimate Σ_y we will apply Weyl's inequality with some rational approximation of $4\alpha d^\ell$. To find such we apply Lemma 4.10 – there exist $(a',q')=1$ and $1 \le q' \le 2N$ such that

$$\left| 4d^\ell \alpha - \frac{a'}{q'} \right| < \frac{1}{q'(2N)} < \frac{1}{(q')^2}.$$

Now we consider the two possibilities

1. $4d^\ell a/q = a'/q'$. Here we can write $4d^\ell a = a'r$ and $q = q'r$ for $r = 4d^\ell a/a' \in \mathbb{Z}$. If there is a prime p such that $p \mid a$ but $p \nmid a'$ it follows that $p \mid r$, so $p \mid q$. But this

yields the contradiction $p \mid (a,q) = 1$. In the same way we see that if $p^k \mid a$ we need to have $p^k \mid a'$. Therefore $a \mid a'$ and $a/a' \leq 1$. So $r \leq 4d^\ell$, $q = q'r \leq q'4d^\ell$ and $q' \geq q/(4d^\ell)$. By the assumptions on q we get

$$\frac{M^{1/2}}{4d^\ell} < q' \leq 2N\,. \tag{4.18}$$

2. $4d^\ell a/q \neq a'/q'$. In this case we form the difference

$$\begin{aligned}\frac{1}{qq'} &\leq \left|4d^\ell\frac{a}{q} - \frac{a'}{q'}\right| = \left|4d^\ell\alpha - 4d^\ell\alpha + 4d^\ell\frac{a}{q} - \frac{a'}{q'}\right| \leq \left|4d^\ell\alpha - \frac{a'}{q'}\right| + 4d^\ell\left|\alpha - \frac{a}{q}\right| \\ &\leq \frac{1}{q'(2N)} + \frac{4d^\ell}{qN} = \frac{q + 8q'd^\ell}{2Nqq'}\,.\end{aligned}$$

When we multiply both sides of the outermost members of the inequality by $qq'2N$ we get $2N \leq q + 8d^\ell q'$. Again by the lemma's assumptions $q \leq N$ and we should have $8d^\ell q' \geq N$, otherwise $q + 8d^\ell q' < 2N$. We conclude that

$$\frac{N}{8d^\ell} \leq q' \leq 2N\,. \tag{4.19}$$

Now we apply Weyl's inequality for $\left|4d^\ell\alpha - a'/q'\right| < 1/(q')^2$ where we combine (4.18) and (4.19) for the lower bound of q' : $\min(M^{1/2}/(4d^\ell), N/(8d^\ell)) \leq q' \leq 2N$ and we take $\epsilon = 2^{-(\ell+2)}$. Then

$$\Sigma_y \ll y^{1+2^{-(\ell+2)}}\left(\frac{1}{q'} + \frac{1}{y} + \frac{q'}{y^\ell}\right)^{2^{1-\ell}}\,.$$

We have

$$(q')^{-1} \leq \max\left(\frac{4d^\ell}{M^{1/2}}, \frac{8d^\ell}{M^{\ell-1}.M^{1/2}}\right) = \frac{4d^\ell}{M^{1/2}}\max\left(1, \frac{2}{M^{\ell-1}}\right) = \frac{4d^\ell}{M^{1/2}}$$

when $\ell \geq 2$ and x is large enough, and $1/y < 1/M^{1-2^{-(\ell+1)}}$. It follows that

$$\Sigma_y \ll y^{1+2^{-(\ell+2)}}\left(\frac{1}{q'} + \frac{1}{y} + \frac{q'}{y^\ell}\right)^{2/2^\ell} \ll M^{1+2^{-(\ell+2)}}\left(\frac{1}{q'} + \frac{1}{y} + \frac{q'}{y^\ell}\right)^{2/2^\ell}\,.$$

The expression in the brackets is

$$\begin{aligned}&\ll \frac{1}{M^{1/2}} + \frac{1}{y} + \frac{N}{y^\ell} \ll \frac{1}{M^{1/2}} + \frac{1}{y} + \frac{M^\ell}{M^{1/2}(M^{1-1/2^{\ell+1}})^\ell} = \frac{1}{M^{1/2}} + \frac{1}{y} + \frac{M^{\ell/2^{\ell+1}}}{M^{1/2}} \\ &\ll M^{-1/2} + M^{-1+1/2^{\ell+1}} + M^{-1/2+\ell/2^{\ell+1}} \ll M^{-1/4}\,,\end{aligned}$$

because for $l \geq 2$ the last summand makes the biggest contribution. But then

$$\Sigma_y \ll M^{1+2^{-(\ell+2)}} M^{-1/2^{\ell+1}} = M^{1-2^{-(\ell+2)}} .$$

Now we insert the last estimate into (4.17). Using that $\sum_{d|\Delta} \ll 1$, $d \ll 1$, $(y+1)^{\ell-1} - y^{\ell-1} \ll y^{\ell-2}$, we get

$$g(4\alpha) \ll M^{\ell-2^{-(\ell+2)}} .$$

□

Lemma 4.14. *If $(q_1, q_2) = 1$, then $G(q_1, a_1)G(q_2, a_2) = G(q_1q_2, a_1q_2 + a_2q_1)$.*

Proof. This is Lemma 5.4 from [2] and follows from Lemma 2.10, [51]. □

Lemma 4.15. *If p is prime and a is integer coprime to p, then $|G(p, a)| \leq (\ell, p-1)p^{1/2}$*

Proof. This is Lemma 5.5 of [2] and follows from Lemma 4.3, [51]. □

Lemma 4.16. *Suppose that $p \mid \Delta$ is prime and let $s := ord_p(4\ell)$. If $p \nmid a$ and $k \geq \max(2, 2s+1)$, then $G(p^k, a) = G(p^k, 4a) = 0$.*

Proof. First we show that $G(p^k, 4a) = 0$. From the assumptions we have $k-s-1 \geq s \geq 0$, so we can represent the residues modulo p^k in the form $u + vp^{k-s-1}$ where u runs through the residues modulo p^{k-s-1} and v – the residues modulo p^{s+1}.

Since $p \mid \Delta$, the condition $(u, p, \Delta) = 1$ is equivalent to $p \nmid u$, and

$$G(p^k, 4a) = \sum_{\substack{u(p^k) \\ p \nmid u}} e\left(\frac{4au^\ell}{p^k}\right) = \sum_{\substack{u(p^{k-s-1}) \\ p \nmid u}} \sum_{v(p^{s+1})} e\left(\frac{4a(u+vp^{k-s-1})^\ell}{p^k}\right) .$$

By the binomial polynomial theorem $(u+vp^{k-s-1})^\ell = \sum_{m=0}^{\ell} \binom{\ell}{m} u^{\ell-m}(vp^{k-s-1})^m$. Consider the possibilities

1. $s = 0$, $m \geq 2$. Here $m(k-s-1) = m(k-1) \geq 2(k-1) \geq 2$ whenever $k \geq 2$, which is true.

2. $s \geq 1$, $m \geq 3$. Now $m(k-s-1) \geq 3(k-s-1) \geq k$ if $2k \geq 3s+3$. We know that $k \geq \max(2, 2s+1)$, hence $2k \geq 4s+2 \geq 3s+3$ if and only if $s \geq 1$. This is true in the regarded case.

3. $s \geq 1$, $m = 2$. We can have $2(k-s-1) \geq k$ following from $k \geq 2s+2$. The only possible problem might arise for $k = 2s+1$. However in this case

$$\frac{4a\binom{\ell}{2}u^{\ell-2}(vp^s)^2}{p^{2s+1}} = \frac{au^{\ell-2}(2\ell)(\ell-1)v^2}{p}$$

and, as $\mathrm{ord}_p(4\ell) = s \geq 1$, in any case $p \mid 2\ell$.

All these show that for $m \geq 2$ the summands from the binomial polynomial contribute integers as arguments of the exponent $e(x)$ so we can write

$$G(p^k, 4a) = \sum_{\substack{u(p^{k-s-1}) \\ p \nmid u}} e\left(\frac{4au^\ell}{p^k}\right) \sum_{v(p^{s+1})} e\left(\frac{4\ell a u^{\ell-1} v}{p^{s+1}}\right).$$

Now $p \nmid a$, $p \nmid u$, and $\mathrm{ord}_p(4\ell) = s$. Therefore, if we write $4\ell = p^s \ell_1$ with $(\ell_1, p) = 1$,

$$\sum_{v(p^{s+1})} e\left(\frac{4\ell a u^{\ell-1} v}{p^{s+1}}\right) = \sum_{v(p^{s+1})} e\left(\frac{\ell_1 a u^{\ell-1} v}{p}\right) = p^s.0 = 0\,.$$

Hence $G(p^k, 4a) = 0$.

The proof that $G(p^k, a) = 0$ is identical for $p \neq 2$. If $p = 2$, notice that

$$\sum_{\substack{u(2^k) \\ 2 \nmid u}} e\left(\frac{4au^\ell}{2^k}\right) = 4 \sum_{\substack{u(2^{k-2}) \\ 2 \nmid u}} e\left(\frac{au^\ell}{2^{k-2}}\right), \tag{4.20}$$

i.e. $G(2^k, a) = G(2^{k+2}, 4a)/4$. When k is not smaller than $\max(2, 2s+1)$, so is $k+2$. This shows that $G(p^k, a) = 0$. □

Lemma 4.17. *If $(q, a) = 1$, then*

$$G(q, 4a) \ll q^{1-1/\ell}\,.$$

Proof. Using Lemma 4.14, 4.15, 4.16 we reduce the statement to Theorem 4.2 from [51]. In [51] one considers the sum

$$S(a, q) = \sum_{x(q)} e\left(\frac{ax^\ell}{q}\right)$$

and for it we have $S(q, a) \ll q^{1-1/\ell}$ when $(q, a) = 1$.

We can reformulate Lemma 4.14: for $(q_1, q_2) = 1$ and $q_1\bar{q}_1 \equiv 1 \pmod{q_2}$, $q_2\bar{q}_2 \equiv 1 \pmod{q_1}$ we have

$$G(q_1q_2, a) = G(q_1, a\bar{q}_2)G(q_2, a\bar{q}_1)\,. \tag{4.21}$$

Still $(q_1, a\bar{q}_2) = (q_2, a\bar{q}_1) = 1$ and the desired estimate of $G(q, 4a)$ does not depend on the second argument, so it suffices to consider only $G(p^k, 4a)$.

Let $p \neq 2$. Then $(p, 4a) = 1$. If $p \nmid \Delta$ the condition $(u, p^k, \Delta) = 1$ is trivial, so $G(p^k, 4a) = S(p^k, 4a)$ and Theorem 4.2 [51] applies. When $p \mid \Delta$ we consider only, because of Lemma 4.16, $k < \max(2, 2s + 1)$. When this maximum is 2, then $k = 1$. In that case, as $\ell \geq 2$, we have

$$G(p, 4a) \ll p^{\frac{1}{2}} \ll p^{1-\frac{1}{\ell}}$$

after Lemma 4.15. Now assume that $s > 0$, i.e. $s \geq 1$. Then

$$G(p^k, 4a) = \sum_{\substack{u(p^k)\\ p\nmid u}} e\left(\frac{4au^\ell}{p^k}\right) = \sum_{u(p^k)} e\left(\frac{4au^\ell}{p^k}\right) - \sum_{\substack{u(p^k)\\ p\mid u}} e\left(\frac{4au^\ell}{p^k}\right) = S(p^k, 4a) + \mathcal{O}(p^{k-1})\,. \tag{4.22}$$

By Theorem 4.2 [51] $S(p^k, 4a) \ll p^{k(1-1/\ell)}$. Obviously we will have $G(p^k, 4a) \ll p^{k(1-1/\ell)}$ if $k \leq \ell$.
Assume that $k > \ell$. As p is odd we have $3^s \leq \ell < k \leq 2s$, which is not true for $s \geq 1$.

When $p = 2$ we can show in an analogous way as in (4.20) that $G(2^k, 4a) = 4G(2^{k-2}, a)$ for $k \geq 2$. We could freely omit to consider the smaller powers of 2 since they contribute small constants to the upper bound we try to show. Also, if $2 \nmid \Delta$, then again $G(2^{k-2}, a) = S(2^{k-2}, a)$. So further regard $2 \mid \Delta$. Like in (4.22), if $k - 2 \leq \ell$ the estimate follows. Assume the contrary – then $2^{s-2} \leq \ell < k - 2 \leq 2s - 2$ which holds only for $s \leq 4$. But this gives $k \leq 8$ – again these contribute only constant to the whole estimate of $G(q, 4a)$. This proves the Lemma. □

Lemma 4.18. *Suppose that $|\beta| \leq 1/2$ and n is a positive integer. Then for*

$$\nu(\beta) = \sum_{m=1}^{n} e(\beta m)$$

we have $\nu(\beta) \ll \min(n, |\beta|^{-1})$.

Proof. This is Lemma 2.8 from [51] when $k = 1$. □

The following is Bombieri's theorem on the large sieve.

Lemma 4.19. *For any complex numbers c_n we have*

$$\sum_{q\le Q}\sum_{(a,q)=1}\left|\sum_{n\le x}c_n e\left(\frac{an}{q}\right)\right|^2 \le (x+Q^2)\sum_{n\le x}|c_n|^2\,.$$

Proof. This is Theorem 2 of §23 in [16]. □

We also recall the following basic facts. The functions bellow are complex-valued $L^2([0,1])$-functions.

Cauchy-Schwartz inequality: For the square-integrable functions f and g we have the inequality

$$\left|\int f(x)\overline{g(x)}dx\right|^2 \le \int |f(x)|^2dx\int |g(x)|^2dx\,.$$

Parseval's identity: For the Fourier transform of $f(x)=\sum_{n=-\infty}^{\infty}c_ne^{inx}$ we have $c_n=\frac{1}{2\pi}\int_{-\pi}^{\pi}f(x)e^{-inx}dx$ and

$$\frac{1}{2\pi}\int_{-\pi}^{\pi}|f(x)|^2dx=\sum_{n=-\infty}^{\infty}|c_n|^2\,.$$

If $f(\alpha)=\sum_{n\le x}c_ne(n\alpha)$, then $f(\alpha)$ is periodic with period 1 and

$$\int_0^1|f(\alpha)|^2d\alpha=\sum_{n\le x}|c_n|^2\,.$$

4.4 The Circle Method

With the conditions from Theorem 4.2 our main aim in this section is to prove the following

Theorem 4.20. *For any $1\le Q\le M^{\min(1/6,\ell/2^{\ell+2})}$ we have*

$$R(x)=\sum_{q\le Q}\sum_{(a,q)=1}\frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta}G(q,-4a)f_1\left(\frac{a}{q}\right)f_2\left(\frac{a}{q}\right)+\mathcal{O}\left(\frac{x^2}{Q^{1/\ell}}\right)\,.$$

Proof. We recall that we search for the number of solutions of (4.1) satisfying conditions (4.2) and

$$p_1 \equiv -5 \pmod{\Delta}, \qquad p_2, p_3 \equiv 3 \pmod{\Delta},$$

so that $p_1 + p_2 p_3 \equiv 4 \pmod 8$ because $16\ell^2 \mid \Delta$. We also use the parameters

$$M = \left(\frac{x}{2}\right)^{1/\ell}, \qquad N = M^{\ell - 1/2} \asymp \frac{x}{M^{1/2}}, \qquad Q \le M^{\min\left(1/6, \ell/2^{(\ell+2)}\right)}. \tag{4.23}$$

By Lemma 4.10 for any real α such that $1/N \le \alpha < 1 + 1/N$ there exists approximation $|\alpha - a/q| < 1/(qN)$ with $1 \le a \le q \le N$ and $(a, q) = 1$. We denote this 'major arc' by

$$\mathfrak{M}(a/q) = \left(\frac{a}{q} - \frac{1}{qN}, \frac{a}{q} + \frac{1}{qN}\right).$$

One easily sees that the major arcs are non-overlapping. Let $q, q' \le M^{1/2}$. Then for $a/q \ne a'/q'$ we have $\mathfrak{M}(a/q) \cap \mathfrak{M}(a'/q') = \emptyset$. This can be seen taking the difference

$$\left|\frac{a}{q} - \frac{a'}{q'}\right| \ge \frac{1}{qq'} > \frac{q + q'}{qq'N} = \frac{1}{qN} + \frac{1}{q'N}.$$

We used that $N = M^{\ell - 1/2} > 2M^{1/2} \ge q + q'$ because $M^{\ell - 1} > 2$ for $\ell \ge 2$ and large enough x. Thus the centers of different major arcs are at a distance larger than the half-lengths of the corresponding intervals. Now we can also define the set of the 'minor arcs'

$$\mathfrak{m} = \left[\frac{1}{N}, 1 + \frac{1}{N}\right) \setminus \bigcup_{q \le M^{1/2}} \bigcup_{(a,q)=1} \mathfrak{M}(a/q).$$

Later we will also need the orthogonality relation

$$\int_0^1 e(\alpha h) d\alpha = \begin{cases} 1 & \text{when } h = 0, \\ 0 & \text{when } h \ne 0. \end{cases} \tag{4.24}$$

As f_1, f_2 and g are periodic functions with period 1, we have

$$\begin{aligned} R(x) &= \int_{1/N}^{1+1/N} f_1(\alpha) f_2(\alpha) g(-4\alpha) d\alpha = \sum_{q \le M^{1/2}} \sum_{(a,q)=1} \int_{\mathfrak{M}(a/q)} f_1(\alpha) f_2(\alpha) g(-4\alpha) d\alpha \\ &+ \int_{\mathfrak{m}} f_1(\alpha) f_2(\alpha) g(-4\alpha) d\alpha. \end{aligned}$$

When α is in $\mathfrak{m}$, it is approximated by a/q where $M^{1/2} < q < N$ and we use Lemma

4.13 to get $g(-4\alpha) \ll M^{\ell-2^{-(\ell+2)}}$. Then

$$\int_{\mathfrak{m}} f_1(\alpha) f_2(\alpha) g(-4\alpha) d\alpha \ll M^{\ell-2^{-(\ell+2)}} \int_{\mathfrak{m}} |f_1(\alpha) f_2(\alpha)| \, d\alpha$$

By Cauchy-Schwarz inequality, Parseval's identity and the fact that in (4.4) and (4.5) $b_n, c_n \leq 2 \ll 1$, we have

$$\begin{aligned} \int_{\mathfrak{m}} |f_1(\alpha) f_2(\alpha)| \, d\alpha &< \int_0^1 |f_1(\alpha) f_2(\alpha)| \, d\alpha < \left(\int_0^1 |f_1(\alpha)|^2 d\alpha \int_0^1 |f_2(\alpha)|^2 d\alpha \right)^{1/2} \\ &= \left(\sum_{n \leq x} |b_n|^2 \sum_{n \leq x} |c_n|^2 \right)^{1/2} \ll (x.x)^{1/2} = x \, . \end{aligned}$$

Thus

$$\int_{\mathfrak{m}} f_1(\alpha) f_2(\alpha) g(-4\alpha) d\alpha \ll M^{\ell-2^{-(\ell+2)}} x = M^{\ell} x . M^{-2^{-(\ell+2)}} \ll \frac{x^2}{M^{2^{-(\ell+2)}}} \, . \tag{4.25}$$

On the 'major arc' $\mathfrak{M}(a/q)$ we use the bound in Lemma 4.12. Note that when $q \leq M^{1/2}$ and $a/q + \eta \in \mathfrak{M}(a/q)$ we have $|\eta| < 1/(qN)$. Then the error term from Lemma 4.12 is $\mathcal{O}(qM^{\ell-1}(1+|\eta|x)) = \mathcal{O}\left(qM^{\ell-1}(1 + M^{\ell}/(qM^{\ell-1/2}))\right) = \mathcal{O}\left(qM^{\ell-1} + M^{\ell-1}M^{1/2}\right) = \mathcal{O}(M^{\ell-1/2})$. Then, by Cauchy-Schwarz inequality and Parseval's identity, for the error term we get

$$\begin{aligned} &\sum_{q \leq M^{1/2}} \sum_{(a,q)=1} \int_{\mathfrak{M}(a/q)} \left| f_1(\frac{a}{q} + \eta) f_2(\frac{a}{q} + \eta) \right| M^{\ell-1} q (1 + |\eta| x) d\eta \\ &\ll M^{\ell-1/2} \int_0^1 |f_1(\alpha) f_2(\alpha)| \, d\alpha \ll M^{\ell-1/2} x \ll \frac{x^2}{M^{1/2}} \, . \end{aligned}$$

The latter error term is smaller than the one in (4.25). Therefore, after Lemma 4.12

$$\begin{aligned} R(x) &= \sum_{q \leq M^{1/2}} \sum_{(a,q)=1} \frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta} G(q,-4a) \int_{-1/qN}^{1/qN} f_1\left(\frac{a}{q} + \eta\right) f_2\left(\frac{a}{q} + \eta\right) V(-4\eta) d\eta \\ &\quad + \mathcal{O}\left(\frac{x^2}{M^{2^{-(\ell+2)}}}\right) \end{aligned}$$

We will use Lemma 4.18: for $|\beta| \leq 1/2$ we have $V(\beta) \ll \min(x, |\beta|^{-1})$. As $|4\eta| \leq 4/qN \leq 1/2$, because $N \asymp x^{1-1/2\ell}$ is greater than 8 for large enough x, we get

$$V(-4\eta) \ll \min(x, |\eta|^{-1}) \, .$$

To estimate the contribution of the terms with $Q < q \le M^{1/2}$ we use the latter inequality and Lemma 4.17:

$$\begin{aligned}
&\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta}G(q,-4a)\int_{-1/qN}^{1/qN} f_1\left(\frac{a}{q}+\eta\right) f_2\left(\frac{a}{q}+\eta\right) V(-4\eta)d\eta\\
\ll\ &\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta}q^{1-1/\ell}\int_{-1/qN}^{1/qN}\left|f_1\left(\frac{a}{q}+\eta\right) f_2\left(\frac{a}{q}+\eta\right) V(-4\eta)\right| d\eta\\
\ll\ & Q^{-1/\ell}\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\int_{-1/2}^{1/2}|\dots|\,d\eta\\
\ll\ & Q^{-1/\ell}\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\left|f_1\left(\frac{a}{q}+\eta\right) f_2\left(\frac{a}{q}+\eta\right)\right| d\eta\\
\ll\ & Q^{-1/\ell}\left(\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\left|f_1\left(\frac{a}{q}+\eta\right)\right|^2 d\eta\right)^{1/2}\cdot\\
&\left(\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})\sum_{Q<q\le M^{1/2}}\sum_{(a,q)=1}\left|f_2\left(\frac{a}{q}+\eta\right)\right|^2 d\eta\right)^{1/2}
\end{aligned}$$

As

$$f_1\left(\frac{a}{q}+\eta\right)=\sum_{n\le x}b_n e(n\eta)e\left(n\frac{a}{q}\right)\qquad\text{and}\qquad f_2\left(\frac{a}{q}+\eta\right)=\sum_{n\le x}c_n e(n\eta)e\left(n\frac{a}{q}\right),$$

when we apply the large sieve for the sum in the upper integrals and use the trivial estimate $\sum_{n\le x}|b_n e(n\eta)|^2 \ll x/\log x$ after (4.10), and $\sum_{n\le x}|c_n e(n\eta)|^2 \ll x/\log x$ after (4.11), we see that the last considered error term is

$$\ll Q^{-1/\ell}\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})(x+M)\frac{x}{\log x}d\eta \ll Q^{-1/\ell}\frac{x^2}{\log x}\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})d\eta\,.$$

The latter integral is $\ll \log x$. Indeed, for $|\eta|^{-1}\ge x$, i.e. $1/x\ge|\eta|$, we have $\min(x,|\eta|^{-1})=x$. So

$$\begin{aligned}
\int_{-1/2}^{1/2}\min(x,|\eta|^{-1})d\eta\ &=\ \int_{-1/x}^{1/x}x d\eta+\int_{-1/2}^{-1/x}\frac{d\eta}{-\eta}+\int_{1/x}^{1/2}\frac{d\eta}{\eta}=x\left(\frac{1}{x}+\frac{1}{x}\right)\\
&+\ 2\int_{1/x}^{1/2}\frac{d\eta}{\eta}=2-2\log 2+2\log x\ll\log x\,.
\end{aligned}$$

Hence the contribution to $R(x)$ of the terms with $Q<q\le M^{1/2}$ is $\mathcal{O}(x^2Q^{-1/\ell})$.

We are left with $q \le Q$. When we extend the range of integration in the corresponding integral from $(-1/qN, 1/qN)$ to $(-1/2, 1/2)$ we get an error term which we estimate by Parseval's identity, Lemma 4.17, and using that $V(-4\eta) \ll |\eta|^{-1} \le qN$ for $1/(qN) \le |\eta| \le 1/2$. The error term in question is

$$\begin{aligned}
&2\sum_{q\le Q}\sum_{(a,q)=1}\frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta}|G(q,-4a)|\int_{1/qN}^{1/2}\left|f_1\left(\frac{a}{q}+\eta\right)f_2\left(\frac{a}{q}+\eta\right)V(-4\eta)\right|d\eta\\
&\ll N\sum_{q\le Q}\sum_{(a,q)=1}q^{1-1/\ell}\int_0^1\left|f_1\left(\frac{a}{q}+\eta\right)f_2\left(\frac{a}{q}+\eta\right)\right|d\eta \ll Nx\sum_{q\le Q}\sum_{(a,q)=1}q^{1-1/\ell}\\
&\ll Nx\sum_{q\le Q}q^{1-1/\ell}.q = Nx\sum_{q\le Q}q^{2-1/\ell} \le NxQ^{2-1/\ell}\sum_{q\le Q}1 \le NxQ^{3-1/\ell}\,.
\end{aligned}$$

Now recall that the parameters satisfy (4.23). It follows that

$$NxQ^{3-1/\ell} \ll x^2M^{-1/2}M^{1/2}Q^{-1/\ell} = x^2Q^{-1/\ell}\,.$$

Until now we got the error terms $\mathcal{O}\left(x^2/M^{2^{-(\ell+2)}}\right)$ and $\mathcal{O}(x^2Q^{-1/\ell})$. After (4.23) $Q \le M^{\ell.2^{-(\ell+2)}}$, so $Q^{-1/\ell} \ge M^{-2^{-(\ell+2)}}$ and the larger error term is $\mathcal{O}(x^2Q^{-1/\ell})$. Collecting all up to now we arrive at

$$R(x) = \sum_{q\le Q}\sum_{(a,q)=1}\frac{(q,\Delta)\varphi(\Delta)}{q\varphi(q,\Delta)\Delta}G(q,-4a)\int_0^1 f_1\left(\frac{a}{q}+\eta\right)f_2\left(\frac{a}{q}+\eta\right)V(-4\eta)d\eta+\mathcal{O}\left(\frac{x^2}{Q^{1/\ell}}\right).$$

The integral, after the orthogonality property, counts $e(p_1\frac{a}{q})e(p_2p_3\frac{a}{q})$ exactly when $p_1 + p_2p_3 = 4n \le 2x$, thus its value is exactly $f_1(a/q)f_2(a/q)$ and this proves the theorem. □

Further we need to compute $f_1(a/q)$ and $f_2(a/q)$. For $q \le Q$ we write $q = dq'$, where d is composed only from primes dividing Δ and $(q', \Delta) = 1$. If $p^k \mid d$ but $p^k \nmid \Delta$, then from $16\ell^2 \mid \Delta$ and $s = \mathrm{ord}_p(4\ell)$ we have $k \ge 2s + 1$. Clearly there is no $p \mid d$ such that $p \nmid \Delta$, so $k \ge 2$. Thus $k \ge \max(2, 2s + 1)$ and after Lemma 4.16 we get $G(p^k, 4a) = 0$. Combining this with Lemma 4.14, and (4.21), we get $G(q, 4a) = 0$ unless $d \mid \Delta$.

Recall that $p_1 \equiv -5 \pmod{\Delta}$ and $p_2p_3 \equiv 9 \pmod{\Delta}$. Let us write $r_1 \equiv -5 \pmod{\Delta}$ and $r_2 \equiv 9 \pmod{\Delta}$. If $d \mid \Delta$ we have

$$f_1\left(\frac{a}{q}\right) = \sum_{x^{1/8}<p_1\le x}e\left(p_1\frac{a}{q}\right) = \sum_{(b,q)=1}e\left(b\frac{a}{q}\right)\sum_{\substack{x^{1/8}<p_1\le x\\ p_1\equiv b(q)}}1 = \sum_{\substack{(b,q)=1\\ b\equiv r_1(d)}}e\left(b\frac{a}{q}\right)\sum_{\substack{x^{1/8}<p_1\le x\\ p_1\equiv b(q')}}1$$

and

$$f_2\left(\frac{a}{q}\right)=\sum_{n\le x}c_n e\left(n\frac{a}{q}\right)=\sum_{(b,q)=1}e\left(b\frac{a}{q}\right)\sum_{\substack{n\le x\\ n\equiv\overline{b}(q)}}c_n=\sum_{\substack{(b,q)=1\\ b\equiv r_2(d)}}e\left(b\frac{a}{q}\right)\sum_{\substack{n\le x\\ n\equiv\overline{b}(q')}}c_n$$

because $c_n=0$ unless $n=p_2p_3\equiv 3^2\equiv r_2 \pmod{\Delta}$. Also in the two functions always $(b,q)=1$, as $x^{1/8}<p_1,p_2,p_3$ and $q\le Q\le M^{\frac{\ell}{2^{\ell+2}}}<x^{1/2^{\ell+2}}<x^{1/8}$ for $\ell\ge 2$. Thus $(p_1,q)=1$ and $n=p_2p_3$ is composed by primes larger than q and $(n,q)=1$.

Similarly to (4.9) we see that

$$\sum_{\substack{x^{1/8}<p_1\le x\\ p_1\equiv\overline{b}(q')}}1=\frac{1}{\varphi(q')}\sum_{x^{1/8}<p_1\le x}1+\mathcal{O}\left(\frac{x}{\log^C x}\right)=\frac{1}{\varphi(q')}f_1(0)+\mathcal{O}\left(\frac{x}{\log^C x}\right).$$

The analogous sum, again by (4.9), is

$$\sum_{\substack{n\le x\\ n\equiv\overline{b}(q')}}c_n=\sum_{p_2}\sum_{\substack{x^{1/4}<p_3\le x/p_2\\ p_3\equiv\overline{b/p_2}(q')}}1=\frac{1}{\varphi(q')}\sum_{p_2}\sum_{p_3}1+\mathcal{O}\left(\frac{x}{\log^C x}\right)=\frac{1}{\varphi(q')}f_2(0)+\mathcal{O}\left(\frac{x}{\log^C x}\right).$$

Here we again used that $\sum_{x^{1/8}<p_2\le x^{1/4}}\frac{1}{p_2}\ll 1$ as was shown in the proof of Lemma 4.5. The latter estimates with $f_i(0)$ are uniform in b and the main term is independent on b. Thus for $i=1,2$ we can write

$$f_i\left(\frac{a}{q}\right)=\frac{1}{\varphi(q')}f_i(0)\sum_{\substack{(b,q)=1\\ b\equiv r_i(d)}}e\left(\frac{ab}{q}\right)+\mathcal{O}\left(\frac{q'x}{\log^C x}\right). \tag{4.26}$$

Each b in the sum above can be written as $b=r_iq'\overline{q'}+b'd$, where $(b',q')=1$ and $q'\overline{q'}\equiv 1 \pmod{d}$. Also recall that for the Ramanujan sum for any positive integer q we have (Theorem 272 [23])

$$\sum_{(b,q)=1}e\left(\frac{ab}{q}\right)=\varphi(q)\frac{\mu(q/(a,q))}{\varphi(q/(a,q))}.$$

Then, since $(a,q)=(a,q')=1$, we have

$$\begin{aligned}\sum_{\substack{(b,q)=1\\ b\equiv r_i(d)}} e\left(\frac{ab}{q}\right) &= \sum_{(b',q')=1} e\left(\frac{a(r_iq'\overline{q'}+b'd)}{q}\right) = e\left(\frac{ar_i\overline{q'}}{d}\right)\sum_{(b',q')=1} e\left(\frac{ab'}{q'}\right)\\ &= e\left(\frac{ar_i\overline{q'}}{d}\right)\varphi(q')\frac{\mu(q'/(a,q'))}{\varphi(q'/(a,q'))} = \mu(q')e\left(\frac{ar_i\overline{q'}}{d}\right).\end{aligned}$$

Recall also Theorem 327 [23] stating that for every positive δ we have $\varphi(n)/n^{1-\delta}\to\infty$. Thus $n/\varphi(n)<n^{\delta}$ for large enough n.

Let us take $Q\le \log^{C/2}x$. Then for $q\le Q$ we have $q/\varphi(q)\ll\log x$ and when we multiply $f_1(a/q)$ with $f_2(a/q)$ from (4.26) the error terms are

$$\mathcal{O}\left(\frac{f_i(0)}{\varphi(q')}.\frac{q'x}{\log^C x}\right)=\mathcal{O}\left(\frac{x}{\log x}\log x\frac{x}{\log^C x}\right)=\mathcal{O}\left(\frac{x^2}{\log^C x}\right)$$

and

$$\mathcal{O}\left(\frac{q'x}{\log^C x}\right)^2=\mathcal{O}\left(\frac{x\log^{C/2}x}{\log^C x}\right)^2=\mathcal{O}\left(\frac{x^2}{\log^C x}\right).$$

Also note that $r_1+r_2\equiv -5+9\equiv 4 \pmod{\Delta}$, thus

$$f_1\left(\frac{a}{q}\right)f_2\left(\frac{a}{q}\right)=\frac{\mu(q')^2}{\varphi(q')^2}e\left(\frac{4a\overline{q'}}{d}\right)f_1(0)f_2(0)+\mathcal{O}\left(\frac{x^2}{\log^C x}\right).$$

Then Theorem 4.20 transforms into

$$\begin{aligned}R(x) &= f_1(0)f_2(0)\frac{\varphi(\Delta)}{\Delta}\sum_{d|\Delta}\sum_{\substack{q'\le Q/d\\(q',\Delta)=1}}\frac{\mu(q')^2(q',\Delta)}{q'\varphi(q')^2\varphi(d)\varphi(q',\Delta)}\sum_{(a,dq')=1}G(dq',-4a)e\left(\frac{4a\overline{q'}}{d}\right)\\ &+ \mathcal{O}\left(\frac{x^2}{Q^{1/\ell}}\right)+\mathcal{O}\left(\frac{x^2Q^{2-1/\ell}}{\log^C x}\right).\end{aligned}$$

The last error term comes from

$$\sum_{q\le Q}\sum_{(a,q)=1}\frac{1}{q}G(q,-4a)\ll\sum_{q\le Q}\sum_{(a,q)=1}\frac{q^{1-1/\ell}}{q}\ll\sum_{q\le Q}q.q^{-1/\ell}\le Q.Q^{1-1/\ell}.$$

Of course $(q', \Delta) = 1$. At this stage we also take $Q = \log^{3\ell} x$ with $C = 6\ell$. Then

$$\frac{x^2 Q^{2-1/\ell}}{\log^C x} = \frac{x^2 (\log^{3\ell} x)^{2-1/\ell}}{\log^{6\ell} x} = \frac{x^2}{\log^3 x}$$

and

$$R(x) = f_1(0) f_2(0) \frac{\varphi(\Delta)}{\Delta} \sum_{d|\Delta} \sum_{\substack{q' \le Q/d \\ (q', \Delta)=1}} \frac{\mu(q')^2}{q' \varphi(q')^2 \varphi(d)} \sum_{(a, dq')=1} G(dq', -4a) e\left(\frac{4a\overline{q'}}{d}\right) + \mathcal{O}\left(\frac{x^2}{\log^3 x}\right) \tag{4.27}$$

In order to examine further the asymptotic formula for $R(x)$ we need to investigate the innermost sum in (4.27). Let us introduce a notation for it:

$$\varkappa(q) = \begin{cases} \sum_{(a,q)=1} G(q, -4a) e\left(\frac{4a\overline{q'}}{d}\right) & \text{for } q = dq' \,, (q', \Delta) = 1 \,, \mu(q')^2 = 1 \,, \text{and } d \mid \Delta \,, \\ 0 & \text{otherwise} \,. \end{cases}$$

4.5 The Sum $\varkappa(q)$

We can easily check that $\varkappa(q)$ is a multiplicative function using Chinese remainder theorem. In particular, $\varkappa(q'd) = \varkappa(q')\varkappa(d)$. Observe that because of the factor $\mu(q')^2$ in (4.27) we will have a contribution of 0 always when $q' \nmid \Delta$ and q' is not square-free. Thus for every $p \nmid \Delta$ we need to compute only $\varkappa(p)$, and for every $p^k \mid \Delta$ we will look at $\varkappa(p^k)$.

$\underline{p \nmid \Delta}$ Here p should be odd and

$$\begin{aligned} \varkappa(p) &= \sum_{(a,p)=1} G(p, -4a) e\left(4a\overline{p}/1\right) = \sum_{(a,p)=1} \sum_{\substack{u(p) \\ (u,p,\Delta)=1}} e\left(\frac{-4au^\ell}{p}\right) \\ &= \sum_{\substack{u(p) \\ (u,(p,\Delta))=1}} \sum_{(a,p)=1} e\left(\frac{-4au^\ell}{p}\right) = \sum_{u(p)} \sum_{(a,p)=1} e\left(\frac{-4au^\ell}{p}\right) \\ &= \sum_{(u,p)=1} \sum_{(a,p)=1} e\left(\frac{-4au^\ell}{p}\right) + \sum_{(a,p)=1} e\left(-4ap^{\ell-1}\right) \\ &= \sum_{(u,p)=1} (-1) + \varphi(p) = -\varphi(p) + \varphi(p) = 0 \,. \end{aligned}$$

But then in (4.27) we actually have only $q' = 1$ and

$$R(x) = f_1(0)f_2(0)\frac{\varphi(\Delta)}{\Delta}\sum_{d|\Delta}\frac{\varkappa(d)}{\varphi(d)} + \mathcal{O}\left(\frac{x^2}{\log^3 x}\right). \tag{4.28}$$

When $d \mid \Delta$ we have

$$\begin{aligned}\varkappa(d) &= \sum_{(a,d)=1}\sum_{\substack{u(d)\\(u,d,\Delta)=1}} e\left(\frac{-4au^\ell}{d}\right)e\left(\frac{4a}{d}\right) = \sum_{(a,d)=1}\sum_{(u,d)=1} e\left(\frac{-4au^\ell}{d}\right)e\left(\frac{4a}{d}\right)\\ &= \sum_{(a,d)=1}\sum_{(u,d)=1} e\left(\frac{-4a(u^\ell-1)}{d}\right)\end{aligned}$$

We introduce the notation

$$\rho(p^k) = \#\{u(p^k):\ u^\ell \equiv 1 \pmod{p^k}\}.$$

We have the following

Lemma 4.21.

$$\rho(p^k) = (\ell, p-1)(\ell, p^{k-1}) \ \textit{if}\ \ p \neq 2,$$
$$\rho(2^k) = \begin{cases} 1 & \textit{if}\ \ 2 \nmid \ell \\ (2\ell, 2^{k-1}) & \textit{if}\ \ 2 \mid \ell. \end{cases}$$

Proof. See the discussion before Lemma 2.13 in §2.6, [51]. □

<u>$p \mid \Delta, p \neq 2$</u>

$$\begin{aligned}\sum_{(a,p)=1}\sum_{(u,p)=1} e\left(\frac{-4a(u^\ell-1)}{p}\right) &= \sum_{\substack{(u,p)=1\\u^\ell\equiv 1(p)}}\sum_{(a,p)=1} e\left(\frac{-4a(u^\ell-1)}{p}\right)\\ &\quad + \sum_{\substack{(u,p)=1\\u^\ell\not\equiv 1(p)}}\sum_{(a,p)=1} e\left(\frac{-4a(u^\ell-1)}{p}\right)\\ = \rho(p)\varphi(p) + (p-1-\rho(p))(-1) &= \rho(p)(p-1) - (p-1) + \rho(p) = p(\ell, p-1) - (p-1)\end{aligned}$$

or

$$\varkappa(p) = p(\ell, p-1) - (p-1). \tag{4.29}$$

$\underline{p^k \mid \Delta\,, k \geq 2\,, p \nmid 2\ell}$ If $p \nmid 2\ell$, we have $\mathrm{ord}_p(4\ell) = s = 0$ and, as $k \geq 2$, from Lemma 4.16 it follows that $G(p^k, -4a) = 0$. Thus

$$\varkappa(p^k) = 0\,. \tag{4.30}$$

So further we assume that $s \geq 1$:

$\underline{p^k \mid \Delta\,, k \geq 2\,, p \mid \ell\,, p \neq 2}$ Here we have

$$\begin{aligned}\varkappa(p^k) &= \sum_{(u,p^k)=1}\sum_{(a,p^k)=1} e\left(\frac{-4a(u^\ell-1)}{p^k}\right) = \sum_{\substack{(u,p^k)=1\\ u^\ell\equiv 1(p^k)}} \ldots + \sum_{\substack{(u,p^k)=1\\ u^\ell\not\equiv 1(p^k)}} \ldots \\ &= \rho(p^k)\varphi(p^k) + \sum_{n=0}^{k-1}\sum_{\substack{(u,p^k)=1\\ p^n\| u^\ell-1}}\sum_{(a,p^k)=1} e\left(\frac{-4a(u^\ell-1)}{p^k}\right).\end{aligned}$$

Obviously $4(u^\ell-1) = Up^n$ with some $p \nmid U$, and the inner sum becomes p^n copies of the Ramanujan sum regarding p^{k-n}(,i.e. $p^n\mu(p^{k-n})$). Therefore, as $\mu(p^{k-n}) = 0$ for $n \leq k-2$ and $\mu(p) = -1$, we have

$$\begin{aligned}\varkappa(p^k) &= \rho(p^k)\varphi(p^k) + \sum_{n=0}^{k-1}\sum_{\substack{(u,p^k)=1\\ p^n\| u^\ell-1}} p^n\mu(p^{k-n}) = \rho(p^k)\varphi(p^k) - p^{k-1}\sum_{\substack{(u,p^k)=1\\ p^{k-1}\| u^\ell-1}} 1 \\ &= \rho(p^k)\varphi(p^k) - p^{k-1}\left(p\rho(p^{k-1}) - \rho(p^k)\right) = \rho(p^k)p^{k-1}(p-1) - p^k\rho(p^{k-1}) \\ &\quad + p^{k-1}\rho(p^k) = p^k(\rho(p^k) - \rho(p^{k-1}))\,.\end{aligned}$$

After Lemma 4.21 in our case we have $\rho(p^k) = (\ell, p-1)(\ell, p^{k-1})$ and

$$\varkappa(p^k) = p^k(\ell, p-1)\left((\ell, p^{k-1}) - (\ell, p^{k-2})\right)\,.$$

Regard the case $2 \leq k \leq s+1$. Then $1 \leq k-1 \leq s = \mathrm{ord}_p(4\ell)$ and as $p \neq 2$, we have $(\ell, p^{k-1}) = p^{k-1}$ and $(\ell, p^{k-2}) = p^{k-2}$. If $k \geq s+2$, then $k-2 \geq s$ and $(\ell, p^{k-2}) = (\ell, p^{k-1}) = p^s$. We combine the results in the considered case:

$$\varkappa(p^k) = \begin{cases} (\ell, p-1)(p^{2k-1} - p^{2k-2}) & \text{if } 2 \leq k \leq s+1\,, \\ 0 & \text{if } k \geq s+2\,. \end{cases} \tag{4.31}$$

$\underline{p=2}$ We will show that

$$\varkappa(2^k) = \begin{cases} 1 & \text{if } k = 1\,, \\ 4 & \text{if } k = 2\,, \\ 16 & \text{if } k = 3\,, \\ 2^{2k-2} & \text{if } 4 \le k \le s+2 \text{ and } 2 \mid \ell, \\ 0 & \text{otherwise}\,, \end{cases} \tag{4.32}$$

where 'otherwise' means either $k \ge 4$ and $2 \nmid \ell$, or $k \ge s+3$ and $2 \mid \ell$.

Clearly

$$\varkappa(2) = \sum_{(u,2)=1} \sum_{(a,2)=1} e\left(\frac{-4a(u^\ell-1)}{2}\right) = e(2.1.(1-1)) = 1\,.$$

Similarly

$$\varkappa(4) = \sum_{(u,4)=1} \sum_{(a,4)=1} e\left(\frac{-4a(u^\ell-1)}{4}\right) = 2.2 = 4$$

and

$$\varkappa(8) = \sum_{(u,8)=1} \sum_{(a,8)=1} e\left(\frac{-4a(u^\ell-1)}{8}\right) = \sum_{(u,8)=1} \sum_{(a,8)=1} e\left(\frac{-a(u^\ell-1)}{2}\right) = 4.4 = 16\,.$$

For $k \ge 4$

$$\begin{aligned} \varkappa(2^k) &= \sum_{(u,2^k)=1} \sum_{(a,2^k)=1} e\left(\frac{-4a(u^\ell-1)}{2^k}\right) = \sum_{(u,2^k)=1} \sum_{(a,2^k)=1} e\left(\frac{-a(u^\ell-1)}{2^{k-2}}\right) \\ &= \sum_{\substack{(u,2^k)=1 \\ u^\ell \equiv 1 (2^{k-2})}} \dots + \sum_{\substack{(u,2^k)=1 \\ u^\ell \not\equiv 1 (2^{k-2})}} \dots \\ &= 2^2\rho(2^{k-2})\varphi(2^k) + \sum_{n=0}^{k-3} \sum_{\substack{(u,2^k)=1 \\ 2^n \| u^\ell - 1}} \sum_{(a,2^k)=1} e\left(\frac{a(u^\ell-1)}{2^{k-2}}\right) \\ &= 4\rho(2^{k-2})\varphi(2^k) + \sum_{n=0}^{k-3} \sum_{\substack{(u,2^k)=1 \\ 2^n \| u^\ell - 1}} 2^{n+2}\mu(2^{k-2-n}) = 4\rho(2^{k-2})\varphi(2^k) - 2^{k-1} \sum_{\substack{(u,2^k)=1 \\ 2^{k-3} \| u^\ell - 1}} 1 \\ &= 4\rho(2^{k-2})\varphi(2^k) - 2^{k-1}\left(2^3\rho(2^{k-3}) - 2^2\rho(2^{k-2})\right)\,. \end{aligned}$$

According to Lemma 4.21 $\rho(2^k) = 1$ if $2 \nmid \ell$, so in this case $\varkappa(2^k) = 4\varphi(2^k) - 2^{k-1}(8-4) = 4.2^{k-1} - 2^{k-1}.4 = 0$.

If 2 divides ℓ we have $\rho(2^k) = (2\ell, 2^{k-1})$,so $\varkappa(2^k) = 4(2\ell, 2^{k-3}).2^{k-1} - 2^{k-1}\big(2^3(2\ell, 2^{k-4}) - 2^2(2\ell, 2^{k-3})\big)$. If $k - 3 \leq s - 1$, then $(2\ell, 2^{k-3}) = 2^{k-3}$ because $2^{s-1} \mid 2\ell$ and $2^{k-3} \mid 2^{s-1}$. Similarly $(2\ell, 2^{k-4}) = 2^{k-4}$. Then $\varkappa(2^k) = 4.2^{k-3}.2^{k-1} - 2^{k-1}(2^3.2^{k-4} - 2^2.2^{k-3}) = 2^{2k-2}$.

If $k - 3 > s - 1$, then also $k - 4 \geq s - 1$ and $(2\ell, 2^{k-3}) = (2\ell, 2^{k-4}) = 2^{s-1}$. Then

$$\varkappa(2^k) = 2^2.2^{s-1}.2^{k-1} - 2^{k-1}(2^3.2^{s-1} - 2^2.2^{s-1}) = 0,$$

and finally this proves (4.32).

4.6 Proof of Theorem 4.2

Here we complete the proof of the main theorem. We need to compute the sum in (4.28). Let us use the shorter notation

$$\kappa = \sum_{d|\Delta} \frac{\varkappa(d)}{\varphi(d)}\,.$$

We only have to combine the results of (4.29), (4.30), (4.31) and (4.32). We get

$$\kappa = \prod_{\substack{p|\Delta \\ p\nmid 2\ell}} \left(1 + \frac{\varkappa(p)}{\varphi(p)}\right) \prod_{p|2\ell} \left(1 + \frac{\varkappa(p)}{\varphi(p)} + \frac{\varkappa(p^2)}{\varphi(p^2)} + \dots\right)\,.$$

The first product equals

$$\prod_{\substack{p|\Delta \\ p\nmid 2\ell}} \left(1 + \frac{p(\ell, p-1) - \varphi(p)}{\varphi(p)}\right) = \prod_{\substack{p|\Delta \\ p\nmid 2\ell}} \frac{p}{\varphi(p)}(\ell, p-1)\,.$$

According to the cases considered in §4.5 we split the other product into two factors

$$\prod_{p|2\ell} = \prod_{\substack{p|2\ell \\ p\neq 2}} \cdot \prod_{p=2} =: \Pi_1\Pi_2\,.$$

For the first factor we have

$$\begin{aligned}
\Pi_1 &= \prod_{\substack{p|2\ell\\ p\neq 2}} \left(1+\frac{p(\ell,p-1)-\varphi(p)}{\varphi(p)}+\sum_{k=2}^{s+1}\frac{(\ell,p-1)(p^{2k-1}-p^{2k-2})}{\varphi(p^k)}\right)\\
&= \prod_{\substack{p|2\ell\\ p\neq 2}} \left(\frac{p}{\varphi(p)}(\ell,p-1)+(\ell,p-1)\sum_{k=2}^{s+1}\frac{p^{2k-2}(p-1)}{p^{k-1}(p-1)}\right)\\
&= \prod_{\substack{p|2\ell\\ p\neq 2}} (\ell,p-1)\left(\frac{p}{\varphi(p)}+\sum_{k=2}^{s+1}p^{k-1}\right)\\
&= \prod_{\substack{p|2\ell\\ p\neq 2}} (\ell,p-1)\left(\frac{p}{\varphi(p)}+p\frac{p^s-1}{p-1}\right)=\prod_{\substack{p|2\ell\\ p\neq 2}} (\ell,p-1)\left(\frac{p}{\varphi(p)}+\frac{p}{\varphi(p)}(p^s-1)\right)\\
&= \prod_{\substack{p|2\ell\\ p\neq 2}} (\ell,p-1)\frac{p}{\varphi(p)}p^s
\end{aligned}$$

For $p=2$ and $2\nmid \ell$ the factor Π_2 is of the form $1+1/\varphi(2)+4/\varphi(2^2)+16/\varphi(2^3)=1+1+2+4=8$. For $2\mid\ell$ we have the factor

$$\begin{aligned}
\Pi_2 &= 1+1+2+4+\sum_{k=4}^{s+2}\frac{2^{2k-2}}{\varphi(2^k)}=8+\sum_{k=4}^{s+2}2^{k-1}\\
&= 8+8\sum_{k=4}^{s+2}2^{k-4}=8+8(2^{s-1}-1)=4.2^s
\end{aligned}$$

Notice that in any case we have

$$\Pi_2=\frac{2}{\varphi(2)}(2,\ell)2^s\,,$$

because for $(2,\ell)=1$ we have $s=ord_2(4\ell)=2$ and $2^s=4$. Putting all these together we arrive at

$$\kappa=\frac{2}{\varphi(2)}(2,\ell)2^s\prod_{\substack{p|\Delta\\ p\nmid 2\ell}}\frac{p}{\varphi(p)}(\ell,p-1)\prod_{\substack{p|2\ell\\ p\neq 2}}\frac{p}{\varphi(p)}(\ell,p-1)p^s=4\ell(2,\ell)\prod_{p|\Delta}\frac{p}{\varphi(p)}(\ell,p-1)\,.$$

Note that $\varphi(\Delta)/\Delta=\prod_{p|\Delta}\varphi(p)/p$ because for any $k\geq 2$ we have $\varphi(p^k)/p^k=p^{k-1}\varphi(p)/p^k=\varphi(p)/p$. That is why when we substitute the expression for κ we achieved

above into (4.28), we get

$$\begin{aligned} R(x) &= f_1(0)f_2(0)\frac{\varphi(\Delta)}{\Delta}4\ell(2,\ell)\prod_{p|\Delta}\frac{p}{\varphi(p)}(\ell,p-1)+\mathcal{O}\left(\frac{x^2}{\log^3 x}\right) \\ &= 4\ell(2,\ell)\prod_{p|\Delta}(\ell,p-1)f_1(0)f_2(0)+\mathcal{O}\left(\frac{x^2}{\log^3 x}\right). \end{aligned}$$

This completes the proof of Theorem 4.2.

Remark 4.22. In [2] the archetype of Theorem 4.2 originally was proven for primes from *Siegel-Walfisz sets* and for a different additive problem. Let $\mathcal{P}$ be an infinite set of primes and q and b be coprime integers so that $\mathcal{P}(x,q,b)$ denotes the number of primes $p\in\mathcal{P}$ with $p\le x$ and $p\equiv b \pmod q$. We say that $\mathcal{P}$ satisfies *Siegel-Walfisz condition for an integer* Δ if for any fixed integer $C>0$

$$\mathcal{P}(x,q,b)=\frac{\gamma}{\varphi(q)}\pi(x)+\mathcal{O}(\frac{x}{\log^C x}) \tag{4.33}$$

uniformly for all $(q,\Delta)=1$ and all b coprime to q. Here $\pi(x)\sim x/\log x$ is the usual prime counting function and $0<\gamma\le 1$ is the density of the primes in $\mathcal{P}$.

The notion of Siegel-Walfisz condition in [2] comes from dealing with conjugacy classes in the Galois group of a number field. The primes whose Frobenius automorphism is in a given conjugacy class correspond to the same residue class modulo a certain Δ. After Chebotarev's density theorem these primes satisfy the Siegel-Walfisz' condition. Further notice that all primes in an arithmetic progression satisfy Siegel-Walfisz theorem (Corollary 5.29 [31]), so a Siegel-Walfisz set could be the set of all primes, but also it could be much smaller. The lower theorem assures that the additive problem (4.1) with primes from Siegel-Walfisz sets has still infinitely many solutions with the same asymptotic formula. The proof of the theorem is identical to the one of Theorem 4.2 and comes from the fact that the corresponding functions $f_1(0)$ and $f_2(0)$ also satisfy (4.10) and (4.11).

Theorem 4.23. *Suppose that Δ,ℓ are positive integers for which $16\ell^2\mid\Delta$ and $(15,\Delta)=1$. Let $\mathcal{P}_1,\mathcal{P}_2$ be infinite sets of primes satisfying Siegel-Walfisz condition for Δ such that for every $p\in\mathcal{P}_1$ we have $p\equiv -5 \pmod\Delta$ and for every $r\in\mathcal{P}_2$ we have $r\equiv 3 \pmod\Delta$. If p_1,p_2,p_3 satisfy the additive problem (4.1) with the conditions (4.2) and in addition*

$p_1 \in \mathcal{P}_1,\ p_2, p_3 \in \mathcal{P}_2,$ *we have*

$$R(x) = 4\ell(2,\ell)\prod_{p|\Delta}(\ell, p-1)f_1(0)f_2(0) + \mathcal{O}\left(\frac{x^2}{\log^3 x}\right).$$

Chapter 5

Effective Lower Bound for the Class Number of a Certain Family of Real Quadratic Fields

5.1 Introduction

In this chapter we give a lower bound for the class number of the real quadratic fields of Yokoi type $d = n^2 + 4$ where n is a certain third degree polynomial. This is a special case of the extensively examined Richaud–Degert discriminants with $a = 1$. There are already lower bounds for the class number of R-D fields described in [41]. They however depend on the number of divisors of n at least. We present an analytic lower bound depending on the discriminant and since Goldfeld's theorem and Gross–Zagier formula are applied the bound will be of the magnitude these theorems could provide, i.e. $(\log d)^{1-\epsilon}$. Note that the expected growth (1.2) is much faster, unfortunately it is ineffective. Our result is also interesting bearing in mind that there is still no effective solution of the class number two problem for discriminants $d = n^2 + 4$.

We consider elliptic curves over the field of rational numbers given by the Weierstrass equation

$$E \ : \ y^2 = x^3 + Ax + B \tag{5.1}$$

with a discriminant $\Delta = -16(4A^3 + 27B^2) \neq 0$ and a conductor N. We denote the group of rational points with the usual $E(\mathbb{Q})$. If E is regarded over any other field or ring K the group of the rational points on E over K is denoted by $E(K)$. By a quadratic twist of the

elliptic curve we understand the curve

$$E^D \ : \ Dy^2 = x^3 + Ax + B\,. \tag{5.2}$$

After replacing (x, y) by $(x/D, y/D^2)$ we get the Weierstrass equation of the twisted elliptic curve

$$E^{D,W} \ : \ y^2 = x^3 + (AD^2)x + (BD^3) \tag{5.3}$$

with a discriminant $\Delta_D = D^6\Delta$. Note that $(x_0, y_0) \in E^D(\mathbb{Q})$ if and only if $(Dx_0, D^2y_0) \in E^{D,W}(\mathbb{Q})$.

The main result of Goldfeld from 1976 is

Theorem (Goldfeld [18]). *Let E be an elliptic curve over $\mathbb{Q}$ with conductor N. If E has complex multiplication and the L-function associated to E has a zero of order g at $s = 1$, then for any real primitive Dirichlet character $\chi \pmod d$ with $(d, N) = 1$ and $d > \exp\exp(c_1 N g^3)$, we have*

$$L(1, \chi) > \frac{c_2}{g^{4g} N^{13}} \frac{(\log d)^{g-\mu-1} \exp\left(-21 g^{1/2} (\log\log d)^{1/2}\right)}{\sqrt{d}}\,,$$

where $\mu = 1$ or 2 is suitably chosen so that $\chi(-N) = (-1)^{g-\mu}$, and the constants $c_1, c_2 > 0$ can be effectively computed and are independent of $g\,, N$ and d.

If the condition $(d, N) = 1$ is dropped, then the upper theorem still holds. In this case, however, the relation $\chi(-N) = (-1)^{g-\mu}$ will have to be replaced by a more complicated one. In our argument we will consider only coprime d and N.

Denote as usual by $h(d)$ the class number of the real quadratic field $\mathbb{Q}(\sqrt{d})$ for the positive fundamental discriminant d. When we plug Dirichlet class number formula (1.1) in the above estimate for $L(1, \chi)$ we get an inequality of the type

$$h(d) \log \epsilon_d \gg (\log d)^{g-\mu-1} e^{-21\sqrt{g(\log\log d)}}\,,$$

where ϵ_d denotes the fundamental unit of $\mathbb{Q}(\sqrt{d})$. Also the exponent on the right-hand side of the upper inequality is greater than $(\log d)^{-\epsilon}$ for any $\epsilon > 0$ and big enough d. Note that if $g \leq 3$ the theorem in this form gives a trivial estimate on the class number for $d > 0$ because $\log \epsilon_d \gg \log d$.

The method of Goldfeld however allows to consider the analytic rank of an elliptic curve over quadratic field (the function $\varphi(s)$ defined in [18] has a zero of high order at $s = 1/2$). This way we aim simultaneously toward high order zero of the L-function of E over $\mathbb{Q}$ and of the twisted L-function by the corresponding real quadratic character. The requirement for complex multiplication of E comes from the level of knowledge on Taniyama–Shimura–Weil conjecture at the time of Goldfeld's work. It was known that the L-function of elliptic curves with complex multiplication equals a certain Hecke L-function with "Größencharakter", thus satisfying a functional equation required for the argument. As Goldfeld himself remarks on p.624 after Theorem 1 [18], a modular elliptic curve would do the work for the proof just the same. In the light of the Modularity theorem from 2001 (Wiles, Taylor et al. [8], [50], [54]) every elliptic curve over $\mathbb{Q}$ is *modular* (this term and the Modularity theorem will be discussed in a greater detail in the next section). Thus we can omit the original condition on complex multiplication of the elliptic curve in Goldfeld's theorem. The theorem can be reformulated as in [19] where the real quadratic case is explained in the remarks following Theorem 1 [19].

Theorem 5.1 (Goldfeld). *Let d be a fundamental discriminant of a real quadratic field. If there exists an elliptic curve E over $\mathbb{Q}$ whose associated base change Hasse-Weil L-function*

$$L_{E/\mathbb{Q}(\sqrt{d})}(s) = L(E,s)L(E^d,s)$$

has a zero of order $g \geq 5$ at $s = 1$, then for every $\epsilon > 0$ there exists an effective computable constant $c_\epsilon(E) > 0$, depending only on ϵ and E, such that

$$h(d)\log\epsilon_d > c_\epsilon(E)(\log d)^{2-\epsilon}\,.$$

Let us look at Yokoi's discriminants $d = n^2 + 4$. In that case the fundamental unit is small, i.e.

$$\log d \ll \log\epsilon_d \ll \log d\,.$$

If we use this fact and we can find an elliptic curve as in Theorem 5.1 we could obtain an effective lower bound of the type

$$h(d) > c_\epsilon(E)(\log d)^{1-\epsilon}\,.$$

The question whether Goldfelds's theorem can be used for a possible extension of the class number problem for Yokoi's discriminants solved in [4] was raised by Biró in [6]. Unfortunately we can assure existence of such elliptic curve only for a small subset of

$d = n^2 + 4$. More precisely, the main result of this chapter is

Theorem 5.2. *Let $n = m(m^2-306)$ for a positive odd integer m, and $N = 2^3 \cdot 3^3 \cdot 103 \cdot 10303$. If $d = n^2 + 4$ is square-free and $\left(\frac{d}{N}\right) = -1$, then for every $\epsilon > 0$ there exists an effective computable constant $c_\epsilon > 0$, depending only on ϵ, such that*

$$h(d) = h(n^2 + 4) > c_\epsilon \left(\log d\right)^{1-\epsilon} .$$

Remark 5.3. We expect that there are infinitely many discriminants d satisfying the assumptions of Theorem 5.2. Let

$$d(x) = x^6 - 612x^4 + 93636x^2 + 4$$

be the polynomial defining the discriminant d for odd positive $x = m$. The polynomial is irreducible in $\mathbb{Z}[x]$ so there are not obvious reasons for it not to be square-free infinitely often. Something more, if we introduce

$$M(X) = \#\{0 < m \leq X \,:\, m \text{ is odd}\,, \mu\left(d(m)\right) \neq 0 \text{ and } \left(\frac{d(m)}{N}\right) = -1\}\,, \tag{5.4}$$

we check numerically that $M(X)/X \approx 0.221$, i.e. the odd positive integers m defining square-free discriminants $d(m)$, which are also quadratic nonresidues modulo N, seem to be of positive density.

A construction similar to the one in the present chapter was already made in [20], where the quadratic twists of E from (5.1) are of the form $D = u.f(u, v)$ for the homogeneous binary polynomial $f(u, v) = u^3 + Au^2v + Bv^3$. In [20] by a 'square-free sieve' argument the authors give a density to a similar quantity as (5.4). However, we are strictly interested in discriminants $d = n^2 + 4 = d(m)$ where $d(m)$ is a polynomial in one variable of degree 6. There exists a lot of literature on estimating square-free, or k-free, polynomials, e.g. [9], [21], [26], [28], [29], [30], but there are no results on one-variable polynomials of degree higher than three.

5.2 Theoretical Background

We remind that the Hasse-Weil L-function associated with the elliptic curve E over $\mathbb{Q}$ given with (5.1) is the series

$$L(E,s) = \prod_{p|\Delta}(1 - t_p p^{-s})^{-1} \prod_{p\nmid\Delta}(1 - t_p p^{-s} + p^{1-2s})^{-1}\,,$$

where

$$t_p = p - N_p$$

and

$$N_p = \#\{(x,y) \pmod p :\ y^2 \equiv x^3 + Ax + B \pmod p\}\,.$$

By the Riemann hypothesis for curves over finite fields one has $|t_p| \le 2\sqrt{p}$ and from this it follows that the series $L(E,s)$ converges absolutely for $\mathrm{Re}(s) > 3/2$.

Introduce the Hecke congruence subgroup

$$\Gamma_0(N) = \left\{ \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \mathbf{SL}(2,\mathbb{Z}) : \gamma \equiv 0 \pmod N \right\},$$

with the usual action on the upper complex half-plane $\mathbb{H}$. Then for the integer k the holomorphic function $f : \mathbb{H} \to \mathbb{C}$ is called a *modular form of weight k and level N* if

$$f\left(\frac{\alpha z + \beta}{\gamma z + \delta}\right) = (\gamma z + \delta)^k f(z),\ \ \forall \begin{pmatrix} \alpha & \beta \\ \gamma & \delta \end{pmatrix} \in \Gamma_0(N)$$

and is holomorphic at all cusps of $\Gamma_0(N)$ (the finite number of intersections of a fundamental domain of $\Gamma_0(N) \setminus \mathbb{H} =: X_0(N)$ with $\mathbb{R} \cup \infty$).

The former Taniyama–Shimura–Weil conjecture, nowadays the Modularity theorem (Theorem 14.6 [31]), states that for every elliptic curve E over the rationals with conductor N there exists a modular form

$$f(z) = \sum_{n=1}^{\infty} \lambda(n) n^{1/2} e(nz)$$

of weight 2 and level N, actually a primitive cusp form, such that

$$L(E, s + 1/2) = L(f, s) = \sum_{n=1}^{\infty} \lambda(n) n^{-s} .$$

It follows that $L(E, s)$ has a holomorphic continuation to the entire complex plane and the completed function $\Lambda(E, s) = (\sqrt{N}/2\pi)^s \Gamma(s) L(E, s)$ satisfies a functional equation $\Lambda(E, s) = \pm\Lambda(E, 2 - s)$. Such elliptic curves are called *modular*, in other words the Modularity theorem asserts that every elliptic curve over the rationals is modular. If we denote by ω the invariant differential form $f(z)dz$ for the congruence group of level N and $z \in X_0(N)$, then the modular parametrization is a non-constant map of Riemann surfaces $\pi : X_0(N) \to E(\mathbb{C})$ induced by the holomorphic function $\pi(z) = \int_z^{\infty} \omega$.

Now, fix $d < 0$ such that $d \equiv r^2 \pmod{4N}$ for some integer $r > 0$, and fix $(a, b, c) \in \mathbb{Z}^3$ and $z \in \mathbb{H}$ satisfying $b^2 - 4ac = d$, $a \equiv 0 \pmod{N}$, $b \equiv r \pmod{2N}$, $az^2 + bz + c = 0$. We call these d's Heegner discriminants. There will be $h(d)$ such points $z_1, z_2, \ldots, z_h$. The Heegner point P_d is defined as the trace

$$P_d = \pi(z_1) + \pi(z_2) + \ldots + \pi(z_h) \in E(\mathbb{Q}(\sqrt{d})) .$$

Note that P'_d depending on $r' \neq r$ could differ from P_d only by a sign and a rational torsion point, so its canonical height is correctly defined.

Gross–Zagier Formula: Gross and Zagier's famous result [22], and Theorem 23.4 [31] for more elementary approach, claims that if E is an elliptic curve over $\mathbb{Q}$ with $L(E, 1) = 0$, then for every Heegner discriminant $d < 0$ satisfying the upper conditions there exists a Heegner point $P_d \in E(\mathbb{Q}(\sqrt{d}))$ such that

$$L'(E, 1) L(E^d, 1) = c_{E,d} \hat{h}(P_d) \tag{5.5}$$

for some real non-zero constant $c_{E,d}$ depending on the elliptic curve E and d. Gross and Zagier give the precise formula for $c_{E,d}$ which, however, we do not need in our argument. Here $\hat{h}$ denotes the canonical height on elliptic curve over a number field (§9.VIII [46]).

We also want to draw attention of a Kolyvagin's result [32]. If for a modular elliptic curve over $\mathbb{Q}$ there is a complex quadratic extension $\mathbb{Q}(\sqrt{d})$ for which the Heegner point P_d is of infinite order, Kolyvagin shows that the Mordell-Weil group $E(\mathbb{Q})$ is finite. Combining

this with Gross–Zagier formula we get

$$L(E,1) \neq 0 \Rightarrow E(\mathbb{Q}) \text{ is finite}\,. \tag{5.6}$$

This is one part of Theorem 1 [33].

5.3 Proof of Theorem 5.2

Recall that for the Hasse-Weil L-function associated to the elliptic curve E we consider a root number $\omega = (-1)^t$, where $\mathrm{ord}_{s=1}L(E,s) = t$. Let ω_D be the root number for E^D. If $(D,N) = 1$ for the conductor N, and $\chi = \chi_D = \left(\frac{D}{\cdot}\right)$ is the real quadratic character of $\mathbb{Q}(\sqrt{D})$, we have $\omega_D = \chi(-N)\omega$ (e.g. (23.48) [31]). The character χ is even, so $\omega_D = \chi(N)\omega$.

Let E be an elliptic curve with $\mathrm{ord}_{s=1}L(E,s) \geq 3$ and $\omega = -1$. Then $\omega_D = -\chi(N)$. If further we require $\chi(N) = -1$ we will have $\omega_D = 1$. If there is a rational point in $E^D(\mathbb{Q})$ that is not a torsion point, then the rank of the Mordell-Weil group $E^D(\mathbb{Q})$ is positive and $E^D(\mathbb{Q})$ is a group of infinite order. After statement (5.6) we have $L(E^D,1) = 0$, i.e. $\mathrm{ord}_{s=1}L(E^D,s) \geq 1$. From $\omega_D = 1$ it will follow that $\mathrm{ord}_{s=1}L(E^D,s) \geq 2$ and the order is even.

We will construct such an elliptic curve for which certain quadratic twists of it satisfy the upper conditions. Then $\mathrm{ord}_{s=1}L(E,s)L(E^D,s) \geq 5$ and this would allow us to apply Theorem 5.1.

From now on $d = n^2+4$ is a square-free odd integer. Look at the twist (5.2) with $y = 1$ and assume that d satisfies the equation

$$d = x_0^3 + Ax_0 + B \tag{5.7}$$

for some $x_0 \in \mathbb{Z}$. Then we have $(x_0, 1) \in E^d(\mathbb{Q})$. The equation (5.7) reads as $n^2 + 4 = x_0^3 + Ax_0 + B$ or $n^2 = x_0^3 + Ax_0 + B - 4$. Let us choose the coefficients A and B in such a way that $g(x) = x^3 + Ax + B - 4 = (x-k)^2(x-l)$ for some integers k and l. This yields $g(k) = g(l) = 0$ and $g'(k) = 0$. Then $g'(k) = 3k^2 + A = 0$, so $A = -3k^2$ and therefore $0 = g(k) = k^3 - 3k^2 \cdot k + B - 4$. Thus $B = 2k^3 + 4$ and finally

$$g(x) = x^3 - 3k^2x + (2k^3+4) - 4 = x^3 - 3k^2x + 2k^3 = (x-k)^2(x+2k)\,.$$

This means that d satisfies (5.7) if and only if

$$n^2 = g(x_0) = (x_0 - k)^2(x_0 + 2k) \tag{5.8}$$

for some integer x_0.

Look at the curve

$$C_k \ : \ y^2 = (x - k)^2(x + 2k)\,.$$

It is well-known/see [46].III.2.5/ that its non-singular points are in one-to-one correspondence with $\mathbb{Q}^*$. What can be easily seen is that if we put $m = y/(x - k)$, we have $m^2 = x + 2k$, so $x = m^2 - 2k$ and $y = m(x - k) = m(m^2 - 3k)$. Hence n satisfies (5.8) exactly when

$$\begin{aligned} x_0 &= m^2 - 2k \\ n &= m(m^2 - 3k)\,, \end{aligned}$$

where m is an odd integer.

We are led to the following claim.

Lemma 5.4. *Let*

$$E_k \ : \ y^2 = x^3 - 3k^2x + (2k^3 + 4) \tag{5.9}$$

be an elliptic curve over $\mathbb{Q}$ with $ord_{s=1}L(E_k, s) \geq 3$ and odd, and a conductor N_k. Let E_k^d be the quadratic twist of E_k with $d = n^2 + 4$ such that $\left(\dfrac{d}{N_k}\right) = -1$. If k is even, then for any $n = m(m^2 - 3k)$, where m is an odd integer, we have

$$ord_{s=1}L(E_k^d, s) \geq 2$$

with a root number $\omega_d = 1$.

Proof. By the argument presented in the beginning of the section it is enough to find a point in $E_k^d(\mathbb{Q})$ which is not a torsion point. We take $Q = (x_0, 1) = (m^2 - 2k, 1) \in E_k^d(\mathbb{Q})$. Clearly, by (5.3), we have $P = (dx_0, d^2) = (d(m^2 - 2k), d^2) \in E_k^{d,W}(\mathbb{Q})$. By Lutz-Nagell theorem/see [46].VIII.7.2/ if P is a torsion point, both the $x(P)$ and $y(P)$ coordinates of P should be integers. We also use the simple fact that if P is a torsion point so is any multiple of it. Let us look at $[2]P$.

The duplication formula [46].III.2.3d, for an elliptic curve given with (5.1), reads

$$x([2]P) = \frac{x^4 - 2Ax^2 - 8Bx + A^2}{4(x^3 + Ax + B)} = \frac{\phi(x)}{4\psi(x)}\,.$$

We are interested in

$$E_k^{d,W} \;:\; y^2 = x^3 + (-3k^2)d^2x + (2k^3 + 4)d^3 \tag{5.10}$$

and in this case $\psi(dx_0) = \psi\left(d(m^2 - 2k)\right) = d^3(x_0^3 - 3k^2x_0 + (2k^3 + 4)) = d^3 \cdot d = d^4$, where we used (5.7). On the other hand

$$\phi(dx_0) = d^4\left(x_0^4 - 2(-3k^2)x_0^2 - 8(2k^3 + 4)x_0 + (-3k^2)^2\right)$$

and clearly $\psi(dx_0)$ divides $\phi(dx_0)$. Note, however, that x_0 is an odd integer for m–odd, and when k is even, as d is also odd, we have $\phi(dx_0) \equiv 1 \pmod 4$. This means that $x([2]P)$ is not an integer, thus according to Lutz-Nagell theorem $[2]P$ is not a torsion point, so P is not torsion either. □

Remark 5.5. Note that $\phi(dx_0) \equiv 0 \pmod 4$ when k is odd, so we could not use the same easy argument to prove that P is not torsion for odd k.

We can finalize the proof if we find an elliptic curve E_k with an odd analytic rank not less than 3 and even k. In the last section we prove unconditionally that the analytic rank of E_{102} is odd and at least 3 by giving a lower bound for the canonical height of any non-torsion point on the curve. The conductor of E_{102} is $N = 2^3 \cdot 3^3 \cdot 103 \cdot 10303$, therefore the statement of Theorem 5.2 follows from Lemma 5.4 and Goldfeld's theorem.

5.4 Analytic Rank of E_{102}

All computer calculations in this section are made in SAGE [49] if not stated otherwise. Through the function `analytic_rank`, which does not return a provably correct result in all cases, we run positive values for k smaller than 200. The data we find is presented in Table 5.1. Note that $k = 102$ is not the only good choice, since after Lemma 5.4 any even integer k that gives E_k with analytic rank three would work for us. Probably in the family given with (5.9) there are infinitely many even k for which $\mathrm{ord}_{s=1}L(E_k, s) = 3$.

Assuming Birch and Swynnerton-Dyer conjecture, which predicts that the analytic and geometric ranks of an elliptic curve over $\mathbb{Q}$ coincide, and by examining the Mordell-Weil

k	conductor N_k
65	$2^5 \cdot 3^3 \cdot 11 \cdot 19 \cdot 73$
102	$2^3 \cdot 3^3 \cdot 103 \cdot 10303$
114	$2^3 \cdot 3^3 \cdot 5 \cdot 13 \cdot 23 \cdot 991$
129	$2^5 \cdot 3^3 \cdot 5 \cdot 7 \cdot 13 \cdot 337$
136	$2^2 \cdot 3^3 \cdot 7 \cdot 43 \cdot 61 \cdot 137$
141	$2^5 \cdot 3^3 \cdot 19 \cdot 71 \cdot 1039$
145	$2^5 \cdot 3^3 \cdot 7 \cdot 19 \cdot 73 \cdot 157$
162	$2^3 \cdot 3^3 \cdot 163 \cdot 26083$
184	$2^2 \cdot 3^3 \cdot 5 \cdot 37 \cdot 151 \cdot 223$
187	$2^4 \cdot 3^3 \cdot 7 \cdot 47 \cdot 4969$
191	$2^4 \cdot 3^3 \cdot 12097$

Table 5.1: Elliptic curves E_k of analytic rank 3

group $E_{102}(\mathbb{Q})$, the analytic rank of E_{102} is 3. However, we want to show an unconditional proof for the fact that this analytic rank is odd and at least 3. This can be achieved if we proceed in a similar way like in [12].

More precisely, SAGE unconditionally returns $\omega = -1$ and $L(E_{102}, 1) = 0$. It also gives $(-2.80575576483894 \cdot 10^{-13}, 4.32590860129513 \cdot 10^{-33})$ as the value of `L.deriv_at1(200000)`. Here the first value is an upper bound for $L'(E_{102}, 1)$, and the second term is the error size.

There are lower bounds for the canonical height of non-torsion points of elliptic curves like the bound of Hindry–Silverman given in Theorem 0.3 [27]. It says that if N is the conductor of E, Δ – the discriminant of its minimal model, and $\sigma = \log|\Delta|/\log N$, then for any non-torsion point $P \in E(\mathbb{Q})$ we have

$$\hat{h}(P) \geq \frac{2\log|\Delta|}{(20\sigma)^8 10^{1.1+4\sigma}}.$$

The discriminant of E_{102} is $\Delta = -2^8 \cdot 3^3 \cdot 103 \cdot 10303$ so the Weierstrass equation (5.9) coincides with its minimal global model. We compute the Hindry–Silverman's bound in our case. It is $7.14186994767245 \cdot 10^{-16}$. Unfortunately it is 'too close' to zero compared to the approximate value of $L'(E_{102}, 1)$ to be able to use it with Gross–Zagier formula. What we do is to find a better lower bound for the rational points on $E_{102}(\mathbb{Q})$.

Lemma 5.6. *For all rational points $P \in E_{102}(\mathbb{Q})/\{0\}$ where*

$$E_{102} \ : \ y^2 = x^3 - 31212x + 2122420$$

we have

$$\hat{h}(P) \geq 0.38744\,,$$

in particular the torsion subgroup of $E_{102}(\mathbb{Q})$ *is the trivial group. Something more, for all non-integral rational points* $P \in E_{102}(\mathbb{Q})/\{0\}$ *we have*

$$\hat{h}(P) \geq 1.48606\,.$$

Note that we use the Silverman's definition for Néron-Tate height [46], which is normalized as being twice smaller than the height given in SAGE. We will denote the latter as $\hat{h}_S$. Also recall that the *infinite point* $\mathcal{O}$ on elliptic curve is given with the projective coordinates $(0:1:0)$ and its canonical height equals zero.

Before we present the proof of Lemma 5.6 we show how to apply it to prove that $L'(E_{102},1) = 0$ and hence $\mathrm{ord}_{s=1}L(E_{102},s) \geq 3$. By list of the Heegner discriminants for E_{102} we take the point H corresponding to the imaginary quadratic field $\mathbb{Q}(\sqrt{-71})$. Recall that Gross–Zagier formula (5.5) claims that if $L(E,1) = 0$ and $d < 0$ is a Heegner discriminant, then there is a Heegner point $P_d \in E(\mathbb{Q}(\sqrt{d}))$ for which

$$L'(E,1)L(E^d,1) = c_{E,d}\hat{h}(P_d)$$

for some real non-zero constant $c_{E,d}$. Through the function `heegner_point_height`, which uses Gross–Zagier formula and computation of L-series with some precision, we see that the canonical height $\hat{h}_S$ of $H = P_{-71}$ is in the interval $[-0.00087635965, 0.00087636244]$:

```
E102.heegner_discriminants_list(4)
[-71, -143, -191, -263]
a71=E102.heegner_point_height(-71,prec=3)
a71.str(style='brackets')
    '[-0.00087635965 .. 0.00087636244]'
```

This means that $0 \leq \hat{h}_S(H) \leq 0.00087636244$. Also, by Corollary 3.3 [42] and $\omega = -1$, it follows that H equals its complex conjugate. Therefore not only H lies on $E_{102}(\mathbb{Q}(\sqrt{-71}))$ but it is a rational point: $H \in E_{102}(\mathbb{Q})$. By Lemma 5.6 it is clear that the Heegner point H is actually the infinite point, because $\hat{h}_S(H) = 2\hat{h}(H) \leq 0.00087636244$. We also check that $L(E_{102}^{-71},1) \neq 0$:

```
E71=E102.quadratic_twist(-71)
E71.lseries().at1(10^7)
```

gives $L(E_{102}^{-71},1) = 0.682040095555640 \pm 1.40979860223528 \cdot 10^{-20}$. Now from $\hat{h}(H) = 0$ and (5.5) it follows $L'(E_{102},1) = 0$.

We will use the Néron's definition of local heights (Theorem 18.1 [46]) such that the canonical height is expressed like the sum $\hat{h}(P) = \sum_{\nu \in M_{\mathbb{Q}}} \lambda_\nu(P)$ (Theorem 18.2 [46]) and the valuation ν arises from a rational prime or is the usual absolute value at the real field. We will write the finite primes with p and for any integer n and $x = x_1/x_2 \in \mathbb{Q}$ such that $(x_1,x_2) = (x_1,p) = (x_2,p) = 1$, we introduce $\mathrm{ord}_\nu(p^n x) = \mathrm{ord}_p(p^n x) := n$, $|p^n x|_\nu := p^{-n}$ and $\nu(p^n x) := n \log p$.

Let E be an elliptic curve defined over the field of rational numbers with the Weierstrass equation

$$E \; : \; y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6 \tag{5.11}$$

and the quantities b_2, b_4, b_6, b_8, c_4 are the ones defined in III.1 [46]. In this notation the duplication formula for the point $P = (x,y) \in E(\mathbb{Q})$ reads

$$x(2P) = \frac{x^4 - b_4 x^2 - 2b_6 x - b_8}{4x^3 + b_2 x^2 + 2b_4 x + b_6} \, .$$

Let $t = 1/x$ and

$$z(x) = 1 - b_4 t^2 - 2b_6 t^3 - b_8 t^4 = \frac{x^4 - b_4 x^2 - 2b_6 x - b_8}{x^4} \, .$$

Let also

$$\begin{aligned} \psi_2 &= 2y + a_1 x + a_3 \\ \psi_3 &= 3x^4 + b_2 x^3 + 3b_4 x^2 + 3b_6 x + b_8 \, . \end{aligned} \tag{5.12}$$

We formulate Theorem 1.2 [47] into the following lemma

Lemma 5.7. *(Local Height at the Archimedean Valuation) Let $E(\mathbb{R})$ does not contain a point P with $x(P) = 0$. Then for all $P \in E(\mathbb{R})/\{O\}$*

$$\lambda_\infty(P) = \frac{1}{2} \log |x(P)| + \frac{1}{8} \sum_{n=0}^{\infty} 4^{-n} \log |z(2^n P)| \, .$$

The following lemma combines Theorem 4.2 [34] and Theorem 5.2b), c), d) [47]:

Lemma 5.8. *(Local Height at Non-Archimedean Valuations) Let $E/\mathbb{Q}$ be an elliptic curve*

given with a Weierstrass equation (5.11) which is minimal at ν and let $P \in E(\mathbb{Q}_\nu)$. Also let ψ_2 and ψ_3 are defined by (5.12).

(a) If

$$ord_\nu(3x^2 + 2a_2x + a_4 - a_1y) \leq 0 \text{ or } ord_\nu(2y + a_1x + a_3) \leq 0\,,$$

then

$$\lambda_\nu(P) = \frac{1}{2}\max(0, \log|x(P)|_\nu)\,.$$

(b) Otherwise, if $ord_\nu(c_4) = 0$, then for $N = ord_\nu(\Delta)$ and $n = \min(ord_\nu(\psi_2(P)), N/2)$

$$\lambda_\nu(P) = \frac{n(N-n)}{2N^2}\log|\Delta|_\nu\,.$$

(c) Otherwise, if $ord_\nu(\psi_3(P)) \geq 3ord_\nu(\psi_2(P))$, then

$$\lambda_\nu(P) = \frac{1}{3}\log|\psi_2(P)|_\nu\,.$$

(d) Otherwise

$$\lambda_\nu(P) = \frac{1}{8}\log|\psi_3(P)|_\nu\,.$$

The discussion in §5 of [47] verifies the correctness of all possible conditions in the different cases.

We see that in our case $a_1 = a_2 = a_3 = 0$, $a_4 = -3k^2$, $a_6 = 2k^3 + 4$ and $\Delta = (-16)(4(-3k^2)^3 + 27(2k^3+4)^2) = -16.16.27.(k^3+1) = -2^8 \cdot 3^3 \cdot 103 \cdot 10303$. We also need the quantities

$$\begin{aligned}
b_2 &= a_1^2 + 4a_2 = 0\,,\\
b_4 &= 2a_4 + a_1a_3 = -6k^2\,,\\
b_6 &= a_3^2 + 4a_6 = 8(k^3+2)\,,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2 = -9k^4\,,\\
c_4 &= b_2^2 - 24b_4 = -24(-6k^2) = 2^4 \cdot 3^2 \cdot k^2 = 2^6 \cdot 3^4 \cdot 17^2
\end{aligned}$$

because $k = 102 = 2 \cdot 3 \cdot 17$. Also

$$\begin{aligned}
\psi_2 &= 2y\\
\psi_3 &= 3x^4 - 18k^2x^2 + 24(k^3+2)x - 9k^4\,.
\end{aligned}$$

Now we are ready to present the proof of Lemma 5.6.

Proof of Lemma 5.6. First we translate Lemma 5.8 for our curve E_{102} defined with (5.9) for $k = 102$. As we mentioned before by the form of the discriminant Δ, such that for any non-Archimedean valuation ν we have $\nu(\Delta) < 12$, and $a_i \in \mathbb{Z}$, it follows that the Weierstrass equation (5.9) is minimal at any ν/ see [46].VII.Remark 1.1/. Then we have

(a) If

$$\mathrm{ord}_\nu(3x^2 - 3k^2) \leq 0 \text{ or } \mathrm{ord}_\nu(2y) \leq 0\,,$$

then

$$\lambda_\nu = \frac{1}{2}\max(0, \log|x(P)|_\nu)\,.$$

(b) Otherwise we are in a case where P does not have a good reduction modulo p and we have $p \mid \Delta$. So, if $\mathrm{ord}_\nu(c_4) = \mathrm{ord}_\nu(2^6 \cdot 3^4 \cdot 17^2) = 0$, i.e. ν comes from 103 or 10303, then $N = \mathrm{ord}_\nu(\Delta) = 1$ and $n = \min(\mathrm{ord}_\nu(\psi_2(P)), N/2) = \min(\mathrm{ord}_\nu(2y), 1/2) = 1/2$. Therefore

$$\lambda_\nu(P) = \frac{1/2(1-1/2)}{2}\log|\Delta|_\nu = \frac{1}{8}\log|\Delta|_\nu\,.$$

(c) Otherwise, i.e. ν is the valuation at the primes 2 or 3 and P fails the conditions of (a), if $\mathrm{ord}_\nu(\psi_3(P)) \geq 3\mathrm{ord}_\nu(\psi_2(P))$, then

$$\lambda_\nu(P) = \frac{1}{3}\log|\psi_2(P)|_\nu = \frac{1}{3}\log|2y|_\nu\,.$$

(d) Otherwise

$$\lambda_\nu(P) = \frac{1}{8}\log|\psi_3(P)|_\nu\,.$$

For any non-torsion point P on $E_{102}(\mathbb{Q})$ let $x(P) = a/b$ for $(a,b) = 1$ and $b > 0$, and $y(P) = y = c/d$ with $(c,d) = 1$, $d > 0$. From equation (5.9) we have

$$\left(\frac{c}{d}\right)^2 = \left(\frac{a}{b}\right)^3 - 3k^2\frac{a}{b} + 2(k^3+2)$$

or the equivalent

$$b^3c^2 = d^2\left(a^3 - 3k^2ab^2 + 2(k^3+2)b^3\right)\,. \tag{5.13}$$

In (a) $\max(0, \log|x(P)|_\nu) = \max(0, \log|a/b|_\nu) > 0$ only if $\log|a/b|_\nu = \mathrm{ord}_\nu(b)\log p > 0$. If the local heights of P at the primes $p \mid \Delta$ are in cases (b),(c) and (d) we have $\mathrm{ord}_\nu\left(3(x^2-k^2)\right) = \mathrm{ord}_\nu\left(3(a^2-k^2)/b^2\right) > 0$. Let ν comes from 2 or 3 and consider cases (c) and (d). If $\mathrm{ord}_\nu(b) > 0$, then $\mathrm{ord}_\nu(a) = 0$, and since $2, 3 \mid k$, we will have $\mathrm{ord}_\nu(3(x^2-k^2)) < 0$ which is impossible. Thus $\mathrm{ord}_2(b) = \mathrm{ord}_3(b) = 0$.

If we are in case (b) ν comes from $q \in \{103, 10303\}$ and we also use that $\mathrm{ord}_\nu(2y) > 0$.

This means that q divides c. If we assume that q divides b, i.e. $\mathrm{ord}_q(b) > 0$, after (5.13) it follows that q divides a as well - a contradiction. Hence in case (b) $\mathrm{ord}_{103}(b) = \mathrm{ord}_{10303}(b) = 0$.

In any case $\mathrm{ord}_\nu(b) = 0$ if P is into (b), (c) or (d) , so in these cases we can add toward the local height expression $(\mathrm{ord}_\nu(b)\log p)/2$. Combining these we get

$$\sum_{\nu\neq\infty}\lambda_\nu(P) = \frac{1}{2}\log b + \tilde{\lambda}_2 + \tilde{\lambda}_3 + \tilde{\lambda}_{103} + \tilde{\lambda}_{10303}\,, \tag{5.14}$$

where $\tilde{\lambda}_p$ for $p \mid \Delta$ are non-zero only if the point P falls into some of the corresponding cases (b), (c) or (d) and then $\tilde{\lambda}_p = \lambda_p(P)$.

Clearly for any $P \in E_{102}(\mathbb{Q})$ falling in case (b) we have

$$\lambda_{103}(P) = \frac{1}{8}\log|\Delta|_\nu = -\frac{1}{8}\log 103 \tag{5.15}$$

$$\lambda_{10303}(P) = \frac{1}{8}\log|\Delta|_\nu = -\frac{1}{8}\log 10303 \tag{5.16}$$

Next we estimate from below λ_2 and λ_3 from cases (c) or (d). Note that in these cases we have both $\mathrm{ord}_\nu\left(3(x^2-k^2)\right) > 0$ and $\mathrm{ord}_\nu(2y) > 0$.

Case $p = 2$**.** Here $\nu(3(a^2-k^2b^2)/b^2) > 0$ and $2 \mid k$, so we get $2 \mid a$. From $\nu(2y) > 0$ it follows that 2 does not divide d. If 2^2 divides c, then the right-hand side of the equality (5.13) should be divisible by 2^4. Note that $8 \mid a^3, 3k^2ab^2$ but $4 \parallel 2(k^3+2)b^3$. As $2 \nmid d$, then the right-hand side of (5.13) is $\equiv 4 \pmod 8$. Therefore we could have at most $2 \parallel c$. The left-hand side of (5.13) is surely divisible by 2 and hence $2 \mid c$. Then the only possibility is $\mathrm{ord}_2(2y) = 2$.

Let us take a look at $\psi_3(P)$. As $2 \nmid b$ we are interested in the 2-order of $b^4\psi_3$:

$$3a^4 - 18k^2a^2b^2 + 24(k^3+2)ab^3 - 9k^4b^4\,. \tag{5.17}$$

The exact power of two dividing the summand $9k^4b^4$ is 4. If $2^2 \mid a$ we will have $2^5 \mid b^4\psi_3 + 9k^4b^4$, thus $2^4 \parallel \psi_3$. If $2 \parallel a$, then $2^4 \parallel 3a^4, 9k^4b^4$ and hence $2^5 \mid b^4\psi_3$. Therefore in any case $\mathrm{ord}_2(\psi_3) \geq 4$. We conclude that for $\mathrm{ord}_2(2y) = 2$ with $\mathrm{ord}_2(\psi_3) \geq 6$ we are in case (c) and

$$\lambda_2(P) = \frac{1}{3}\log|\psi_2(P)|_\nu = \frac{1}{3}\log|2y|_\nu = -\frac{2}{3}\log 2\,.$$

If $\mathrm{ord}_2(\psi_3)$ is 4 or 5, then according to (d)

$$\lambda_2(P) = \frac{1}{8}\log|\psi_3(P)|_\nu = -\frac{1}{8}\cdot 4\log 2 = -\frac{1}{2}\log 2$$

or

$$\lambda_2(P) = \frac{1}{8}\log|\psi_3(P)|_\nu = -\frac{1}{8}\cdot 5\log 2 = -\frac{5}{8}\log 2\,.$$

In any case we get

$$\lambda_2(P) \geq -\frac{2}{3}\log 2\,. \tag{5.18}$$

Case $p = 3$. Again from $\nu(3(a^2 - k^2b^2)/b^2) > 0$ and $\nu(2c/d) > 0$ it follows that $3 \mid c$ and $3 \nmid b, d$. Look at $b^4\psi_3(P)$ at (5.17). We see that $\psi_3/3 \equiv a^4 + 16ab^3 \equiv a(a^3 + b^3) \pmod 3$ because $3 \mid k$. If we use $3 \mid c$ in (5.13) we see that $3^2 \mid a^3 + 4b^3$. If $3 \mid a$ we should have $3 \mid b$ – a contradiction, hence $3 \nmid a$. If $3^2 \mid a^3 + b^3$, then as it already divides $a^3 + 4b^3$, it would follow $3^2 \mid 3b^3$ which is impossible. Therefore at most $3 \parallel a^3 + b^3$ and finally at most $3^2 \parallel \psi_3$, i.e. $\mathrm{ord}_3(\psi_3(P)) \leq 2$. In this case we always have $\mathrm{ord}_\nu(\psi_3(P)) < 3\mathrm{ord}_\nu(\psi_2(P))$, that is situation (d) with $\lambda_3(P) = \log|\psi_3(P)|_\nu/8 = -(\mathrm{ord}_3(\psi_3)\log 3)/8$. Then, since the 3-order of $\psi_3(P)$ is at most 2, in any case

$$\lambda_3(P) \geq -\frac{1}{4}\log 3\,. \tag{5.19}$$

When we combine the estimates (5.15), (5.16), (5.18) and (5.19) into equation (5.14) we come to

$$\sum_{\nu\neq\infty}\lambda_\nu(P) \geq \frac{1}{2}\log b - \frac{2}{3}\log 2 - \frac{1}{4}\log 3 - \frac{1}{8}\log 103 - \frac{1}{8}\log 10303 \geq \frac{1}{2}\log b - 2.47112\,. \tag{5.20}$$

Case $p = \infty$. For computing λ_∞ we apply Lemma 5.7. It can be seen from the graphic of E_{102} that there are points on $E_{102}(\mathbb{R})$ with $x(P) = 0$. So we want to translate $x \to x + r$ such that $x + r > 0$ for every $x \in E_{102}(\mathbb{R})$. On page 340 of [47] Silverman calls this transformation *the shifting trick*. Indeed, by Theorem 18.3.a) [46] it follows that the local height at Archimedean valuations depends only on the isomorphism class of $E/\mathbb{Q}_\nu$.

If after the translation with r we denote $E_{102} \to E'_{102}$ and $P \to P'$, by the above-mentioned property of the local height $\lambda_\infty(P) = \lambda_\infty(P')$. Note that with the change $x \to x + r$ the discriminant stays the same. Then

$$\lambda_\infty(P) = \frac{1}{2}\log(x + r) + \frac{1}{2}\sum_{n=0}^{\infty}\frac{\log(z(2^nP'))}{4^{n+1}}\,.$$

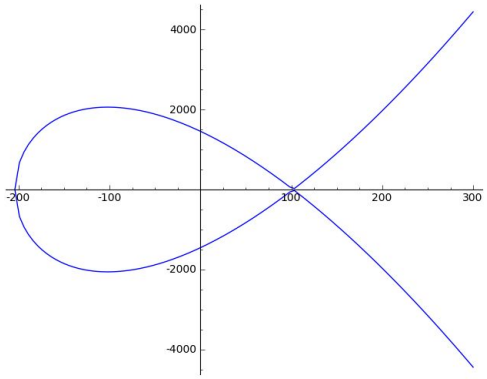


Figure 5.1: Graphics of E_{102}

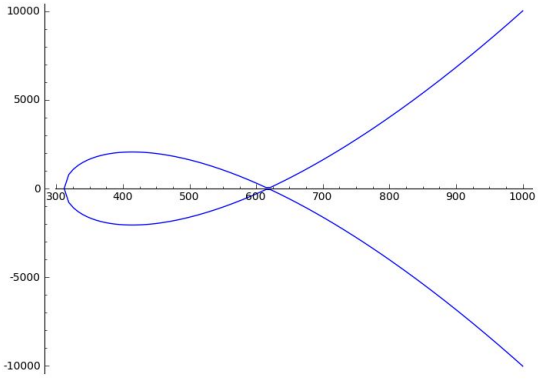


Figure 5.2: Graphics of E'_{102} translated to the right

We take $r = 516$ after we check numerically that with this r we achieve the best lower bound of $z(x)$ for $x \geq x_0$ where x_0 is the only real root of the equation $(x-r)^3 - 31212(x-r) + 2122420 = 0$. More precisely we run the MATHEMATICA procedure

```
Proc[r_] := (
  f[x_] := x^3 - 3*102^2*x + 2*102^3 + 4;
  f1[x_] := f[x - r];
  Clear[a];
  b2 := 4*Coefficient[f1[a], a, 2];
  b4 := 2*Coefficient[f1[a], a, 1];
  b6 := 4*Coefficient[f1[a], a, 0];
  b8 := 4*Coefficient[f1[a], a, 2]*Coefficient[f1[a], a, 0] -
    Coefficient[f1[a], a, 1]^2;
  P1[x_] := x^4 - b4*x^2 - 2*b6*x - b8;
  x0 = x /. Last[N[FindInstance[f1[x] == 0, x, Reals]]];
  minZ = Log[First[NMinimize[{P1[x]/x^4 , x >= x0}, x]]];
```

```
  Return [(minZ/3 + Log[x0])/2];
  ).
```

and we check with

```
For[r = 205, r < 1000, r += 50, Print[r, " ", Proc[r]]]
```

and

```
For[r = 515, r < 525, r ++, Print[r, " ", Proc[r]]]
```

that $r = 516$ gives the best lower bound

$$\lambda_\infty(P) \geq \frac{1}{2}\left\{\log x_0 + \frac{1}{3}\log\left(\min_{x\geq x_0} z(x)\right)\right\} \geq 2.85856\,. \tag{5.21}$$

If we straight apply this estimate for any point $P \in E_{102}(\mathbb{Q})/\{0\}$ including the integral points, we have $b \geq 1$, so after (5.20)

$$\hat{h}(P) \geq \sum_{\nu\neq\infty} \lambda_\nu(P) + \lambda_\infty(P) \geq -2.47112 + 2.85856 \geq 0.38744\,.$$

This lower bound is already much better than Hindry-Silverman's bound. Note that it holds for all integral points as well, including the torsion points different from the infinite point. It follows that the only torsion point on $E_{102}(\mathbb{Q})$ is $\mathcal{O} = (0:1:0)$.

We still try to achieve better lower bound at the non-Archimedean local heights for non-integral points. Looking at (5.13), we see that for any prime power $q \parallel b$ we get $q^3 \parallel d^2$ and it follows that every q is on even power, i.e. b is a perfect square. If $2 \mid b$ we have $b \geq 4$. As from $2 \mid b$ it follows that the local height $\lambda_2(P)$ cannot fall into cases (c) and (d), it is given with case (a). Then

$$\sum_{\nu\neq\infty} \lambda_\nu(P) \geq \frac{1}{2}\log 4 - \frac{1}{4}\log 3 - \frac{1}{8}\log 103 - \frac{1}{8}\log 10303 \geq -1.31587\,.$$

If $2 \nmid b$ we should have $b \geq 3^2$ and

$$\sum_{\nu\neq\infty} \lambda_\nu(P) \geq \frac{1}{2}\log 9 - \frac{2}{3}\log 2 - \frac{1}{4}\log 3 - \frac{1}{8}\log 103 - \frac{1}{8}\log 10303 \geq -1.3725\,.$$

From the latter estimates and (5.21) we have

$$\hat{h}(P) \geq 2.85856 - 1.3725 = 1.48606$$

for any non-integral point $P \in E_{102}(\mathbb{Q})$. This proves the lemma. □

We check that $L^{(3)}(E,1) \neq 0$ by `E102.analytic_rank(leading_coefficient=True)`, because the coefficient is far from zero: SAGE gives

$$\lim_{s\to 1} \frac{L(E,s)}{(s-1)^3} \approx 264.870335957636575\,.$$

For our goal $\mathrm{ord}_{s=1}L(E_{102},s) \geq 3$ is enough so we do not delve more in the precision of the last computation. It suggests that $\mathrm{ord}_{s=1}L(E_{102},s) = 3$, as predicted by Birch and Swinnerton-Dyer conjecture.

In SAGE we get a list of (half of) the integral points in $E(\mathbb{Z})$:

```
E102=EllipticCurve([-31212,2122420])
int=E102.integral_points(); int
  [(-204 : 2 : 1), (-90 : 2050 : 1), (57 : 727 : 1), (102 : 2 : 1), (108 :
   106 : 1), (114 : 214 : 1), (618 : 14794 : 1)]
[E102.point(p).height() for p in int]
  [5.03043808899566, 4.49202786617760, 4.32825858449646, 1.25760952224891,
   2.52198481475949, 2.70002260714301, 5.48053264226463]
```

This way we find the point with the minimal height on E_{102}. This is $M = (102, 2)$, and its negative, with a canonical height $\hat{h}(M) = \hat{h}_S(M)/2 \approx 0.628804761$.

Chapter 6

Class Number One Problem for Certain Real Quadratic Fields II

6.1 Introduction

The last chapter of the thesis introduces results from a joint work with András Biró and Katalin Gyarmati which is still in progress. A huge part of the work is a computer calculation in SAGE which is not presented here but we try to give the theoretical background in bigger detail. The reason of omitting the code is that it is quite bulky. Still it is an important part of the proof, so its effect will be explained later in the chapter.

Let us consider the quadratic fields $K = \mathbb{Q}(\sqrt{d})$ with class group $Cl(d)$ and order of the class group $h(d)$. Like in Chapter 3 we investigate the class number one problem for square-free $d = (an)^2 + 4a$ and positive odd integers a and n. The aim of this joint work is to solve effectively the class number one problem for all R-D discriminants $d = (an)^2 + 4a$. What we succeeded till now is to solve the problem for a huge class of residues of a and n modulo some certain fixed parameter. We believe that in the future we can achieve our final goal in a similar way using more 'arrows' like in [4], [5].

Our main result up to this moment says:

Theorem 6.1. *There is a set*

$$H_0 \subseteq H := \{(A, N) : \ 0 \leq A, N \leq 5 \cdot 7 \cdot 13 \cdot 19 - 1\}$$

satisfying $|H_0| = 17718$ *and the following property: if* $d = (an)^2 + 4a$ *is square-free for odd positive integers* a *and* n *with* $a > 19$ *and* $an > 2 \cdot 7 \cdot 13 \cdot 19$*, and* $h(d) = 1$*, then there is*

an element $(A, N) \in H_0$ *such that*

$$a \equiv A \pmod{5 \cdot 7 \cdot 13 \cdot 19},$$

$$n \equiv N \pmod{5 \cdot 7 \cdot 13 \cdot 19}.$$

Note that $|H_0|/|H|$ is approximately 0.00024, so the theorem shows that we can exclude most of the pairs (a, n) of the residue classes modulo $5 \cdot 7 \cdot 13 \cdot 19$. By Claim 2.6 and $a \equiv 3 \pmod 4$ we still have the remaining possibilities $a = 3$, 11. However these cases are of the same depth as Yokoi's conjecture and we have solved their class number one problem in identical way as in [4].

6.2 Biró-Granville's Theorem

In [7] Biró and Granville give a finite formula for a partial zeta function at 0. They illustrate its efficiency with successful solving of the class number one problem for some one parameter R-D discriminants where $a = 1$. Here we restate their main theorem.

Let χ is a Dirichlet character of conductor q. Recall the sectoral zeta function we introduced in (3.2) – for the fractional ideal I and the zeta function corresponding to the ideal class of I

$$\zeta_I(s, \chi) := \sum_{\mathfrak{a}} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s}$$

where the summation is over all integral ideals $\mathfrak{a}$ equivalent to I in the ideal class group $Cl(d)$. Let us also consider a quadratic form f with discriminant d and introduce the sum

$$G(f, \chi) := \sum_{1 \le u, v \le q-1} \chi\left(f(u, v)\right) \frac{u}{q} \frac{v}{q}. \tag{6.1}$$

Let the element $\beta \in K$ be totally positive, i.e. $\beta \gg 0$. Then according to the theory of cycles of reduced forms corresponding to a given ideal, e.g. §53 in [24], the ideal I of K has a $\mathbb{Z}$-basis (ν_1, ν_2) for which $\nu_1 \gg 0$ and $\alpha = \nu_2/\nu_1$ satisfies $0 < \alpha < 1$. Something more, the regular continued fraction expansion of α is purely periodic:

$$\alpha = [0, \overline{a_1, \ldots, a_\ell}]$$

for some positive ℓ (which is the least period) and $a_1, \ldots, a_\ell$. Here $a_{j+\ell} = a_j$ for every

$j \geq 1$. Further for $n \geq 1$ denote

$$\frac{p_n}{q_n} = [0, a_1, \ldots, a_n]$$

and write $\alpha_n := p_n - q_n\alpha$ with $\alpha_{-1} = 1$ and $\alpha_0 = -\alpha$. Define also for $j = 1, 2, \ldots$

$$Q_j(x, y) = \frac{1}{NI} \left(\nu_1\alpha_{j-1}x + \nu_1\alpha_j y\right) \left(\overline{\nu_1\alpha}_{j-1}x + \overline{\nu_1\alpha}_j y\right)$$

and

$$f_j(x, y) = (-1)^j Q_j(x, y).$$

Now for the Gauss sum

$$\tau(\chi) := \sum_{a(q)} \chi(a) e\left(\frac{a}{q}\right)$$

introduce the expression

$$\beta_\chi := \frac{1}{\pi^2}\chi(-1)\tau(\chi)^2 L(2, \overline{\chi}^2). \tag{6.2}$$

Also recall that a character χ is called *odd* if $\chi(-1) = -1$.

In [7] the following main result is proven

Theorem 6.2 (Biró, Granville [7]). *Suppose that χ is an odd primitive character with conductor $q > 1$ and $(q, 2d) = 1$. With the notations as above we have*

$$\frac{1}{2}\zeta_I(0, \chi) = \sum_{j=1}^{\ell} G(f_j, \chi) + \frac{1}{2}\chi(d)\left(\frac{d}{q}\right)\beta_\chi \sum_{j=1}^{\ell} a_j \overline{\chi}\left(f_j(1, 0)\right).$$

Let $\mathfrak{L}_\chi$ be the field formed by adjoining to $\mathbb{Q}$ all the values of the character χ and $\mathcal{O}_{\mathfrak{L}_\chi}$ be its ring of integers. Recall that in §4.3 of [52] we can find the following equation for the L-function and odd character χ:

$$L(0, \chi) = -\sum_{1 \leq a \leq q} \chi(a)\frac{a}{q}. \tag{6.3}$$

Also consider the quadratic real character $\chi_d = \left(\frac{\cdot}{d}\right)$. Note that $d \equiv 1 \pmod 4$, so $\left(\frac{-1}{d}\right) = (-1)^{(d-1)/2} = 1$ and χ_d is an even character. Then we can state

Claim 6.3. *For the odd character χ with conductor q and $d \equiv 1 \pmod 4$ such that $(q, d) = 1$ the quantity $L(0, \chi\chi_d)$ is an algebraic integer in the number field $\mathfrak{L}_\chi$.*

This can be shown in the same way as the corresponding statement above Fact A [4], using formula (6.3) for the odd character $\chi\chi_d$ and the fact that q and d are coprime. The other result generalizing Fact B [4] is Claim 2.6.

The structure of the chapter is the following: in the next section §6.3 we apply Theorem 6.2 for the specific discriminant we use. For this purpose we need some results for continued fractions and techniques regarding their arithmetic. The main result we get is stated in Lemma 6.5. In section §6.4 we investigate the different factors in the equation of Lemma 6.5 that would be of later use. The proof of Theorem 6.1 is explained in §6.5 and in the last section we show how to compute faster the sum $G(f_1, \chi)$, something very useful for the huge calculations we perform.

6.3 Application of Theorem 6.2 for Our Special Discriminant

We use that $d \equiv 1 \pmod 4$, so the ring of integers $\mathcal{O}_K$ of the field K is of the type $\mathcal{O}_K = \mathbb{Z}\left[1, (\sqrt{d}+1)/2\right]$. Introduce

$$\alpha = \frac{\sqrt{d} - an}{2}\,.$$

We have $0 < \alpha < 1$ and we take the fractional ideal $I = \mathbb{Z}[1, \alpha]$. Clearly $I = \mathcal{O}_K$ and we apply Theorem 6.2 to compute the partial zeta function for the class of principal ideals corresponding to I.

However to apply the upper formula for the function ζ_I we need the continued fraction expansion of α.

By the paper of Schinzel [45] we have that

$$\sqrt{d} = [an, \overline{\frac{1}{2}(n-1), 1, 1, \frac{1}{2}(an-1), 2n, \frac{1}{2}(an-1), 1, 1, \frac{1}{2}(n-1), 2an}\,]. \tag{6.4}$$

Let $\gamma = \sqrt{d} - an$. Then we need to find the expansion of $\gamma/2 = \alpha$. For this sake we use the following rules which are part of the algorithm described without a proof by Beck in [3], page 78. We give three of the operations – the only ones we actually need to apply.

Lemma 6.4. *Let H mean "Halving", D - "Doubling" and S - "Special operation" applied after D. In order to find the half of a number given in a regular continued fraction expansion with m – some coefficient in the expansion, we have the rules:*

a) $H(2m) = mD$ *(halving $2m$ gives m; next double the following pattern);*

b) $D(m, 1) = (2m + 1)S$ *(after D we apply the "Special operation");*

c) $S(1, m) = (2m + 1)H$.

Proof. Let ν and μ denote part of the expansion in the form

$$\cfrac{1}{n + \cfrac{1}{\ddots}}$$

for some positive integer n. It is clear that $\nu < 1$ and $\mu < 1$.

When we want to halve the denominator of the fraction in the form $\dfrac{1}{2m + \nu}$ we have

$$\frac{1}{\frac{1}{2}(2m + \nu)} = \cfrac{1}{m + \cfrac{1}{2\left(n + \cfrac{1}{\ddots}\right)}}$$

so the next part of the expansion should be doubled. This proves a).

To show b) we double the denominator of an expression of the type $\dfrac{1}{m + \dfrac{1}{1 + \nu}}$. So we have

$$\frac{1}{2\left(m + \frac{1}{1+\nu}\right)} = \frac{1}{2m + \frac{2}{1+\nu}} = \frac{1}{2m + \frac{1+\nu+1-\nu}{1+\nu}} = \frac{1}{(2m+1) + \frac{1-\nu}{1+\nu}}.$$

We showed what S means exactly: it transforms expression of the type $\dfrac{1 - \nu}{1 + \nu}$.

In the case c) we consider $\nu = \dfrac{1}{1 + \dfrac{1}{m + \mu}}$.

Then

$$\begin{aligned}\frac{1-\nu}{1+\nu} &= \frac{1-\dfrac{1}{1+\dfrac{1}{m+\mu}}}{1+\dfrac{1}{1+\dfrac{1}{m+\mu}}} = \frac{1-\dfrac{m+\mu}{m+\mu+1}}{1+\dfrac{m+\mu}{m+\mu+1}} \\ &= \frac{m+\mu+1-m-\mu}{m+\mu+1+m+\mu} = \frac{1}{(2m+1)+2\mu} = \frac{1}{(2m+1)+\dfrac{1}{\dfrac{1}{2}\left(n+\dfrac{1}{\ddots}\right)}}\,.\end{aligned}$$

This proves c). □

To obtain the expansion of $\alpha = \gamma/2$ we now apply Lemma 6.4 for (6.4) with the integer part an replaced by 0. We have

$$\gamma = [\underbrace{0}_{H}, \overline{\underbrace{\frac{1}{2}(n-1),1}_{D},\underbrace{1,\frac{1}{2}(an-1)}_{S},\underbrace{2n}_{H},\underbrace{\frac{1}{2}(an-1),1}_{D},\underbrace{1,\frac{1}{2}(n-1)}_{S},\underbrace{2an}_{H}}}].$$

Thus

$$\frac{\gamma}{2} = [0, \overline{n, an}\,]. \tag{6.5}$$

Using the notation from §6.2 we have $\ell = 2$, since we consider $a > 1$, and

$$\frac{1}{2}\zeta_I(0,\chi) = \sum_{j=1}^{2} G(f_j,\chi) + \frac{1}{2}\chi(d)\left(\frac{d}{q}\right)\beta_\chi \sum_{j=1}^{2} a_j\overline{\chi}(f_j(1,0)). \tag{6.6}$$

Here $p_1/q_1 = [0;n] = 1/n$ and $p_2/q_2 = 1/(n+1/an) = an/(an^2+1)$ and $\alpha_1 = 1-n\alpha$, $\alpha_2 = an-(an^2+1)\alpha$.

By the choice of the ideal $I = \mathcal{O}_K$ we have that $NI = 1$ and $\nu_1 = 1$ and so

$$Q_j(x,y) = \alpha_{j-1}\overline{\alpha}_{j-1}x^2 + (\alpha_{j-1}\overline{\alpha}_j + \alpha_j\overline{\alpha}_{j-1})xy + \alpha_j\overline{\alpha}_j y^2\,. \tag{6.7}$$

We recall that α is the positive root of the equation (3.9): $x^2 + (an)x - a = 0$. Then

$\alpha + \bar{\alpha} = -an$ and $\alpha\bar{\alpha} = -a$. We use these to compute

$$\begin{aligned} Q_1(x,y) &= \alpha_0\bar{\alpha}_0 x^2 + (\alpha_0\bar{\alpha}_1 + \alpha_1\bar{\alpha}_0)xy + \alpha_1\bar{\alpha}_1 y^2 \\ &= \alpha\bar{\alpha}x^2 + (-\alpha(1-n\bar{\alpha}) - \bar{\alpha}(1-n\alpha))\,xy + (1-n\alpha)(1-n\bar{\alpha})y^2 \\ &= -ax^2 - anxy + y^2. \end{aligned}$$

The coefficient in front of y^2 is 1 and it follows also from the fact that $1 - n\bar{\alpha} = \varepsilon_d > 1$ is the fundamental unit of $\mathcal{O}_K$ (see §2.3). Similarly

$$\begin{aligned} Q_2(x,y) &= \alpha_1\bar{\alpha}_1 x^2 + (\alpha_1\bar{\alpha}_2 + \alpha_2\bar{\alpha}_1)xy + \alpha_2\bar{\alpha}_2 y^2 \\ &= (1-n\alpha)(1-n\bar{\alpha})x^2 \\ &\quad + \left\{(1-n\alpha)\left(an - (an^2+1)\bar{\alpha}\right) + (1-n\bar{\alpha})\left(an - (an^2+1)\alpha\right)\right\} xy \\ &\quad + \left(an - (an^2+1)\alpha\right)\left(an - (an^2+1)\bar{\alpha}\right) y^2 \\ &= x^2 + anxy - ay^2. \end{aligned}$$

So

$$f_1(x,y) = ax^2 + anxy - y^2 \tag{6.8}$$

and

$$f_2(x,y) = x^2 + anxy - ay^2\,. \tag{6.9}$$

It is no surprise that these are the same quadratic forms as (3.10) and (3.11). We see that $f_1(1,0) = a$ and $f_2(1,0) = 1$. Introduce

$$c_a := a + \overline{\chi}(a)\,. \tag{6.10}$$

When we substitute in (6.6) we get

$$\frac{1}{2}\zeta_I(0,\chi) = G(f_1,\chi) + G(f_2,\chi) + \frac{n}{2}\chi(d)\left(\frac{d}{q}\right)\beta_\chi c_a\,. \tag{6.11}$$

Now assume that we are in a field K where $h(d) = 1$. Then all integral ideals are principal. So our ideal class zeta function equals the Dedekind zeta function:

$$\zeta_I(s,\chi) = \sum_{\mathfrak{a}\lhd\mathcal{O}_K} \frac{\chi(N\mathfrak{a})}{(N\mathfrak{a})^s} = \zeta_K(s,\chi)\,. \tag{6.12}$$

We need also the following equality for the L-function and odd character χ which can be

found in §4.3 of [52]:

$$\zeta_K(s,\chi) = L(s,\chi)L(s,\chi\chi_d)\,. \tag{6.13}$$

Let us further denote

$$m_\chi := \sum_{1\le a<q} a\chi(a) = -qL(0,\chi)\,. \tag{6.14}$$

Then from (6.12) and (6.13) we have

$$q\zeta_I(0,\chi) = qL(0,\chi)L(0,\chi\chi_d) = -m_\chi L(0,\chi\chi_d)\,.$$

Plugging in the latter equality (6.11) we get

$$-\frac{1}{2}m_\chi L(0,\chi\chi_d) = q\bigg(G(f_1,\chi) + G(f_2,\chi) + \frac{n}{2}\chi(d)\left(\frac{d}{q}\right)\beta_\chi c_a)\bigg)\,. \tag{6.15}$$

Introduce the notation

$$C_\chi(a,n) := q\bigg(G(f_1,\chi) + G(f_2,\chi)\bigg)\,. \tag{6.16}$$

Then (6.15) transforms into

Lemma 6.5. *With the upper notations, if $h(d) = 1$, we have*

$$-m_\chi L(0,\chi\chi_d) = 2C_\chi(a,n) + nq\chi(d)\left(\frac{d}{q}\right)\beta_\chi c_a\,.$$

Take a prime ideal $\mathfrak{R}$ in $\mathcal{O}_{\mathfrak{L}_\chi}$ lying above a rational prime r such that $m_\chi \in \mathfrak{R}$. We get a formula that in some sense generalizes formula (2.10) in [4] just like Yokoi's discriminant $d = n^2+4$ is a special case of the discriminant we consider. Indeed, by Claim 6.3 we have $L(0,\chi\chi_d) \in \mathcal{O}_{\mathfrak{L}_\chi}$ so $-m_\chi L(0,\chi\chi_d) \equiv 0 \pmod{\mathfrak{R}}$. Then by Lemma 6.5 we have

$$0 \equiv 2C_\chi(a,n) + n\chi(d)\left(\frac{d}{q}\right)q\beta_\chi c_a \pmod{\mathfrak{R}}\,. \tag{6.17}$$

Require also $(\mathfrak{R}, q\beta_\chi) = 1$ and $(\mathfrak{R}, c_a) = 1$. Then we transform (6.17) into

$$n \equiv -2\overline{\chi}(d)\left(\frac{d}{q}\right)\frac{C_\chi(a,n)}{c_a q\beta_\chi} \pmod{\mathfrak{R}}\,. \tag{6.18}$$

One can check that if we substitute $a = 1$ in (6.18) we arrive at the same formula, as if we apply Theorem 6.2 for $a = 1$. Then (6.18) is exactly formula (2.10) in [4].

This also follows from the fact that the two formulae for the residue n modulo $\mathfrak{R}$ in [4] and [7] for Yokoi's discriminants are equivalent, though this is not explicitly noted in [7].

Let us assume that the parameter a in the formula (6.18) is congruent to 1 modulo $\mathfrak{R}$ and modulo q. Then

$$c_a = a + \bar{\chi}(a) \equiv 1 + \bar{\chi}(1) \equiv 2 \pmod{\mathfrak{R}}$$

and in this case we have

$$n \equiv -\overline{\chi}(d) \left(\frac{d}{q}\right) \frac{C_\chi(1,n)}{q\beta_\chi} \pmod{\mathfrak{R}}. \tag{6.19}$$

We notice that this is formula (10.1) in [7] with the change of notation: our $C_\chi(1,n)$ is twice the value of C_χ defined in [7]. For the proof of the Yokoi's conjecture the original Biró's graph have been used

$$\begin{array}{ccccc} 175 & & & & \\ \downarrow & \searrow & & & \\ 1861 & \longleftarrow & 61 & \longrightarrow & 41 \end{array} \tag{6.20}$$

and we checked that the graph

$$\begin{array}{ccccccc} 175 & & & & & & \\ \downarrow & \searrow & & & & & \\ 1861 & & 61 & \longrightarrow & 41 & \longrightarrow & 11 \end{array}$$

also proves Yokoi's conjecture. A meaning of 'graph' close to the original definition in [4] would be explained in §6.5.

Now denote $M := 41 \cdot 61 \cdot 175 \cdot 1861$. If $a \equiv 1 \pmod{M}$ the formula (6.19) is valid for all members of the graph (6.20) and this is exactly formula (10.1) from [7] where the Yokoi's case is solved. Therefore this solves the class number one problem for the infinite class of discriminants $d = (an)^2 + 4a$ with $a \equiv 1 \pmod{M}$. Notice that the vertices in the second graph are the same as in (6.20) plus one more, 11. Therefore having resolved $a \equiv 1 \pmod{M}$, the case $a \equiv 1 \pmod{M \cdot 11}$ is also included in it.

Remark 6.6. If q and r divide n in the general case where $a > 1$ the congruence (6.17) yields only the trivial $0 \equiv 0 \pmod{\mathfrak{R}}$ because in that case $C_\chi(a,n) = 0$ (this will be shown

in Lemma 6.11 in the next section). This was the motivation for using real character χ in Chapter 3 and investigating only the case $q \mid n$. But in the case $q \nmid n$ we can exclude a lot of residue classes on the basis of (6.17), as we will explain in §6.5.

6.4 Further Remarks on Lemma 6.5

First we find a more simple finite form for β_χ. Let

$$\gamma_\chi := \sum_{n=1}^{q-1} \chi^2(n) \frac{n^2}{q^2} \tag{6.21}$$

and consider the Jacobi sum

$$J_\chi := \sum_{\substack{a,b \pmod q \\ a+b\equiv 1 \pmod q}} \chi(a)\chi(b)\,.$$

The following claim shows that β_χ is actually not only algebraic integer but also computable in finitely many steps which is not at all evident from definition (6.2). The claim is proven in §6 of [7].

Lemma 6.7. *Let χ be a primitive character of order greater than 2. For the unique way to write $\chi = \chi_+\chi_-$ where χ_+, χ_- are primitive characters of coprime conductors q_+, q_- respectively, such that χ_- has order 2, and χ_+^2 is also primitive, we have*

$$\beta_\chi = \chi_+(-1) J_{\chi_+} \gamma_\chi \mu(q_-) \prod_{p \mid q_-} \frac{p^2\chi_+^2(p) - 1}{p\chi_+^2(p) - 1}\,.$$

The following statement(§9 in [7]) reduces with a half the required checks in the computer calculations performed for this chapter. As the exposition in [7] is somewhat sketchy we give here a detailed proof.

Lemma 6.8. *For odd complex character χ with conductor $q > 2$ such that $(q, 2d) = 1$ we have*

$$G(f_1, \chi) = G(f_2, \chi)\,.$$

Proof. In (6.1) we change the summation by $u \to v\,, v \to q - u$. Then for the new variables

again $1 \le v, q-u \le q-1$. Now

$$\begin{aligned} G(f_1,\chi) &= \sum_{1\le u,v\le q-1} \chi(av^2+anv(q-u)-u^2)\frac{v}{q}\frac{q-u}{q} \\ &= \sum_{1\le u,v\le q-1} \chi(av^2-anvu-u^2)\frac{v}{q}\frac{-u}{q} + \sum_{1\le u,v\le q-1} \chi(av^2-anvu-u^2)\frac{v}{q} \\ &= \sum_{1\le u,v\le q-1} \chi(-1)\chi(-av^2+anvu+u^2)\frac{v}{q}\frac{-u}{q} - \sum_{1\le u,v\le q-1} \chi(f_2(u,v))\frac{v}{q} \\ &= \sum_{1\le u,v\le q-1} \chi(f_2(u,v))\frac{u}{q}\frac{v}{q} - \sum_{1\le u,v\le q-1} \chi(f_2(u,v))\frac{v}{q}\,. \end{aligned}$$

We use the notation

$$g(\chi,f,h) := \sum_{1\le m,n\le q-1} \chi(f(m,n))h(\frac{n}{q}) \tag{6.22}$$

for the quadratic form $f(x,y) = Ax^2+Bxy+Cy^2$ with square-free discriminant $\Delta = B^2-4AC$ and $h(x)\in\mathbb{Z}[x]$.

Therefore we have

$$G(f_1,\chi) = G(f_2,\chi) - g(\chi,f_2,t)\,.$$

We will prove that

$$g(\chi,f_2,t) = 0\,. \tag{6.23}$$

We will make it by showing that $g(\chi,f_2,1)=0$ and $g(\chi,f_2,t-1/2)=0$.

First notice that there is a g with $(g,q)=1$ such that $\chi(g)\neq 0,1$ and one can find r,s for which $g\equiv r^2-\Delta s^2 \pmod q$. The argument that follows is for square-free q and the one for general q follows easily. The existence of such r and s follows from the theory of norm residues modulo q in $\mathbb{Q}(\sqrt{\Delta})$ for $(q,\Delta)=1$, see Theorem 138 and Lemma from §47 in [24]. Basically we use that the group of norm residues modulo q is big, take element g_1 from it and then choose g to be g_1 or $4g_1$ depending on the residue of the discriminant of the field modulo 4. In this case $r^2-\Delta s^2$ is the norm, or four times the norm, of an algebraic integer in $\mathbb{Q}(\sqrt{\Delta})$.

Now if we choose M and N satisfying

$$(2AM+BN)+\sqrt{\Delta}N = \Big((2Am+Bn)+\sqrt{\Delta}n\Big)\,(r+\sqrt{\Delta}s)$$

we get

$$\Big((2AM+BN)+\sqrt{\Delta}N\Big)\Big((2AM+BN)-\sqrt{\Delta}N\Big)=4Af(M,N)=4Af(m,n)(r^2-\Delta s^2)\,.$$

From definition (3.11) the coefficient A of f_2 equals 1, i.e. $(A,q)=1$, so we get $f_2(M,N)\equiv f_2(m,n)g \pmod q$. One checks that

$$\begin{pmatrix} M \\ N \end{pmatrix}=\begin{pmatrix} r-Bs & -2Cs \\ 2As & r+Bs \end{pmatrix}\begin{pmatrix} m \\ n \end{pmatrix}$$

with determinant of the upper matrix, denoted by $\mathfrak{T}$, equal to $r^2-\Delta s^2\neq 0$. Since $\mathfrak{T}$ is invertible and m and n are linear forms of M and N, if some of the latter do not take each residue modulo q exactly q times, then some of the residues m or n will not either. Therefore when $0\leq m,n\leq q-1$ also $0\leq M,N \pmod q\leq q-1$. Notice as well that

$$g(\chi,f,1)=\sum_{0\leq m,n\leq q-1}\chi(f(m,n))$$

because χ is not a real character and

$$\sum_{0\leq m\leq q-1}\chi(Am^2)=\sum_{0\leq n\leq q-1}\chi(Cn^2)=0\,.$$

That is why we can substitute m and n with M and N in the sum $g(\chi,f_2,1)$. We get $g(\chi,f_2,1)=\chi(g)g(\chi,f_2,1)$. Hence

$$g(\chi,f_2,1)=\sum_{1\leq m,n\leq q-1}\chi(f(m,n))=0\,. \tag{6.24}$$

Further, consider the Bernoulli polynomial $B_1(x):=x-\dfrac{1}{2}$. We notice that $B_1(1-x)=\dfrac{1}{2}-x=-B_1(x)$. Therefore $\chi(f(m,n))B_1\left(\dfrac{n}{q}\right)=-\chi\left(f(q-m,q-n)\right)B_1\left(\dfrac{q-n}{q}\right)$ and

$$\begin{aligned} g(\chi,f,B_1) &= \sum_{1\leq m,n\leq q-1}\chi(f(m,n))B_1(\frac{n}{q})=-\sum_{1\leq m,n\leq q-1}\chi(f(q-m,q-n))B_1(\frac{q-n}{q}) \\ &= -g(\chi,f,B_1)\,. \end{aligned}$$

We got that $g(\chi,f,B_1)=0$. This and (6.24) yield (6.23) and therefore we complete the proof. □

If we apply real characters we get:

Remark 6.9. It could be checked that for odd *real* character $\chi = \left(\frac{\cdot}{q}\right)$ with conductor $q \equiv 3 \pmod 4$ such that $(q, d) = 1$ we have

$$G(f_1, \chi) = G(f_2, \chi) - \frac{1}{2}\left(1 - \left(\frac{a}{q}\right)\right)\varphi(q)$$

where $\varphi(q)$ is the Euler function. Thus $G(f_1, \chi) = G(f_2, \chi)$ only if $\chi(a) = 1$. This is only one of the many reasons why simply taking χ to be a real character does not seem to solve the whole class number one problem for $d = (an)^2 + 4a$ via Lemma 6.5 .

Further we state

Lemma 6.10. *For any odd character χ with conductor $q > 2$ we have*

$$C_\chi(a, q - n) = -C_\chi(a, n)\,.$$

Proof. To show this we substitute $n \to q - n$ in the definition of $G(f_1, \chi)$:

$$\begin{aligned} G(f_1, \chi)_{q-n} &= \sum_{1 \le x,y \le q-1} \chi(ax^2 + a(q-n)xy - y^2)\frac{x}{q}\frac{y}{q} \\ &= \sum_{1 \le x,y \le q-1} \chi(ax^2 - anxy - y^2)\frac{x}{q}\frac{y}{q} \\ &= \sum_{1 \le x,y \le q-1} \chi(-1)\chi(-ax^2 + anxy + y^2)\frac{x}{q}\frac{y}{q} \\ &= -G(f_2, \chi)_n\,. \end{aligned}$$

Thus we have that

$$\frac{1}{q}C_\chi(a, q-n) = G(f_1, \chi)_{q-n} + G(f_2, \chi)_{q-n} = -G(f_2, \chi)_n - G(f_1, \chi)_n = -\frac{1}{q}C_\chi(a, n)\,.$$

□

Applying this lemma we can always compute only the first half of the residues n modulo q whenever we need the value of $C_\chi(a, n)$. As an immediate corollary we also get

Lemma 6.11. *For any integer a we have*

$$C_\chi(a, 0) = 0\,.$$

Indeed, $C_\chi(a,0) = C_\chi(a,q-0) = -C_\chi(a,0)$ and therefore the claim. This also means that for any n divisible by q we have $C_\chi(a,n) = 0$.

We also asked ourselves how the equation of Lemma 6.5 behaves when $\mathfrak{R}$ divides (q) itself. Let q be a prime number, g_q be a primitive root modulo q and $\zeta_q = e\,(1/(q-1))$ be a root of unity of order $\varphi(q) = q-1$. Consider the primitive character χ_q with conductor q such that $\chi_q(g_q) = \zeta_q$. Then $\chi(-1) = -1$, $\mathfrak{L}_{\chi_q} = \mathbb{Q}(\zeta_q)$ and $\mathcal{O}_{\mathfrak{L}_{\chi_q}} = \mathbb{Z}[\zeta_q]$ by Theorem 2.6 [52]. Also it is clear that $\beta_{\chi_q} = -\gamma_{\chi_q} J_{\chi_q}$ after Lemma 6.7 .

From Lemma 6.5, (6.16) and Lemma 6.8 we get

$$-qm_{\chi_q} L(0,\chi_q\chi_d) = 4q^2 G(f_1,\chi_q) + nq^2\chi_q(d)\left(\frac{d}{q}\right)\gamma_{\chi_q} J_{\chi_q} c_a\,.$$

By the ideal decomposition of the Jacobi sum in $\mathbb{Z}[\zeta_q]$ we know that J_{χ_q} is in some of the ideals above q. This could be seen in [53], a paper which is a good reference on the properties of Jacobi sums. Further one can show that m_{χ_q}, $q^2\gamma_{\chi_q}$ are in almost all prime ideals in $\mathbb{Z}[\zeta_q]$ over q. Thus one wants to check

$$4q^2 G(f_1,\chi_q) \equiv 0 \pmod{\mathfrak{R}_q^2}$$

for such a prime ideal $\mathfrak{R}_q$ over q where m_{χ_q}, J_{χ_q}, $q^2\gamma_{\chi_q} \in \mathfrak{R}_q$. Unfortunately computer checks show that the upper congruence on $G(f_1,\chi_q)$ is trivially fulfilled for any prime q. Therefore it is certainly necessary to take $\mathfrak{R}$ over a prime rational r different from q.

6.5 On the Proof of Theorem 6.1 and Further Plans

Suppose now that χ is an odd primitive character modulo $q > 1$ and $(q,2d) = 1$. Assume, in addition, that χ is a complex character, i.e. $\chi^2 \neq 1$. In this case below we will use Lemma 6.8 and Lemma 6.7. By (6.16) and (6.17) we get

$$\begin{aligned} 4q^2\left(\prod_{p|q^-}\left(p\chi_+^2(p)-1\right)\right) G\left(f_1,\chi\right) \quad + \\ +n\chi(d)\left(\frac{d}{q}\right) c_a q^2 J_{\chi_+}\gamma_\chi\mu(q_-)\chi_+(-1)\left(\prod_{p|q^-}\left(p^2\chi_+^2(p)-1\right)\right) \quad \equiv \quad 0 \pmod{\mathfrak{R}}\,, \end{aligned} \tag{6.25}$$

where the ideal $\mathfrak{R}$ lies above the rational prime r, $m_\chi \in \mathfrak{R}$ and $(r, q) = 1$. Then it is clear, using (6.1), the definition of f_1 (6.8) and (6.10) that the truth of (6.25) depends only on the residues of a and n modulo qr.

Let us now define a directed graph in a similar but slightly different way than in [4]. Let us denote by an arrow

$$q \to r$$

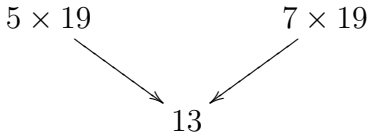
that the following conditions are true: $q > 1$ is an odd integer, there is an odd primitive character χ modulo q such that $\chi^2 \neq 1$, and there is a prime ideal $\mathfrak{R}$ of $\mathfrak{L}_\chi$ such that $\mathfrak{R}$ lies above the odd rational prime r, which satisfies $(r, q) = 1$ and $m_\chi \in \mathfrak{R}$. The latter condition can arise for example for an odd character if $r \mid h^-(q)$, where $h^-(q)$ is the relative class number of the cyclotomic field $\mathbb{Q}(\zeta_q)$ for $\zeta_q = e\,(1/\varphi(q))$ (Theorem 4.17 [52]). All arrows we use are derived from Table §3 for relative class numbers in [52].

Let $q \to r$ holds. Then by the considerations above and by Claim 2.6 we get that if $h(d) = 1$ for the square-free discriminant $d = (an)^2 + 4a$ satisfying $qr < an/2$, and a is greater than any prime factor of qr, then

$$\left(\frac{(an)^2 + 4a}{p}\right) = -1 \tag{6.26}$$

for every prime divisor p of qr, and (6.25) also holds. We see that (6.26), similarly to (6.25), depends only on the residues of a and n modulo qr.

Our Theorem 6.1 follows by using the concrete arrows



Indeed, $5 \cdot 19 \cdot 13$ and $7 \cdot 19 \cdot 13$ divides $5 \cdot 7 \cdot 13 \cdot 19$, so if we fix the residues of a and n modulo $5 \cdot 7 \cdot 13 \cdot 19$, then the residues of a and n modulo qr are determined for both of the two concrete arrows. Checking (6.25) and (6.26) for both arrows and for every $(a, n) \in H$ (see Theorem 6.1 for the set H) we obtain Theorem 6.1.

We explained above the theoretical background of the proof of Theorem 6.1. However, very hard computations were also needed to get the result, and we used SAGE for these

computations. We also used a slight simplification of the formula for $G(f_1, \chi)$ in order to make the computations faster. We will present this simplification in the next section.

We outline finally our future plans. Besides the arrows already used we want to apply also the following ones:

$$13 \times 19 \to 3, 5, 7, 73,$$

$$3 \times 5 \times 19 \to 37, 73,$$

$$7 \times 13 \to 37,$$

$$7 \times 19 \to 3, 37, 73.$$

By heuristic considerations we hope that these arrows will yield that $h(d) = 1$ is possible only in the case when n is divisible by all the prime factors involved, i.e. if 3, 5, 7, 13, 19, 37 and 73 divide n. In case there are a few exceptions, there are still a lot of possibilities with numbers q, r already mentioned and also with

$$q = 3^2 \cdot 19,\ 3^3 \cdot 7,\ 5 \cdot 7^2,\ 3^2 \cdot 7^2\,,$$

$$r = 109,\ 127,\ 163,\ 181\,.$$

We remark that we use these specific arrows because this part of the graph is fairly dense (i.e. there are many arrows connecting the above-mentioned vertices), and this gives good chance to exclude residue classes.

So we expect that we will be able to prove a theorem that $h(d) = 1$ is possible only if a certain large integer divides n. But as Remark 6.6 shows, it is unavoidable (using only the method of the present chapter) that such exceptional cases remain. However, we have also a method (see Chapter 3) to exclude cases $m \mid n$ for certain fixed integers m. Therefore the methods of Chapter 3 and the present chapter are complementary in some sense. So we can hope that combining these two methods and choosing the parameters in a lucky way finally we will be able to determine every field with $h(d) = 1$ in the family $d = (an)^2 + 4a$.

6.6 Quicker Computation of $G(f_1, \chi)$

Let q be a square-free positive integer. If χ is a character modulo q and A, B, C are integers, let

$$T_{\chi,q}(A,B,C) := \sum_{0 \le u,v \le q-1} \chi\left(Au^2 + Buv + Cv^2\right) uv\,. \tag{6.27}$$

We are interested in this sum in order to compute $G(f,\chi)$ from (6.1), but we divide it into smaller parts according to the greatest common divisors (u,q) and (v,q), and we first compute these smaller parts. We introduce a definition.

Let q be a square-free positive integer, and let d_1 and d_2 be two positive divisors of q. If χ is a character modulo q and A, B, C are integers, let $S_{\chi,q,d_1,d_2}(A,B,C)$ denote the following sum:

$$\sum_{u \in R(q/d_1)} \sum_{v \in R(q/d_2)} \chi\left(A(d_1u)^2 + B(d_1u)(d_2v) + C(d_2v)^2\right) uv\,, \tag{6.28}$$

where

$$R(m) := \{a :\ 0 \le a \le m-1,\ (a,m) = 1\}\,.$$

By (6.27) and (6.28), and taking $(u,q) = d_1$ and $(v,q) = d_2$, we get

$$T_{\chi,q}(A,B,C) = \sum_{d_1 | q,\, d_1 < q} \sum_{d_2 | q,\, d_2 < q} d_1 d_2 S_{\chi,q,d_1,d_2}(A,B,C)\ , \tag{6.29}$$

so it is enough to deal with (6.28) in order to compute (6.27).

Let us assume now that $(d_1,d_2) = 1$ and with the definition $d_3 := q/d_1d_2$ we also have $(d_1,d_3) = (d_2,d_3) = 1$. Then there are characters χ_{d_i} modulo d_i for $1 \le i \le 3$ such that

$$\chi = \chi_{d_1}\chi_{d_2}\chi_{d_3}\,. \tag{6.30}$$

We regard $S_{\chi,q,d_1,d_2}(A,B,C)$ as the inner product of the functions

$$f_1(u,v) = f_1(u,v;\chi) = \chi\left(A(d_1u)^2 + B(d_1u)(d_2v) + C(d_2v)^2\right) \tag{6.31}$$

and

$$f_2(u,v) = uv\,,$$

and we compute this inner product using the dual group, i.e. the group of characters. Denote by $X(n)$ the group of characters modulo n, then by the orthogonality relations for characters we see that $S_{\chi,q,d_1,d_2}(A,B,C)$ equals

$$\sum_{\substack{u_1,u_2\in R(q/d_1)\\ v_1,v_2\in R(q/d_2)}} f_1(u_1,v_1)u_2v_2\left(\frac{\sum_{\chi_1\in X\left(\frac{q}{d_1}\right),\chi_2\in X\left(\frac{q}{d_2}\right)}\chi_1\left(\frac{u_2}{u_1}\right)\chi_2\left(\frac{v_2}{v_1}\right)}{\varphi\left(\frac{q}{d_1}\right)\varphi\left(\frac{q}{d_2}\right)}\right).$$

Here $\varphi(x)$ is the Euler function. For $\psi\in X(n)$ let $m(n,\psi)=m_\psi=\sum_{a=0}^{n-1}a\psi(a)$. Then changing the order of summations we get that $S_{\chi,q,d_1,d_2}(A,B,C)$ equals

$$\frac{\sum_{\chi_1\in X\left(\frac{q}{d_1}\right),\chi_2\in X\left(\frac{q}{d_2}\right)}m\left(\frac{q}{d_1},\chi_1\right)m\left(\frac{q}{d_2},\chi_2\right)}{\varphi\left(\frac{q}{d_1}\right)\varphi\left(\frac{q}{d_2}\right)}\Sigma\,, \tag{6.32}$$

where

$$\Sigma=\sum_{u_1\in R(q/d_1),v_1\in R(q/d_2)}\frac{\chi\left(A\left(d_1u_1\right)^2+B\left(d_1d_2u_1v_1\right)+C\left(d_2v_1\right)^2\right)}{\chi_1\left(u_1\right)\chi_2\left(v_1\right)}\,. \tag{6.33}$$

Now, χ_1 is a character modulo d_2d_3, and $(d_2,d_3)=1$, so there are characters χ_{1,d_2} modulo d_2 and χ_{1,d_3} modulo d_3 such that

$$\chi_1=\chi_{1,d_2}\chi_{1,d_3}\,. \tag{6.34}$$

Similarly, there are characters χ_{2,d_1} modulo d_1 and χ_{2,d_3} modulo d_3 such that

$$\chi_2=\chi_{2,d_1}\chi_{2,d_3}\,. \tag{6.35}$$

Then using (6.30) and the notation (6.31) we see that Σ equals

$$\sum_{u_1\in R(q/d_1),v_1\in R(q/d_2)}\frac{\chi_{d_1}\left(C\left(d_2v_1\right)^2\right)\chi_{d_2}\left(A\left(d_1u_1\right)^2\right)f_1\left(u_1,v_1;\chi_{d_3}\right)}{\chi_{1,d_2}\left(u_1\right)\chi_{1,d_3}\left(u_1\right)\chi_{2,d_1}\left(v_1\right)\chi_{2,d_3}\left(v_1\right)}.$$

Let

$$u_1=Xd_2+Yd_3,$$

$$v_1=Zd_1+Vd_3,$$

then Σ equals the product of the following three lines:

$$\sum_{X,Z\in R(d_3)} \frac{\chi_{d_3}\left(A\left(d_1Xd_2\right)^2+B\left(d_1d_2Xd_2Zd_1\right)+C\left(d_2Zd_1\right)^2\right)}{\chi_{1,d_3}\left(Xd_2\right)\chi_{2,d_3}\left(Zd_1\right)}\,, \tag{6.36}$$

$$\sum_{Y\in R(d_2)} \frac{\chi_{d_2}\left(A\left(d_1Yd_3\right)^2\right)}{\chi_{1,d_2}\left(Yd_3\right)}\,, \tag{6.37}$$

$$\sum_{V\in R(d_1)} \frac{\chi_{d_1}\left(C\left(d_2Vd_3\right)^2\right)}{\chi_{2,d_1}\left(Vd_3\right)}\,. \tag{6.38}$$

By the orthogonality property of characters we have (6.37) is 0 unless

$$\chi_{1,d_2}=\chi_{d_2}^2\,, \tag{6.39}$$

and (6.38) is 0 unless

$$\chi_{2,d_1}=\chi_{d_1}^2\,. \tag{6.40}$$

And if (6.39) and (6.40) are true, then the product of (6.37) and (6.38) equals

$$\varphi\left(d_2\right)\chi_{d_2}\left(A\left(d_1\right)^2\right)\varphi\left(d_1\right)\chi_{d_1}\left(C\left(d_2\right)^2\right)\,. \tag{6.41}$$

We see by the substitution $r=X/Z$ that (6.36) is 0 unless

$$\chi_{d_3}^2=\chi_{1,d_3}\chi_{2,d_3}\,, \tag{6.42}$$

and if (6.42) is true, then (6.36) equals

$$\varphi\left(d_3\right)\frac{\chi_{d_3}\left(\left(d_1d_2\right)^2\right)}{\chi_{1,d_3}\left(d_2\right)\chi_{2,d_3}\left(d_1\right)}\sum_{r\in R(d_3)}\frac{\chi_{d_3}\left(Ar^2+Br+C\right)}{\chi_{1,d_3}\left(r\right)},$$

which can be written as

$$\varphi\left(d_3\right)\chi_{1,d_3}\left(d_1\right)\chi_{2,d_3}\left(d_2\right)U_{d_3}\left(\chi_{d_3},\chi_{1,d_3},A,B,C\right)\,, \tag{6.43}$$

using, in general, the notation

$$U_n\left(\psi_1,\psi_2,A,B,C\right)=\sum_{r\in R(n)}\frac{\psi_1\left(Ar^2+Br+C\right)}{\psi_2\left(r\right)} \tag{6.44}$$

for $\psi_1, \psi_2 \in X(n)$. From (6.30), (6.34) and (6.35) we see that (6.39), (6.40) and (6.42) are true if and only if $\chi^2 = \chi_1\chi_2$. And if $\chi^2 = \chi_1\chi_2$, then we have by (6.36), (6.37), (6.38), (6.41) and (6.43) that

$$\Sigma = \varphi(q)\,\chi_{d_2}\left(A(d_1)^2\right)\chi_{d_1}\left(C(d_2)^2\right)\chi_{1,d_3}(d_1)\,\chi_{2,d_3}(d_2)\,U_{d_3}(\chi_{d_3}, \chi_{1,d_3}, A, B, C).$$

Therefore finally we get by (6.32) and (6.33) that $S_{\chi,q,d_1,d_2}(A, B, C)$ equals

$$\frac{\chi_{d_2}\left(A(d_1)^2\right)\chi_{d_1}\left(C(d_2)^2\right)}{\varphi(d_3)} \tag{6.45}$$

times

$$\sum m\left(\frac{q}{d_1}, \chi_1\right) m\left(\frac{q}{d_2}, \chi_2\right)\chi_{1,d_3}(d_1)\,\chi_{2,d_3}(d_2)\,U_{d_3}(\chi_{d_3}, \chi_{1,d_3}, A, B, C)\ , \tag{6.46}$$

where the summation is over characters χ_1, χ_2 satisfying the following conditions:

$$\chi_1 \in X\left(\frac{q}{d_1}\right), \chi_2 \in X\left(\frac{q}{d_2}\right), \chi_1\chi_2 = \chi^2.$$

We now make some minor remarks before stating our lemma.

Assume that χ^2 is not the principal character. Then we may assume that χ_1 and χ_2 are odd. Indeed, it is clear that either both of them are odd or both of them are even, and that at least one of them is nonprincipal. If, for example, χ_1 is even and nonprincipal, then it is easy to see that $m(q/d_1, \chi_1) = 0$. It follows that if $d_3 = 1$, then the whole sum is 0, since in that case $\chi_1\chi_2 = \chi^2$ and $(q/d_1, q/d_2) = 1$ imply that χ_1 and χ_2 are squares, hence they are even.

Observe also that if $(d_1, d_2) > 1$, then $S_{\chi,q,d_1,d_2}(A, B, C) = 0$ by (6.28), as any value of the character χ in the definition of the sum is 0.

Let n be a positive integer and $\psi_1, \psi_2 \in X(n)$. We show a multiplicativity property of the function U_n. Let $n = \prod_{i=1}^{k} n_i$, where the integers n_i are pairwise relatively prime. Then

$$\psi_j = \prod_{i=1}^{k} \psi_{j,i}$$

for $1 \le j \le 2$, where $\psi_{j,i}$ is a character mod n_i for $1 \le j \le 2$, $1 \le i \le k$. Any $r \in R(n)$

can be uniquely written in this way:

$$r \equiv \sum_{i=1}^{k} r_i \frac{n}{n_i} \pmod{n},$$

where $r_i \in R(n_i)$. Then we see using (6.44) that $U_n(\psi_1, \psi_2, A, B, C)$ equals

$$\sum_{r_1 \in R(n_1)} \sum_{r_2 \in R(n_2)} \cdots \sum_{r_k \in R(n_k)} \frac{\prod_{i=1}^{k} \psi_{1,i}\left(A\left(r_i \frac{n}{n_i}\right)^2 + B r_i \frac{n}{n_i} + C\right)}{\prod_{i=1}^{k} \psi_{2,i}\left(r_i \frac{n}{n_i}\right)},$$

hence

$$U_n(\psi_1, \psi_2, A, B, C) = \prod_{i=1}^{k} U_{n_i}(\psi_{1,i}, \psi_{2,i}, A, B, C).$$

From (6.29), (6.45), (6.46) and the considerations above we get the following lemma.

Lemma 6.12. *Assume that χ^2 is not principal, and q is square-free. Remember that $X(n)$ denotes the group of characters modulo n, let $X^-(n)$ denote the group of odd characters modulo n, and recall $m(n, \psi) = \sum_{a=0}^{n-1} a\psi(a)$ and the notations (6.27), (6.44). Then*

$$T_{\chi,q}(A, B, C) = \sum_{(d_1,d_2) \in H} \frac{d_1 d_2 \chi_{d_2}\left(A(d_1)^2\right) \chi_{d_1}\left(C(d_2)^2\right)}{\varphi(d_3)} \Sigma_{d_1,d_2}, \tag{6.47}$$

where

$$\Sigma_{d_1,d_2} = \sum m\left(\frac{q}{d_1}, \chi_1\right) m\left(\frac{q}{d_2}, \chi_2\right) \chi_{1,d_3}(d_1) \chi_{2,d_3}(d_2) \prod_{p \mid d_3} U_p(\chi_p, \chi_{1,p}, A, B, C), \tag{6.48}$$

and the summation here is over characters χ_1, χ_2 satisfying the following conditions:

$$\chi_1 \in X^-\left(\frac{q}{d_1}\right), \ \chi_2 \in X^-\left(\frac{q}{d_2}\right), \ \chi_1\chi_2 = \chi^2.$$

Here, with $\mathbf{Z}_+$ denoting the set of positive integers,

$$H = \{(d_1, d_2) \in \mathbf{Z}_+^2 : \ d_1 d_2 \mid q, \ d_1 d_2 < q, \ (d_1, d_2) = 1\},$$

$d_3 = q/d_1 d_2$, and

$$\chi = \prod_{p \mid q} \chi_p, \ \chi_1 = \prod_{p \mid q} \chi_{1,p}, \ \chi_2 = \prod_{p \mid q} \chi_{2,p},$$

where χ_p, $\chi_{1,p}$, $\chi_{2,p}$ are characters modulo p, and if d is a divisor of q, then

$$\chi_d := \prod_{p|d} \chi_p,\ \chi_{1,d} := \prod_{p|d} \chi_{1,p},\ \chi_{2,d} = \prod_{p|d} \chi_{2,p}.$$

Remark 6.13. The statement of the lemma is not very simple, but our computations become shorter using this lemma. Indeed, for the computation of $G(f_1, \chi)$ for every possible pair of parameters we have to compute $T_{\chi,q}(A, AN, -1)$ for given χ and q, for every pair $0 \le A, N \le q-1$. Using the definition of $T_{\chi,q}$, i.e. formula (6.27), we can do it in around q^4 steps: the number of (A, N) pairs is q^2, and for every pair we have a sum of q^2 terms in (6.27).

For simplicity let us assume that q has boundedly many prime factors. Then for given A and N the sum (6.47) has boundedly many terms, and (6.48) has $O(q)$ terms. So using Lemma 6.12 we can compute $T_{\chi,q}(A, AN, -1)$ for all the pairs $0 \le A, N \le q-1$ in $O(q^3)$ terms (instead of the trivial way of computation in $O(q^4)$ steps mentioned above). Of course, at the beginning we have to compute the building blocks

$$m\left(\frac{q}{d}, \psi\right) \qquad \text{for} \quad d\,|q,\ 1 \le d < q,\ \psi \in X\left(\frac{q}{d}\right)$$

and

$$U_p(\chi_p, \psi, A, B, -1) \qquad \text{for} \quad p\,|q,\ \psi \in X(p), \quad 0 \le A \le p-1, \quad 0 \le B \le 1$$

(it is easy to see from the definition (6.44) that we can indeed assume $0 \le B \le 1$, since the case of a general B can be computed from these cases), and these building blocks can also be computed in $O(q^3)$ steps.

Appendix A

Proof of Lemma 3.4

The proof here represents word for word the proof of Corollary 4.2 in [7] which we use in Chapter 3. We give it in order to keep the presentation of Chapter 3 as self-contained as possible.

Proof of Lemma 3.4. As it was first realized in [4], the value of the function $Z_{I,\omega,q}(0)$ in the Yokoi's case $a = 1$ can be computed using a result of Shintani. This is also the way in the most general case of real quadratic field K that Lemma 3.4 treats.

Let for the matrix $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ with positive elements and $x > 0, y \geq 0$ we define the zeta function

$$\zeta\left(s, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (x,y)\right) := \sum_{n_1,n_2=0}^{\infty} (a(n_1+x)+b(n_2+y))^{-s}(c(n_1+x)+d(n_2+y))^{-s}\,.$$

Then we have

Claim A.1 (Shintani). *For any $a, b, c, d, x > 0$ and $y \geq 0$ the function $\zeta\left(s, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (x,y)\right)$ is absolutely convergent for $\Re s > 1$, extends meromorphically to the whole complex plane and*

$$\zeta\left(s, \begin{pmatrix} a & b \\ c & d \end{pmatrix}, (x,y)\right) = B_1(x)B_1(y) + \frac{1}{4}\left(B_2(x)\left(\frac{c}{d}+\frac{a}{b}\right) + B_2(y)\left(\frac{d}{c}+\frac{b}{a}\right)\right).$$

Note that $A = \left\lceil \frac{tC-D}{q} \right\rceil = \frac{tC-D+q\delta}{q} = tc - d + \delta$ and therefore $0 \leq A \leq t$. Let $\beta = Xe + Ye^*$ for some rationals $X > 0, Y \geq 0$. Write $X = qx + qn_1$ and $Y = qy + qn_2$ for some nonnegative integers n_1 and n_2 and rational numbers $0 < x \leq 1\,, 0 \leq y < 1$ which

can be done in a unique way. Then on the one hand,

$$\beta\bar{\beta} = q^2 \left(e(n_1+x) + e^*(n_2+y)\right)\left(\bar{e}(n_1+x) + \overline{e^*}(n_2+y)\right)$$

and on the other hand we have that $\beta \in I$ and $\beta \equiv \omega \pmod{q}$ hold if and only if $xe + ye^* - (ce+df) \in I$. Therefore

$$Z(s) = \frac{1}{q^{2s}} \sum_{(x,y)\in R(C,D)} \zeta\left(s, \begin{pmatrix} e & e^* \\ \bar{e} & \overline{e^*} \end{pmatrix}, (x,y)\right)$$

where $R(C,D) := \{(x,y) \in \mathbb{Q}^2 : 0 < x \leq 1\,, 0 \leq y < 1\,, xe + ye^* - (ce+df) \in I\}$. Therefore by Claim A.1 we get

$$Z(0) = \sum_{(x,y)\in R(C,D)} \left(B_1(x)B_1(y) + Tr\left(\frac{e}{4e^*}\right)B_2(x) + Tr\left(\frac{e^*}{4e}\right)B_2(y)\right).$$

We observe that for any m, n we have

$$\frac{mf+ne}{q} = \frac{(n-\frac{m}{t})e + \frac{m}{t}e^*}{q}$$

and so it is easy to see that the possibilities for (m,n) having $(x,y) \in R(C,D)$ with

$$(x,y) = \left(\frac{1}{q}\left(n - \frac{m}{t}\right), \frac{1}{q}\frac{m}{t}\right)$$

are

$$m_j = D + jq\,, n_j = C + q\left[1 + \frac{j}{t} - \frac{(tC-D)/q}{t}\right]$$

with an integer $0 \leq j \leq t-1$. This is so because the possible values of m are obviously these t values, and once m is fixed, n is unique. Now

$$0 < 1 + \frac{j}{t} - \frac{(tC-D)/q}{t} < 2, \text{ so } n_j = \begin{cases} C & \text{if } 0 \leq j < A \\ C+q & \text{if } A \leq j < t \end{cases},$$

and therefore

$$Z(0) = \sum_{j=0}^{t-1} \left(B_1(x_j)B_1(y_j) + Tr\left(\frac{e}{4e^*}\right)B_2(x_j) + Tr\left(\frac{e^*}{4e}\right)B_2(y_j)\right)$$

where $y_j = \frac{d+j}{t}$ for $0 \le j < t$ and $x_j = \begin{cases} c - y_j & \text{if } 0 \le j < A \\ c + 1 - y_j & \text{if } A \le j < t \end{cases}$

Now, by (3.8) we have

$$\sum_{j=0}^{t-1} B_2(y_j) = \sum_{j=0}^{t-1} B_2(\frac{d+j}{t}) = \frac{1}{t} B_2(d)$$

and

$$\begin{aligned} \sum_{j=0}^{t-1} B_2(x_j) &= \sum_{j=0}^{A-1} B_2\left(\frac{A-j-\delta}{t}\right) + \sum_{j=A}^{t-1} B_2\left(\frac{t+A-j-\delta}{t}\right) \\ &= \sum_{k=1}^{t} B_2\left(\frac{k-\delta}{t}\right) = \sum_{l=0}^{t-1} B_2\left(\frac{\delta+l}{t}\right) = \frac{1}{t} B_2(\delta)\,. \end{aligned}$$

Now since $B_2(x) + B_2(y) + 2B_1(x)B_1(y) = (x+y-1)^2 - 1/6$ we easily deduce that

$$\sum_{j=0}^{t-1} (B_2(x_j) + B_2(y_j) + 2B_1(x_j)B_1(y_j)) = A(c-1)^2 + (t-A)c^2 - \frac{t}{6}\,.$$

The result then follows from the last four displayed equations, and the facts that

$$Tr\left(\frac{e}{4te^*}\right) - \frac{1}{2t} = Tr\left(\frac{-f}{4e^*}\right) \text{ and } Tr\left(\frac{e^*}{4te}\right) - \frac{1}{2t} = Tr\left(\frac{f}{4e}\right)\,.$$

□

Bibliography

[1] A. Baker, *Linear forms in the logarithms of algebraic numbers*, Mathematika 13 (1966), 204–216

[2] A. Balog and K. Ono, *Elements of class groups and Shafarevich-Tate groups of elliptic curves*, Duke Math. J. (2003), no. 1, 35–63

[3] J. Beck, *Diophantine approximation and quadratic fields*, 55–93, in: Number Theory, Eds.: György, Pethö, Sós, Walter de Gruyter, 1998

[4] A. Biró, *Yokoi's conjecture*, Acta Arith. 106 (2003), no. 1, 85–104

[5] A. Biró, *Chowla's conjecture*, Acta Arith. 107 (2003), no. 2, 179–194

[6] A. Biró, *On the class number one problem for some special real quadratic fields*, Proc. of the 2003 Nagoya Conference "On Yokoi-Chowla Conjecture and Related Problems", Furukawa Total Pr. Co., 2004, 1–9

[7] A. Biró, A. Granville, *Zeta function for ideal classes in real quadratic fields, at s=0*, to appear in J. Number Theory

[8] C. Breuil, B. Conrad, F. Diamond, R. Taylor, *On the modularity of elliptic curves over $\mathbb{Q}$: wild 3-adic exercises*, J. Amer. Math. Soc. 14 (2001), 843–939

[9] T. D. Browning, *Power-free values of polynomials*, Arch. Math. (Basel) 96 (2011), no. 2, 139–150

[10] J. Brüdern, K. Kawada, T. D. Wooley, *Additive representation in thin sequences, II: The binary Goldbach problem*, Mathematica 47 (2000), no. 1-2, 117–125

[11] D. A. Buell, *Class groups of quadratic fields*, Math. Comp. 135 (1976), 610–623

[12] J. P. Buhler, B. H. Gross, D. B. Zagier, *On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3*, Math. Comp. 44 (1985), 473–481

[13] D. Byeon, H. Kim, *Class number 1 criteria for real quadratic fields of Richaud-Degert type.*, J. Number Theory 57 (1996), no. 2, 328–339

[14] D. Byeon, M. Kim, J. Lee, *Mollin's conjecture*, Acta Arith. 126 (2007), 99–114

[15] D. Byeon, Sh. Lee, *Divisibility of class numbers of imaginary quadratic fields whose discriminant has only two prime factors*, Proc. Japan Acad. 84 (2008), Ser. A, 8–10

[16] H. Davenport, *Multiplicative Number Theory*, Third Ed., Springer, 2000

[17] G. Degert, *Über die Bestimmung der Grundeinheit gewisser reellquadratischer Zhalkörper*, Abh. Math. Sem. Univ. Hamburg 22 (1958), 92–97

[18] D. Goldfeld, *The class number of quadratic fields and the conjectures of Birch and Swinnerton-Dyer*, Ann. Scuola Norm. Sup. Pisa 3 (1976), no. 4, 623–663

[19] D. Goldfeld, *The Gauss class number problem for imaginary quadratic fields* , in: Heegner Points and Rankin L-Series , Eds.: Darmon, Zhang , Cambridge Univ. Press, 2004

[20] F. Gouvẽa and B. Mazur, *The square-free sieve and the rank of elliptic curves*, J. Amer. Math. Soc. 4 (1991), 1–23

[21] G. Greaves, *Power-free values of binary forms*, Quart. J. Math. 43 (1992), 45–65.

[22] B. H. Gross and D. B. Zagier, *Heegner points and derivatives of L-series* , Invent. math. 84 (1986) , 225–320

[23] G. H. Hardy, E. M. Wright, *An Introduction to the Theory of Numbers*, Oxford Univ. Press, 1979

[24] E. Hecke, *Lectures on the Theory of Algebraic Numbers*, Springer, 1981

[25] K.Heegner, *Diophantische Analysis und Modulfunktionen*, Math. Z. 56 (1952), 227–253

[26] H. Helfgott, *Power-free values, large deviations and integer points on irrational curves*, J. Théor. Nombres Bordeaux 19 (2007), 433–472

[27] M. Hindry, J. H. Silverman, *The Canonical Height and integral points on elliptic curves*, Invent. Math. 93 (1988), 419–450

[28] C. Hooley, *On the power-free values of polynomials*, Mathematika 14 (1967), 21–26

[29] C. Hooley, *On power-free numbers and polynomials, II*, J. reine angew. Math. 295 (1977), 1–21

[30] C. Hooley, *On the power-free values of polynomials in two variables*, 235–266, in: Analytic number theory, Cambridge Univ. Press, 2009

[31] H. Iwaniec, E. Kowalski, *Analytic Number Theory*, Amer. Math. Soc., Providence, RI, 2004

[32] V. A. Kolyvagin, *The Mordell-Weil and Shafarevich-Tate groups for Weil elliptic curves*, Izv. Akad. Nauk SSSR Ser. Mat.(6) 52 (1988), 1154-1180

[33] V. A. Kolyvagin, *On the Mordell-Weil group and the Shafarevich-Tate group of modular elliptic curves*, Proc. of the ICM, Kyoto, Japan, 1990, 429–436

[34] S. Lang, *Elliptic curves: Diophantine Analysis* , Springer, 1978

[35] K. Lapkova, *Class number one problem for real quadratic fields of certain type*, to appear in Acta Arith.

[36] K. Lapkova, *Divisibility of class numbers of imaginary quadratic fields whose discriminant has only three prime factors*, to appear in Acta Mathem. Hung.

[37] K. Lapkova, *Effective lower bound for the class number of a certain family of real quadratic fields*, submitted

[38] J. Lee, *The complete determination of wide Richaud-Degert types which are not 5 modulo 8 with class number one*, Acta Arith. 140 (2009), no. 1, 1–29

[39] R. A. Mollin, *Necessary and sufficient conditions for the class number of real quadratic field to be one, and a conjecture of S. Chowla*, Proc. Amer. Math. Soc. 102 (1988), 17–21

[40] R. A. Mollin, H. C. Williams, *Solution of the class number one problem for real quadratic fields of extended Richaud-Degert type (with one possible exception)*, Number theory (Banff, AB, 1988), 417–425, de Gruyter, Berlin, 1990.

[41] R. A. Mollin, L.-C. Zhang, P. Kemp, *A lower bound for the class number of a real quadratic field of ERD type*, Canad. Math. Bull. Vol. 37 (1), 1994, 90–96

[42] H. Nakazato, *Heegner points on modular elliptic curves*, Proc. Japan Acad. 72 (1996), Ser. A, 223–225

[43] F. Nemenzo, H. Wada, *An Elementary Proof of Gauss Genus Theorem*, Proc. Japan Acad. 58, Ser. A (1992), 94–95

[44] J. Oesterle, *Le probleme de Gauss sur le nombre de classes*, Enseign. Math. 34 (1988), 43–67

[45] A. Schinzel, *On some problems of the arithmetical theory of continued fractions*, Acta Arith. 6 (1960-1961), 393–413

[46] J. Silverman , *The Arithmetic of Elliptic Curves* , Second Ed., Springer, 2010

[47] J. Silverman , *Computing heights on elliptic curves*, Math. Comp. 51 (1988), 339–358

[48] K. Soundararajan, *Divisibility of class numbers of imaginary quadratic fields*, J. London Math. Soc. (2) 61 (2000), no. 3, 681–690

[49] W. A. Stein et al., *Sage Mathematics Software (Version 4.8)*, The Sage Development Team, 2012, `http://www.sagemath.org`.

[50] R. Taylor, A. Wiles, *Ring-theoretic properties of certain Hecke algebras*, Ann. of Math.(2) 141 (1995), 553–572

[51] R. C. Vaughan, *The Hardy-Littlewood Method*, Cambridge Tracts in Math. 80, Cambridge Univ. Press, 1981

[52] L. C. Washington, *Introduction to Cyclotomic Fields*, Springer, 1996

[53] A. Weil, *Jacobi sums as "grössencharaktere"*, Trans. Amer. Math. Soc. 7 (1952), 487–495

[54] A. Wiles, *Modular elliptic curves and Fermat's last theorem*, Ann. of Math. (2) 141 (1995), 443–551