UNIVERSITÀ DEGLI STUDI DI PADOVA

Dipartimento di Matematica "Tullio Levi Civita"

Corso di Laurea Magistrale in Matematica

On the size of the fundamental unit of real quadratic fields

Referente:
Prof. Marco Andrea Garuti

Candidato:
Francesco Stocco
n. m. 1205558

15 Luglio - Anno Accademico 2019/2020

To Beatrice

Introduction

In 1801, Gauss presented several conjectures in his *Disquisitiones Arithmeticae* [11]. In particular, articles 303 and 304 are focused on class numbers in the context of binary quadratic forms. Today, we can rephrase these conjectures in the language of quadratic fields.

In article 303 Gauss deals with complex quadratic fields, i.e. fields of the shape $\mathbb{Q}(\sqrt{d})$ for $d < 0$, and surmises that the cardinality of the ideal class group $h(d) \to \infty$ as $d \to -\infty$. Moreover, he provides a list of complex quadratic fields of class number one, which supposes to be exhaustive. The first fact was proven by Heilbronn in 1934, see [13]. In the same year Heilbronn and Linfoot [14] were able to conclude that beside the nine known complex quadratic fields with class number one, there is at most another one. The nonexistence of the tenth field was guaranteed by Baker [1] and Stark [22].

On the other side, in article 304 Gauss conjectures that there are infinitely many real quadratic fields with class number one. This is still an open problem. However, the Cohen-Lenstra heuristics [2] suggests that the probability a_p of a real quadratic field having class number divisible by an odd prime p is

$$a_p = 1 - \prod_{j=2}^{\infty}\Big(1 - \frac{1}{p^j}\Big).$$

They predict that for real quadratic fields the probability of the odd part of the class group being the identity is

$$\prod_{p\geq 3}(1 - a_p) = 0.7544598...$$

This implies that the above value should be the probability that $h(d) = 1$ for quadratic fields such that the 2-part of the class group is trivial.

To conclude the theorem on primes in arithmetic progression, Dirichlet introduced L-functions and discovered the correspondence between real primitive characters and quadratic fields. This allowed him to produce his class number formula which establishes a relation between the ideal class number and the fundamental unit of a quadratic field. The latter is going to be our main interest.

This manuscript follows closely the paper by Étienne Fouvry and Florent Jouve *A positive density of fundamental discriminants with large regulator*, see [7]. The aim of this work is to develop the results contained therein to make them more accessible for an interested reader.

In Chapter 1 we present some asymptotic estimates of arithmetic functions, which play a central role in the subsequent discussions. We introduce the fundamental unit $\varepsilon(D)$ of a quadratic field and the fundamental solution ε_d to the Pell's equation. Roughly speaking, let D be a positive fundamental discriminant, then the group of invertible elements of the ring of integers of the real quadratic field $\mathbb{Q}(\sqrt{D})$ is essentially generated by $\varepsilon(D)$.

Similarly, let d be a nonsquare positive integer, then the solutions of the Pell's equation $T^2 - dU^2 = 1$ are completely determined by ε_d.

Chapter 2 is focused on proving the class number formula in the quadratic case. Usually, such result is deduced from the study of equivalence classes of binary quadratic forms since historically this has been the first approach, see [[23], Ch. 5]. However, we try to give a direct argument avoiding the treatment of quadratic forms.

It is widely believed that most of the time $\varepsilon(D)$, ε_d are huge compared to the size of D or d and this fact is confirmed by numerical evidence. In this direction, Fouvry and Jouve have proved that there is a positive density of positive fundamental discriminants D such that the fundamental unit $\varepsilon(D)$ of the field $\mathbb{Q}(\sqrt{D})$ is essentially greater than D^3. It is noteworthy that the fundamental discriminants with fundamental unit of large size exhibited by the two authors satisfy a very particular divisibility condition, which is pointed out in Chapter 3 while we reserve Chapter 4 for the proof of the main result.

It is well known that any information on the size of $\varepsilon(D)$ can be interpreted in terms of the ordinary class number $h(D)$ of the field $\mathbb{Q}(\sqrt{D})$. Indeed, Chapter 5 is devoted to show an estimate of the class number average size applying the theory viewed in the fourth chapter.

In the lines of the main result, we spend the last chapter to introduce a more general conjecture due to C. Hooley, see [[16], Conj. 1].

Acknowledgments

First of all, I would like to thank the Algant Bordeaux coordinator Prof. Dajano Tossici for supporting us and being always available during this last year. I want also to express my gratitude to my supervisor Prof. Florent Jouve, who has introduced me to the field of analytic number theory and who has been the best mentor I could ever have wished for being always on my side whenever I got stuck. Despite the distance from my country, I felt at home thanks to their professional and human sensitivity.

Secondly, I am glad to Prof. Maurizio Cailotto and Prof. Alberto Tonolo, of Padua's university, for their helpfulness and sincerity. I must also mention my fellow students and friends Marta and Luigi. They have encouraged me in the challenging experience of university studies and they have shown me the best way I know to approach mathematical issues.

Finally, I thank all members of the "Condorcet Italian family" for sharing with me this time away from my parents and making every day enjoyable, in particular I want to say a word on Greta for taking care of me along these months.

Contents

Chapter 1

Preliminaries

1.1 Arithmetic functions

Definition 1.1. An *arithmetic function* is a map $f:\ \mathbb{N}\setminus\{0\}\longrightarrow\mathbb{C}$.
An arithmetic function f is said to be *multiplicative* (resp. *additive*) if:

$$f(nm)=f(n)f(m)\quad (f(nm)=f(n)+f(m))$$

for all n,m such that $(n,m)=1$.
Moreover, we say f is *completely multiplicative* (resp. *completely additive*) if the same holds in the case $(n,m)\neq 1$.

Example 1.2. Now we recall some examples needed in this work:

- The *Moebius function* is a multiplicative arithmetic function defined as follows:

$$\begin{aligned}\mu:\ \mathbb{N}\setminus\{0\}&\longrightarrow\{-1,0,1\}\\ 1&\longmapsto 1\\ n&\longmapsto(-1)^k\ \text{ if } n \text{ is the product of } k \text{ distinct primes}\\ n&\longmapsto 0\qquad\ \text{ if } n \text{ is not squarefree.}\end{aligned}$$

- The *Euler totient function* φ is a multiplicative arithmetic function defined as follows:

$$\begin{aligned}\varphi:\ \mathbb{N}\setminus\{0\}&\longrightarrow\mathbb{N}\\ n&\longmapsto\#\{m\in\{0,\dots,n-1\}:(m,n)=1\}.\end{aligned}$$

  In particular, let $n=p_1^{r_1}\dots p_t^{r_t}$ be the prime factorization of n, then

$$\varphi(n)=\varphi(p_1^{r_1}\dots p_t^{r_t})=\varphi(p_1^{r_1})\dots\varphi(p_t^{r_t})=(p_1^{r_1}-p_1^{r_1-1})\dots(p_t^{r_t}-p_t^{r_t-1}).$$

- The *Prime omega function* is an additive arithmetic function defined as follows:

$$\begin{aligned}\omega:\ \mathbb{N}\setminus\{0\}&\longrightarrow\mathbb{N}\\ n&\longmapsto\sum_{\substack{p|n\\ p\,prime}}1.\end{aligned}$$

  Let $\kappa\in\mathbb{R}^+$, ω gives rise to a multiplicative arithmetic function:

$$\begin{aligned}\kappa^\omega:\ \mathbb{N}\setminus\{0\}&\longrightarrow\mathbb{R}\\ n&\longmapsto\kappa^{\omega(n)}.\end{aligned}$$

- The *Divisor function* is a multiplicative function defined as follows:

$$\begin{aligned}\tau:\ \mathbb{N}\setminus\{0\} &\longrightarrow \mathbb{N}\\ n &\longmapsto \sum_{d\mid n} 1.\end{aligned}$$

  (Observe that this function is often denoted also by σ or d.)
  Notice that for all positive integers n

$$2^{\omega(n)} \leq \tau(n). \tag{1.1}$$

- Let K be a number field and $\mathcal{O}_K$ be its ring of integers. We can consider the arithmetic function F defined as follows:

$$\begin{aligned}F:\ \mathbb{N}\setminus\{0\} &\longrightarrow \mathbb{N}\\ n &\longmapsto \#\mathfrak{I}(n)\end{aligned}$$

  where $\mathfrak{I}(n) := \{\mathfrak{a} \trianglelefteq \mathcal{O}_K : N(\mathfrak{a}) = n\}$ and $N(\mathfrak{a})$ denotes the norm of the ideal $\mathfrak{a}$.

Lemma 1.3. *The arithmetic function F is multiplicative.*

Proof. We want to prove that if $(a,b)=1$ then the following map is bijective.

$$\begin{aligned}\mathfrak{I}(a)\times\mathfrak{I}(b) &\longrightarrow \mathfrak{I}(ab)\\ (\mathfrak{a},\mathfrak{b}) &\longmapsto \mathfrak{a}\mathfrak{b}\end{aligned}$$

First we observe that the map is well defined by multiplicativity of N. If $\mathfrak{a}$ is of norm a and $\mathfrak{b}$ is of norm b, then

$$N(\mathfrak{a}\mathfrak{b}) = N(\mathfrak{a})N(\mathfrak{b}) = ab$$

and so $\mathfrak{a}\mathfrak{b}$ is in the set $\mathfrak{I}(ab)$.
The second step is to prove the injectivity. This follows from the coprimality of a,b. Indeed if a and b are coprime as integers then (a) and (b) are coprime as ideals. The ideals of $\mathfrak{I}(a)$ divide (a) and the ideals of $\mathfrak{I}(b)$ divide (b), hence the ideals of $\mathfrak{I}(a)$ are coprime with the ideals of $\mathfrak{I}(b)$. Therefore if $\mathfrak{a},\mathfrak{a}' \in \mathfrak{I}(a)$ and $\mathfrak{b},\mathfrak{b}' \in \mathfrak{I}(b)$ are such that $\mathfrak{a}\mathfrak{b} = \mathfrak{a}'\mathfrak{b}'$ then $\mathfrak{a}$ divides $\mathfrak{a}'\mathfrak{b}'$ and $\mathfrak{a}'$ divides $\mathfrak{a}\mathfrak{b}$. Now it's clear that the unique possibility is that $\mathfrak{a} = \mathfrak{a}'$ and $\mathfrak{b} = \mathfrak{b}'$.
The last step is to prove the surjectivity. Let $\mathfrak{c}$ be an ideal in $\mathfrak{I}(ab)$. Set

$$\mathfrak{a}_1 := (\mathfrak{c},(a)) \qquad \mathfrak{b}_1 := (\mathfrak{c},(b)).$$

We have

$$\mathfrak{a}_1\mathfrak{b}_1 = (\mathfrak{c}^2, a\mathfrak{c}, b\mathfrak{c}, (ab)) = \mathfrak{c}(\mathfrak{c},(a),(b),\frac{(ab)}{\mathfrak{c}})$$

and the coprimality of (a) and (b) implies

$$\mathfrak{a}_1\mathfrak{b}_1 = \mathfrak{c}.$$

Now we have that $N(\mathfrak{a}_1)$ divides a^2 by definition of $\mathfrak{a}_1$ and in the same way $N(\mathfrak{b}_1)$ divides b^2. From

$$N(\mathfrak{a}_1)N(\mathfrak{b}_1) = ab, \qquad (a,b)=1$$

we conclude the proof. □

Lemma 1.4. *Let f be an arithmetic function. If f is multiplicative, then so is the arithmetic function g defined by*

$$g(n) = \sum_{d|n} f(d).$$

Proof. Let n, n' be positive integers such that $(n, n') = 1$. We see

$$g(nn') = \sum_{d|nn'} f(d) = \sum_{\substack{c|n \\ c'|n'}} f(cc') = \sum_{\substack{c|n \\ c'|n'}} f(c)f(c') = g(n)g(n'),$$

where in the second equality we've used $(n, n') = 1$ and in the third one $(c, c') = 1$ together with the assumption that f is multiplicative. □

1.1.1 Some average sizes of arithmetic functions

Lemma 1.5. *Let n be a positive integer, then*

$$\sum_{d|n} \mu(d) = \begin{cases} 1 & if\, n = 1 \\ 0 & if\, n > 1. \end{cases}$$

Proof. If $n = 1$,

$$\sum_{d|1} \mu(d) = \mu(1) = 1.$$

If $n > 1$ then let $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$ be its prime factorization. In $\sum_{d|n} \mu(d)$, the divisors such that $\mu(d) \neq 0$ are squarefree:

$$\begin{aligned}\sum_{d|n} \mu(d) &= \mu(1) + \mu(p_1) + \cdots + \mu(p_k) + \mu(p_1p_2) + \cdots + \mu(p_{k-1}p_k) + \cdots + \mu(p_1p_2 \dots p_k) \\ &= \underbrace{\binom{k}{0}(-1)^0}_{=\mu(1)=1} + \binom{k}{1}(-1) + \binom{k}{2}(-1)^2 + \cdots + \binom{k}{k}(-1)^k \\ &= \sum_{n=0}^{k} \binom{k}{n}(-1)^n \underbrace{=}_{Newton's\, formula} (1-1)^k = 0.\end{aligned}$$

□

Remark 1.6. The above result proves that μ is the inverse of

$$\begin{aligned} \mathbb{1} :\ \mathbb{N} \setminus \{0\} &\longrightarrow \{1\} \\ n &\longmapsto 1 \end{aligned}$$

in terms of Dirichlet's convolution of arithmetic functions, see [[15], Ch. 1].

Corollary 1.7. *Let n be a positive integer, then*

$$\mu^2(n) = \sum_{d^2|n} \mu(d).$$

Proof. If n is squarefree then $\mu^2(n) = 1$. The unique possibility for d s.t. $d^2|n$ is 1, so $\sum_{d^2|n} \mu(d) = \mu(1) = 1$.
If n is not squarefree then $\mu^2(n) = 0$. We can factorize n as $n = \alpha^2 m$, where $\alpha \neq 1$ and m is squarefree. Now if $d^2|n$ then $d|\alpha$ and conversely if $d|\alpha$ then $d^2|n$, therefore by the previous lemma:

$$\sum_{d^2|n} \mu(d) = \sum_{d|\alpha} \mu(d) = 0.$$

□

Lemma 1.8. *Let n be a positive integer, then*

$$\varphi(n) = \sum_{d|n} \mu(d) \frac{n}{d} = n \sum_{d|n} \frac{\mu(d)}{d}.$$

Proof. Lemma 1.4 implies that $\sum_{d|\cdot} \frac{\mu(d)}{d}$ is multiplicative since $\frac{\mu}{\mathrm{Id}}$ is so. Thus, to prove the formula is enough to check it on powers of prime numbers. Let p be a prime number and $k \in \mathbb{N}^*$, then

$$\frac{\varphi(p^k)}{p^k} = \frac{p^k - p^{k-1}}{p^k} = 1 - \frac{1}{p}$$
$$\sum_{d|p^k} \frac{\mu(d)}{d} = 1 - \frac{1}{p} + 0 + \cdots + 0 = 1 - \frac{1}{p}.$$

□

Remark 1.9. The above result can be restated as $\varphi = \mu * \mathrm{Id}$, where $*$ is the Dirichlet convolution of arithmetic functions. Notice that following the same lines of this proof we can present a different and simpler strategy to show also Lemma 1.5.

Corollary 1.10. *Let n, m be positive integers, then*

$$\sum_{\substack{k \leq n \\ (k,m)=1}} 1 = n \frac{\varphi(m)}{m} + O(2^{\omega(m)}).$$

Proof. Using Lemma 1.5,

$$\begin{aligned} \sum_{\substack{k \leq n \\ (k,m)=1}} 1 &= \sum_{k \leq n} \sum_{d|(k,m)} \mu(d) = \sum_{d|m} \mu(d) \sum_{\substack{k \leq n \\ d|k}} 1 \\ &= \sum_{d|m} \mu(d) \left\lfloor \frac{n}{d} \right\rfloor = n \sum_{d|m} \frac{\mu(d)}{d} + \sum_{d|m} \mu(d) c_d, \end{aligned}$$

where $|c_d| < 1$. Notice that

$$\left| \sum_{d|m} \mu(d) c_d \right| \leq \sum_{d|m} \mu^2(d) |c_d| < \sum_{d|m} \mu^2(d) \underbrace{=}_{\substack{\text{we'll see it later} \\ \text{Lemma 1.15}}} 2^{\omega(m)}$$

and hence we conclude using the above lemma. □

Lemma 1.11. *Let x be a positive real number greater than 1 and $k,l \in \mathbb{Z}_{\geq 1}$ such that $(k,l)=1$. Let $Q(x,k,l)$ be the cardinality of the set of squarefree positive integers $m \leq x$ and $m \equiv l \mod k$. Then we have*

$$Q(x,k,l) = \frac{x}{k}\frac{1}{\zeta(2)} \prod_{\substack{p|k \\ p\, prime}} \left(1-\frac{1}{p^2}\right)^{-1} + O(x^{\frac{1}{2}})$$

where the implied constant does not depend on k,l and ζ is the Riemann zeta function.

Proof. Using Corollary 1.7, we get

$$Q(x,k,l) = \sum_{\substack{m \leq x \\ m \equiv l \mod k}} \mu^2(m) = \sum_{\substack{m \leq x \\ m \equiv l \mod k}} \sum_{d^2|m} \mu(d).$$

In order to switch the two summations observe that

$$(l,k)=1 \Rightarrow (m,k)=1 \Rightarrow (d,k)=1$$

and hence

$$\begin{aligned} Q(x,k,l) &= \sum_{\substack{d \leq x^{\frac{1}{2}} \\ (d,k)=1}} \sum_{\substack{n \leq \frac{x}{d^2} \\ d^2 n \equiv l\,(k)}} \mu(d) = \sum_{\substack{d \leq x^{\frac{1}{2}} \\ (d,k)=1}} \mu(d) \sum_{\substack{n \leq \frac{x}{d^2} \\ d^2 n \equiv l\,(k)}} 1 \\ &= \sum_{\substack{d \leq x^{\frac{1}{2}} \\ (d,k)=1}} \mu(d)\left(\frac{x}{kd^2}+O(1)\right) = \frac{x}{k} \sum_{\substack{d \leq x^{\frac{1}{2}} \\ (d,k)=1}} \frac{\mu(d)}{d^2} + O(x^{\frac{1}{2}}). \end{aligned}$$

Observe now that

$$\sum_{\substack{d \leq x^{\frac{1}{2}} \\ (d,k)=1}} \frac{\mu(d)}{d^2} = \sum_{\substack{d=1 \\ (d,k)=1}}^{\infty} \frac{\mu(d)}{d^2} + O\left(\sum_{d > x^{\frac{1}{2}}} \frac{1}{d^2}\right) = \sum_{\substack{d=1 \\ (d,k)=1}}^{\infty} \frac{\mu(d)}{d^2} + O(x^{-\frac{1}{2}}),$$

$$\sum_{\substack{d=1 \\ (d,k)=1}}^{\infty} \frac{\mu(d)}{d^2} = \prod_{p\, prime}\left(1-\frac{1}{p^2}\right) \prod_{\substack{p|k \\ p\, prime}} \left(1-\frac{1}{p^2}\right)^{-1} = \frac{1}{\zeta(2)} \prod_{\substack{p|k \\ p\, prime}} \left(1-\frac{1}{p^2}\right)^{-1}.$$

Therefore

$$Q(x,k,l) = \frac{x}{k}\frac{1}{\zeta(2)} \prod_{\substack{p|k \\ p\, prime}} \left(1-\frac{1}{p^2}\right)^{-1} + O(x^{\frac{1}{2}}) + O(\frac{x}{k}x^{-\frac{1}{2}})$$

which concludes the proof. □

Remark 1.12. Let's now compute the above formula in the particular case $k=4$ and $l=3$, we will need it later. Recall that $\zeta(2) = \sum \frac{1}{n^2} = \frac{\pi^2}{6}$, then

$$Q(x,4,3) = \frac{x}{4}(1-4^{-1})^{-1}\frac{6}{\pi^2} + O(x^{\frac{1}{2}}) = \frac{2}{\pi^2}x + O(x^{\frac{1}{2}}).$$

Moreover, the following holds:

$$\begin{aligned} \sum_{m \leq x} \mu^2(m) &= Q(x,4,3) + Q(x,4,1) + Q(x,4,2) \\ &= Q(x,4,2) + \frac{4}{\pi^2}x + O(x^{\frac{1}{2}}). \end{aligned}$$

To get an asymptotic estimate of $Q(x,4,2)$ we cannot use the previous result since $(2,4)\neq 1$ but trivially $Q(x,2,4)\leq x$, this allows to conclude

$$\sum_{m\leq x}\mu^2(m)=O(x).$$

However, one can be more explicit and indeed

$$\sum_{m\leq x}\mu^2(m)=\frac{6}{\pi^2}x+O(x^{\frac{1}{2}}),$$

see [[15], Th. 2.18].

Corollary 1.13. *Let t be an odd number then*

$$\sum_{\substack{m\leq x\\ m\equiv 3\,(4)\\ (m,t)=1}}\mu^2(m)=\frac{2}{\pi^2}\prod_{\substack{p|t\\ p\,prime}}\left(1+\frac{1}{p}\right)^{-1}x+O(2^{\omega(t)}x^{\frac{1}{2}}).$$

Proof. Applying Corollary 1.10 together with the fact $(4,t)=1$,

$$\begin{aligned}\sum_{\substack{m\leq x\\ m\equiv 3\,(4)\\ (m,t)=1}}\mu^2(m)&=\sum_{\substack{m\leq x\\ m\equiv 3\,(4)\\ (m,t)=1}}\sum_{d^2|m}\mu(d)=\sum_{\substack{d\leq x^{\frac{1}{2}}\\ (d,4)=1\\ (d,t)=1}}\sum_{\substack{n\leq\frac{x}{d^2}\\ d^2n\equiv 3\,(4)\\ (n,t)=1}}\mu(d)\\ &=\sum_{\substack{d\leq x^{\frac{1}{2}}\\ (d,4)=1\\ (d,t)=1}}\mu(d)\left(\frac{x}{4d^2}\frac{\varphi(t)}{t}+O(2^{\omega(t)})\right)=\frac{\varphi(t)}{t}\frac{x}{4}\sum_{\substack{d\leq x^{\frac{1}{2}}\\ (d,4)=1\\ (d,t)=1}}\frac{\mu(d)}{d^2}+O(2^{\omega(t)}x^{\frac{1}{2}}).\end{aligned}$$

Similarly to what we've done in the previous proof we have that

$$\begin{aligned}\sum_{\substack{d\leq x^{\frac{1}{2}}\\ (d,4)=1\\ (d,t)=1}}\frac{\mu(d)}{d^2}&=\prod_{p\,prime}\left(1-\frac{1}{p^2}\right)\prod_{\substack{p|4t\\ p\,prime}}\left(1-\frac{1}{p^2}\right)^{-1}+O(x^{-\frac{1}{2}})\\ &\underbrace{=}_{(4,t)=1}\frac{6}{\pi^2}\prod_{\substack{p|4\\ p\,prime}}\left(1-\frac{1}{p^2}\right)^{-1}\prod_{\substack{p|t\\ p\,prime}}\left(1-\frac{1}{p^2}\right)^{-1}+O(x^{-\frac{1}{2}})\\ &=\frac{4}{3}\frac{6}{\pi^2}\prod_{\substack{p|t\\ p\,prime}}\left(1-\frac{1}{p^2}\right)^{-1}+O(x^{-\frac{1}{2}})\end{aligned}$$

and hence

$$\sum_{\substack{m\leq x\\ m\equiv 3\,(4)\\ (m,t)=1}}\mu^2(m)=\frac{2}{\pi^2}\frac{\varphi(t)}{t}\prod_{\substack{p|t\\ p\,prime}}\left(1-\frac{1}{p^2}\right)^{-1}x+O(2^{\omega(t)}x^{\frac{1}{2}}).$$

To conclude, let $t = p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}$ be its prime factorization and observe that

$$\begin{aligned}\frac{\varphi(t)}{t} \prod_{\substack{p \mid t \\ p\, prime}} \left(1 - \frac{1}{p^2}\right)^{-1} &= \frac{p_1^{a_1}\left(1-\frac{1}{p_1}\right) \dots p_n^{a_n}\left(1-\frac{1}{p_n}\right)}{p_1^{a_1} p_2^{a_2} \dots p_n^{a_n}} \prod_{i=1}^{n} \left(\left(1-\frac{1}{p_i}\right)\left(1+\frac{1}{p_i}\right)\right)^{-1} \\ &= \prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right) \prod_{i=1}^{n}\left(1-\frac{1}{p_i}\right)^{-1} \prod_{i=1}^{n}\left(1+\frac{1}{p_i}\right)^{-1} \\ &= \prod_{i=1}^{n}\left(1+\frac{1}{p_i}\right)^{-1}.\end{aligned}$$

□

Remark 1.14. Notice that in the previous proof the important thing is that t and $k = 4$ are coprime. Hence we could restate the previous corollary in a more general setting requiring only $(t, k) = 1$.

Lemma 1.15. *Let n be any positive natural number, then*

$$2^{\omega(n)} = \sum_{d \mid n} \mu^2(d),$$

i.e. $2^{\omega} = \mu^2 * \mathbb{1}$.

Proof. If $n = 1$ we have

$$\omega(1) = 0 \implies 2^{\omega(1)} = 1$$

and

$$\sum_{d \mid 1} \mu^2(d) = \mu^2(1) = 1.$$

If $n > 1$ let $n = p_1^{a_1} p_2^{a_2} \dots p_m^{a_m}$ be its prime factorization, we have

$$2^{\omega(n)} = \#\mathcal{P}(\{p_1, \dots, p_m\})$$

and notice that there's a bijective map

$$\begin{aligned}\mathcal{P}(\{p_1, \dots, p_m\}) &\longrightarrow \{\text{squarefree divisors of } n\} \\ \mathcal{S} &\longmapsto \prod_{p \in \mathcal{S}} p.\end{aligned}$$

We are done since clearly

$$\#\{\text{squarefree divisors of } n\} = \sum_{d \mid n} \mu^2(d).$$

□

Remark 1.16. Notice that, also in this case, we can provide an easier proof of Lemma 1.15 using the multiplicativity of the involved functions and computing their values at prime powers.

Lemma 1.17. *Let n be a positive integer, then*

1.
$$\sum_{d|n} 2^{\omega(d)} = \tau(n^2)$$
i.e. $\tau^{(2)} = 2^{\omega} * \mathbb{1}$*, where* $\tau^{(2)}(n) := \tau(n^2)$*;*

2. assuming $\mu^2(n) = 1$*, we have also*
$$\tau(n^2) = 3^{\omega(n)}.$$

Proof. Notice that $\tau^{(2)}$ is multiplicative since τ is so and hence, as we did in Lemma 1.8, it's enough to check equalities on powers of prime numbers.

1. Let p be a prime number and k any positive integer, then
$$\sum_{d|p^k} 2^{\omega(d)} = 2^{\omega(1)} + 2^{\omega(p)} + \cdots + 2^{\omega(p^k)} = 1 + 2 + \cdots + 2 = 2k + 1$$
$$\tau(p^{2k}) = \sum_{d|p^{2k}} 1 = 2k + 1.$$

2. In the second case we have to work only with squarefree integers and so we consider just a prime integer p.
$$\tau(p^2) = \sum_{d|p^2} 1 = 3$$
$$3^{\omega(p)} = 3^1 = 3.$$

□

We recall without proof the *Summation by part formula.* A discussion of it can be found on [[15], Ch. 2].

Theorem 1.18. *Let* $a : \mathbb{N}\backslash\{0\} \to \mathbb{C}$ *be an arithmetic function, let* $x \geq 1$ *be real number and* $f : [1, x] \to \mathbb{C}$ *a function with continuous derivative on* $[1, x]$*. Then we have*
$$\sum_{n\leq x} a(n)f(n) = A(x)f(x) - \int_1^x A(t)f'(t)dt$$
where $A(x) = \sum_{n\leq x} a(n)$*.*

Lemma 1.19. *Let* x *be a positive real number greater than* 1*, then*
$$\sum_{n\leq x} 2^{\omega(n)} = \frac{6}{\pi^2} x \log x + O(x).$$

Proof. Applying Lemma 1.15,
$$\sum_{n\leq x} 2^{\omega(n)} = \sum_{n\leq x}\sum_{d|n} \mu^2(d) = \sum_{d\leq x} \mu^2(d) \sum_{\substack{n\leq x\\ d|n}} 1$$
$$= \sum_{d\leq x} \mu^2(d)\Big(\frac{x}{d} + O(1)\Big) = x \sum_{d\leq x} \frac{\mu^2(d)}{d} + O(x).$$

Using Summation by part formula and Remark 1.12,

$$\begin{aligned}\sum_{d\leq x}\frac{\mu^2(d)}{d} &= \frac{1}{x}\sum_{d\leq x}\mu^2(d) + \int_1^x \left(\sum_{d\leq t}\mu^2(d)\right)\frac{1}{t^2}\,dt \\ &= \int_1^x \frac{6}{\pi^2}\frac{1}{t}\,dt + O\left(\int_1^x \frac{t^{\frac{1}{2}}}{t^2}\,dt\right) + O(1) \\ &= \frac{6}{\pi^2}\log x + O(x^{-\frac{1}{2}}) + O(1).\end{aligned}$$

Substituting this expression in the previous one, we conclude the proof. □

Corollary 1.20. *Let x be a positive real number greater than* 1*, then*

$$\sum_{n\leq x}\frac{2^{\omega(n)}}{n} = \frac{3}{\pi^2}\log^2 x + O(\log x).$$

Proof. Applying Th. 1.18 and the above lemma,

$$\begin{aligned}\sum_{n\leq x}\frac{2^{\omega(n)}}{n} &= \frac{1}{x}\sum_{n\leq x}2^{\omega(n)} + \int_1^x \left(\sum_{n\leq t}2^{\omega(n)}\right)\frac{1}{t^2}\,dt \\ &= \int_1^x \frac{6}{\pi^2}\frac{\log t}{t}\,dt + O\left(\int_1^x \frac{t}{t^2}\,dt\right) + O(\log x) \\ &= \frac{3}{\pi^2}\log^2 x + O(\log x).\end{aligned}$$

□

1.1.2 Legendre symbol and extensions

To conclude this section, we recall the definitions of the *Legendre symbol* and its extensions. For an exhaustive treatment of its properties the reader can check [[23], Ch. 4].

Definition 1.21. For p an odd prime and a an integer, the *Legendre symbol* is defined by

$$\left(\frac{a}{p}\right) := \begin{cases} 1 & \text{if } p\nmid a,\ a \text{ is a square mod } p \\ 0 & \text{if } p|a \\ -1 & \text{if } a \text{ is not a square mod } p.\end{cases}$$

Definition 1.22. For any integers a, b with $b \geq 3$ and odd, the *Jacobi symbol* is defined as follows. Write b as a product of primes (they don't have to be distinct) $b = \prod_{i=1}^n p_i$ then

$$\begin{aligned}\left(\frac{a}{1}\right) &:= 1 \\ \left(\frac{a}{b}\right) &:= \prod_{i=1}^n \left(\frac{a}{p_j}\right)\end{aligned}$$

where on the right hand side is used a Legendre symbol.

Definition 1.23. For any integers a, b with b even and positive and $a \equiv 0, 1 \mod 4$, the *Kronecker symbol* is defined as follows.

$$\left(\frac{a}{b}\right) := \begin{cases} 0 & \text{if } 4|a \\ \left(\frac{b}{|a|}\right) & \text{if } a \equiv 1 \mod 4 \end{cases}$$

where $\left(\frac{b}{|a|}\right)$ is a Jacobi symbol. In the case b odd and positive, the Kronecker symbol is defined as the Jacobi symbol.

Lemma 1.24. *Let $k \in \{1, 3\}$. We have that*

$$\sum_{\substack{d \leq x \\ d \equiv k \mod 4}} \mu^2(d)\left(\frac{d}{n}\right) = O(nx^{\frac{1}{2}})$$

holds uniformly for $x \geq 1$ and for any positive odd nonsquare integer n.

Proof. Let $\mathcal{C} = \{l \in \{0, \dots, n-1\} | (l, n) = 1\}$, observing that $\left(\frac{d}{n}\right) = 0$ if $(d, n) \neq 1$ we rewrite

$$\begin{aligned} \sum_{\substack{d \leq x \\ d \equiv k \mod 4}} \mu^2(d)\left(\frac{d}{n}\right) &= \sum_{l \in \mathcal{C}} \sum_{\substack{d \leq x \\ d \equiv k \mod 4 \\ d \equiv l \mod n}} \mu^2(d)\left(\frac{d}{n}\right) \\ &= \sum_{l \in \mathcal{C}} \left(\frac{l}{n}\right) \sum_{\substack{d \leq x \\ d \equiv k \mod 4 \\ d \equiv l \mod n}} \mu^2(d). \end{aligned}$$

Since $(4, n) = 1$, we can apply the Chinese Remainder Theorem to get a unique solution m_{kl} modulo $4n$ of the system

$$\begin{cases} y \equiv k \mod 4 \\ y \equiv l \mod n. \end{cases}$$

Notice that $(m_{kl}, 4n) = 1$ and so, by Lemma 1.11, there exists $c(n) > 0$ such that

$$\begin{aligned} \sum_{\substack{d \leq x \\ d \equiv k \mod 4}} \mu^2(d)\left(\frac{d}{n}\right) &= \sum_{l \in \mathcal{C}} \left(\frac{l}{n}\right) \sum_{\substack{d \leq x \\ d \equiv m_{kl} \mod 4n}} \mu^2(d) \\ &= \sum_{l \in \mathcal{C}} \left(\frac{l}{n}\right)(c(n)x + O(x^{\frac{1}{2}})) \\ &= c(n)x \sum_{l \in \mathcal{C}} \left(\frac{l}{n}\right) + \sum_{l \in \mathcal{C}} \left(\frac{l}{n}\right) O(x^{\frac{1}{2}}) = O(nx^{\frac{1}{2}}). \end{aligned}$$

In the last equality we've used the fact that the Jacobi symbol has modulus less or equal than 1 and that the sum of Jacobi symbols over a full set of representatives of reduced classes modulo n vanishes (we will see it later in Lemma 2.3). □

1.2 Quadratic fields and fundamental unit

Definition 1.25. An integer D is called a *fundamental discriminant* if it is the discriminant of a quadratic field K.

Remark 1.26. Let us recall the following facts.

1. Let d be a squarefree integer, $d \notin \{0, 1\}$:

    - if $d \equiv 1 \mod 4$ then $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\frac{1+\sqrt{d}}{2}]$ and the discriminant of the quadratic field $\mathbb{Q}(\sqrt{d})$ is $D = d$;
    - if $d \equiv 2, 3 \mod 4$ then $\mathcal{O}_{\mathbb{Q}(\sqrt{d})} = \mathbb{Z}[\sqrt{d}]$ and the discriminant of the quadratic field $\mathbb{Q}(\sqrt{d})$ is $D = 4d$.

2. As a consequence, 0 and 1 are not fundamental discriminants. Moreover, if D is a fundamental discriminant then either $D \equiv 1 \mod 4$ squarefree or $D \equiv 0 \mod 4$ and $\frac{D}{4} \equiv 2, 3 \mod 4$ squarefree.

3. If D is the discriminant of a quadratic field K then $K = \mathbb{Q}(\sqrt{D}) = \mathbb{Q}(\sqrt{d})$ and an integral basis of K is given by $\{1, \omega\}$ where $\omega = \frac{D+\sqrt{D}}{2}$. Indeed it's immediate to see that $\mathbb{Z}[\omega] = \mathcal{O}_K$.

We recall now *Dirichlet's theorem on the structure of units* in the particular case of real quadratic fields. For the proof we refer to [[20], Ch. 5].

Theorem 1.27. *Let $\mathcal{O}_K^*$ be the group of units of the ring of integers of a real quadratic field K. Then there exists a unique element $u > 1$ such that*

$$\mathcal{O}_K^* = \{\pm u^k : k \in \mathbb{Z}\}.$$

$\mathcal{O}_K^*$ is infinite and we call u the fundamental unit of the field K.

We will consider the case $K = \mathbb{Q}(\sqrt{D})$ a real quadratic field where $D > 1$ is the discriminant. Let $\varepsilon(D)$ be the fundamental unit, we define the *regulator* as $R(D) := \log \varepsilon(D)$. For instance, $R(D)$ appears in the computation of the ideal class number $h(D)$, as we will see in the next chapter.

Definition 1.28. Let D be a fundamental discriminant of a quadratic field K. We define the *ideal class number* $h(D)$ as the cardinality of the *ideal class group* Cl_D i.e. the set of equivalence classes of nonzero ideals of $\mathcal{O}_K$ under the relation

$$\mathfrak{a} \sim \mathfrak{b} \Leftrightarrow \exists\ x, y \in \mathcal{O}_K \backslash \{0\} \text{ s.t. } x\mathfrak{a} = y\mathfrak{b}.$$

Remark 1.29. - Recall that Cl_D is indeed a group and is finite. For the proof we refer to [[20], Ch. 3 Cor. 1, Ch. 5 Cor. 2].

- Cl_D is isomorphic to the group G_D of fractional ideals of $\mathcal{O}_K$ modulo the subgroup P_D of principal fractional ideals through the group homomorphism

$$\begin{aligned} Cl_D &\longrightarrow {}^{G_D}\!/\!_{P_D} \\ [\mathfrak{a}]_\sim &\longmapsto \mathfrak{a}P_D. \end{aligned}$$

  It's immediate to prove that this map is a bijection since any fractional ideal is equivalent to an integral ideal by clearing denominators.

- We define the *narrow ideal class group* C_D as G_D modulo P_D^+, where P_D^+ is the subgroup of P_D consisting of principal fractional ideals generated by an element of positive norm.

1.3 Pell's equation and fundamental solution

The strategy to detect units in $\mathcal{O}_K$ is looking for elements of norm ±1. In this direction a similar but not completely equivalent problem is the study of the *fundamental solution* ε_d to the *Pell equation*

$$T^2 - dU^2 = 1 \tag{1.2}$$

where d is defined as in Remark 1.26 and T, U are the unknowns. A solution (T, U) is represented as $T + U\sqrt{d}$.

The following result is the analogous of Th. 1.27 for the Pell equation. An exhaustive discussion of the proof can be found on [[4], Ch. 7].

Theorem 1.30. *Let d be a nonsquare positive integer. Then there exists $\varepsilon_d = T + U\sqrt{d}$ a minimal solution of* (1.2) *greater than 1. Then the set of solutions of* (1.2) *is infinite and has the shape:*

$$\{\pm\varepsilon_d^n : n \in \mathbb{Z}\}.$$

ε_d is called the fundamental solution.

Notice that if we consider D a positive fundamental discriminant and $d = \frac{D}{(4,D)}$, $\varepsilon(D)$ and ε_d can be different essentially because the fundamental unit allows -1 as norm and 2 as denominator. However, by Th. 1.27 we get that ε_d is always a power of $\varepsilon(D)$ since it is an invertible element in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$.

Lemma 1.31. *Let d, D be as above. If $2^2 \mid\mid D$ then $\varepsilon(D)$ has norm 1 and hence is equal to ε_d.*

Proof. Since $2^2 \mid\mid D$ we have that $d \equiv 3 \mod 4$. This implies that there exists a prime p such that $p \mid d$ and $p \equiv 3 \mod 4$. Reducing the equation $T^2 - dU^2 = -1$ modulo p we obtain $T^2 \equiv -1 \mod p$ which has no solutions since -1 is a square modulo p if and only if $p \equiv 1 \mod 4$.
Therefore $\varepsilon(D) = T + U\sqrt{d}$ must be an element of norm 1 and is equal to ε_d since it is the minimal solution greater than 1 of (1.2). □

Remark 1.32.

- The above proof says something more. If there exists a prime $p \equiv 3 \mod 4$ such that $p \mid d$ then the *negative* Pell equation

  $$T^2 - dU^2 = -1$$

  admits no solutions.
  The same holds also for $T^2 - dU^2 = -4$.

- Observe also that in the case $p \equiv 1 \mod 4$ the equation

  $$T'^2 - pU'^2 = -1$$

  always admits a solution. Let $\varepsilon_p = T + U\sqrt{p}$ be the fundamental solution of $T^2 - pU^2 = 1$.

  $$2 \mid T \implies U^2 \equiv -1 \mod 4$$

  which is impossible since -1 is not a square modulo 4. We deduce T odd and U even since $pU^2 = T^2 - 1$. We have

  $$\frac{T+1}{2}\frac{T-1}{2} = p\Big(\frac{U}{2}\Big)^2,$$

therefore either

$$\begin{cases} \frac{T+1}{2} = U_1^2 \\ \frac{T-1}{2} = pU_2^2 \end{cases} \quad \text{or} \quad \begin{cases} \frac{T+1}{2} = pU_1^2 \\ \frac{T-1}{2} = U_2^2. \end{cases}$$

In the first case

$$\frac{T+1}{2} - \frac{T-1}{2} = U_1^2 - pU_2^2 = 1$$

contradicts the minimality of ε_p since

$$(U_1 + U_2\sqrt{p})^2 = U_1^2 + U_2^2 p + 2U_1U_2\sqrt{p} = T + U\sqrt{p}.$$

In the second case we detect a solution of $T'^2 - pU'^2 = -1$ since

$$\frac{T-1}{2} - \frac{T+1}{2} = U_2^2 - pU_1^2 = -1.$$

Lemma 1.33. *Let d, D as before and let n be the positive integer such that $\varepsilon(D)^n = \varepsilon_d$. Then $n \le 6$.*

Proof.

- If $d \equiv 3 \mod 4$ then $n = 1$ by the previous lemma.
- If $d \equiv 2 \mod 4$ then $\varepsilon(D) = T + U\sqrt{d}$ could have norm -1, in this case we have to compute its square to get ε_d and therefore $n \le 2$.
- If $d \equiv 1 \mod 4$ and $\varepsilon(D)$ has the shape $T + U\sqrt{d}$ we can apply the same previous reasoning. In the other case $\varepsilon(D) = \frac{a+b\sqrt{d}}{2}$, where $a, b \equiv 1(2)$, we are going to prove that $\varepsilon(D)^3 \in \mathbb{Z}[\sqrt{d}]$ and so, up to squaring, we are done.

$$\varepsilon(D)^3 = \frac{1}{8}(a^3 + 3a^2b\sqrt{d} + 3ab^2d + b^3d\sqrt{d}) = \frac{1}{8}[a(a^2 + 3b^2d) + b(3a^2 + b^2d)\sqrt{d}]$$

Now we would see that $a^2 + 3b^2d$ and $3a^2 + b^2d$ are divisible by 8. Notice that $a^2, b^2 \equiv 1(8)$, thus

$$a^2 + 3b^2 \equiv 1 + 3d \mod 8$$
$$3a^2 + b^2d \equiv 3 + d \mod 8.$$

If $d \equiv 5(8)$ then $1 + 3d, 3 + d \equiv 0(8)$. We conclude the lemma proving that in this situation d cannot be congruent to 1 modulo 8.
Indeed $\varepsilon(D) = \frac{a+b\sqrt{d}}{2}$ is such that $a^2 - b^2d = \pm 4$. If we look at this modulo 8, assuming $d \equiv 1(8)$, we get $a^2 - b^2 \equiv 4(8)$ and this is absurd since $a^2, b^2 \equiv 1(8)$.

□

Example 1.34. One may wonder if the values of n presented in this proof are the minimal ones. Indeed:

- if $d = 10$ then $\varepsilon(40) = 3 + \sqrt{10}$ and $\varepsilon_{10} = 19 + 6\sqrt{10} = \varepsilon(40)^2$;
- If $d = 5$ then $\varepsilon(5) = \frac{1+\sqrt{5}}{2}$ and $\varepsilon_5 = 9 + 4\sqrt{5} = \varepsilon(5)^6$.

Remark 1.35. Let d be any nonzero nonsquare integer which factorizes as $d = \alpha^2 d'$ where d' is squarefree. The fundamental solutions of the Pell equations $T^2 - dU^2 = 1$ and $T'^2 - d'U'^2 = 1$ are related as follows.

$$\varepsilon_d = T + U\sqrt{d} = T + U\alpha\sqrt{d'}$$

We see that from ε_d we get a solution of the equation $T'^2 - d'U'^2 = 1$ and by Th. 1.30 there exists an integer n, which is positive since $\varepsilon_d > 1$, such that $\varepsilon_d = \varepsilon_{d'}^n$. The strategy to detect this n is to write powers of $\varepsilon_{d'}$ as

$$\varepsilon_{d'}^m = \frac{\varepsilon_{d'}^m + \varepsilon_{d'}^{-m}}{2} + \frac{\varepsilon_{d'}^m - \varepsilon_{d'}^{-m}}{2\sqrt{d'}}\sqrt{d'}$$

and look for the minimal $m > 1$ such that $\alpha \mid \frac{\varepsilon_{d'}^m - \varepsilon_{d'}^{-m}}{2\sqrt{d'}}$. In fact, if such divisibility condition holds we obtain a solution of $T^2 - dU^2 = 1$ from $\varepsilon_{d'}^m$.

Of course, we would relate more explicitly m and α. Let $\alpha = p_1^{a_1} \cdots p_n^{a_n}$ be its prime factorization, we assume to know for each $i = 1, \dots, n$ the smallest integer ν_i such that $p_i \mid u_{\nu_i} := \frac{\varepsilon_{d'}^{\nu_i} - \varepsilon_{d'}^{-\nu_i}}{2\sqrt{d'}}$ and the exponent δ_i such that $p_i^{\delta_i} || u_{\nu_i}$. Let e_i be any positive integer, from ν_i, δ_i we can immediately recover ϵ_i satisfying $p_i^{\delta_i + \epsilon_i} || u_{\nu_i e_i}$. Indeed, let θ and η be two positive integers such that

$$\begin{cases} \theta^2 - \eta^2 d' = 1 \\ p^k || \eta, \end{cases}$$

we set

$$t + u\sqrt{d'} := (\theta + \eta\sqrt{d'})^l,$$

where $l \in \mathbb{Z}_{>0}$. Developing the above exponentiation, we have

$$u = \eta\theta^{l-1} l + \eta^3 \sum_{j=1}^{\lceil \frac{l}{2} \rceil - 1} \binom{l}{2j+1} \eta^{2j-2} \theta^{l-2j-1} d'^j.$$

Observing that $p \nmid \theta$ we get

$$\begin{cases} p^k || u & \text{if } (l, p) = 1 \\ p^{k+1} || u & \text{if } l = p \end{cases}$$

and hence we deduce by iteration that

$$p^{k+k'} || u \qquad \text{if } p^{k'} || l.$$

Therefore, to have $p_i^{a_i} | u_{\nu_i e_i}$ we need to verify $p_i^{\max(0, a_i - \delta_i)} | e_i$ and we conclude

$$m = \operatorname{lcm}\Big(\nu_1 p_1^{\max(0, a_1 - \delta_1)}, \dots, \nu_n p_n^{\max(0, a_n - \delta_n)}\Big).$$

Remark 1.36. Let D, d be as usual. Since $\varepsilon(D), \varepsilon_d > 1$, it's easy to show that if $\varepsilon(D) = \frac{a + b\sqrt{d}}{2}$ then $a, b \geq 1$ and in the same way if $\varepsilon_d = T + U\sqrt{d}$ then $T, U \geq 1$.

Chapter 2

Analytic class number formula

In this chapter we present the main steps for a proof of the class number formula in the quadratic case. We will follow basilcally [[18], Ch. 8] with some inputs from [[12], Ch. 7].

2.1 Dirichlet Characters and main statement

Definition 2.1. Let G be any group. A group homomorphism $f : G \longrightarrow \mathbb{C}^*$ is called a *character of G.*
Now let $G = \left(\mathbb{Z}/_{m\mathbb{Z}}\right)^*$. Corresponding to each character f of G we define an arithmetic function χ_f as follows.

$$\chi_f(n) = \begin{cases} f([n]) & \text{if } (n,m) = 1 \\ 0 & \text{if } (n,m) > 1 \end{cases}$$

A function χ of this shape is called a *Dirichlet character modulo m.*
We will denote by χ_0 the *principal Dirichlet character modulo m* corresponding to the map $f \equiv 1$.

Remark 2.2. An arithmetic function χ is a Dirichlet character modulo m if and only if satisfies for all a, b and for n not coprime to m

$$\begin{aligned} \chi(ab) &= \chi(a)\chi(b) \\ \chi(a+m) &= \chi(a) \\ \chi(n) &= 0. \end{aligned}$$

Notice also that if $\chi(n) \neq 0$ it must be a root of unity and so $|\chi(n)| = 1$. This follows from the fact that χ corresponds to a group homomorphism $f : G \longrightarrow \mathbb{C}^*$ and here G is finite so there exists an e such that $f([n])^e = 1$.

Lemma 2.3. *If χ is a Dirichlet character modulo m, then*

$$\sum_{n=1}^{m} \chi(n) = \begin{cases} \varphi(m) & \text{if } \chi = \chi_0 \\ 0 & \text{if } \chi \neq \chi_0. \end{cases}$$

Proof. The case $\chi = \chi_0$ is obvious from the definition. If $\chi \neq \chi_0$ then there exists a such that $\chi(a) \neq 1$ and $(a, m) = 1$. We have

$$\chi(a)\sum_{n=1}^{m}\chi(n) = \sum_{n=1}^{m}\chi(an) = \sum_{n=1}^{m}\chi(n)$$

and thus

$$(\chi(a)-1)\sum_{n=1}^{m}\chi(n)=0$$

which concludes the proof. □

Definition 2.4. Let χ be a Dirichlet character modulo m. We define the *conductor* m^* of χ as the smallest divisor of m such that $\chi=\chi_0\chi^*$, where χ_0 is the principal character modulo m and χ^* is a Dirichlet character modulo m^*.
If $m=m^*$ then χ is said to be *primitive.*

Lemma 2.5. *If $(n,m)=1$ and χ_n (resp. χ_m) is a primitive Dirichlet character modulo n (resp. m), then the product $\chi_n\chi_m$ is primitive modulo nm.*

Proof. The duality between abelian groups and their character groups, see [[23], Th. 4.15], implies that the group of Dirichlet characters modulo nm is isomorphic to $\left(\mathbb{Z}/_{nm\mathbb{Z}}\right)^*$ and hence, by Chinese Remainder Theorem, to $\left(\mathbb{Z}/_{n\mathbb{Z}}\right)^*\times\left(\mathbb{Z}/_{m\mathbb{Z}}\right)^*$ since $(n,m)=1$. This means that any character modulo nm can be written uniquely as a product of a character modulo n with a character modulo m. By uniqueness of this factorization, we deduce the statement. □

Example 2.6.

- Let p be an odd prime number then the Legendre symbol $\left(\frac{\cdot}{p}\right)$ is a primitive character modulo p.
- Let n be an odd *squarefree* positive integer then, applying the previous result, the Jacobi symbol $\left(\frac{\cdot}{n}\right)$ is a primitive character modulo n. More generally, if n is an odd positive *nonsquare* integer then $\left(\frac{\cdot}{n}\right)$ is a Dirichlet character modulo n but not necessarily primitive.

For a more precise treatment of Dirichlet characters the reader can check [[17], Ch. 3].

Definition 2.7. Let χ be a non-principal Dirichlet character modulo m and let s be a complex variable. We define the *Dirichlet L-function attached to* χ by

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

Remark 2.8. $L(s,\chi)$ is absolutely convergent for $Re(s)>1$. However, it is also convergent for $s=1$ which is going to be our case of interest.

Lemma 2.9. *Let χ be a non-principal Dirichlet character modulo m. Then*

$$|L(1,\chi)|\leq\log m+1.$$

Proof. By Th. 1.18 we have

$$\sum_{n\leq x}\frac{\chi(n)}{n}=\frac{1}{x}\sum_{n\leq x}\chi(n)+\int_1^x\frac{1}{t^2}\sum_{n\leq t}\chi(n)\,dt$$

and by Lemma 2.3 $|\sum_{n\leq x}\chi(n)|<m$, hence

$$L(1,\chi)=\lim_{x\to\infty}\sum_{n\leq x}\frac{\chi(n)}{n}=\int_1^{\infty}\frac{1}{t^2}\sum_{n\leq t}\chi(n)\,dt.$$

Now

$$|L(1,\chi)| = \left| \int_1^\infty \frac{1}{t^2} \sum_{n\le t} \chi(n)\, dt \right| \le \int_1^m \frac{1}{t^2} \Big| \sum_{n\le t} \chi(n) \Big|\, dt + \int_m^\infty \frac{1}{t^2} \Big| \sum_{n\le t} \chi(n) \Big|\, dt$$

and since $|\sum_{n\le t} \chi(n)| \le t$ for $1 \le t \le m$, we get

$$|L(1,\chi)| \le \int_1^m \frac{1}{t}\, dt + m \int_m^\infty \frac{1}{t^2}\, dt = \log m + 1.$$

□

Let D be a fundamental discriminant. In our discussion we will consider the non-principal Dirichlet character modulo D, χ_D, given by the Kronecker symbol $\left(\frac{D}{\cdot}\right)$ with its attached L-function.
Now we are ready to state the main theorem.

Theorem 2.10. *Let D be a fundamental discriminant and k_D be the Dirichlet structure constant defined as follows:*

$$k_D := \begin{cases} \dfrac{2\pi}{w\sqrt{|D|}} & \text{if } D < 0 \\ \dfrac{2R(D)}{\sqrt{D}} & \text{if } D > 0, \end{cases}$$

where w is the number of roots of unity in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. Then

$$h(D) = \frac{L(1,\chi_D)}{k_D}.$$

Remark 2.11. We have that

$$w = \begin{cases} 6 & \text{if } D = -3 \\ 4 & \text{if } D = -4 \\ 2 & \text{if } D < -4. \end{cases}$$

Let d be a squarefree negative integer. The explicit values of w follow from the following facts:

- the negative Pell equations $T^2 - dU^2 = -1$ and $T^2 - dU^2 = -4$ have no solutions since d is negative;

- if $d \equiv 2, 3(4)$ the unique Pell equation which has non trivial solutions is $T^2 + U^2 = 1$. It has 2 more solutions and corresponds to the case $D = -4$;

- if $d \equiv 1(4)$ the unique Pell equation which has non trivial solutions is $T^2 + 3U^2 = 4$. It has 4 more solutions and corresponds to the case $D = -3$.

The strategy for the proof of the *class number formula* is to count the ideals of $\mathcal{O}_K$ with norm bounded by a certain $t > 0$ in two different ways.

2.2 First part of the proof

Definition 2.12. Let D be a fundamental discriminant, let $\mathcal{C} \in Cl_D$ and $t > 0$. We define $H(\mathcal{C}, t)$ as the number of distinct ideals $\mathfrak{a} \in \mathcal{C}^{-1}$ such that $N(\mathfrak{a}) < t$. We denote by $G(\mathfrak{a}, t)$ the number of distinct principal ideals (α), where $\alpha \in \mathfrak{a}$ is such that $0 < N((\alpha)) < t$.

Lemma 2.13. *If $\mathfrak{a} \in \mathcal{C}$ and $t > 0$ then*

$$H(\mathcal{C}, t) = G(\mathfrak{a}, tN(\mathfrak{a})).$$

Proof. $(\geq)$ Let $\alpha \in \mathfrak{a}$ such that $0 < N((\alpha)) < tN(\mathfrak{a})$. Since (α) is principal there exists $\mathfrak{b} \in \mathcal{C}^{-1}$ such that $(\alpha) = \mathfrak{a}\mathfrak{b}$ and therefore

$$N((\alpha)) = N(\mathfrak{a})N(\mathfrak{b}) < tN(\mathfrak{a}) \implies N(\mathfrak{b}) < t.$$

$(\leq)$ Let $\mathfrak{b} \in \mathcal{C}^{-1}$ such that $N(\mathfrak{b}) < t$. In particular there exists α such that $\mathfrak{a}\mathfrak{b} = (\alpha)$ and so $N((\alpha)) < tN(\mathfrak{a})$.

Thus, every $\mathfrak{b} \in \mathcal{C}^{-1}$ of norm bounded by t corresponds uniquely to a principal ideal $(\alpha) \subseteq \mathfrak{a}$ with $N((\alpha)) < tN(\mathfrak{a})$. □

We are going to present several technical lemmas which are needed to prove the first important result.

Lemma 2.14. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$. Then there exist $a, c \in \mathbb{Z}_{>0}$ and $b \in \mathbb{Z}_{\geq 0}$ such that $\mathfrak{a} = a\mathbb{Z} + (b + c\omega)\mathbb{Z}$, where ω is defined in Remark 1.26, and $N(\mathfrak{a}) = ac$.*

Proof. Omitted. See [[18], § 4.4]. □

Lemma 2.15. *Let $D > 0$ be a fundamental discriminant. For any nonzero $\beta \in \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ there exists a unique $\alpha > 0$ such that $(\beta) = (\alpha)$ and*

$$1 \leq \left|\frac{\alpha}{\bar{\alpha}}\right| < \varepsilon(D)^2,$$

where $\bar{\alpha}$ denotes the Galois conjugate of α. We call α the primary associate to β.

Proof. If β and γ are associate, i.e. $(\beta) = (\gamma)$, then there exists $n \in \mathbb{Z}$ such that $\gamma = \pm\varepsilon(D)^n\beta$. We get

$$\log|\gamma| = \log|\beta| + n\log\varepsilon(D)$$

and

$$\log|\bar{\gamma}| = \log|\bar{\beta}| + n\log|\overline{\varepsilon(D)}|.$$

We have also $\log\varepsilon(D) + \log|\overline{\varepsilon(D)}| = 0$ since $\varepsilon(D)|\overline{\varepsilon(D)}| = 1$. Then by the previous expressions we conclude that

$$\log\left|\frac{\gamma}{\bar{\gamma}}\right| = \log\left|\frac{\beta}{\bar{\beta}}\right| + 2n\log\varepsilon(D).$$

Notice that $\varepsilon(D) > 1$ and so the quantity $\log\varepsilon(D)$ is always positive.
Now let $\lambda = \log|\beta/\bar{\beta}|$, then

$$0 \leq \log\left|\frac{\gamma}{\bar{\gamma}}\right| < 2\log\varepsilon(D) \Leftrightarrow n = -\left\lfloor\frac{\lambda}{2\log\varepsilon(D)}\right\rfloor$$

and we fix this value of n. To conclude the proof it remains to choose the sign in order to have $\gamma > 0$. □

We need also a simple result which allows us to count lattice points in a certain region of the plane.

Lemma 2.16. *Let Γ be a continuous arc with continuous derivative in $\mathbb{R}^2$ such that the radius of curvature R is greater or equal to $r > 0$. Suppose that at each point of Γ is drawn a circle of radius r, we denote by $\Gamma(r)$ the resulting domain and by $|\Gamma|$ the length of the arc. Then the area $|\Gamma(r)|$ satisfies*

$$|\Gamma(r)| \leq 2r|\Gamma| + \pi r^2.$$

Proof. Let (x, y) and (x', y') be two points on Γ. If (x', y') approaches (x, y) let ds be their distance on Γ. Since $R \geq r$ the element of area dA is

$$dA = 2(r \cdot ds) = 2r\, ds.$$

Integrating along Γ and adding the areas of the two semicircles at the end points of Γ, we get

$$|\Gamma(r)| \leq 2r|\Gamma| + 2\frac{1}{2}\pi r^2.$$

□

Corollary 2.17. *Let A be a region bounded by a curve Γ consisting of a finite number n of arcs $\Gamma_1, \dots \Gamma_n$ satisfying the conditions of the previous lemma with $r_i \geq \sqrt{2}$ for $i = 1, \dots n$. Then if $M(A)$ is the number of points of the lattice $\Lambda := \{(x, y) : x, y \in \mathbb{Z}\}$ in A or on Γ_i, then*

$$M(A) = |A| + O(|\Gamma|)$$

where $|A|$ is the area of the region A.

Proof. We draw a circle of radius $\sqrt{2}$ around each point of Γ. In this way, if there is a point (x, y) of Λ close to the boundary of Γ we are adding to our region the remaining parts of all 1×1 squares described by elements in Λ in which (x, y) is contained. Therefore applying the previous lemma we get

$$M(A) = |A| + O\left(\sum_{i=1}^{n} |\Gamma_i(\sqrt{2})|\right) = |A| + O\left(\sum_{i=1}^{n} |\Gamma_i|\right) = |A| + O(|\Gamma|).$$

□

Theorem 2.18. *Let D be a fundamental discriminant, $t > 0$ and $\mathcal{C} \in Cl_D$. Then*

$$H(\mathcal{C}, t) = k_D t + O(\sqrt{t}).$$

Proof. Let $\mathfrak{a} \in \mathcal{C}$, we want to compute $G(\mathfrak{a}, tN(\mathfrak{a}))$. By Lemma 2.14, $\mathfrak{a} = \alpha_1\mathbb{Z} + \alpha_2\mathbb{Z}$ where $\alpha_1 = a$, $\alpha_2 = b + c\omega$ and $N(\mathfrak{a}) = ac$, with $a, c \in \mathbb{Z}_{>0}$, $b \in \mathbb{Z}_{\geq 0}$ and $\omega = (D + \sqrt{D})/2$.
Let $\alpha \in \mathfrak{a}$ then there exist $x, y \in \mathbb{Z}$ such that $\alpha = \alpha_1 x + \alpha_2 y$, $\bar{\alpha} = \bar{\alpha_1} x + \bar{\alpha_2} y$. Putting $A := \alpha_1\bar{\alpha_1} = \alpha_1^2$, $B := \alpha_1\bar{\alpha_2} + \alpha_2\bar{\alpha_1}$ and $C := \alpha_2\bar{\alpha_2}$, we get

$$N((\alpha)) = |\alpha\bar{\alpha}| = |Ax^2 + Bxy + Cy^2|.$$

Therefore, to determine $G(\mathfrak{a}, tN(\mathfrak{a}))$ we need to count the number of pairs $(x, y) \in \mathbb{Z}^2$ such that

$$|Ax^2 + Bxy + Cy^2| < tN(\mathfrak{a}). \tag{2.1}$$

However, if β is an associate of α then $(\alpha) = (\beta)$ and so we have to count the pairs (x, y) in such a way that avoids redundancies.
(i) Case $D > 0$.
By Lemma 2.15 we have to select only those values of α such that $\alpha > 0$ and $1 \leq |\alpha/\bar{\alpha}| < \varepsilon(D)^2$, i.e.

$$1 \leq \left| \frac{\alpha_1 x + \alpha_2 y}{\bar{\alpha_1} x + \bar{\alpha_2} y} \right| < \varepsilon(D)^2, \qquad \alpha_1 x + \alpha_2 y > 0.$$

Let $\mathcal{A}$ be the region determined by the previous inequalities and (2.1), then its surface area is

$$|\mathcal{A}| = \int\int dx\, dy.$$

We do the following change of variables

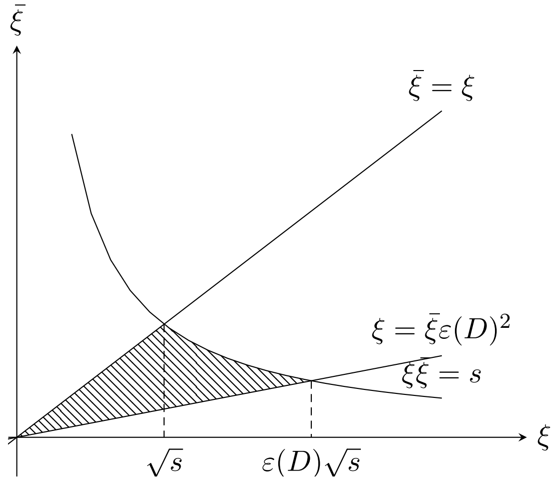
$$\begin{cases} \xi & = \alpha_1 x + \alpha_2 y \\ \bar{\xi} & = \bar{\alpha_1} x + \bar{\alpha_2} y. \end{cases} \tag{2.2}$$

ξ and $\bar{\xi}$ satisfy

$$|\xi\bar{\xi}| < tN(\mathfrak{a}) =: s, \qquad 1 \leq \left|\frac{\xi}{\bar{\xi}}\right| < \varepsilon(D)^2, \qquad \xi > 0.$$

These conditions in the $\xi\bar{\xi}$-plane define two sectors of equal area of an hyperbola. We deal with the sector defined by

$$\xi > \bar{\xi} > 0, \qquad \xi\bar{\xi} < s, \qquad \frac{\xi}{\bar{\xi}} < \varepsilon(D)^2.$$



The jacobian of the trasformation (2.2) is

$$\alpha_1\bar{\alpha_2} - \alpha_2\bar{\alpha_1} = ab + ac\frac{D - \sqrt{D}}{2} - ab - ac\frac{D + \sqrt{D}}{2} = -ac\sqrt{D} = -N(\mathfrak{a})\sqrt{D},$$

thus

$$\begin{aligned} |\mathcal{A}| &= \frac{2}{N(\mathfrak{a})\sqrt{D}} \int\int d\bar{\xi}\, d\xi \\ &= \frac{2}{N(\mathfrak{a})\sqrt{D}} \left(\int_0^{\sqrt{s}} \left(\int_{\frac{\xi}{\varepsilon(D)^2}}^{\xi} d\bar{\xi} \right) d\xi + \int_{\sqrt{s}}^{\varepsilon(D)\sqrt{s}} \left(\int_{\frac{\xi}{\varepsilon(D)^2}}^{\frac{s}{\xi}} d\bar{\xi} \right) d\xi \right) \\ &= \frac{2s \log \varepsilon(D)}{N(\mathfrak{a})\sqrt{D}} = \frac{2R(D)t}{\sqrt{D}}. \end{aligned}$$

The length of the hyperbolic arc which bounds $\mathcal{A}$ is

$$\int_{\sqrt{s}}^{\varepsilon(D)\sqrt{s}} \sqrt{1+\left(\frac{\sqrt{s}}{u}\right)^4}\,du \underbrace{=}_{\frac{u}{\sqrt{s}}\to v} \sqrt{s}\underbrace{\int_1^{\varepsilon(D)} \sqrt{1+\frac{1}{v^4}}\,dv}_{<\infty} = O(\sqrt{t})$$

and also the lengths of the other two sides are trivially $O(\sqrt{t})$. Therefore since the radius of curvature increases with t, we get from Corollary 2.17

$$G(\mathfrak{a}, tN(\mathfrak{a})) = \frac{2R(D)t}{\sqrt{D}} + O(\sqrt{t}).$$

(ii) Case $D < 0$.
The region given by (2.1) describes an ellipse of area, see [[3], p. 160] for instance,

$$\frac{2\pi}{\sqrt{\left|\frac{4AC}{(tN(\mathfrak{a}))^2} - \frac{B^2}{(tN(\mathfrak{a}))^2}\right|}} = \frac{2\pi t}{\sqrt{\left|\frac{1}{ac}(4AC - B^2)\right|}} = \frac{2\pi t}{\sqrt{|D|}}$$

where the second equality is determined by

$$\begin{aligned} 4AC - B^2 &= 4\alpha_1\bar{\alpha_1}\alpha_2\bar{\alpha_2} - (\alpha_1\bar{\alpha_2} + \alpha_2\bar{\alpha_1})^2 \\ &= a^2[(2b + c(D+\sqrt{D}))(2b + c(D-\sqrt{D})) - (2b+cD)^2] \\ &= a^2[(2b+cD)^2 - (c\sqrt{D})^2 - (2b+cD)^2] = -a^2c^2D. \end{aligned}$$

There are only w associates to every α and the ellipse is clearly delimited by a curve of length $O(\sqrt{t})$, then Corollary 2.17 implies

$$G(\mathfrak{a}, tN(\mathfrak{a})) = \frac{2\pi t}{w\sqrt{|D|}} + O(\sqrt{t})$$

which concludes the proof applying Lemma 2.13. □

Corollary 2.19. *Let D be a fundamental discriminant and $H(t)$ be the number of distinct ideals $\mathfrak{a}$ of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ such that $N(\mathfrak{a}) \leq t$ then*

$$H(t) = h(D)k_D t + O(\sqrt{t}).$$

Proof. We have

$$H(t) = \sum_{\mathcal{C}\in Cl_D} H(\mathcal{C}, t) + O(1),$$

where $O(1)$ is determined by the fact that we are caring about $N(\mathfrak{a}) \leq t$ and not only $N(\mathfrak{a}) < t$. The statement follows from the previous theorem and the finiteness of Cl_D. □

2.3 Second part of the proof

Remark 2.20. Let D be a fundamental discriminant and $K = \mathbb{Q}(\sqrt{D})$. We recall that (see [[20], Th. 25]):

- if $\left(\frac{D}{p}\right) = 0$ then p ramifies in $\mathcal{O}_K$;
- if $\left(\frac{D}{p}\right) = 1$ then p splits completely in $\mathcal{O}_K$;

- if $\left(\frac{D}{p}\right) = -1$ then p is inert.

Lemma 2.21. *Let p be a prime number, D be a fundamental discriminant and $k \in \mathbb{Z}_{>0}$, then the number of ideals of norm p^k in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ is*

$$F(p^k) = \sum_{i=0}^{k} \left(\frac{D}{p^i}\right) = 1 + \sum_{i=1}^{k} \left(\frac{D}{p}\right)^i .$$

Proof.

- If $\left(\frac{D}{p}\right) = 0$ then $(p) = \mathfrak{p}^2$, where $\mathfrak{p}$ is a prime ideal. If $N(\mathfrak{a}) = p^k$ then $\mathfrak{a} = \mathfrak{p}^u$ and $u = k$, hence $F(p^k) = 1$.
- If $\left(\frac{D}{p}\right) = 1$ then $(p) = \mathfrak{p}\mathfrak{p}'$, where $\mathfrak{p}, \mathfrak{p}'$ are distinct prime ideals. If $N(\mathfrak{a}) = p^k$ then $\mathfrak{a} = \mathfrak{p}^u \mathfrak{p}'^{u'}$ such that $u + u' = k$. Therefore the $k+1$ pairs $(u, u-k)$, for $u = 0, \dots k$, produce exactly $k+1$ distinct ideals $\mathfrak{a}$ and so $F(p^k) = k+1$.
- If $\left(\frac{D}{p}\right) = -1$ then p is inert. If $N(\mathfrak{a}) = p^k$ we must have $\mathfrak{a} = (p)^u$ where $2u = k$. In particular
$$F(p^k) = \begin{cases} 1 & \text{if } k \text{ is even} \\ 0 & \text{if } k \text{ is odd} \end{cases}$$
which concludes the proof.

□

Corollary 2.22. *For each $n \in \mathbb{Z}_{>0}$ we have*

$$F(n) = \sum_{m|n} \left(\frac{D}{m}\right).$$

Proof. Let $n = p_1^{e_1} \dots p_k^{e_k}$ be the prime factorization of n, since we've proved F is multiplicative we have

$$\begin{aligned} F(n) &= F(p_1^{e_1}) \dots F(p_k^{e_k}) \\ &= \prod_{i=0}^{k} \sum_{j_i=0}^{e_i} \left(\frac{D}{p^{j_i}}\right) \\ &= \sum_{\substack{j_1=0,\dots e_1 \\ \vdots \\ j_k=0,\dots e_k}} \left(\frac{D}{p_1^{j_1} \dots p_k^{j_k}}\right) = \sum_{m|n} \left(\frac{D}{m}\right). \end{aligned}$$

□

Remark 2.23. From the previous corollary we obtain another way to compute $H(t)$.

$$H(t) = \sum_{1 \le n \le t} F(n) = \sum_{1 \le n \le t} \sum_{m|n} \left(\frac{D}{m}\right)$$

Theorem 2.24. *We have*

$$\lim_{t \to \infty} \frac{H(t)}{t} = L(1, \chi_D).$$

Proof. Let $M(t,m)$ be the number of positive integers not exceeding $\frac{t}{m}$, here m is a positive integer. Notice that

$$M(t,m) = \sum_{1\leq n\leq \frac{t}{m}} 1 = \sum_{\substack{1\leq n\leq t\\ m|n}} 1$$

and if $m > t$ we have $M(t,m) = 0$.

$$\begin{aligned}\frac{H(t)}{t} &= \frac{1}{t}\sum_{1\leq n\leq t}\sum_{m|n}\left(\frac{D}{m}\right) = \frac{1}{t}\sum_{1\leq m\leq t}\left(\frac{D}{m}\right)\sum_{\substack{1\leq n\leq t\\ m|n}} 1\\ &= \frac{1}{t}\sum_{1\leq m\leq t}\left(\frac{D}{m}\right)M(t,m) = \sum_{m=1}^{\infty}\left(\frac{D}{m}\right)\frac{M(t,m)}{t}\end{aligned}$$

Observe now that $\frac{M(t,m)}{t} \leq \frac{1}{m}$ for all t, hence by 2.9

$$\frac{H(t)}{t} \leq \sum_{m=1}^{\infty}\left(\frac{D}{m}\right)\frac{1}{m} = L(1,\chi_D) \leq \log D + 1$$

and so $\frac{H(t)}{t}$ converges uniformly in t.
Finally $\lim_{t\to\infty}\frac{M(t,m)}{t} = \frac{1}{m}$, therefore

$$\lim_{t\to\infty}\frac{H(t)}{t} = \sum_{m=1}^{\infty}\left(\frac{D}{m}\right)\lim_{t\to\infty}\frac{M(t,m)}{t} = L(1,\chi_D)$$

which implies

$$H(t) = L(1,\chi_D)t + o(t).$$

□

proof of Theorem 2.10. Comparing Corollary 2.19 and the previous result we conclude the proof of the *class number formula.* □

2.4 A first bound on $\varepsilon(D)$

Lemma 2.25. *Let D be a positive fundamental discriminant, then there exists an absolute constant C such that*

$$\frac{\sqrt{D}}{2} < \varepsilon(D) \leq \exp(C\sqrt{D}\log D).$$

Proof. (i) If $D \equiv 0(4)$ then $D = 4d$, d squarefree

$$\varepsilon(D) = a + b\sqrt{d} \text{ s.t. } a,b \geq 1 \implies \varepsilon(D) > \sqrt{d} = \frac{\sqrt{D}}{2}.$$

If $D \equiv 1(4)$ then $D = d$ squarefree

$$\varepsilon(D) = \frac{a+b\sqrt{d}}{2} \text{ s.t. } a,b \geq 1, a \equiv b \mod 2 \implies \varepsilon(D) > \frac{\sqrt{d}}{2} = \frac{\sqrt{D}}{2}.$$

(ii) By the class number formula we have

$$\log\varepsilon(D) = \frac{L(1,\chi_D)\sqrt{D}}{2h(D)} \implies \varepsilon(D) = \exp\Big(\frac{L(1,\chi_D)\sqrt{D}}{2h(D)}\Big).$$

Now, we have trivially $h(D) \geq 1$ and by Lemma 2.9

$$\varepsilon(D) \leq \exp\Big(\frac{(\log D + 1)\sqrt{D}}{2}\Big),$$

which concludes the proof. □

Corollary 2.26. *Let d be a positive squarefree integer, then there exists an absolute constant C such that*

$$2\sqrt{d} < \varepsilon_d \leq \exp(C\sqrt{d}\log d).$$

Proof. (i) We have $\varepsilon_d = t + u\sqrt{d}$ where $t, u \geq 1$ and

$$t = \sqrt{1 + du^2} > \sqrt{d} \implies \varepsilon_d > 2\sqrt{d}.$$

(ii) The second inequality follows from Lemma 1.33 and the previous result. □

Remark 2.27. Notice that in the previous corollary the assumption d squarefree is not needed to prove the first inequality. Indeed for any positive nonsquare integer d

$$\varepsilon_d > 2\sqrt{d}.$$

Example 2.28. Let's consider $d = n^2 - 1$ where n is a nonzero integer and can be assumed positive. We claim that $\varepsilon_d = n + \sqrt{d}$.
We see immediately that $n + \sqrt{d}$ represents a solution of $T^2 - (n^2 - 1)U^2 = 1$ and is strictly greater than 1. Hence there exists an $m \in \mathbb{Z}_{>0}$ such that $(\varepsilon_d)^m = n + \sqrt{d}$.
Let $\varepsilon_d = a + b\sqrt{d}$, if $m > 1$ then the coefficient of $\sqrt{d}$ in $(\varepsilon_d)^m$ is strictly greater than 1 since $a, b \geq 1$. This does not fit with $(\varepsilon_d)^m = n + \sqrt{d}$, therefore $m = 1$.

This example shows that the lower bound of the previous corollary is the best possible since

$$\varepsilon_d - 2\sqrt{d} = n + \sqrt{n^2 - 1} - 2\sqrt{n^2 - 1}$$

could get arbitrarily close to 0 by increasing the value of n.

Chapter 3

A divisibility property of ideal norms in $O_{\mathbb{Q}(\sqrt{D})}$

Definition 3.1. Let D be a positive fundamental discriminant. We define D' as the *kernel* of D, i.e. the product of the distinct prime divisors of D. In particular

$$D' = \begin{cases} D & \text{if } D \equiv 1 \mod 4 \\ \frac{D}{2} & \text{if } D = 4d, d \equiv 3 \mod 4 \\ \frac{D}{4} & \text{if } D = 4d, d \equiv 2 \mod 4. \end{cases}$$

Finally, we denote by Fund^+ the set of positive fundamental discriminants D such that $\varepsilon(D)$ has norm 1.

Remark 3.2. Notice that if $2^2 \mid\mid D$ then automatically $D \in \mathrm{Fund}^+$. This follows from Lemma 1.31.

The aim of this chapter is the proof of the following result.

Theorem 3.3. *For every $D \in \mathrm{Fund}^+$ there exist exactly two distinct positive divisors of D' among the set of norms of principal ideals of $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$, both different from 1 and $\frac{D}{(4,D)}$. We denote by $\Phi(D)$ the minimum of these two distinct divisors of D'.*

3.1 Legendre and Dirichlet's transformation

Remark 3.4. Let d be a nonsquare positive integer. We rewrite (1.2) as

$$\frac{T^2-1}{d} = U^2. \tag{3.1}$$

Now

$$d \mid T^2 - 1 \implies d = (T^2-1, d) = ((T+1)(T-1), d)$$

and since $(T+1, T-1) \in \{1, 2\}$, we are led to consider the two corresponding cases:

- If $(T+1, T-1) = 1$ i.e. T is even, then we deduce

$$d = (T+1, d)(T-1, d)$$

and we set $d_1 := (T+1, d)$, $d_2 := (T-1, d)$. Combining this splitting of d with (3.1) we obtain a system of equations

$$\begin{cases} T+1 = d_1U_1^2 \\ T-1 = d_2U_2^2 \\ d = d_1d_2 \\ U = U_1U_2 \\ (T+1, T-1) = 1 \end{cases} \iff \begin{cases} d_1U_1^2 - d_2U_2^2 = 2 \\ T = -1 + d_1U_1^2 \\ d = d_1d_2 \\ U = U_1U_2 \\ 2 \nmid d_1U_1, \end{cases} \tag{3.2}$$

where $2 \nmid d_1U_1$ is needed to express the coprimality of $T+1$ and $T-1$.

- If $(T+1, T-1) = 2$ we have to consider two subcases.
  - If $4 \nmid d$ then U is even and (3.1) can be written as

$$\frac{\frac{T+1}{2} \cdot \frac{T-1}{2}}{d} = \left(\frac{U}{2}\right)^2.$$

Now $(\frac{T+1}{2}, \frac{T-1}{2}) = 1$. We set $d_1 := (\frac{T+1}{2}, d)$, $d_2 := (\frac{T-1}{2}, d)$ and so applying the previous reasoning we obtain the following system of equations.

$$\begin{cases} \frac{T+1}{2} = d_1U_1^2 \\ \frac{T-1}{2} = d_2U_2^2 \\ d = d_1d_2 \\ \frac{U}{2} = U_1U_2 \\ 4 \nmid d \end{cases} \iff \begin{cases} d_1U_1^2 - d_2U_2^2 = 1 \\ T = -1 + 2d_1U_1^2 \\ d = d_1d_2 \\ U = 2U_1U_2 \\ 4 \nmid d. \end{cases} \tag{3.3}$$

  - If $4|d$ then (3.1) can be written as

$$\frac{\frac{T+1}{2} \cdot \frac{T-1}{2}}{\frac{d}{4}} = U^2.$$

Since $(\frac{T+1}{2}, \frac{T-1}{2}) = 1$ we factorize

$$\frac{d}{4} = \left(\frac{T+1}{2}, \frac{d}{4}\right)\left(\frac{T-1}{2}, \frac{d}{4}\right)$$

and we set $d_1 := (\frac{T+1}{2}, \frac{d}{4})$, $d_2 := (\frac{T-1}{2}, \frac{d}{4})$. Following the same previous idea, we obtain a system of equations

$$\begin{cases} \frac{T+1}{2} = d_1U_1^2 \\ \frac{T-1}{2} = d_2U_2^2 \\ \frac{d}{4} = d_1d_2 \\ U = U_1U_2 \end{cases} \iff \begin{cases} d_1U_1^2 - d_2U_2^2 = 1 \\ T = -1 + 2d_1U_1^2 \\ d = 4d_1d_2 \\ U = U_1U_2. \end{cases} \tag{3.4}$$

We summarize the above discussion in the following lemma.

Lemma 3.5. *Let $d, U \in \mathbb{Z}_{>0}$. Set*

$$\mathcal{A}(d, U) := \{T \geq 1 \mid T^2 - dU^2 = 1\}$$

and

$$\mathcal{B}(d,U) := \begin{cases} \{(d_1,d_2,U_1,U_2) \in \mathbb{Z}^4_{>0} \mid U_1U_2 = U, d_1d_2 = d, d_1U_1^2 - d_2U_2^2 = 2\} & \textit{if } 2 \nmid dU \\ \{(d_1,d_2,U_1,U_2) \in \mathbb{Z}^4_{>0} \mid 2U_1U_2 = U, d_1d_2 = d, d_1U_1^2 - d_2U_2^2 = 1\} & \textit{if } 2|dU, 4 \nmid d \\ \{(d_1,d_2,U_1,U_2) \in \mathbb{Z}^4_{>0} \mid U_1U_2 = U, 4d_1d_2 = d, d_1U_1^2 - d_2U_2^2 = 1\} & \textit{if } 4 \mid d. \end{cases}$$

Then in each case we have

$$\#\mathcal{A}(d,U) = \#\mathcal{B}(d,U) \in \{0,1\}.$$

Proof. Clearly $\#\mathcal{A}(d,U) \in \{0,1\}$.

- If $2 \nmid dU$, to prove $\#\mathcal{B}(d,U) \in \{0,1\}$ we fix a quadruple $(d_1,d_2,U_1,U_2) \in \mathcal{B}(d,U)$ and we show that the values of d_1, U_1 are prescribed by those of d, U. Observe that

$$d_1U_1^2 - 1 = d_2U_2^2 + 1 \implies (d_1U_1^2-1)^2 = (d_1U_1^2-1)(d_2U_2^2+1) = dU^2 + 1,$$

thus $d_1U_1^2 - 1$ is determined by d, U and the same holds for the gcd $(d_1U_1^2, d)$. We want to see that this gcd is indeed d_1. Let $q = (U_1, d_2)$ then

$$\begin{cases} q \mid d_1U_1^2 - d_2U_2^2 = 2 \\ 2 \nmid dU \end{cases} \implies q = 1 \implies (d_1U_1^2, d) = d_1.$$

We've just seen that d_1 and $d_1U_1^2$ are completely determined by d, U. Thus the same holds also for U_1.

- If $2 \mid dU, 4 \nmid d$, to prove $\#\mathcal{B}(d,U) \in \{0,1\}$ we fix a quadruple $(d_1,d_2,U_1,U_2) \in \mathcal{B}(d,U)$ and we proceed as before.

$$2d_1U_1^2 - 1 = 2d_2U_2^2 + 1 \Rightarrow (2d_1U_1^2-1)^2 = (2d_1U_1^2-1)(2d_2U_2^2+1) = dU^2 + 1,$$

thus $2d_1U_1^2 - 1$ is determined by d, U and the same holds for the gcd $(d_1U_1^2, d)$ which is trivially d_1 since $(U_1, d_2) \mid d_1U_1^2 - d_2U_2^2 = 1$.

- If $4 \mid d$ the argument is precisely the same as in the previous case.

To conclude the proof we show both the implications

$$\#\mathcal{A}(d,U) = 1 \implies \#\mathcal{B}(d,U) \geq 1$$
$$\#\mathcal{B}(d,U) = 1 \implies \#\mathcal{A}(d,U) \geq 1$$

hold. The first implication follows directly from the previous remark.
To prove the second one we notice that a quadruple $(d_1,d_2,U_1,U_2) \in \mathcal{B}(d,U)$ gives rise to an element

$$\begin{cases} T := d_1U_1^2 - 1 & \text{if } 2 \nmid dU \\ T := 2d_1U_1^2 - 1 & \text{otherwise} \end{cases}$$

belonging to $\mathcal{A}(d,U)$. □

To deal with the case $D \equiv 1 \mod 4$ we will need a little variation of the above discussion which takes care of the Pell Equation $T^2 - dU^2 = 4$.

Lemma 3.6. *Let $d, U \in \mathbb{Z}_{>0}$ such that $2 \nmid d$. Let's define*

$$\begin{aligned}\tilde{\mathcal{A}}(d,U) :=&\{T \geq 1 \mid T^2 - dU^2 = 4\}\\ \tilde{\mathcal{B}}(d,U) :=&\{(d_1,d_2,U_1,U_2) \in \mathbb{Z}^4_{>0} \mid U_1U_2 = U, d_1d_2 = d, d_1U_1^2 - d_2U_2^2 = 4\}.\end{aligned}$$

Then we have

$$\begin{aligned}\tilde{\mathcal{A}}(d,U) &= 2 \cdot \mathcal{A}\Big(d, \frac{U}{2}\Big) &&\text{if } 2 \mid U\\ \#\tilde{\mathcal{A}}(d,U) &= \#\tilde{\mathcal{B}}(d,U) \in \{0,1\} &&\text{if } 2 \nmid U.\end{aligned}$$

Proof. Clearly $\#\tilde{\mathcal{A}}(d,U) \in \{0,1\}$.
To prove $\#\tilde{\mathcal{B}}(d,U) \in \{0,1\}$ we fix a quadruple $(d_1,d_2,U_1,U_2) \in \mathcal{B}(d,U)$ and we show that the values of d_1, U_1 are prescribed by those of d, U. Observe that

$$d_1U_1^2 - 2 = d_2U_2^2 + 2 \implies (d_1U_1^2 - 2)^2 = (d_1U_1^2 - 2)(d_2U_2^2 + 2) = dU^2 + 4,$$

thus $d_1U_1^2 - 1$ is determined by d, U and the same holds for the gcd $(d_1U_1^2, d)$. Let $q = (U_1, d_2)$ then

$$\begin{cases} q \mid d_1U_1^2 - d_2U_2^2 = 4 \\ 2 \nmid d \Rightarrow 2 \nmid d_2 \end{cases} \implies q = 1 \implies (d_1U_1^2, d) = d_1$$

and we conclude as before.

Let's prove the two equalities.

- Case $2 \mid U$.
  ($\subseteq$) If $T \in \tilde{\mathcal{A}}(d,U)$ then $T^2 - dU^2 = 4$ and reducing modulo 4 we get $2 \mid T$. Hence
  $$4\Big(\Big(\frac{T}{2}\Big)^2 - d\Big(\frac{U}{2}\Big)^2\Big) = 4 \cdot 1 \implies \frac{T}{2} \in \mathcal{A}\Big(d, \frac{U}{2}\Big).$$
  ($\supseteq$) If $\tilde{T} \in \mathcal{A}\Big(d, \frac{U}{2}\Big)$ then
  $$\tilde{T}^2 - d\Big(\frac{U}{2}\Big)^2 = 1 \implies (2\tilde{T})^2 - dU^2 = 4 \implies 2\tilde{T} \in \tilde{\mathcal{A}}(d,U).$$
- Case $2 \nmid U$.
  ($\leq$) If $T \in \tilde{\mathcal{A}}(d,U)$ then $T^2 - dU^2 = 4$ and so
  $$\frac{(T+2)(T-2)}{d} = U^2.$$
  Now since $2 \nmid dU$ we deduce $2 \nmid T$ and hence $(T+2, T-2) = 1$. We can factorize
  $$d = (T+2,d)(T-2,d)$$
  and set $d_1 := (T+2,d)$, $d_2 := (T-2,d)$. Finally
  $$\begin{cases} U_1 := \sqrt{\frac{T+2}{d_1}} \\ U_2 := \sqrt{\frac{T-2}{d_2}} \end{cases} \Rightarrow \begin{cases} U_1U_2 = U \\ d_1U_1^2 - d_2U_2^2 = 4 \end{cases} \Rightarrow (d_1,d_2,U_1,U_2) \in \tilde{\mathcal{B}}(d,U).$$

($\geq$) If $(d_1, d_2, U_1, U_2) \in \tilde{\mathcal{B}}(d, U)$ then we set

$$\begin{aligned} T &:= d_2U_2^2 + 2 = d_1U_1^2 - 2 \\ U &:= U_1U_2 \end{aligned}$$

and we conclude the proof computing

$$\begin{aligned} T^2 - dU^2 &= (d_1U_1^2 - 2)(d_2U_2^2 + 2) - dU_1^2U_2^2 \\ &= dU_1^2U_2^2 + 2(d_1U_1^2 - d_2U_2^2) - 4 - dU_1^2U_2^2 \\ &= 2(d_1U_1^2 - d_2U_2^2) - 4 = 4. \end{aligned}$$

□

Remark 3.7. Notice that the implicit decomposition of Lemma 3.5

$$(d, U) \mapsto (d_1, d_2, U_1, U_2)$$

should be seen as a square rooting process. Indeed, a solution $T + U\sqrt{d}$ of (1.2) produces via Lemma 3.5 the algebraic integer $U_1\sqrt{d_1} + U_2\sqrt{d_2}$ such that

$$\begin{aligned} (U_1\sqrt{d_1} + U_2\sqrt{d_2})^2 &= d_1U_1^2 + d_2U_2^2 + 2U_1U_2\sqrt{d_1d_2} \\ &= \begin{cases} T + U\sqrt{d} & \text{if } T \text{ odd} \\ 2(T + U\sqrt{d}) & \text{if } T \text{ even.} \end{cases} \end{aligned}$$

An analogous observation could be done easily also for Lemma 3.6.

Remark 3.8. Let's consider now the special case where $d = p \equiv \pm 1 \mod 4$ is a prime number. In this case d can be only factored as $d = d_1d_2$ in two ways: either

$$\begin{cases} d_1 = 1 \\ d_2 = p \end{cases} \qquad \text{or} \qquad \begin{cases} d_1 = p \\ d_2 = 1. \end{cases}$$

Hence the study of (1.2) is reduced to the four equations

$$U_1^2 - pU_2^2 = \begin{cases} \pm 2 & \text{if } 2 \nmid U \\ \pm 1 & \text{if } 2 \mid U. \end{cases}$$

Since we are looking for nontrivial solutions we have $U_2 \geq 1$, we deduce $U_1 \geq \sqrt{p-2}$ and therefore $U \geq \sqrt{p-2}$ in any case. Let ρ be a solution of $T^2 - pU^2 = 1$ then

$$\begin{aligned} \rho &= \sqrt{pU^2 + 1} + U\sqrt{p} \\ &\geq \sqrt{p(p-2) + 1} + \sqrt{p(p-2)} \\ &> 2\sqrt{p(p-2)} > p, \end{aligned}$$

where the last inequality holds since $p \geq 3$. Hence, we deduce that the fundamental solution

$$\varepsilon_p > p$$

and, by Lemma 1.31, if $p \equiv 3 \mod 4$ the fundamental unit

$$\varepsilon(4p) > p.$$

Notice that the same holds in the case $p = 2$:

$$\varepsilon_2 = 3 + 2\sqrt{2} > 2, \qquad \varepsilon(8) = 1 + \sqrt{2} > 2.$$

3.2 Gauss's theorem on the 2-rank of C_D

Recall from Remark 1.29 the definition of the narrow ideal class group C_D.

Definition 3.9. Let K be a quadratic field of discriminant D. An element $a \in K^*$ is said to be *totally positive* if a^σ is positive for all embeddings $\sigma : N \to \mathbb{R}$.
The totally positive elements of K form a subgroup K^+ of K^* and we write $U_D^+ = U_D \cap K^+$ for the subgroup of totally positive units ($U_D = \mathcal{O}_K^*$).

Notice that if K is imaginary, i.e. has no real embeddings, then total positivity is no restriction. Hence $K^+ = K^*$, $U_D^+ = U_D$ and $Cl_D = C_D$.

Lemma 3.10. *Let K be a quadratic field and suppose $a \in K$ is such that $N_{K/\mathbb{Q}}(a) = 1$. Then there exists $b \in K^*$ such that $a = \frac{b^\sigma}{b}$ where σ denotes the non-trivial automorphism of $K/\mathbb{Q}$.*

Proof. If $a = -1$ we take $b = \sqrt{d}$. Otherwise we set $b = (1+a)^{-1}$ and then

$$\frac{1+a}{1+a^\sigma} = \frac{(1+a)a}{(1+a^\sigma)a} = \frac{(1+a)a}{a+1} = a.$$

□

Lemma 3.11. *Let K be a quadratic field. Let σ be the non-trivial automorphism of $K/\mathbb{Q}$ and let $\mathfrak{a}$ be a fractional ideal of $\mathcal{O}_K$ with the property that $\mathfrak{a}^\sigma = \mathfrak{a}$. Then $\mathfrak{a} = r\mathfrak{q}$ where $r \in \mathbb{Q}_{>0}$ and $\mathfrak{q}$ is a squarefree ideal divisible only by prime ideals lying over ramified primes.*

Proof. Up to computing a greatest common divisors and keeping it in mind we can assume $\mathfrak{a}$ be an integral ideal.
Consider the prime factorization $\mathfrak{a} = \mathfrak{p_1}^{e_1} \dots \mathfrak{p_n}^{e_n}$, by multiplicativity of the norm we have

$$N(\mathfrak{a}) = N(\mathfrak{p_1}^{e_1} \dots \mathfrak{p_n}^{e_n}) = N(\mathfrak{p_1})^{e_1} \dots N(\mathfrak{p_n})^{e_n}.$$

Let $\mathfrak{p}$ be a prime ideal over a prime p then $(N(\mathfrak{p})) = (p) = \mathfrak{p}\mathfrak{p}^\sigma$ since the Galois group acts transitively on primes above a prime integer p. We deduce that $(N(\mathfrak{a})) = \mathfrak{a}\mathfrak{a}^\sigma$.
We can assume the $\mathfrak{p_i}$'s are such that $\mathfrak{p_i}\mathfrak{p_i}^\sigma = (p_i) \neq (p_j) = \mathfrak{p_j}\mathfrak{p_j}^\sigma$ for $i \neq j$ and so in particular we can assume $\mathfrak{p_i} \neq \mathfrak{p_j}^\sigma$ for $i \neq j$. If it is so then we can write, wlog $i < j, e_i \geq e_j$,

$$\mathfrak{a} = \underbrace{p_j^{e_j}}_{\in \mathbb{Z}_{>0}} \mathfrak{p_1}^{e_1} \dots \mathfrak{p_i}^{e_i - e_j} \dots \mathfrak{p_j}^0 \dots \mathfrak{p_n}^{e_n} \tag{3.5}$$

and in order to reach our aim we can work without the factor $(p_j^{e_j})$.
Suppose now that $\mathfrak{a} = \mathfrak{a}^\sigma$, we get

$$\begin{aligned}(N(\mathfrak{a})) = \mathfrak{a}\mathfrak{a}^\sigma = \mathfrak{a}^2 = \\ = \mathfrak{p_1}^{e_1} \dots \mathfrak{p_n}^{e_n} (\mathfrak{p_1}^\sigma)^{e_1} \dots (\mathfrak{p_n}^\sigma)^{e_n} = \mathfrak{p_1}^{2e_1} \dots \mathfrak{p_n}^{2e_n}\end{aligned}$$

and by uniqueness of factorization $\mathfrak{p_i}^\sigma = \mathfrak{p_i}$ for all i otherwise $\mathfrak{p_i} = \mathfrak{p_j}^\sigma$ for some $i \neq j$ and this contradicts our assumption.
We immediately deduce that $\mathfrak{p_i}$'s are lying over ramified primes since $\mathfrak{p_i}^2 = (p_i)$. In particular

$$\mathfrak{a} = r_1 r_2 r_3 \mathfrak{p_1}^{l_1} \dots \mathfrak{p_n}^{l_n}$$

where $r_1 \in \mathbb{Q}_{>0}$ is given by the first assumption, $r_2 \in \mathbb{Z}_{>0}$ is determined by (3.5) , $r_3 := p_1^{\lfloor \frac{e_1}{2} \rfloor} \dots p_n^{\lfloor \frac{e_n}{2} \rfloor} \in \mathbb{Z}_{>0}$ and $l_i \in \{0, 1\}$. □

Remark 3.12. Recall that the ramified primes p in a quadratic field of fundamental discriminant D are exactly the ones dividing D.

Theorem 3.13. *Let K be a quadratic field and let D be its discriminant. Let $\mathcal{S}$ be the group of $\mathcal{O}_K$-fractional ideals of the form $\prod_j \mathfrak{p_j}^{v_j}$, where the $\mathfrak{p_j}$'s denote prime ideals lying over ramified primes and $v_i \in \mathbb{Z}$ for all j. We define the group homomorphism*

$$\begin{aligned} \nu : \mathcal{S} &\longrightarrow C_D \\ \mathfrak{a} &\longmapsto [\mathfrak{a}]. \end{aligned}$$

Let $C_{D,2} := \{g \in C_D : g^2 = 1\}$ and $\mathcal{S}^2 := \{\mathfrak{a}^2 : \mathfrak{a} \in \mathcal{S}\}$ then ν induces a surjection

$$\tilde{\nu} : {}^{\mathcal{S}}\!/_{\mathcal{S}^2} \longrightarrow C_{D,2}$$

whose kernel has order 2.

Proof. We split the proof in two parts.

- Let's prove that $\operatorname{im} \nu = C_{D,2}$.
  ($\subseteq$) As we've already noticed, if $\mathfrak{p}$ denotes a prime ideal of $\mathcal{O}_K$ dividing a ramified prime p then $\mathfrak{p}^2 = (p) \in P_D^+$. This implies that $\mathcal{S}^2 \subseteq \ker \nu$ and hence $\operatorname{im} \nu \subseteq C_{D,2}$.
  ($\supseteq$) Let σ be the non-trivial automorphism of $K/\mathbb{Q}$ and c be an element of C_D. Notice that c has always an integral ideal $\mathfrak{a}$ as representative.

  $$\mathfrak{a}\mathfrak{a}^\sigma = (N(\mathfrak{a})) \implies c^{1+\sigma} = 1$$

  thus

  $$c^{1-\sigma} = c^{1+\sigma} c^{-2\sigma} = c^{-2\sigma}$$

  which implies the equalities

  $$\begin{cases} C_{D,2} = \ker(1 - \sigma : C_D \to C_D) \\ (C_D)^2 = (C_D)^{1-\sigma}. \end{cases} \tag{3.6}$$

  Now suppose $c^2 = 1$ and choose an ideal $\mathfrak{a}$ which is a representative of c. Then by (3.6) there exists $a \in K^+$ such that $\mathfrak{a}^{1-\sigma} = (a)$ and so

  $$(N_{K/\mathbb{Q}}(a)) = (a^{1+\sigma}) = \mathfrak{a}^{(1-\sigma)(1+\sigma)} = (N(\mathfrak{a})^{1-\sigma}) = \mathcal{O}_K.$$

  It follows that $N_{K/\mathbb{Q}}(a) = \pm 1$ and so, since $a \in K^+$, $N_{K/\mathbb{Q}}(a) = 1$. Hence by Lemma 3.10 there exists $b \in K^*$ such that $a = b^{\sigma - 1}$. Since $a \in K^+$, b and b^σ must have the same sign and so, up to change the sign, we can assume b totally positive. Now

  $$\mathfrak{a}^{1-\sigma} = (a) = (b^{\sigma-1}) \implies b^\sigma \mathfrak{a}^\sigma = b\mathfrak{a}$$

  and so by Lemma 3.11

  $$b\mathfrak{a} = r\mathfrak{a}_1, \qquad r \in \mathbb{Q}_{>0}, \mathfrak{a}_1 \in \mathcal{S}.$$

  We conclude $\operatorname{im} \nu \supseteq C_{D,2}$ showing

  $$\nu(\mathfrak{a}_1) = [\mathfrak{a}_1] = [r\mathfrak{a}_1] = [\mathfrak{a}] = c.$$

- The aim of the second part is to prove $[\ker\nu : \mathcal{S}^2] = 2$.
First, we notice that if $v \in U_D^+$ then $v^{1+\sigma} = N_{K/\mathbb{Q}}(v) = 1$. Hence the identity
$$v^{1-\sigma} = v^{1+\sigma+1-\sigma} = v^2$$
implies
$$(U_D^+)^{1-\sigma} = (U_D^+)^2. \tag{3.7}$$
Suppose $\mathfrak{a} \in \ker\nu$ so $\mathfrak{a} = (a)$ for some $a \in K^+$, since $\mathfrak{a} \in \mathcal{S}$ we have clearly $\mathfrak{a}^\sigma = \mathfrak{a}$. Hence
$$\mathcal{O}_K = \mathfrak{a}^{1-\sigma} = (a^{1-\sigma}) \Rightarrow a^{1-\sigma} \in U_D \underbrace{\Rightarrow}_{a\in K^+} a^{1-\sigma} \in U_D^+.$$
Given $\mathfrak{a}$, a is unique only up to a totally positive multiplicative unit; however (3.7) implies that for $v \in U_D^+$
$$a^{1-\sigma} \equiv (av)^{1-\sigma} \mod (U_D^+)^2.$$
Thus we deduce a well defined group homomorphism
$$\begin{aligned}\rho : \ker\nu &\longrightarrow U_D^+ / (U_D^+)^2\\ \mathfrak{a} &\longmapsto a^{1-\sigma}.\end{aligned}$$
Let's prove that $\ker\rho = \mathcal{S}^2$ and ρ is surjective.
  - ($\supseteq$) Again, if $\mathfrak{a} \in \mathcal{S}$ then $\mathfrak{a}^2 = (a)$ for some $a \in \mathbb{Q}_{>0}$. So $\mathfrak{a}^2 \in \ker\nu$ but also
  $$\mathfrak{a}^2 = (a) \longmapsto \rho(\mathfrak{a}^2) = [a^{1-\sigma}] = [1]$$
  and so $\mathcal{S}^2 \subseteq \ker\rho$.
  ($\subseteq$) Conversely, if $a \in K^+$ with $(a) \in \ker\rho$, then by (3.7) $a^{1-\sigma} = v^2 = v^{1-\sigma}$ for some $v \in U_D^+$. Then $(av^{-1})^\sigma = av^{-1}$ means that this element is fixed by the action of the Galois group and so $av^{-1} \in \mathbb{Q}_{>0}$,
  $$\begin{cases} av^{-1} \in \mathbb{Q}_{>0} \\ (av^{-1}) = (a) \in \mathcal{S} \end{cases} \implies (a) \in \mathcal{S}^2.$$
  This concludes that also $\ker\rho \subseteq \mathcal{S}^2$.
  - Let now $v \in U_D^+$ so $N_{K/\mathbb{Q}}(v) = 1$, thus by Lemma 3.10 there exists $a \in K^*$ such that $a^{1-\sigma} = v$. As we said in the first part of the proof, we can assume a totally positive. Moreover
  $$(a)^\sigma = (a^\sigma v) = (a),$$
  then applying Lemma 3.11 we can write $a = ra_1$, where $r \in \mathbb{Q}_{>0}$, $a_1 \in K^+$ and $(a_1) \in \mathcal{S}$ (in particular is in $\ker\nu$). Hence
  $$a_1^{1-\sigma} = a^{1-\sigma} = v \implies \rho((a_1)) \equiv v \mod (U_D^+)^2$$
  and this shows that ρ is surjective.

So far we've proven

$$\ker \nu/_{\mathcal{S}^2} \cong U_D^+/_{(U_D^+)^2}.$$

We conclude the proof of the theorem showing that one always has

$$[U_D^+ : (U_D^+)^2] = 2.$$

If K is real then we deduce from Dirichlet's unit theorem that U_D^+ is infinite and cyclic, therefore the previous equality holds. In the other case, if K is imaginary then it follows from Remark 2.11 that $U_D^+ = U_D = \mu_D$ where μ_D is the cyclic group of roots of unity in K and it's of order w. Notice that w is always even and so the number of squares in μ_D is the half of w, therefore the previous equality holds.

□

3.3 Proof of the main statement

In this section we are going to prove Th. 3.3. We will need a preliminary result that we present without proof, see [[21], § 3.3.5] for an exhaustive discussion of it.

Theorem 3.14. *Let D be a positive fundamental discriminant. There exists a group F_∞ such that one has a short exact sequence*

$$1 \longrightarrow F_\infty \longrightarrow C_D \longrightarrow Cl_D \longrightarrow 1,$$

in particular $|F_\infty| = [P_D : P_D^+]$ is at most 2.
Moreover $|F_\infty|$ is exactly 2 if and only if $\varepsilon(D)$ is of norm 1.

proof of Theorem 3.3. Let p_i's be the pairwise distinct ramified primes in $\mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ for $1 \leq i \leq t$, i.e. the distinct prime divisors of D. We denote by $\mathfrak{p}_i \trianglelefteq \mathcal{O}_{\mathbb{Q}(\sqrt{D})}$ the prime ideal above p_i for all i and we define

$$M := \{\mathfrak{p}_1{}^{\delta_1} \dots \mathfrak{p}_t{}^{\delta_t} \mid \delta_i \in \{0,1\} \text{ for all } i\}$$

which is the set of ideals of norm dividing D'.
In the notation of Th. 3.13 we notice that M generates the group $\mathcal{S}$ and one has the surjection

$$\tilde{\nu} : \mathcal{S}/_{\mathcal{S}^2} \longrightarrow C_{D,2}$$

whose kernel has order 2. Hence each class in $C_{D,2}$ has exactly two representatives $\mathfrak{a}_1 := \mathfrak{p}_1{}^{\alpha_1} \dots \mathfrak{p}_t{}^{\alpha_t}$, $\mathfrak{a}_2 := \mathfrak{p}_1{}^{\beta_1} \dots \mathfrak{p}_t{}^{\beta_t}$ in $\mathcal{S}/_{\mathcal{S}^2}$. Up to multiplying or diving by $(p_i) \in \mathcal{S}^2$ for some i we can assume $\alpha_j, \beta_j \in \{0,1\}$ and so $\mathfrak{a}_1, \mathfrak{a}_2 \in M$.
In particular P_D^+, which is the trivial class of $C_{D,2}$, has two representatives in M: (1) and a non-trivial ideal $\mathfrak{a} \in M$.
By definition of M we have $N(\mathfrak{a}) \mid D'$. We want to see that $N(\mathfrak{a}) \neq \frac{D}{(D,4)}$. Assume $(a) = \mathfrak{a} = \mathfrak{p}_1{}^{\alpha_1} \dots \mathfrak{p}_t{}^{\alpha_t}$ is such that $N(\mathfrak{a}) = \frac{D}{(D,4)}$, then

$$(N(\mathfrak{a})) = \mathfrak{p}_1{}^{2\alpha_1} \dots \mathfrak{p}_t{}^{2\alpha_t} = \mathfrak{a}^2 = (a^2)$$

and we can assume $a^2 = \frac{D}{(D,4)}$. We deduce that $\mathfrak{a} = (\sqrt{\frac{D}{(D,4)}})$ but this leads to a contradiction since D positive and so $\sqrt{\frac{D}{(D,4)}}$ is of norm $-\frac{D}{(D,4)}$, which is negative, but $\mathfrak{a}$ is representative of the trivial class in $C_{D,2}$.

Thanks to the Legendre-Dirichlet transformation presented in the previous section we can describe explicitly the ideal $\mathfrak{a}$. To detect the ideal $\mathfrak{a}$, recall that it has to be different from (1), principal and generated by an element of positive norm. These conditions automatically imply that $\mathfrak{a}$ is the ideal we're looking for. We are going to split this discussion in three cases, according to divisibility properties of D.

1. Case $2^2 \mid\mid D$, i.e. $D = 4d$, $d \equiv 3 \mod 4$.
   $\varepsilon(D) = T + U\sqrt{d}$ is such that $T^2 - dU^2 = 1$ since $D \in \text{Fund}^+$.

   - If T is even we consider the system of equations (3.2). We see that the integer $2d_1 > 1$ divides
     $$D' = \frac{D}{2} = 2d = 2d_1 d_2$$
     and the algebraic integer $d_1U_1 + U_2\sqrt{d}$ is of norm
     $$N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(d_1U_1 + U_2\sqrt{d}) = d_1^2U_1^2 - dU_2^2 = d_1(d_1U_1^2 - d_2U_2^2) = 2d_1 > 1.$$
     Hence we set $\mathfrak{a} := (d_1U_1 + U_2\sqrt{d})$. Observe also that $U_1\sqrt{d} + U_2d_2$ is of norm $-2d_2 < 0$.
   - If T is odd we consider the system of equations (3.3). By Remark 3.7
     $$\varepsilon(D) = T + U\sqrt{D} = (U_1\sqrt{d_1} + U_2\sqrt{d_2})^2.$$
     If $d_1 = 1$ then $d = d_2$ and $U_1\sqrt{d_1} + U_2\sqrt{d_2} = U_1 + U_2\sqrt{d}$ will be such that $U_1^2 - dU_2^2 = 1$ which contradicts the minimality of $\varepsilon(D)$, therefore $d_1 > 1$. The algebraic integer $d_1U_1 + U_2\sqrt{d}$ is of norm
     $$N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}(d_1U_1 + U_2\sqrt{d}) = d_1^2U_1^2 - dU_2^2 = d_1(d_1U_1^2 - d_2U_2^2) = d_1 > 1.$$
     Hence we set $\mathfrak{a} := (d_1U_1 + U_2\sqrt{d})$. Observe also that $U_1\sqrt{d} + U_2d_2$ is of norm $-d_2 < 0$.

2. Case $2 \nmid D$, i.e. $D = d$, $d \equiv 1 \mod 4$.
   $\varepsilon(D) = \frac{T+U\sqrt{d}}{2}$ where $T \equiv U \mod 2$. If T and U are both even we can argue as in the previous case with $\frac{T}{2}$ odd. Indeed, if $\frac{T}{2}$ even then
   $$\left(\frac{T}{2}\right)^2 - d\left(\frac{U}{2}\right)^2 = 1 \underbrace{\Longrightarrow}_{\text{reducing mod 4}} \left(\frac{U}{2}\right)^2 \equiv -1 \mod 4$$
   and this is not possible since -1 is not a square modulo 4. Assume now T, U both odd and fix the notation as in Lemma 3.6. T and U satisfy $T^2 - dU^2 = 4$ and
   $$\varepsilon(D) = \frac{T + U\sqrt{d}}{2} = \left(\frac{U_1\sqrt{d_1} + U_2\sqrt{d_2}}{2}\right)^2.$$
   As before, if $d_1 = 1$ this contradicts the minimality of $\varepsilon(D)$ since $\frac{U_1+U_2\sqrt{d}}{2}$ becomes of norm 1, therefore $d_1 > 1$. The algebraic integer $\frac{d_1U_1+U_2\sqrt{d}}{2}$ is of norm
   $$N_{\mathbb{Q}(\sqrt{D})/\mathbb{Q}}\left(\frac{d_1U_1 + U_2\sqrt{d}}{2}\right) = \frac{d_1^2U_1^2 - dU_2^2}{4} = d_1\frac{d_1U_1^2 - d_2U_2^2}{4} = d_1 > 1.$$
   Hence we set $\mathfrak{a} := (\frac{d_1U_1+U_2\sqrt{d}}{2})$. Observe also that $\frac{U_1\sqrt{d}+d_2U_2}{2}$ is of norm $-d_2 < 0$.

3. Case $2^3 \mid D$, i.e. $D = 4d$, $d \equiv 2 \mod 4$.
   $\varepsilon(D) = T + U\sqrt{d}$ and satisfies $T^2 - dU^2 = 1$. Rewriting it as

$$dU^2 = T^2 - 1 = (T-1)(T+1)$$

   we deduce T odd and U even, since $2 \mid\mid d$. We consider the system of equations (3.3) and by Remark 3.7

$$\varepsilon(D) = (U_1\sqrt{d_1} + U_2\sqrt{d_2})^2.$$

   As before we deduce $d_1 > 1$ and we set $\mathfrak{a} := (d_1U_1 + U_2\sqrt{d})$. Again, the algebraic number $U_1\sqrt{d} + d_2U_2$ is of norm $-d_2 < 0$.

At this point we want to understand how the elements of P_D are represented in M. Th. 3.14, together with $D \in \text{Fund}^+$, implies $[P_D : P_D^+] = 2$ and then P_D has four representatives in M by the above discussion. We can give an explicit description of these four ideals.
P_D is the disjoint union of two cosets with respect to the subgroup P_D^+. In the coset P_D^+ we have already exhibited the two elements

$$(1), \qquad \mathfrak{a} = (a).$$

We now investigate the last two elements coming from the other coset. In this coset has to lie the ideal

$$(\sqrt{d}),$$

since the algebraic integer $\sqrt{d}$ has norm $-d < 0$ dividing D', in particular this implies that $(\sqrt{d}) \in M$. Let $\mathfrak{b}$ be the fourth ideal we are looking for. From what we've observed during the discussion of $\mathfrak{a}$, we realize that

$$\mathfrak{b} = \begin{cases} \left(\dfrac{U_1\sqrt{d} + d_2U_2}{2}\right) & \text{if } D = d \equiv 1 \mod 4 \\ (U_1\sqrt{d} + d_2U_2) & \text{otherwise.} \end{cases}$$

Finally, if $2^2 || D = 4d$ and $\varepsilon(D) = T + U\sqrt{d}$ with T even, then

$$\begin{cases} N((1)) = 1 & N((\sqrt{d})) = d \\ N(\mathfrak{a}) = 2d_1 & N(\mathfrak{b}) = 2d_2, \end{cases}$$

otherwise

$$\begin{cases} N((1)) = 1 & N((\sqrt{d})) = d \\ N(\mathfrak{a}) = d_1 & N(\mathfrak{b}) = d_2. \end{cases}$$

□

Remark 3.15. Observe that, in the notation of the previous proof, starting from the ideals $(a), (\sqrt{d})$ we can present a constructive way to detect the fourth ideal $\mathfrak{b}$.
In the decomposition of $(a\sqrt{d})$ as a product of prime ideals, the $\mathfrak{p}_i$'s are the only prime ideals that may appear. Reducing the exponent of each $\mathfrak{p}_i$ modulo 2 and recalling that ${\mathfrak{p}_i}^2 = (p_i)$ for each i, we obtain a principal ideal

$$\mathfrak{b} := {\mathfrak{p}_1}^{\delta_1} \dots {\mathfrak{p}_t}^{\delta_t} = \left(\frac{a\sqrt{d}}{\prod_{i=1}^{t} p_i^{\gamma_i}}\right) \in M,$$

where $\delta_i \in \{0,1\}$ and $\gamma_i \in \mathbb{N}$.
The generator of this ideal has negative norm and is different from $(\sqrt{d})$, otherwise this implies $(a) = (1)$ which is not the case.

Recall now $d = d_1 d_2$ and $\mathfrak{a}, (\sqrt{d}) \in M$. In the cases $N(\mathfrak{a}) = d_1$, we have $N(\mathfrak{a}) \mid d$ therefore all primes appearing in the factorization of $\mathfrak{a}$ appear also in the factorization of the ideal $(\sqrt{d})$, i.e. $\mathfrak{a} \mid (\sqrt{d})$.

$$(a\sqrt{d}) = \frac{\mathfrak{a}}{\mathfrak{a}}(a)(\sqrt{d}) = \mathfrak{a}^2 \frac{(\sqrt{d})}{\mathfrak{a}} \implies \mathfrak{b} = \frac{(\sqrt{d})}{\mathfrak{a}}, N(\mathfrak{b}) = d_2$$

Now, if $N(\mathfrak{a}) = 2d_1$ what we said in the previous case is true except for the prime ideal $\mathfrak{p}$ above 2, i.e. $\mathfrak{a} \mid \mathfrak{p}(\sqrt{d})$. In the construction of $\mathfrak{b}$, multiplying $(a\sqrt{d})$ by (2) has no influence since the last one is equal to $\mathfrak{p}^2$.

$$(2a\sqrt{d}) = \mathfrak{a}^2 \frac{(2\sqrt{d})}{\mathfrak{a}} \implies \mathfrak{b} = \frac{(2\sqrt{d})}{(a)}, N(\mathfrak{b}) = \frac{4d}{2d_1} = 2d_2$$

From the above proof, we deduce an explicit description of $\Phi(D)$.

Corollary 3.16. *Let $D \in \mathrm{Fund}^+$ and $d := \frac{D}{(4,D)}$. Let $d = d_1 d_2$ be the coprime factorization of d obtained from (3.2), (3.3) or Lemma 3.6. Then*

$$\Phi(D) = \begin{cases} \min(2d_1, 2d_2) & \text{if } 2^2 \mid\mid D, T \text{ even} \\ \min(d_1, d_2) & \text{otherwise,} \end{cases}$$

where in the first case $\varepsilon(D) = T + U\sqrt{d}$.

Remark 3.17. As a consequence

$$\Phi(D) < \begin{cases} \sqrt{D} & \text{if } 2^2 \mid\mid D, T \text{ even} \\ \sqrt{d} & \text{otherwise,} \end{cases}$$

where in the first case $\varepsilon(D) = T + U\sqrt{d}$.

Example 3.18. Let $D = 12$ then $D' = 6$ and $d = 3$, we have $\varepsilon(D) = 2 + \sqrt{3}$ and so we are in the first case of the previous corollary/remark. In the notation of the main theorem

$$\begin{aligned} (\sqrt{d}) &= (\sqrt{3}) & N_{\mathbb{Q}(\sqrt{12})/\mathbb{Q}}(\sqrt{3}) &= -3 \mid D', \\ \mathfrak{a} &= (3 + \sqrt{3}) & N_{\mathbb{Q}(\sqrt{12})/\mathbb{Q}}(3 + \sqrt{3}) &= 6 \mid D'. \end{aligned}$$

To detect $\mathfrak{b}$ we follow the constructive strategy:

$$\mathfrak{a}(\sqrt{d}) = (3)(1 + \sqrt{3}) \implies \mathfrak{b} = (1 + \sqrt{3}),$$

since $(3)(1 + \sqrt{3})$ is congruent to $(1 + \sqrt{3})$ modulo squares. Notice that

$$N_{\mathbb{Q}(\sqrt{12})/\mathbb{Q}}(1 + \sqrt{3}) = -2 \mid D',$$

therefore

$$\Phi(D) = \min(2, 6) = 2 \not< \sqrt{d} = \sqrt{3}.$$

This example shows that one cannot extend the previous remark to assert that $\Phi(D) < \sqrt{d}$ for any $D \in \mathrm{Fund}^+$. One observes also that at most one of $2d_1, 2d_2$ is larger than d, otherwise if $2d_1, 2d_2 \geq d$ leads to a contradiction since $d = d_1 d_2$.

Remark 3.19. Let D be a positive fundamental discriminant which is not in Fund^+ and $d = \frac{D}{(D,4)}$. In the notation of the proof of Th. 3.3, we have $P_D = P_D^+$ and so the number of representatives of P_D in M is two. Clearly the first representative is (1); we deduce the second one from the fact that $\varepsilon(D)$ has norm -1 and so d is the norm of the totally positive algebraic integer $\varepsilon(D)\sqrt{d}$. Therefore, in this case we conclude that the only two divisors of D' among norms of integral principal ideals generated by totally positive elements are 1 and d.

Chapter 4

Density of Fundamental Discriminants

4.1 Density and main statement

Definition 4.1. Let $\mathcal{S}$ be a subset of positive integers, $\mathcal{S}$ is said to have *positive density* if

$$\liminf_{x\to\infty} \frac{\#\{n \in \mathcal{S} : 1 \leq n \leq x\}}{x} > 0.$$

The set $\mathcal{S}$ is said to be *negligible* if

$$\limsup_{x\to\infty} \frac{\#\{n \in \mathcal{S} : 1 \leq n \leq x\}}{x} = 0.$$

Notation 4.2. The expression $f(x) \ll g(x)$ means essentially $f(x) \leq O(g(x))$ as $x \to \infty$.

Remark 4.3. Let $\mathcal{F}$ be the set of positive fundamental discriminants and let $x \in \mathbb{R}_{>1}$, we want to estimate

$$\#\{D \in \mathcal{F} : 1 \leq D \leq x\}.$$

Any fundamental discriminant $1 \leq D \leq x$ corresponds to a unique squarefree integer $d = \frac{D}{(4,D)}$ such that $1 \leq d \leq x$ and, on the other hand, any squarefree integer $1 \leq d \leq \frac{x}{4}$ corresponds uniquely to a fundamental discriminant $1 \leq D \leq x$. Then

$$\sum_{n\leq \frac{x}{4}} \mu^2(n) \leq \#\{D \in \mathcal{F} : 1 \leq D \leq x\} \leq \sum_{n\leq x} \mu^2(n).$$

By Remark 1.12, we deduce $\#\{D \in \mathcal{F} : 1 \leq D \leq x\} \gg x$ and therefore

$$\liminf_{x\to\infty} \frac{\#\{D \in \mathcal{F} : 1 \leq D \leq x\}}{x} > 0,$$

which means that the set of fundamental discrimants has positive density.

We are going to deal only with fundamental discriminants D such that $\varepsilon(D)$ has positive norm, i.e. $\text{Fund}^+ \subset \mathcal{F}$; one can see that this is not a "big restriction" in terms of density. The evidence of this fact is represented by an important result from Landau, see [[5], § 7.5].

Theorem 4.4. *Let x be a positive real number greater than 1, the set of integers $1 \leq n \leq x$ that can be written as a sum of two squares has cardinality*

$$\#\{1 \leq n \leq x : n = a^2 + b^2, a, b \in \mathbb{N}_{>0}\} = O\Big(\frac{x}{\sqrt{\log x}}\Big).$$

We need also an elementary number theory result, see [[19], § 18].

Theorem 4.5. *Let n be a positive integer, then*

$$n = a^2 + b^2 \qquad \exists\, a, b \in \mathbb{N}_{>0}$$

if and only if any prime $p \equiv 3 \mod 4$ dividing n appears with even exponent in its factorization.

Remark 4.6. At this point, we are ready to investigate the density of the set $\mathcal{F} \setminus \mathrm{Fund}^+$. Remark 1.32 implies that if $D \in \mathcal{F}$ and $\varepsilon(D)$ has norm -1, then D is in the set of *special discriminants*. These are the positive fundamental discriminants only divisible by 2 or primes congruent to 1 modulo 4. Therefore, applying Th. 4.5,

$$\begin{aligned}\{1 \leq D \leq x : D \in \mathcal{F} \setminus \mathrm{Fund}^+\} &\subset \{1 \leq D \leq x : D \in \mathcal{F}, (p|D \Rightarrow p = 2 \text{ or } p \equiv 1(4))\} \\ &\subset \{1 \leq n \leq x : (p|n \Rightarrow p = 2 \text{ or } p \equiv 1(4))\} \\ &\subset \{1 \leq n \leq x : n = a^2 + b^2, \exists\, a, b \in \mathbb{N}_{>0}\}.\end{aligned}$$

Finally, Th. 4.4 allows us to conclude that the set $\mathcal{F} \setminus \mathrm{Fund}^+$ is negligible, since

$$\limsup_{x \to \infty} \frac{\#\{D \in \mathcal{F} \setminus \mathrm{Fund}^+ : 1 \leq n \leq x\}}{x} \leq \limsup_{x \to \infty} \frac{\#\{1 \leq n \leq x : n = a^2 + b^2\}}{x} = 0.$$

The aim of this chapter is to prove that there is a positive density of fundamental discriminants $D > 0$ with large regulator $R(D)$. More precisely, the following theorem says that the fundamental unit $\varepsilon(D)$ is essentially greater than D^3 for a positive density of D's.

Theorem 4.7. *For every $\delta > 0$ there exists $x_0(\delta) > 0$ and $c_0(\delta) > 0$ such that*

$$\#\{D \in \mathrm{Fund}^+ : x < D \leq 2x, 2^2 || D, \Phi(D) < D^\delta, \varepsilon(D) \geq D^{3-\delta}\} \geq c_0(\delta) x \tag{4.1}$$

for every $x > x_0(\delta)$, where $\Phi(D)$ is defined in Th. 3.3.
The condition $2^2||D$ can be replaced by $8 \mid D$ or $2 \nmid D$.

Remark 4.8. One may object that there is some redundancy in imposing both conditions $D \in \mathrm{Fund}^+$ and $2^2||D$ by Lemma 1.31. However the norm of the fundamental unit is of course no longer automatically positive in the cases $2 \nmid D$ and $8 \mid D$, as one can deduce from Example 1.34.

4.2 $D \in \mathrm{Fund}^+$ with small regulator

In this section we are going to deal only with the case $2^2||D$.

Notation 4.9. The letter p always denotes a prime number. The condition $n \sim N$ means that the integer n has to satisfy the inequalities $N < n \leq 2N$. However, it will be clear from the context when the symbol $\sim$ denotes asymptotic behavior of functions.

Now, we recall a stronger version of the *Dirichlet's prime number theorem in arithmetic progression* which is a consequence of the *Siegel-Walfisz Theorem*, the reader can find a complete treatment of it in [[24], Th. 8.17].

Theorem 4.10. *Let q, a be integers satisfying $q \geq 1$ and $(a, q) = 1$ and x be a positive real number. Define as $\pi(x; q, a)$ the cardinality of the set of prime numbers congruent to a modulo q and not exceeding x. For every constant $A > 0$, there exists a constant $c = c(A)$ such that*

$$\pi(x; q, a) = \frac{\mathrm{Li}(x)}{\varphi(q)} + O(x \exp(-c\sqrt{\log x})),$$

holds uniformly for $x \geq 3$ and for $q \leq \log^A x$, where $\mathrm{Li}(x) = \int_2^x \frac{1}{\log t}\, dt$.

Remark 4.11. Applying integration by part

$$\begin{aligned}\mathrm{Li}(x) &= \frac{x}{\log x} - \frac{2}{\log 2} - \int_2^x \frac{t(-1)}{t(\log t)^2}\, dt \\ &= \frac{x}{\log x} - \frac{2}{\log 2} + \int_2^x \frac{1}{(\log t)^2}\, dt \\ &= \frac{x}{\log x} + O\Big(\frac{x}{\log^2 x}\Big).\end{aligned}$$

Let D be a fundamental discriminant such that $2^2||D$, hence $d = \frac{D}{4}$ is squarefree and congruent to 3 modulo 4. Let K be the quadratic field $\mathbb{Q}(\sqrt{D})$, as we said in the first chapter

$$\mathcal{O}_K = \mathbb{Z}[\sqrt{d}]$$

and by Lemma 1.31

$$T + U\sqrt{d} \in \mathcal{O}_K^* \Leftrightarrow T^2 - dU^2 = 1.$$

Our strategy is to construct a sequence of fundamental discriminants D with large $\varepsilon(D) = \varepsilon_d$ starting from,

$$d = pm,$$

where $p \equiv 3 \mod 4$ and $m \equiv 1 \mod 4$ is squarefree. We keep in mind that m will be small compared to p, hence m is coprime with p.

Definition 4.12. Let m be a squarefree integer and $x \geq 2$ a real number, we define

$$\mathcal{D}_m(x) := \{pm : pm \sim x, p \geq 7, p \equiv 3 \mod 4\}.$$

Let $\delta = \delta(x) > 0$, we define

$$\mathcal{D}_m(x, \delta) := \{pm \in \mathcal{D}_m(x) : \varepsilon_{pm} \leq (4pm)^{3-\delta}\}.$$

Notice that the condition $p \geq 7$ is not so restrictive and will be clear later. The set $\mathcal{D}_m(x, \delta)$ should be thought as the subset of $\mathcal{D}_m(x)$ of elements pm with small ε_{pm}.

Remark 4.13. Consider the cardinality of the set $\mathcal{D}_m(x)$ and define the variable $y := \frac{x}{m}$. We can assume $y \geq 3$ since m is fixed and we are interested in $\mathcal{D}_m(x)$ as $x \to \infty$. It's clear from the definition that

$$\#\mathcal{D}_m(x) = \pi(2y; 4, 3) - \pi(y; 4, 3).$$

Applying Th. 4.10, we get

$$\#\mathcal{D}_m(x) = \frac{2y}{\varphi(4)\log(2y)} - \frac{y}{\varphi(4)\log y} + O\Big(\frac{y}{\log^2 y}\Big)$$

where

$$\begin{aligned}\frac{2y}{\varphi(4)\log(2y)}-\frac{y}{\varphi(4)\log y}&=y\Big(\frac{1}{\log(2y)}-\frac{1}{2\log y}\Big)\\&=\frac{y}{2}\Big(\frac{2\log y-\log 2-\log y}{\log y(\log 2+\log y)}\Big)=\frac{y}{2}\left(\frac{1-\frac{\log 2}{\log y}}{\log 2+\log y}\right).\end{aligned}$$

Therefore

$$\begin{aligned}\#\mathcal{D}_m(x)&=\frac{y}{2\log y}+O\Big(\frac{y}{\log^2 y}\Big)\\&=\frac{x}{2m\log\frac{x}{m}}+O\Big(\frac{x}{m\log^2\frac{x}{m}}\Big).\end{aligned}$$

In particular we see that for any $0<\epsilon<1$,

$$\Big|\#\mathcal{D}_m(x)-\frac{x}{2m\log\frac{x}{m}}\Big|\ll\frac{x}{\log^2 x}\tag{4.2}$$

holds uniformly for $m\le x^{\epsilon}$.

Remark 4.14. Let $C=\langle\xi\rangle$ be a cyclic group of even order $2n$. We recall that an element $g\in C$ admits at most two square roots.
Suppose that $\alpha^2=\beta^2=\gamma^2=g$, where α,β,γ are distinct elements of C. Without loss of generality, we can assume that there exist $1\le c<b<a\le 2n$ integers such that

$$\xi^a=\alpha,\xi^b=\beta,\xi^c=\gamma\implies\xi^{2a}=\xi^{2b}=\xi^{2c}=g.$$

Then

$$\begin{cases}\xi^{2(a-b)}=1\Rightarrow 2n>a-b=dn\Rightarrow d=1\\ \xi^{2(b-c)}=1\Rightarrow 2n>b-c=d'n\Rightarrow d'=1,\end{cases}$$

hence we get a contradiction since

$$2n>a-c=a-b+b-c=n+n=2n.$$

Theorem 4.15. *For every $\kappa>1$ there exists $c(\kappa)>0$ such that the inequality*

$$\#\mathcal{D}_m(x,\delta)\le c(\kappa)(3^{\omega(m)}m^{-1}x^{\frac12}\log^2 x+\kappa^{\omega(m)}m^{\frac12}x^{1-\frac{\delta}{2}}\log x),$$

holds for every $x\ge 2$, for every odd squarefree $m\le\sqrt{x}$ and for every $\delta=\delta(x)>0$.

Proof. Counting also solutions that may not be fundamental produces the inequality

$$\#\mathcal{D}_m(x,\delta)\le\#\{(p,T,U)\in\mathbb{N}^3_{>0}\mid pm\in\mathcal{D}_m(x),T^2-pmU^2=1,T+U\sqrt{pm}\le(4pm)^{3-\delta}\}.$$

We want to apply Lemma 3.5 with the choice $d=pm$, where m satisfies

$$2\nmid m,\qquad\mu^2(m)=1.$$

Notice that we are not requiring $m\equiv 1\mod 4$ up to now.
Let $m_1m_2=m$ be a decomposition of m. We consider the equation

$$m_1U_1^2-pm_2U_2^2=\eta\qquad\text{for }\eta\in\{\pm1,\pm2\}.\tag{4.3}$$

By the starting inequality and using the values of T appearing in (3.2) and (3.3) we get

$$\begin{aligned}
\#\mathcal{D}_m(x,\delta) &\leq \#\{(p,T,U)\in\mathbb{N}^3_{>0}|pm\in\mathcal{D}_m(x), T^2-pmU^2=1, T+U\sqrt{pm}\leq(4pm)^{3-\delta}\}\\
&=\sum_{U\geq 1}\#\{(p,T)\in\mathbb{N}^2_{>0}|pm\in\mathcal{D}_m(x), T^2-pmU^2=1, T+U\sqrt{pm}\leq(4pm)^{3-\delta}\}\\
&=\sum_{U\geq 1}\#\Big\{(p,m_1,m_2,U_1,U_2)\in\mathbb{N}^4_{>0}|m_1m_2=m, pm\in\mathcal{D}_m(x), U_1U_2=U,\\
&\qquad m_1U_1^2-pm_2U_2^2=\pm 2, -1+m_1U_1^2+U_1U_2\sqrt{pm}\leq(4pm)^{3-\delta}\Big\}+\\
&+\sum_{U\geq 1}\#\Big\{(p,m_1,m_2,U_1,U_2)\in\mathbb{N}^4_{>0}|m_1m_2=m, pm\in\mathcal{D}_m(x), 2U_1U_2=U,\\
&\qquad m_1U_1^2-pm_2U_2^2=\pm 1, -1+2m_1U_1^2+2U_1U_2\sqrt{pm}\leq(4pm)^{3-\delta}\Big\}=,
\end{aligned}$$

removing the condition in the product U_1U_2 we can forget about the external sum indexed by U,

$$\begin{aligned}
&=\#\Big\{(p,m_1,m_2,U_1,U_2)\in\mathbb{N}^4_{>0}|m_1m_2=m, pm\in\mathcal{D}_m(x),\\
&\qquad m_1U_1^2-pm_2U_2^2=\pm 2, -1+m_1U_1^2+U_1U_2\sqrt{pm}\leq(4pm)^{3-\delta}\Big\}+\\
&+\#\Big\{(p,m_1,m_2,U_1,U_2)\in\mathbb{N}^4_{>0}|m_1m_2=m, pm\in\mathcal{D}_m(x),\\
&\qquad m_1U_1^2-pm_2U_2^2=\pm 1, -1+2m_1U_1^2+2U_1U_2\sqrt{pm}\leq(4pm)^{3-\delta}\Big\}\\
&=\sum_{m_1m_2=m}\sum_{\eta=\pm 2}\#\Big\{(p,U_1,U_2)\in\mathbb{N}^3_{>0}|pm\in\mathcal{D}_m(x), m_1U_1^2-pm_2U_2^2=\eta,\\
&\qquad -1+m_1U_1^2+U_1U_2\sqrt{pm}\leq(4pm)^{3-\delta}\Big\}+\\
&+\sum_{m_1m_2=m}\sum_{\eta=\pm 1}\#\Big\{(p,U_1,U_2)\in\mathbb{N}^3_{>0}|pm\in\mathcal{D}_m(x), m_1U_1^2-pm_2U_2^2=\eta,\\
&\qquad -1+2m_1U_1^2+2U_1U_2\sqrt{pm}\leq(4pm)^{3-\delta}\Big\}.
\end{aligned} \tag{4.4}$$

To simplify the above inequality, we provide a bound for U_1, U_2 in terms of x, m, δ. We have

$$\begin{cases} m_1U_1^2-\eta=pm_2U_2^2\geq 7\\ \eta\in\{\pm 1,\pm 2\}\end{cases} \implies m_1U_1^2\geq 5$$

and therefore

$$2m_1U_1^2\geq m_1U_1^2+5\geq m_1U_1^2-\eta=pm_2U_2^2=\frac{1}{2}m_1U_1^2+\underbrace{\frac{1}{2}m_1U_1^2-\eta}_{\geq 0}\geq\frac{1}{2}m_1U_1^2.$$

Multiplying these inequalities by $\frac{m_1}{pm}$

$$\frac{1}{2}\frac{(m_1U_1)^2}{pm}\leq U_2^2\leq 2\frac{(m_1U_1)^2}{pm}\leq\frac{(2m_1U_1)^2}{pm},$$

using the assumption $pm\sim x$ and computing square roots, we obtain

$$\frac{1}{2}m_1U_1x^{-\frac{1}{2}}\leq U_2\leq 2m_1U_1x^{-\frac{1}{2}}. \tag{4.5}$$

From the inequalities defining the sets in the (4.4) we deduce

$$U_1U_2\sqrt{pm}\leq 64(pm)^{3-\delta}$$

and so

$$U_1U_2 \leq 400x^{\frac{5}{2}-\delta}.$$

From the previous inequality and (4.5), we have

$$U_2^2 \leq 2m_1U_1U_2x^{-\frac{1}{2}} \leq 800m_1x^{2-\delta} \leq 30^2m_1x^{2-\delta}$$

and so

$$U_2 \leq 30m_1^{\frac{1}{2}}x^{1-\frac{\delta}{2}} \qquad U_1 \leq 2m_1^{-1}x^{\frac{1}{2}}U_2. \tag{4.6}$$

Now we remove the condition that p is prime in (4.4). We deduce the inequality

$$\#\mathcal{D}_m(x,\delta) \leq \sum_{m_1m_2=m}\sum_{\eta=\pm1,\pm2} F(m_1,m_2,\eta), \tag{4.7}$$

where $F(m_1,m_2,\eta)$ is the number of solutions to the congruence

$$m_1U_1^2 \equiv \eta \mod m_2U_2^2,$$

with (U_1,U_2) subject to (4.6).
Let $\rho_{\eta,m_1}(t)$ be the number of solutions $0 \leq u < t$ to the congruence

$$m_1u^2 - \eta \equiv 0 \mod t,$$

where $\eta \in \{\pm1,\pm2\}$ and m_1 is odd. Let $t = p_1^{k_1}\dots p_l^{k_l}$ be the prime factorization of t, the Chinese Remainder Theorem allows us to reduce the study of $\rho_{\eta,m_1}(t)$ to $\rho_{\eta,m_1}(p_i^{k_i})$ with $p_i^{k_i}||t$ for all $1 \leq i \leq l$. Observe that in any case $(m_1,\eta) = 1$ and this implies that, if the previous congruence has a solution, we have $(m_1,p_i) = 1$ for every i. Indeed, if $p_i \mid m_1$ and $m_1u^2 - \eta \equiv 0(p_i)$ we obtain $p_i|\eta$ which is absurd. Hence m_1 is invertible modulo $p_i^{k_i}$ for every i.
In the case p_i odd, we have also $(\eta,p_i) = 1$ and so the equation

$$u^2 \equiv \eta m_1^{-1} \mod p_i^{k_i}$$

has at most two solutions since $\left(\mathbb{Z}/p_i^k\mathbb{Z}\right)^*$ is cyclic of even order and we apply the previous remark.
Let's consider now the equation

$$u^2 \equiv \eta m_1^{-1} \mod 2^k$$

in the case $p_i = 2$ for some i. Assume $(\eta,2) = 2$. If $k = 1$ then we obtain a unique solution for $u = 0$. If $k > 1$ then

$$2 \mid \eta \Rightarrow 2 \mid m_1u^2 \Rightarrow 2 \mid u \Rightarrow 4 \mid u^2 \Rightarrow 4 \mid \eta,$$

which is impossible since $\eta \in \{\pm1,\pm2\}$. Finally, we can assume $(\eta,2) = 1$. If $k = 1$ the above equation has only one solution else it has at most four solutions since $\left(\mathbb{Z}/2^k\mathbb{Z}\right)^*$ is cyclic of even order or the product of two cyclic groups of even order (see [[23], § 4.2] for instance).
So we've just proven that $\rho_{\eta,m_1}(2^k) \leq 4$ and $\rho_{\eta,m_1}(p^k) \leq 2$ for any p odd, $k \geq 1$. Then

$$\rho_{\eta,m_1}(t) \leq 2^{\omega(t)+1} \text{ for any } t \geq 1. \tag{4.8}$$

Looking back at (4.7), we have

$$\begin{aligned} F(m_1,m_2,\eta) &= \#\{(U_1,U_2)\in\mathbb{N}^2_{>0} | m_1U_1^2 \equiv \eta(m_2U_2^2), U_2 \le 30m_1^{\frac{1}{2}}x^{1-\frac{\delta}{2}}, U_1 \le 2m_1^{-1}x^{\frac{1}{2}}U_2\} \\ &= \sum_{U_2\le 30m_1^{\frac{1}{2}}x^{1-\frac{\delta}{2}}} \#\{U_1\in\mathbb{N}_{>0} | m_1U_1^2 \equiv \eta(m_2U_2^2), U_1 \le 2m_1^{-1}x^{\frac{1}{2}}U_2\}. \end{aligned}$$

We need to take care of the fact that if U_1 is an element in the right hand side set and

$$1 \le U_1 + nm_2U_2^2 \le 2m_1^{-1}x^{\frac{1}{2}}U_2 \ \exists n\in\mathbb{Z},$$

then also this element is in the same set. Thus, we split the range of U_1 in subintervals of length $m_2U_2^2$.

$$1 \le U_1 \le 2m_1^{-1}x^{\frac{1}{2}}U_2 \implies \frac{2m_1^{-1}x^{\frac{1}{2}}U_2 - 1}{m_2U_2^2} < 2\frac{x^{\frac{1}{2}}}{m_1m_2U_2}$$

and so the number of subintervals is less than

$$\left\lfloor 2\frac{x^{\frac{1}{2}}}{m_1m_2U_2}\right\rfloor + 1 \le 2\frac{x^{\frac{1}{2}}}{m_1m_2U_2} + 1.$$

At this point

$$\begin{aligned} F(m_1,m_2,\eta) &\le \sum_{U_2\le 30m_1^{\frac{1}{2}}x^{1-\frac{\delta}{2}}} \Big(2\frac{x^{\frac{1}{2}}}{m_1m_2U_2}+1\Big)\#\{U_1 | m_1U_1^2 \equiv \eta(m_2U_2^2), U_1 < m_2U_2^2\} \\ &= \sum_{U_2\le 30m_1^{\frac{1}{2}}x^{1-\frac{\delta}{2}}} \Big(2\frac{x^{\frac{1}{2}}}{m_1m_2U_2}+1\Big)\rho_{\eta,m_1}(m_2U_2^2). \end{aligned}$$

Inserting (4.8) and the above inequality in (4.7), noting also that η runs in a set of cardinality 4, we obtain

$$\begin{aligned} \#\mathcal{D}_m(x,\delta) &\le 8\sum_{m_1m_2=m}\ \sum_{U_2\le 30m_1^{\frac{1}{2}}x^{1-\frac{\delta}{2}}} 2^{\omega(m_2U_2)}\Big(2\frac{x^{\frac{1}{2}}}{m_1m_2U_2}+1\Big) \\ &\le 16\frac{x^{\frac{1}{2}}}{m}\Sigma_1 + 8\Sigma_2, \end{aligned} \tag{4.9}$$

with

$$\begin{aligned} \Sigma_1 &:= \sum_{m_1m_2=m} 2^{\omega(m_2)} \sum_{U_2\le 30m_1^{\frac{1}{2}}x^{1-\frac{\delta}{2}}} \frac{2^{\omega(U_2)}}{U_2}, \\ \Sigma_2 &:= \sum_{m_1m_2=m} 2^{\omega(m_2)} \sum_{U_2\le 30m_1^{\frac{1}{2}}x^{1-\frac{\delta}{2}}} 2^{\omega(U_2)}. \end{aligned}$$

We used the fact that clearly $\omega(m_2U_2) \le \omega(m_2)+\omega(U_2)$. Applying Lemma 1.19 and Corollary 1.20, we get

$$\Sigma_1 \ll \sum_{m_1m_2=m} 2^{\omega(m_2)}\log^2 x \underbrace{=}_{\substack{\text{Lemma 1.17}\\ \mu^2(m)=1}} 3^{\omega(m)}\log^2 x,$$

$$\Sigma_2 \ll x^{1-\frac{\delta}{2}}\log x \sum_{m_1m_2=m} 2^{\omega(m_2)}m_1^{\frac{1}{2}} = m^{\frac{1}{2}}x^{1-\frac{\delta}{2}}\log x \sum_{m_1m_2=m}\frac{2^{\omega(m_2)}}{\sqrt{m_2}}.$$

Keeping in mind m is *odd and squarefree*, by multiplicativity we see

$$\sum_{m_2|m} \frac{2^{\omega(m_2)}}{\sqrt{m_2}} = \prod_{p|m}\left(\frac{2^{\omega(1)}}{1} + \frac{2^{\omega(p)}}{\sqrt{p}}\right) = \prod_{p|m}\left(1 + \frac{2}{\sqrt{p}}\right)$$

since $p^2 \nmid m$ for any p. If we fix any $\kappa > 1$ we can find a prime p_κ such that

$$\left(1 + \frac{2}{\sqrt{p_\kappa}}\right) \leq \kappa.$$

This allows us to deduce

$$\begin{aligned} \sum_{m_2|m} \frac{2^{\omega(m_2)}}{\sqrt{m_2}} &= \prod_{p|m}\left(1 + \frac{2}{\sqrt{p}}\right) = \prod_{\substack{p|m \\ p<p_\kappa}}\left(1 + \frac{2}{\sqrt{p}}\right) \prod_{\substack{p|m \\ p\geq p_\kappa}}\left(1 + \frac{2}{\sqrt{p}}\right) \\ &\leq \prod_{p<p_\kappa}\left(1 + \frac{2}{\sqrt{p}}\right)\kappa^{\omega(m)} = c(\kappa)\kappa^{\omega(m)}. \end{aligned}$$

Hence

$$\Sigma_2 \ll_\kappa \kappa^{\omega(m)} m^{\frac{1}{2}} x^{1-\frac{\delta}{2}} \log x,$$

putting everything together in (4.9), we conclude the proof. □

4.3 $D \in \mathrm{Fund}^+$ with large regulator

We are going to present the proof of the main theorem stated in Section 4.1.

Proof of Th. 4.7, case $2^2||D$. Let γ be a constant satisfying $0 \leq \gamma \leq \frac{1}{2}$. Let

$$\mathcal{D}^\gamma(x) := \bigcup_m \mathcal{D}_m(x),$$

where the union is taken over the integers m satisfying

$$1 \leq m \leq x^\gamma, \qquad \mu^2(m) = 1, \qquad m \equiv 1 \mod 4. \tag{4.10}$$

Assume $pm = p'm' \in \mathcal{D}_m(x) \cap \mathcal{D}_{m'}(x)$. We have $pm, p'm' \sim x$ and $m, m' \leq x^\gamma$, hence for x big enough we see $m < p$ and $m' < p'$. Looking at the factorization of $pm = p'm'$ we deduce $p = p'$ and therefore $m = m'$. This reasoning shows that if $m \neq m'$ then $\mathcal{D}_m(x)$ and $\mathcal{D}_{m'}(x)$ are disjoint. In particular, we have

$$\#\mathcal{D}^\gamma(x) = \sum_{m \text{ satisfies (4.10)}} \#\mathcal{D}_m(x) = \sum_{\substack{1\leq m\leq x^\gamma \\ m\equiv 1 \mod 4}} \mu^2(m)\#\mathcal{D}_m(x).$$

Using the uniform behavior we've see in (4.2) and Th. 1.18, we get for $x \to \infty$

$$\begin{aligned} \#\mathcal{D}^\gamma(x) &\sim \sum_{\substack{1\leq m\leq x^\gamma \\ m\equiv 1 \mod 4}} \frac{\mu^2(m)x}{2m\log\frac{x}{m}} = x \sum_{\substack{1\leq m\leq x^\gamma \\ m\equiv 1 \mod 4}} \mu^2(m)\frac{1}{2m\log\frac{x}{m}} \\ &= \frac{x}{2x^\gamma\log\frac{x}{x^\gamma}} \sum_{\substack{1\leq m\leq x^\gamma \\ m\equiv 1 \mod 4}} \mu^2(m) - x\int_1^{x^\gamma} \Big(\sum_{\substack{1\leq m\leq t \\ m\equiv 1 \mod 4}} \mu^2(m)\Big) \cdot \Big(\frac{1}{2t\log\frac{x}{t}}\Big)' dt \end{aligned}$$

and by Lemma 1.11

$$\#\mathcal{D}^\gamma(x) \sim f(x) := \frac{x}{\pi^2(1-\gamma)\log x} - \frac{x}{2}\int_1^{x^\gamma} \Big(\sum_{\substack{1\le m\le t\\ m\equiv 1 \mod 4}} \mu^2(m)\Big) \cdot \frac{1+\log\frac{t}{x}}{t^2\log^2\frac{t}{x}}\, dt.$$

Keeping in mind

- $$\Big(-\frac{1}{\log\frac{t}{x}}\Big)' = \frac{1}{t\log^2\frac{t}{x}}$$
- $$\Big(\log\log\frac{x}{t}\Big)' = \frac{1}{t\log\frac{t}{x}}$$
- $$\sum_{\substack{1\le m\le t\\ m\equiv 1 \mod 4}} \mu^2(m) = \frac{2}{\pi^2}t + O(t^{\frac12}),$$

we obtain

$$\begin{aligned} f(x) &= -\frac{x}{\pi^2}\int_1^{x^\gamma} t\frac{1+\log\frac{t}{x}}{t^2\log^2\frac{t}{x}}\, dt - \frac{x}{2}\int_1^{x^\gamma} O(t^{\frac12})\frac{1+\log\frac{t}{x}}{t^2\log^2\frac{t}{x}}\, dt + O\Big(\frac{x}{\log x}\Big)\\ &= -\frac{x}{\pi^2}\Big[\log\log\frac{x}{t} - \frac{1}{\log\frac{t}{x}}\Big]_1^{x^\gamma} - \frac{x}{2}\int_1^{x^\gamma} O(t^{\frac12})\frac{1+\log\frac{t}{x}}{t^2\log^2\frac{t}{x}}\, dt + O\Big(\frac{x}{\log x}\Big)\\ &= -\frac{\log(1-\gamma)}{\pi^2}x + \frac{x\gamma}{\pi^2(\gamma-1)\log x} + O\Big(\frac{x}{\log x}\Big) + o(x) = -\frac{\log(1-\gamma)}{\pi^2}x + o(x). \end{aligned}$$

We deduce that for any $\gamma_0 > 0$ and for $x \to \infty$, one has

$$\#\mathcal{D}^\gamma(x) \sim -\frac{\log(1-\gamma)}{\pi^2}x$$

uniformly for $\gamma_0 \le \gamma \le \frac12$. The definition of γ_0 allows us to conclude the uniformity since it avoids the pathological case in which the coefficient $\log(1-\gamma)$ of the main term becomes too small with respect to x.

As we've already noticed if $m \ne m'$ then $\mathcal{D}_m(x)$ and $\mathcal{D}_{m'}(x)$ are disjoint. Let $\delta > 0$, we consider

$$\begin{aligned} \mathcal{E}(x,\delta) &:= \bigsqcup_{m \text{ sat. } (4.10)} (\mathcal{D}_m(x)\backslash\mathcal{D}_m(x,\delta))\\ &= \mathcal{D}^\gamma(x)\Big\backslash\Big(\bigsqcup_{m \text{ sat. } (4.10)} \mathcal{D}_m(x,\delta)\Big). \end{aligned}$$

Every element $pm \in \mathcal{E}(x,\delta)$ is squarefree and congruent to 3 modulo 4. Hence $D := 4pm$ is a fundamental discriminant which satisfies

$$\varepsilon_{pm} = \varepsilon(D) \ge D^{3-\delta}, \qquad 4x < D \le 8x.$$

We set $\gamma = \frac{\delta}{4}$. In the notation of the proof of Th. 4.15 and Corollary 3.16 we have $\frac{D}{4} = d_1d_2$, $d_1 = m_1$ and $d_2 = pm_2$. Therefore, up to multiply by 2, $\Phi(D) = m_1 \mid m$ and $m \le x^\gamma = x^{\frac{\delta}{4}}$. Thus the condition $\Phi(D) < D^\delta$ is automatically satisfied since $x^{\frac{\delta}{4}}$ is much smaller than D^δ. We've just proven

$$4\cdot\mathcal{E}\Big(\frac{x}{4},\delta\Big) \subseteq \{D \in \mathrm{Fund}^+ : x < D \le 2x, 2^2||D, \Phi(D) < D^\delta, \varepsilon(D) \ge D^{3-\delta}\}.$$

Applying Th. 4.15 with the choice $\kappa = 2$, the asymptotic formula for $\mathcal{D}^{\frac{\delta}{4}}(x)$ and recalling Lemma 1.19, we deduce

$$\begin{aligned}\#\mathcal{E}(x,\delta) &\geq -\frac{(1-o(1))\log(1-\frac{\delta}{4})}{\pi^2}\cdot x - O\Big(x^{1-\frac{\delta}{2}}\log x \sum_{m\leq x^{\frac{\delta}{4}}} 2^{\omega(m)}m^{\frac{1}{2}}\Big)\\ &\geq -\frac{(1-o(1))\log(1-\frac{\delta}{4})}{\pi^2}\cdot x - O(x^{1-\frac{\delta}{2}}x^{\frac{\delta}{8}}x^{\frac{\delta}{4}}\log^2 x)\\ &= -\frac{(1-o(1))\log(1-\frac{\delta}{4})}{\pi^2}\cdot x\end{aligned}$$

which proves the main statement. □

Remark 4.16. The proof in the other cases follows precisely the same lines of the case $2^2||D$ with some very little variations pointed out below.

- *Case* $8 \mid D$, $d = \frac{D}{4}$.
  In this case, the fact that $D \in \text{Fund}^+$ is no longer guaranteed which means that the negative Pell equation $T^2 - dU^2 = -1$ may be solvable. To avoid this inconvenience we change the definition of the set

  $$\mathcal{D}_m(x) := \{2pm : 2pm \sim x, p \equiv 3 \mod 4\}$$

  and so, by Remark 1.32, $d \in \mathcal{D}_m(x)$ implies $D \in \text{Fund}^+$.

- *Case* $2 \nmid D$, $d = D$.
  As in the previous case we have to modify the set $\mathcal{D}_m(x)$ with respect to the above proof, in order to deal with $D \in \text{Fund}^+$. In particular, we wish that $T^2 - dU^2 = -4$ admits no solutions and hence, we define

  $$\mathcal{D}_m(x) := \{pm : pm \sim x, p \equiv 3 \mod 4, p \geq 19\}.$$

  Notice also that in this case Lemma 3.5 is not enough and the missing parts are covered by Lemma 3.6.

Chapter 5

Average size of the class number of $\mathbb{Q}(\sqrt{D})$

In this chapter we present a result related to ideal class number of real quadratic fields applying what we've seen in Ch. 4 concerning the size of the fundamental unit.

Let D be the discriminant of a real quadratic field $K := \mathbb{Q}(\sqrt{D})$ and $h(D)$ the ideal class number of the same field. Recall that, from Th. 2.10, we know

$$h(D) = \frac{L(1,\chi_D)}{2R(D)}\sqrt{D},$$

where $R(D) = \log \varepsilon(D)$ and χ_D is the Dirichlet character given by the Kronecker symbol $\big(\frac{D}{\cdot}\big)$. The aim of this chapter is the proof of the following estimation.

Theorem 5.1. *Let C_0 denote the converging Euler product:*

$$C_0 := \prod_{p\geq 3}\Big(1 + \frac{p}{(p+1)^2(p-1)}\Big).$$

There exists a constant $\delta > 0$ such that, for every sufficiently large x, the following inequality holds

$$\Sigma(x) := \sum_{\substack{D\leq x\\ 2^2||D}} h(D) \leq \Big(\frac{8}{21\pi^2}C_0 - \delta\Big)\frac{x^{\frac{3}{2}}}{\log x}. \tag{5.1}$$

5.1 Preparatory lemmas

We split the argument in some steps.

Lemma 5.2. *Define the positive valued functions*

$$\kappa(D) := \frac{R(D)}{\log D}, \qquad \xi(D) := L(1,\chi_D)\sqrt{D}$$

and

$$\tilde{\Sigma}(x) := \sum_{\substack{D\leq x\\ 2^2||D}} \frac{\xi(D)}{\kappa(D)}.$$

Then to prove (5.1) *is enough to verify that*

$$\tilde{\Sigma}(x) \leq 2\Big(\frac{8}{21\pi^2}C_0 - 2\delta\Big)x^{\frac{3}{2}}.$$

Proof. Applying Th. 1.18,

$$\begin{aligned}\Sigma(x) &= \sum_{\substack{D\le x\\ 2^2\|D}} \frac{L(1,\chi_D)}{2R(D)}\sqrt{D} = \sum_{\substack{D\le x\\ 2^2\|D}} \frac{L(1,\chi_D)\sqrt{D}\log D}{R(D)}\cdot\frac{1}{2\log D}\\ &= \tilde{\Sigma}(x)\frac{1}{2\log x} - \int_4^x \tilde{\Sigma}(t)\Big(\frac{1}{2\log t}\Big)' dt = \tilde{\Sigma}(x)\frac{1}{2\log x} + \int_4^x \tilde{\Sigma}(t)\frac{1}{2t\log^2 t}\,dt.\end{aligned}$$

Let $C := 2\Big(\frac{8}{21\pi^2}C_0 - 2\delta\Big)$, by hypothesis we have

$$\begin{aligned}\Sigma(x) &\le \frac{\tilde{\Sigma}(x)}{2\log x} + \int_4^x Ct^{\frac{3}{2}}\frac{1}{2t\log^2 t}\,dt\\ &= \frac{\tilde{\Sigma}(x)}{2\log x} + \frac{C}{2}\int_4^x \frac{\sqrt{t}}{\log^2 t}\,dt\\ &= \frac{\tilde{\Sigma}(x)}{2\log x} + \frac{C}{4}\int_2^{\sqrt{x}} \frac{y^2}{\log^2 y}\,dy.\end{aligned}$$

To conclude the proof we need to study individually the integral in the above sum.

1. Applying Remark 4.11 to

$$\mathrm{Li}(x^{\frac{3}{2}}) = \int_2^{x^{\frac{3}{2}}} \frac{1}{\log t}\,dt \underbrace{=}_{t\mapsto y^3} \int_{2^{\frac{1}{3}}}^{\sqrt{x}} \frac{3y^2}{\log(y^3)}\,dy = \int_2^{\sqrt{x}} \frac{y^2}{\log y}\,dy + O(1),$$

   we deduce

$$\int_2^{\sqrt{x}} \frac{y^2}{\log y}\,dy = \frac{x^{\frac{3}{2}}}{\log(x^{\frac{3}{2}})} + o\Big(\frac{x^{\frac{3}{2}}}{\log x}\Big) = \frac{2}{3}\frac{x^{\frac{3}{2}}}{\log x} + o\Big(\frac{x^{\frac{3}{2}}}{\log x}\Big).$$

2. Notice that

$$\Big(\frac{y^3}{\log y}\Big)' = \frac{3y^2\log y - y^2}{\log^2 y} = \frac{3y^2}{\log y} - \frac{y^2}{\log^2 y}$$

   and we get

$$\begin{aligned}\int_2^{\sqrt{x}} \frac{y^2}{\log^2 y}\,dy &= \int_2^{\sqrt{x}} \Big(\frac{3y^2}{\log y} - \frac{3y^2}{\log y} + \frac{y^2}{\log^2 y}\Big)\,dy = \int_2^{\sqrt{x}} \frac{3y^2}{\log y}\,dy - \int_2^{\sqrt{x}} \Big(\frac{y^3}{\log y}\Big)' dy\\ &= 3\,\mathrm{Li}(x^{\frac{3}{2}}) - \frac{x^{\frac{3}{2}}}{\log(x^{\frac{1}{2}})} + O(1) = 3\frac{2}{3}\frac{x^{\frac{3}{2}}}{\log x} - 2\frac{x^{\frac{3}{2}}}{\log x} + o\Big(\frac{x^{\frac{3}{2}}}{\log x}\Big) = o\Big(\frac{x^{\frac{3}{2}}}{\log x}\Big).\end{aligned}$$

Therefore

$$\Sigma(x) \le \frac{\tilde{\Sigma}(x)}{2\log x} + o\Big(\frac{x^{\frac{3}{2}}}{\log x}\Big) \le \Big(\frac{8}{21\pi^2}C_0 - 2\delta\Big)\frac{x^{\frac{3}{2}}}{\log x} + \delta\frac{x^{\frac{3}{2}}}{\log x}$$

which concludes the proof. □

Remark 5.3. Trivially, the above lemma is essentially an equivalence. Assume the estimation (5.1), then

$$\tilde{\Sigma}(x) = \sum_{\substack{D\le x\\ 2^2\|D}} \frac{L(1,\chi_D)}{R(D)}\sqrt{D}\log D \le 2\log x\Sigma(x) \le 2\Big(\frac{8}{21\pi^2}C_0 - \delta\Big)x^{\frac{3}{2}}.$$

We state without proving the following result; the reader can check [[9], Prop. 12] to find a good discussion of it.

Lemma 5.4. *For every $A > 0$ there exists $c(A) > 0$, such that for every bounded complex sequences (α_m), (β_n) and for every M, N satisfying the inequalities $M, N \geq \max(2, \log^A(MN))$, one has the inequality*

$$\Big|\sum_{m\sim M}\sum_{n\sim N}\alpha_m\beta_n\mu^2(2m)\mu^2(2n)\Big(\frac{m}{n}\Big)\Big| \leq c(A)||(\alpha)||_\infty||(\beta)||_\infty MN\log^{-\frac{A}{2}}(MN).$$

Lemma 5.5. *The following holds*

$$\sum_{2\nmid t} t^{-2}\prod_{p|t}\Big(1+\frac{1}{p}\Big)^{-1} = \prod_{p\geq 3}\Big(1+\frac{p}{(p+1)^2(p-1)}\Big).$$

Proof. Let t be an odd integer and let $t = p_1^{a_1}\cdots p_n^{a_n}$ be its prime factorization. We observe that $p_i \geq 3$ for all $i = 1, \dots n$ and

$$t^{-2}\prod_{p|t}\Big(1+\frac{1}{p}\Big)^{-1} = \frac{1}{p_1^{2a_1}\cdots p_n^{2a_n}}\frac{p_1}{p_1+1}\cdots\frac{p_n}{p_n+1}.$$

Let $\{p_m\}_m$ be the sequence of odd primes, then

$$\begin{aligned}\sum_{2\nmid t} t^{-2}\prod_{p|t}\Big(1+\frac{1}{p}\Big)^{-1} &= \lim_{m\to\infty}\lim_{M\to\infty}\sum_{\mathcal{S}\subseteq\{1,\dots m\}}\prod_{j\in\mathcal{S}}\sum_{1\leq i_j\leq M}\frac{p_j}{p_j^{2i_j}(p_j+1)}\\ &= \lim_{m\to\infty}\lim_{M\to\infty}\prod_{k=1}^{m}\Big[1+\Big(\frac{p_k}{p_k+1}\Big)\frac{1}{p_k^2}+\cdots+\Big(\frac{p_k}{p_k+1}\Big)\frac{1}{p_k^{2M}}\Big]\\ &= \lim_{m\to\infty}\lim_{M\to\infty}\prod_{k=1}^{m}\Big[1+\Big(\frac{p_k}{p_k+1}\Big)\sum_{i_k=1}^{M}\frac{1}{p_k^{2i_k}}\Big]\\ &= \lim_{m\to\infty}\prod_{k=1}^{m}\Big[1+\Big(\frac{p_k}{p_k+1}\Big)\Big(\frac{p_k^2}{p_k^2-1}-1\Big)\Big] = \prod_{p\geq 3}\Big(1+\frac{p}{(p+1)^2(p-1)}\Big).\end{aligned}$$

□

Lemma 5.6. *As $y \to \infty$, one has*

$$\sum_{\substack{d\leq y\\ d\equiv 3 \mod 4}}\mu^2(d)L(1,\chi_{4d})\sqrt{d} \sim \frac{4C_0}{3\pi^2}y^{\frac{3}{2}},$$

where C_0 is defined as in Th. 5.1 and χ_{4d} is the Dirichlet character defined by the Kronecker symbol $\Big(\frac{4d}{\cdot}\Big)$.

Proof. Let n be a natural number,

$$\begin{aligned}2 \mid n &\implies \Big(\frac{4d}{n}\Big) = 0\\ 2 \nmid n &\implies \Big(\frac{4d}{n}\Big) = \Big(\frac{2}{n}\Big)^2\Big(\frac{d}{n}\Big) = \Big(\frac{d}{n}\Big).\end{aligned}$$

Therefore, let $\mathcal{S}_1(y)$ be the sum we want to evaluate, we have the equality

$$\mathcal{S}_1(y) = \sum_{\substack{d\leq y\\ d\equiv 3 \mod 4}} \mu^2(d)\sqrt{d}\sum_{\substack{n\geq 1\\ 2\nmid n}} \frac{1}{n}\Big(\frac{d}{n}\Big)$$

which involves a Jacobi symbol. We want to express the infinite sum in n as a finite sum with a small error term.

$$\begin{aligned}\sum_{\substack{n\geq 1\\ 2\nmid n}} \frac{1}{n}\Big(\frac{d}{n}\Big) &= \sum_{\substack{1\leq n\leq y^2\\ 2\nmid n}} \frac{1}{n}\Big(\frac{d}{n}\Big) + \sum_{\substack{n>y^2\\ 2\nmid n}} \frac{1}{n}\Big(\frac{d}{n}\Big)\\ &= \sum_{\substack{1\leq n\leq y^2\\ 2\nmid n}} \frac{1}{n}\Big(\frac{d}{n}\Big) + \lim_{z\to\infty} \sum_{\substack{y^2<n\leq z\\ 2\nmid n}} \frac{1}{n}\Big(\frac{d}{n}\Big)\end{aligned}$$

Using partial summation formula, we can express

$$\sum_{\substack{y^2<n\leq z\\ 2\nmid n}} \frac{1}{n}\Big(\frac{d}{n}\Big) = \frac{1}{z}\sum_{\substack{1\leq n\leq z\\ 2\nmid n}} \Big(\frac{d}{n}\Big) - \frac{1}{y^2}\sum_{\substack{1\leq n\leq y^2\\ 2\nmid n}} \Big(\frac{d}{n}\Big) + \int_{y^2}^{z} \frac{1}{t^2}\sum_{\substack{1\leq n\leq t\\ 2\nmid n}} \Big(\frac{d}{n}\Big)\,dt.$$

Recall that χ_{4d} is the Dirichlet character modulo $4d$ and so the sum over n varying in any interval of length $4d$ of the symbols $\left(\frac{4d}{n}\right)$ is equal to zero. Hence, passing to the limit for $z\to\infty$ in the previous expression we obtain

$$\sum_{\substack{n>y^2\\ 2\nmid n}} \frac{1}{n}\Big(\frac{d}{n}\Big) = \int_{y^2}^{\infty} \frac{1}{t^2}\sum_{\substack{1\leq n\leq t\\ 2\nmid n}} \Big(\frac{d}{n}\Big)\,dt - \frac{1}{y^2}\sum_{\substack{1\leq n\leq y^2\\ 2\nmid n}} \Big(\frac{d}{n}\Big)$$

and estimating the absolute value

$$\Big|\sum_{\substack{n>y^2\\ 2\nmid n}} \frac{1}{n}\Big(\frac{d}{n}\Big)\Big| \leq 4d\Big|\int_{y^2}^{\infty} \frac{1}{t^2}\,dt\Big| + \frac{4d}{y^2} = \frac{8d}{y^2},$$

we get that

$$\sum_{\substack{n\geq 1\\ 2\nmid n}} \frac{1}{n}\Big(\frac{d}{n}\Big) = \sum_{\substack{1\leq n\leq y^2\\ 2\nmid n}} \frac{1}{n}\Big(\frac{d}{n}\Big) + O(y^{-1})$$

uniformly for $d\leq y$. Observe also that $y^{-1}\sum_{d\leq y}\mu^2(d)\sqrt{d} \ll y^{-1}\cdot y\cdot y^{\frac{1}{2}}$. Then, distinguishing the cases n square or not, we can write the sum $\mathcal{S}_1$ as

$$\mathcal{S}_1(y) = Mt_1(y) + Er_1(y) + O(y^{\frac{1}{2}}),$$

where

$$Mt_1(y) := \sum_{\substack{d\leq y\\ d\equiv 3 \mod 4}} \sum_{\substack{1\leq t\leq y\\ (t,2d)=1}} \mu^2(d)\frac{\sqrt{d}}{t^2},$$

$$Er_1(y) := \sum_{\substack{d\leq y\\ d\equiv 3 \mod 4}} \sum_{\substack{1\leq n\leq y^2\\ 2\nmid n, n\neq\square}} \mu^2(d)\frac{\sqrt{d}}{n}\Big(\frac{d}{n}\Big).$$

We are going to study Mt_1 and Er_1 individually.

We first consider Er_1, we want to show that it behaves as an error term. We split the double sum which defines Er_1 in subsums where the sizes of d and n are controlled. We define

$$Er_1(D,N) := \sum_{\substack{d\sim D\\ d\equiv 3 \mod 4}} \sum_{\substack{n\sim N\\ 2\nmid n, n\neq\square}} \mu^2(d)\frac{\sqrt{d}}{n}\Big(\frac{d}{n}\Big),$$

where $D\leq\frac{y}{2}$, $N\leq\frac{y^2}{2}$. Notice that the number of intervals of the shape $D<d\leq 2D$ (resp. $N<n\leq 2N$) to cover the interval $1\leq d\leq y$ (resp. $1\leq n\leq y^2$) is $O(\log y)$, hence we are dealing with $O(\log^2 y)$ subsums $Er_1(D,N)$. Our purpose is to show

$$Er_1(y)=o(y^{\frac{3}{2}}) \qquad y\to\infty$$

and to do so, we want to prove that in all cases

$$Er_1(D,N)=O(y^{\frac{3}{2}}\log^{-3}y).$$

Observe that the trivial bound is

$$|Er_1(D,N)| = \Big|\sum_{\substack{d\sim D\\ d\equiv 3 \mod 4}} \sum_{\substack{n\sim N\\ 2\nmid n, n\neq\square}} \mu^2(d)\frac{\sqrt{d}}{n}\Big(\frac{d}{n}\Big)\Big| \ll \sum_{d\sim D}\sum_{n\sim N}\frac{\sqrt{d}}{n} \ll DN\frac{\sqrt{D}}{N} = D^{\frac{3}{2}},$$

then the desired estimation is proved when $D\leq y\log^{-2}y$. From now on, we suppose

$$D>y\log^{-2}y.$$

We decompose n as the product l^2n' where n' is squarefree and we rewrite the double summation:

$$\sum_{\substack{d\sim D\\ d\equiv 3 \mod 4}} \sum_{\substack{n\sim N\\ 2\nmid n, n\neq\square}} \mu^2(d)\frac{\sqrt{d}}{n}\Big(\frac{d}{n}\Big) = \sum_{\substack{l\leq\sqrt{N}\\ 2\nmid l}} \sum_{\substack{d\sim D\\ d\equiv 3 \mod 4}} \sum_{\substack{n'\sim Nl^{-2}\\ 2\nmid n'}} \mu^2(n')\mu^2(d)\frac{\sqrt{d}}{n'l^2}\Big(\frac{d}{n'l^2}\Big)$$

$$\underbrace{=}_{2\nmid d} \sum_{\substack{l\leq\sqrt{N}\\ 2\nmid l}} \frac{1}{l^2} \sum_{\substack{d\sim D\\ d\equiv 3 \mod 4}} \sum_{n'\sim Nl^{-2}} \mu^2(2n')\mu^2(2d)\frac{\sqrt{d}}{n'}\Big(\frac{d}{l}\Big)^2\Big(\frac{d}{n'}\Big).$$

Furthermore, splitting the sum according to $l\leq N^{\frac{1}{4}}$ or $l>N^{\frac{1}{4}}$ and applying Lemma 5.4 in the first case, the trivial bound in the second one; we obtain fo every $A>0$

$$\begin{aligned}|Er_1(D,N)| &\leq \sum_{l\leq N^{\frac{1}{4}}}\frac{1}{l^2}\Big|\sum_{\substack{d\sim D\\ d\equiv 3(4)}}\sum_{n'\sim Nl^{-2}}\mu^2(2n')\mu^2(2d)\frac{\sqrt{d}}{n'}\Big(\frac{d}{l}\Big)^2\Big(\frac{d}{n'}\Big)\Big| + \sum_{N^{\frac{1}{4}}<l\leq\sqrt{N}}\frac{1}{l^2}\sum_{\substack{d\sim D\\ n'\sim Nl^{-2}}}\frac{\sqrt{d}}{n'}\\ &\ll_A D^{\frac{3}{2}}\log^{-\frac{A}{2}}(DN^{\frac{1}{2}})\sum_{l\leq N^{\frac{1}{4}}}\frac{1}{l^2} + D^{\frac{3}{2}}\sum_{N^{\frac{1}{4}}<l\leq\sqrt{N}}\frac{1}{l^2}\\ &\ll_A D^{\frac{3}{2}}\log^{-\frac{A}{2}}(DN) + D^{\frac{3}{2}}N^{-\frac{1}{4}}.\end{aligned}$$

To verify that the first term of the above sum is the main one we have to see that

$$D^{\frac{3}{2}}N^{-\frac{1}{4}} \ll_A D^{\frac{3}{2}}\log^{-\frac{A}{2}}(DN) \Leftrightarrow \log^{\frac{A}{2}}(DN) \ll_A N^{\frac{1}{4}}.$$

Recall that $D \ll y, N \ll y^2$, thus it's enough to prove $\log^{\frac{A}{2}} y \ll_A N^{\frac{1}{4}}$ which is clearly true for N large enough. For instance we can set $A = 20$ and $N \geq \log^{100} y$; we have, for $y > 1$,

$$\log^{10} y \leq \log^{25} y \leq N^{\frac{1}{4}}$$

and we conclude

$$|Er_1(D,N)| \ll D^{\frac{3}{2}} \log^{-10}(DN).$$

It's immediate to deduce that

$$|Er_1(D,N)| \ll D^{\frac{3}{2}} \log^{-10}(DN) \ll y^{\frac{3}{2}} \log^{-3} y.$$

Just an observation, to apply Lemma 5.4 we need $D, Nl^{-2} \geq \max(2, \log^A(DNl^{-2}))$ and indeed this condition is verified since, for y large enough,

$$D > y \log^{-2} y \geq \log^{20}(y^3) \geq \max(2, \log^A(DNl^{-2})),$$
$$Nl^{-2} \geq N^{\frac{1}{2}} \geq \log^{50} y \geq \log^{20}(y^3) \geq \max(2, \log^A(DNl^{-2})).$$

It remains to consider the case

$$D > y \log^{-2} y, \qquad N \leq \log^{100} y.$$

Lemma 1.24 says that

$$\sum_{\substack{d \sim D \\ d \equiv 3 \mod 4}} \mu^2(d) \Big(\frac{d}{n}\Big) = O(nD^{\frac{1}{2}}).$$

Applying summation formula

$$\sum_{\substack{d \sim D \\ d \equiv 3 \mod 4}} \mu^2(d) \Big(\frac{d}{n}\Big) \sqrt{d} = O(nD^{\frac{1}{2}})D^{\frac{1}{2}} + \int_D^{2D} O(nt^{\frac{1}{2}}) \frac{1}{t^{\frac{1}{2}}}\, dt = O(nD),$$

then

$$|Er_1(D,N)| = \sum_{n \sim N} \frac{1}{n} O(nD) = O(DN)$$

and thus

$$|Er_1(D,N)| \ll y \log^{100} y \ll y^{\frac{3}{2}} \log^{-3} y.$$

The proof of $Er_1(y) = o(y^{\frac{3}{2}})$ is now concluded.

Let's investigate the term Mt_1. Applying summation formula and Corollary 1.13, we estimate the following sum

$$\begin{aligned}\sum_{\substack{d \leq y \\ (d,t)=1 \\ d \equiv 3 \mod 4}} \mu^2(d)\sqrt{d} &= \sqrt{y} \sum_{\substack{d \leq y \\ (d,t)=1 \\ d \equiv 3(4)}} \mu^2(d) - \frac{1}{2} \int_3^y \frac{1}{z^{\frac{1}{2}}} \sum_{\substack{d \leq z \\ (d,t)=1 \\ d \equiv 3(4)}} \mu^2(d)\, dz \\ &= \frac{2}{\pi^2} \prod_{p|t} \Big(1 + \frac{1}{p}\Big)^{-1} y^{\frac{3}{2}} - \frac{1}{\pi^2} \prod_{p|t} \Big(1 + \frac{1}{p}\Big)^{-1} \int_3^y \sqrt{z}\, dz + O(2^{\omega(t)} y) \\ &= \frac{4}{3\pi^2} \prod_{p|t} \Big(1 + \frac{1}{p}\Big)^{-1} y^{\frac{3}{2}} + O(2^{\omega(t)} y).\end{aligned}$$

Now, swapping the double summation which defines $Mt_1(y)$ and recalling Corollary 1.20, we see

$$\begin{aligned} Mt_1(y) &= \sum_{\substack{t\le y\\ 2\nmid t}} \frac{1}{t^2} \sum_{\substack{d\le y\\ (d,t)=1\\ d\equiv 3(4)}} \mu^2(d)\sqrt{d} \\ &= \sum_{\substack{t\le y\\ 2\nmid t}} \frac{4}{3t^2\pi^2}\prod_{p\mid t}\Big(1+\frac{1}{p}\Big)^{-1} y^{\frac{3}{2}} + O\Big(\frac{2^{\omega(t)}}{t^2}y\Big) \\ &= \frac{4}{3\pi^2}y^{\frac{3}{2}}\sum_{2\nmid t} t^{-2}\prod_{p\mid t}\Big(1+\frac{1}{p}\Big)^{-1} + o(y\log^2 y). \end{aligned}$$

This, together with the previous lemma and the estimation of Er_1, concludes the proof. □

We will need also a variation of the above result, we present all the details for completeness. The proof requires another consequence of *Siegel-Walfisz Theorem*, see [[17], Cor. 5.29].

Lemma 5.7. *Let $q > 2$ be a positive integer. For any primitive Dirichlet character χ modulo q one has*

$$\sum_{p\le x}\chi(p) \ll_A \sqrt{q}x\log^{-A} x$$

for any $x \ge 2$ and for any $A > 0$.

Lemma 5.8. *Let $0 < \gamma < \frac{1}{2}$, for any $x \ge 0$ we define*

$$\tilde{\mathcal{F}}_2(x) := \{d : d = pm, \mu^2(d) = 1, pm \sim \frac{x}{8}, m \le x^\gamma, p \equiv 3(4), m \equiv 1(4)\},$$

then there exists $C > 0$ such that for $x \to \infty$

$$\sum_{d\in\tilde{\mathcal{F}}_2(x)} L(1,\chi_{4d})\sqrt{d} \sim C\gamma x^{\frac{3}{2}}.$$

The asymptotic is uniform for $\gamma_0 \le \gamma < \frac{1}{2}$, whenever $0 < \gamma_0 < \frac{1}{4}$.

Proof. Let $\mathcal{S}_2(x)$ be the sum we want to evaluate, we have

$$\mathcal{S}_2(x) = \sum_{d\in\tilde{\mathcal{F}}_2(x)} \sqrt{d}\sum_{\substack{n\ge 1\\ 2\nmid n}}\frac{1}{n}\Big(\frac{d}{n}\Big) = \sum_{\substack{m\le x^\gamma\\ m\equiv 1 \mod 4}} \mu^2(m) \sum_{\substack{p\sim\frac{x}{8m}\\ p\equiv 3 \mod 4}} \sqrt{pm}\sum_{\substack{n\ge 1\\ 2\nmid n}}\frac{1}{n}\Big(\frac{pm}{n}\Big).$$

As in Lemma 5.6, we split the sum as

$$\mathcal{S}_2(x) = Mt_2(x) + Er_2(x) + O(x^{\frac{1}{2}}),$$

where

$$Mt_2(x) := \sum_{\substack{m\le x^\gamma\\ m\equiv 1 \mod 4}} \sum_{\substack{p\sim\frac{x}{8m}\\ p\equiv 3 \mod 4}} \sum_{\substack{1\le t\le x\\ (t,2pm)=1}} \mu^2(m)\frac{\sqrt{pm}}{t^2},$$

$$Er_2(x) := \sum_{\substack{m\le x^\gamma\\ m\equiv 1 \mod 4}} \sum_{\substack{p\sim\frac{x}{8m}\\ p\equiv 3 \mod 4}} \sum_{\substack{1\le n\le x^2\\ 2\nmid n, n\neq\square}} \mu^2(m)\frac{\sqrt{pm}}{n}\Big(\frac{pm}{n}\Big).$$

We decompose Er_2 in $O(\log x)$ sums defined by

$$Er_2(N) := \sum_{\substack{m\le x^\gamma\\ m\equiv 1 \mod 4}} \sum_{\substack{p\sim \frac{x}{m}\\ p\equiv 3 \mod 4}} \sum_{\substack{n\sim N\\ 2\nmid n, n\neq\square}} \mu^2(m)\frac{\sqrt{pm}}{n}\Big(\frac{pm}{n}\Big),$$

where $N \le \frac{x^2}{2}$. We want to prove that in all cases

$$Er_2(N) = O(x^{\frac{3}{2}}\log^{-2} x).$$

Following closely the part of the previous proof in which we apply Lemma 5.4, we obtain

$$|Er_2(N)| \ll x^{\frac{3}{2}}\log x \log^{-10}(x^{1-\gamma}N) \ll x^{\frac{3}{2}}\log^{-2} x$$

uniformly for $N \ge \log^{100} x$. It remains to deal with the case

$$N \le \log^{100} x.$$

Let χ_0 be the principal Dirichlet character modulo 4 and let χ_1 be the (unique and primitive) non-principal character modulo 4 defined by $\chi_1(3) = -1$. It's easy to check that

$$\mathbb{1}_{3 \mod 4} = \frac{1}{2}(\chi_0(3)\chi_0 + \chi_1(3)\chi_1) = \frac{\chi_0-\chi_1}{2};$$

notice that this follows also from a more general fact, i.e. the orthogonality of characters. Let n be odd and nonsquare, we decompose it as the product l^2n' where $n' \neq 1, 2$ is squarefree.

$$\begin{aligned}\alpha(x,n) &:= \sum_{\substack{m\le x^\gamma\\ m\equiv 1 \mod 4}} \sum_{\substack{p\sim \frac{D}{m}\\ p\equiv 3 \mod 4}} \mu^2(m)\Big(\frac{pm}{n}\Big)\\ &= \sum_{\substack{m\le x^\gamma\\ m\equiv 1 \mod 4}} \mu^2(m)\Big(\frac{m}{n}\Big)\sum_{p\sim\frac{D}{m}}\Big(\frac{p}{n'}\Big)\Big(\frac{p}{l}\Big)^2\mathbb{1}_{3 \mod 4}(p)\\ &= \sum_{\substack{m\le x^\gamma\\ m\equiv 1 \mod 4}} \mu^2(m)\Big(\frac{m}{n}\Big)\Big[O(\omega(n)) + \frac{1}{2}\sum_{p\sim\frac{D}{m}}\Big(\frac{p}{n'}\Big) - \frac{1}{2}\sum_{p\sim\frac{D}{m}}\Big(\frac{p}{n'}\Big)\chi_1(p)\Big]\end{aligned}$$

Since n' is squarefree then $\Big(\frac{\cdot}{n'}\Big)$ is a primitive character modulo n' and since $(4, n') \neq 1$ the product $\Big(\frac{\cdot}{n'}\Big)\chi_1$ is a primitive character modulo $4n'$ by Lemma 2.5. Applying the above result we obtain, for any $B > 0$,

$$\begin{aligned}\alpha(x,n) &\ll_B \sum_{\substack{m\le x^\gamma\\ m\equiv 1 \mod 4}} \Big[\omega(n) + \sqrt{4n'}\frac{D}{m}\log^{-B}\Big(\frac{D}{m}\Big) + \sqrt{n'}\frac{D}{m}\log^{-B}\Big(\frac{D}{m}\Big)\Big]\\ &\ll_B x^\gamma\omega(n) + \sqrt{n'}D\log^{-B}(Dx^{-\gamma})\log x.\end{aligned}$$

Moreover, recall that we are assuming $D > x\log^{-3} x$, $n \ll \log^{100} x$, $\gamma < \frac{1}{2}$. Therefore, for any $A > 0$, we get

$$\alpha(x,n) \ll_A \sqrt{n}D\log^{-A} D.$$

We deduce

$$\begin{aligned} Er_2(D,N) &\ll_A D^{\frac{3}{2}} \log^{-A} D \sum_{n\sim N} \frac{1}{n}\sqrt{n} \\ &\ll_A D^{\frac{3}{2}} N^{\frac{1}{2}} \log^{-A} D \ll_A x^{\frac{3}{2}} \log^{-A}(x\log^{-3} x) \log^{50} x, \end{aligned}$$

which concludes the proof of $Er_2(x) = o(x^{\frac{3}{2}})$ choosing A large enough.

As regards Mt_2,

$$\begin{aligned} Mt_2(x) &= \sum_{\substack{m\le x^\gamma \\ m\equiv 1 \mod 4}} \sum_{\substack{1\le t\le x \\ (t,2m)=1}} \sum_{\substack{p\sim\frac{x}{8m} \\ p\equiv 3 \mod 4 \\ (p,t)=1}} \mu^2(m)\frac{\sqrt{pm}}{t^2} \\ &= \sum_{\substack{1\le t\le x \\ 2\nmid t}} \frac{1}{t^2} \sum_{\substack{m\le x^\gamma \\ m\equiv 1 \mod 4 \\ (m,t)=1}} \mu^2(m)\sqrt{m} \sum_{\substack{p\sim\frac{x}{8m} \\ p\equiv 3 \mod 4 \\ (p,t)=1}} \sqrt{p}. \end{aligned}$$

In the inner sum we can forget about the condition $(p,t) = 1$, up to consider an error term $O(\omega(t))$ which is very small compared with the all summation since $t \le x$. Reasoning as in Remark 4.2, we see that the inner sum runs over a set of primes of cardinality $\sim x(16m\log\frac{x}{m})^{-1}$, uniformly for $m \le x^\gamma$. Hence, as $x \to \infty$,

$$\sum_{\substack{p\sim\frac{x}{8m} \\ p\equiv 3 \mod 4 \\ (p,t)=1}} \sqrt{p} \sim \sum_{\substack{p\sim\frac{x}{8m} \\ p\equiv 3 \mod 4}} \sqrt{p}$$

and

$$\frac{x\sqrt{\frac{x}{8m}}}{16m\log\frac{x}{m}} \lesssim \sum_{\substack{p\sim\frac{x}{8m} \\ p\equiv 3 \mod 4}} \sqrt{p} \lesssim \frac{x\sqrt{\frac{x}{4m}}}{16m\log\frac{x}{m}}$$

uniformly in m. We deduce that there exists a constant $\frac{1}{32\sqrt{2}} \le c_1 \le \frac{1}{32}$ such that

$$Mt_2(x) \sim c_1 x^{\frac{3}{2}} \sum_{\substack{1\le t\le x \\ 2\nmid t}} \frac{1}{t^2} \sum_{\substack{m\le x^\gamma \\ m\equiv 1 \mod 4 \\ (m,t)=1}} \frac{\mu^2(m)}{m\log\frac{x}{m}}.$$

Observe that

$$\frac{1}{\log x} \sum_{\substack{m\le x^\gamma \\ m\equiv 1 \mod 4 \\ (m,t)=1}} \frac{\mu^2(m)}{m} \le \sum_{\substack{m\le x^\gamma \\ m\equiv 1 \mod 4 \\ (m,t)=1}} \frac{\mu^2(m)}{m\log\frac{x}{m}} \le \frac{1}{(1-\gamma)\log x} \sum_{\substack{m\le x^\gamma \\ m\equiv 1 \mod 4 \\ (m,t)=1}} \frac{\mu^2(m)}{m}.$$

Fixing γ_0 as in the statement and applying Th. 1.18 to Corollary 1.13, we obtain

$$\sum_{\substack{m\le x^\gamma \\ m\equiv 1 \mod 4 \\ (m,t)=1}} \frac{\mu^2(m)}{m} \sim \frac{2}{\pi^2} \prod_{p\mid t}\left(1+\frac{1}{p}\right)^{-1} \gamma\log x$$

uniformly for $\gamma_0 \leq \gamma < \frac{1}{2}$ and $t \leq x$. Notice that the error term following from Corollary 1.13 can be ignored for $t \leq x$ as we did in the previous proof. We deduce that there is a constant $\frac{2}{\pi^2} \leq c_2 \leq \frac{4}{\pi^2}$, since $\gamma < \frac{1}{2}$, such that

$$Mt_2(x) \sim c_1 c_2 \gamma x^{\frac{3}{2}} \sum_{\substack{1 \leq t \leq x \\ 2 \nmid t}} t^2 \prod_{p|t} \left(1 + \frac{1}{p}\right)^{-1} \sim C\gamma x^{\frac{3}{2}}$$

where $C := C_0 c_1 c_2$ is absolute and C_0 is defined as in Lemma 5.6. In particular

$$\frac{1}{16\sqrt{2}\pi^2} C_0 \leq C \leq \frac{1}{4\pi^2} C_0.$$

The proof is now concluded. □

5.2 Proof of the asymptotic estimate

We state without proof a result from [[8], Th. 1].

Theorem 5.9. *For every positive ϵ, one has*

$$\#\{(d, \varepsilon_d) : 2 \leq d \leq x, d \neq \square, \varepsilon_d \leq d^{\frac{1}{2}+\alpha}\} = O_\epsilon(x^{\frac{\alpha}{3}+\frac{7}{12}+\epsilon})$$

uniformly for $\alpha > 0$ and $x \geq 2$.

Putting everything together, we are ready to start the main proof.

Proof of Theorem 5.1. According to Lemma 5.2, our aim is to prove that

$$\tilde{\Sigma}(x) \leq 2\Big(\frac{8}{21\pi^2} C_0 - 2\delta\Big) x^{\frac{3}{2}}.$$

Let γ, η, η' be small positive numbers and let $\mathcal{E}(x) := \{D : D \leq x, 2^2 || D, D \text{ fund disc}\}$ be the set of indices over which our summation is performed. Writing down any D as the product $4d$, we see that $D \in \mathcal{E}(x)$ if and only if $d \in \mathcal{F}(x)$, where

$$\mathcal{F}(x) := \{d : \mu^2(d) = 1, d \equiv 3 \mod 4, d \leq \frac{x}{4}\}.$$

We consider the set $\mathcal{F}(x)$ as the disjoint union of three subsets defined as follows:

$$\begin{aligned}
\mathcal{F}_1(x) &:= \Big\{d \in \mathcal{F}(x) : \kappa(4d) \leq \frac{7}{4} - \eta'\Big\} \\
\mathcal{F}_2(x) &:= \Big\{d \in \mathcal{F}(x) : \kappa(4d) > \frac{7}{4} - \eta', d = pm, pm \sim \frac{x}{8}, p \equiv 3(4), m \equiv 1(4), m \leq x^\gamma\Big\} \\
\mathcal{G}(x) &:= \mathcal{F}(x) \Big\backslash (\mathcal{F}_1(x) \cup \mathcal{F}_2(x)).
\end{aligned}$$

We split further the set $\mathcal{F}_2(x)$ into the two disjoint subsets

$$\begin{aligned}
\mathcal{F}_2^-(x) &:= \Big\{d \in \mathcal{F}_2(x) : \kappa(4d) \leq \frac{7}{4} + \eta\} \\
\mathcal{F}_2^+(x) &:= \Big\{d \in \mathcal{F}_2(x) : \kappa(4d) > \frac{7}{4} + \eta\}.
\end{aligned}$$

Using this decomposition, we write

$$\tilde{\Sigma}(x) = \sigma_{\mathcal{F}_1}(x) + \sigma_{\mathcal{F}_2^-}(x) + \sigma_{\mathcal{F}_2^+}(x) + \sigma_{\mathcal{G}}(x),$$

where each term on the right-hand side is a sum over the corresponding subset of $\mathcal{F}(x)$. We are going to consider each of these terms individually.

First, we investigate the cardinality of $\mathcal{F}_1(x)$ and the related summation. Avoiding sufficiently small d's, we have

$$\#\mathcal{F}_1(x) = O(1) + \#\Big\{d : \mu^2(d) = 1, d \equiv 3(4), 4^{\frac{7}{2\eta'}-2} \le d \le \frac{x}{4}, \varepsilon_d \le (4d)^{\frac{7}{4}-\eta'}\Big\}.$$

Let $\mathcal{S}(x)$ be the the set defined on the right-hand side, it's contained in the set

$$\tilde{\mathcal{S}}(x) := \Big\{d : d \ne \Box, 4^{\frac{7}{2\eta'}-2} \le d \le \frac{x}{4}, \varepsilon_d \le (4d)^{\frac{7}{4}-\eta'}\Big\}$$

and so $\#\mathcal{F}_1(x) \ll \#\tilde{\mathcal{S}}(x)$. Theorem 5.9 says that, for any $\epsilon > 0$,

$$\#\Big\{d : d \ne \Box, 4^{\frac{7}{2\eta'}-2} \le d \le \frac{x}{4}, \varepsilon_d \le d^{\frac{1}{2}+\alpha}\Big\} = O_\epsilon(x^{\frac{\alpha}{3}+\frac{7}{12}+\epsilon})$$

and we set $\alpha = \frac{5}{4} - \frac{\eta'}{2}$, $\epsilon = \frac{\eta'}{24}$. In particular, we notice that for any d in the above set

$$d \ge 4^{\frac{7}{2\eta'}-2} \Leftrightarrow d^{\frac{\eta'}{2}} \ge 4^{\frac{7}{4}-\eta'} \Leftrightarrow \frac{\eta'}{2} \ge \Big(\frac{7}{4} - \eta'\Big) \log_d 4$$

and so

$$\alpha = \frac{5}{4} - \frac{\eta'}{2} \ge \Big(\frac{7}{4} - \eta'\Big) \log_d 4 + \frac{5}{4} - \eta'.$$

This inequality implies that

$$d^{\frac{1}{2}+\alpha} \ge d^{\frac{1}{2}+\frac{5}{4}-\eta'} 4^{\frac{7}{4}-\eta'} = (4d)^{\frac{7}{4}-\eta'}$$

and we deduce

$$\#\mathcal{F}_1(x) \ll \#\tilde{\mathcal{S}}(x) \ll_\epsilon x^{\frac{\alpha}{3}+\frac{7}{12}+\epsilon} = x^{1-\frac{\eta'}{8}}.$$

We recall that if $D = 4d$ is a fundamental discriminant such that $2^2 || D$ then $\varepsilon_d = \varepsilon(D)$ and so, by Corollary 2.26, $\kappa(4d) \ge \frac{1}{2}$. Applying also Lemma 2.9, we obtain

$$\sigma_{\mathcal{F}_1}(x) = \sum_{d \in \mathcal{F}_1(x)} \frac{L(1, \chi_{4d})\sqrt{4d}}{\kappa(4d)} \ll_{\eta'} x^{\frac{1}{2}} x^{1-\frac{\eta'}{8}} \log x = x^{\frac{3}{2}-\frac{\eta'}{8}} \log x.$$

In the notation of Th. 4.15 we have, for any $\lambda > 0$,

$$\mathcal{D}_m(x, \lambda) = \{pm : pm \sim x, p \equiv 3 \mod 4, p \ge 7, \varepsilon_{pm} \le (4pm)^{3-\lambda}\},$$
$$\mathcal{F}_2^-(x) = \{pm : \mu^2(m) = 1, pm \sim \frac{x}{8}, p \equiv 3(4), m \equiv 1(4), m \le x^\gamma, (4pm)^{\frac{7}{4}-\eta'} < \varepsilon_{pm} \le (4pm)^{\frac{7}{4}+\eta}\}.$$

We set

$$3 - \lambda = \frac{7}{4} + \eta \implies \lambda = \frac{5}{4} - \eta;$$

$\lambda > 0$ for $\eta < \frac{5}{4}$. Applying Th. 4.15, we see

$$\begin{aligned}\#\mathcal{F}_2^-(x) &\leq \# \bigcup_{\substack{m\leq x^\gamma\\ m\equiv 1(4)\\ \mu^2(m)=1}} \mathcal{D}_m\Big(\frac{x}{8},\lambda\Big) = \sum_{\substack{m\leq x^\gamma\\ m\equiv 1(4)\\ \mu^2(m)=1}} \mathcal{D}_m\Big(\frac{x}{8},\lambda\Big)\\ &\ll \sum_{\substack{m\leq x^\gamma\\ m\equiv 1(4)\\ \mu^2(m)=1}} \Big(\frac{3^{\omega(m)}}{m}x^{\frac{1}{2}}\log^2 x + 2^{\omega(m)}m^{\frac{1}{2}}x^{1-\frac{\lambda}{2}}\log x\Big)\\ &= x^{\frac{1}{2}}\log^2 x \sum_{\substack{m\leq x^\gamma\\ m\equiv 1(4)\\ \mu^2(m)=1}} \frac{3^{\omega(m)}}{m} + x^{\frac{3}{8}+\frac{\eta}{2}}\log x \sum_{\substack{m\leq x^\gamma\\ m\equiv 1(4)\\ \mu^2(m)=1}} 2^{\omega(m)}\sqrt{m}\\ &\ll x^{\frac{1}{2}+\gamma}\log^2 x + x^{\frac{3}{8}+\frac{\eta}{2}+\frac{3\gamma}{2}}\log^2 x.\end{aligned}$$

Now, setting $\gamma = \frac{\eta}{3}$ and observing that for η small enough

$$\frac{1}{2}+\frac{\eta}{3} \geq \frac{3}{8}+\eta, \qquad \Big(\eta \leq \frac{3}{8}\Big)$$

we get

$$\#\mathcal{F}_2^-(x) \ll x^{\frac{1}{2}+\frac{\eta}{3}}\log^2 x.$$

In the same same way of the case $\mathcal{F}_1(x)$, we deduce

$$\sigma_{\mathcal{F}_2^-}(x) \ll x^{1+\frac{\eta}{3}}\log^3 x.$$

As a consequence of the definitions of $\mathcal{G}(x)$ and $\mathcal{F}_2^-(x)$:

$$\begin{aligned}\sigma_{\mathcal{F}_2^+}(x) + \sigma_{\mathcal{G}}(x) &\leq \frac{1}{\frac{7}{4}+\eta}\sum_{d\in\mathcal{F}_2^+(x)}\xi(4d) + \frac{1}{\frac{7}{4}-\eta'}\sum_{d\in\mathcal{G}(x)}\xi(4d)\\ &= \frac{1}{\frac{7}{4}+\eta}\sum_{d\in\mathcal{F}_2^+(x)}\xi(4d) + \frac{1}{\frac{7}{4}-\eta'}\Bigg(\sum_{d\in\mathcal{F}(x)}\xi(4d) - \sum_{d\in\mathcal{F}_1(x)\cup\mathcal{F}_2(x)}\xi(4d)\Bigg).\end{aligned}$$

Let $\tilde{\mathcal{F}}_2(x)$ be as in Lemma 5.8, we have clearly

$$\mathcal{F}_2^+(x) \subset \tilde{\mathcal{F}}_2(x) \subset \mathcal{F}_1(x)\cup\mathcal{F}_2(x)$$

and the class number formula, presented in the second chapter, guarantees that the values of the $L-$function we are considering are positive, so the same is true for $\xi(4d)$. We can deduce

$$\sigma_{\mathcal{F}_2^+}(x) + \sigma_{\mathcal{G}}(x) \leq \frac{1}{\frac{7}{4}-\eta'}\sum_{d\in\mathcal{F}(x)}\xi(4d) - \frac{\eta+\eta'}{(\frac{7}{4}+\eta)(\frac{7}{4}-\eta')}\sum_{d\in\tilde{\mathcal{F}}_2(x)}\xi(4d).$$

It remains to evaluate each of the above two sums. To do so, is enough to apply Lemma 5.6 to the first one and Lemma 5.8 to the second with the choice $\gamma = \frac{\eta}{3}$. Therefore

$$\begin{aligned}\tilde{\Sigma}(x) &= \sigma_{\mathcal{F}_2^+}(x) + \sigma_{\mathcal{G}}(x) + \sigma_{\mathcal{F}_1}(x) + \sigma_{\mathcal{F}_2^-}(x)\\ &\leq \left[\frac{4C_0}{3\pi^2(\frac{7}{4}-\eta')}(1+o(1)) - \frac{C(\eta+\eta')\eta}{3(\frac{7}{4}+\eta)(\frac{7}{4}-\eta')}(1+o_\eta(1))\right]x^{\frac{3}{2}} + o_{\eta,\eta'}(x^{\frac{3}{2}}).\end{aligned}$$

Then by fixing η and η' small enough, we conclude that for x sufficiently large

$$\tilde{\Sigma}(x) \leq K_0 x^{\frac{3}{2}}, \qquad K_0 < \frac{16C_0}{21\pi^2}.$$

□

Chapter 6

On Hooley's conjecture

The main theorem of the fourth chapter on a positive density of fundamental discriminants with large regulator belongs to a family of results which goes in the direction of a conjecture due to C. Hooley. This final chapter will be devoted to present the proven part of the conjecture following [[16], § 2] and [[6], § 2].

6.1 One more arithmetic function

In this section we discuss a little variation of the multiplicative arithmetic function 2^{ω}.

In the notation of the proof of Th. 4.15, we set

$$\rho(u) := \rho_{1,1}(u^2), \qquad u \in \mathbb{Z}_{>0}.$$

More precisely the arithmetic function $u \mapsto \rho(u)$ denotes the cardinality of the set

$$\mathcal{R}(u) := \{\Omega \mod u^2 : \Omega^2 \equiv 1 \mod u^2\}.$$

The multiplicativity of ρ is guaranteed by the Chinese Remainder Theorem while its values are completely determined by

$$\begin{cases} \rho(2) = 2 \\ \rho(2^k) = 4 & \text{for } k \geq 2 \\ \rho(p^l) = 2 & \text{for } p \geq 3, l \geq 1. \end{cases}$$

Lemma 6.1. *Let x be a positive real number greater than 1. Then*

$$\sum_{u \leq x} \rho(u) = \frac{8}{\pi^2} x \log x + O(x).$$

Proof. The trivial relation

$$\begin{cases} \rho(u) = 2^{\omega(u)} & \text{if } 4 \nmid u \\ \rho(u) = 2 \cdot 2^{\omega(u)} & \text{if } 4 \mid u \end{cases}$$

allows us to split the sum as follows

$$\sum_{u \leq x} \rho(u) = 2 \sum_{\substack{u \leq x \\ 4 \mid u}} 2^{\omega(u)} + \sum_{\substack{u \leq x \\ 4 \nmid u}} 2^{\omega(u)} = \sum_{\substack{u \leq x \\ 4 \mid u}} 2^{\omega(u)} + \sum_{u \leq x} 2^{\omega(u)}.$$

Remember that $2^{\omega(u)} = \sum_{d|u}\mu^2(d)$, we investigate the first term of the above equation.

$$\begin{aligned}
\sum_{\substack{u\le x\\4|u}} 2^{\omega(u)} &= \sum_{\substack{u\le x\\4|u}}\sum_{d|u}\mu^2(d) = \sum_{d\le x}\mu^2(d)\sum_{\substack{u\le x\\4|u\\d|u}} 1\\
&= \sum_{\substack{d\le x\\2\nmid d}}\mu^2(d)\sum_{\substack{u\le x\\4d|u}}1 + \sum_{\substack{d\le x\\2||d}}\mu^2(d)\sum_{\substack{u\le x\\2d|u}}1 + \sum_{\substack{d\le x\\4|d}}\underbrace{\mu^2(d)}_{=0}\sum_{\substack{u\le x\\d|u}}1\\
&= \frac{x}{4}\sum_{\substack{d\le x\\d\equiv 1,3 \mod 4}}\frac{\mu^2(d)}{d} + \frac{x}{2}\sum_{\substack{d\le x\\d\equiv 2 \mod 4}}\frac{\mu^2(d)}{d} + O(x)
\end{aligned}$$

Following the last part of the proof of Lemma 1.19 and keeping in mind Remark 1.12, we deduce

$$\sum_{\substack{u\le x\\4|u}} 2^{\omega(u)} = \frac{x}{4}\Big(\frac{4}{\pi^2}\log x\Big) + \frac{x}{2}\Big(\frac{2}{\pi^2}\log x\Big) + O(x) = \frac{2}{\pi^2}x\log x + O(x).$$

Therefore, applying Lemma 1.19 we conclude

$$\sum_{u\le x}\rho(u) = \Big(\frac{6}{\pi^2}+\frac{2}{\pi^2}\Big)x\log x + O(x).$$

□

Corollary 6.2. *Let x be a real number greater than 1 and let $\alpha > 0$. Then*

$$\sum_{u\le x}\frac{\rho(u)}{u} = \frac{4}{\pi^2}\log^2 x + O(\log x)$$

and

$$\sum_{u\le x}\frac{\rho(u)}{u^{1-\frac{1}{2\alpha}}} = \frac{16\alpha}{\pi^2}x^{\frac{1}{2\alpha}}\log x + O((1+\alpha^2)x^{\frac{1}{2\alpha}}).$$

Proof. Both formulas follow directly from Th. 1.18 and the above lemma. We have

- $$\begin{aligned}
\sum_{u\le x}\frac{\rho(u)}{u} &= \frac{1}{x}\sum_{u\le x}\rho(u) + \int_1^x\frac{1}{t^2}\sum_{u\le t}\rho(u)\,dt\\
&= \frac{8}{\pi^2}\log x + O(1) + \frac{8}{\pi^2}\int_1^x\frac{\log t}{t}\,dt + O(\log x)\\
&= \frac{4}{\pi^2}\log^2 x + O(\log x),
\end{aligned}$$

- $$\begin{aligned}
\sum_{u\le x}\frac{\rho(u)}{u^{1-\frac{1}{2\alpha}}} &= \frac{1}{x^{1-\frac{1}{2\alpha}}}\sum_{u\le x}\rho(u) + \Big(1-\frac{1}{2\alpha}\Big)\int_1^x\frac{1}{t^{2-\frac{1}{2\alpha}}}\sum_{u\le t}\rho(u)\,dt\\
&= \frac{8}{\pi^2}x^{\frac{1}{2\alpha}}\log x + O(x^{\frac{1}{2\alpha}}) + \frac{8}{\pi^2}\Big(1-\frac{1}{2\alpha}\Big)\int_1^x\frac{\log t}{t^{1-\frac{1}{2\alpha}}}\,dt + O((1+\alpha)x^{\frac{1}{2\alpha}})\\
&= \frac{8}{\pi^2}x^{\frac{1}{2\alpha}}\log x + \frac{8}{\pi^2}\Big(1-\frac{1}{2\alpha}\Big)2\alpha\Big(x^{\frac{1}{2\alpha}}\log x - \int_1^x t^{\frac{1}{2\alpha}-1}\,dt\Big) + O((1+\alpha)x^{\frac{1}{2\alpha}})\\
&= \frac{16\alpha}{\pi^2}x^{\frac{1}{2\alpha}}\log x + O((1+\alpha^2)x^{\frac{1}{2\alpha}}).
\end{aligned}$$

□

6.2 Hooley's conjecture for $\alpha \leq \frac{1}{2}$

Notation 6.3. Let's consider again Pell's equation $T^2 - dU^2 = 1$, we set as usual the fundamental solution ε_d and we let η_d be any solution. Let $\alpha > 0$ and $x \geq 2$, we consider the two sets

$$\mathcal{S}(x,\alpha) := \{(\eta_d, d) : 2 \leq d \leq x, d \neq \square, \varepsilon_d \leq \eta_d \leq d^{\frac{1}{2}+\alpha}\}$$
$$\mathcal{S}^f(x,\alpha) := \{(\varepsilon_d, d) : 2 \leq d \leq x, d \neq \square, \varepsilon_d \leq d^{\frac{1}{2}+\alpha}\}$$

and

$$S(x,\alpha) := \#\mathcal{S}(x,\alpha), \qquad S^f(x,\alpha) := \#\mathcal{S}^f(x,\alpha).$$

Remark 6.4.

- Observe that it doesn't make sense to consider the above sets with the value $\alpha = 0$. Indeed Remark 2.27 says that $\varepsilon_d > 2\sqrt{d}$ and so $\mathcal{S}(x,0) = \mathcal{S}^f(x,0) = \varnothing$.
- If $d \in \mathcal{S}^f(x,\alpha)$ then the same d appears in $\mathcal{S}(x,\alpha)$ with multiplicity $\lfloor (\frac{1}{2}+\alpha)\log_{\varepsilon_d} d \rfloor$.
- If d' is such that $d'^2 \mid d$, then any η_d is also an $\eta_{\frac{d}{d'^2}}$. Thus distinct pairs of $\mathcal{S}(x,\alpha)$ may have the same first component.

Theorem 6.5. *Let ϵ be any real number satisfying $0 < \epsilon < \frac{1}{2}$ and $x \geq 2$. One has*

$$S(x,\alpha) = S^f(x,\alpha) = \frac{4\alpha^2}{\pi^2} x^{\frac{1}{2}} \log^2 x + O(x^{\frac{1}{2}} \log x),$$

where $\epsilon \leq \alpha \leq \frac{1}{2}$.

We need a preliminary lemma to develop the argument of the proof.

Lemma 6.6. *Let $\alpha > 0$. Then there exists a function $u \mapsto A_\alpha(u)$ defined for $u \geq 1$ such that*

$$A_\alpha(u)u - (A_\alpha(u)u)^{-(1+\frac{1}{\alpha})} = 2u$$

which is of $\mathcal{C}^\infty$-class and satisfies the inequalities

$$2 \leq A_\alpha(u) \leq 2 + u^{-1}(2u)^{-(1+\frac{1}{\alpha})}.$$

Proof. Let's consider the function

$$G_\alpha : (0,\infty)^2 \to \mathbb{R}$$
$$(x,y) \longmapsto 2x - y + y^{-(1+\frac{1}{\alpha})}.$$

The analytic implicit function theorem implies that the set $\{(x,y) \in (0,\infty)^2 : G_\alpha(x,y) = 0\}$ can be represented as the graph of an analytic function $y = f_\alpha(x)$. To be precise, the theorem gives a local description of the above set of zeros but in this particular case one sees that the description can be extended to the whole domain.

Moreover, for every fixed x the continuous function $G_\alpha(x,\cdot)$ is clearly decreasing and

$$G_\alpha(x,2x) = (2x)^{-(1+\frac{1}{\alpha})} > 0,$$
$$G_\alpha(x, 2x + (2x)^{-(1+\frac{1}{\alpha})}) = -(2x)^{-(1+\frac{1}{\alpha})} + (2x + (2x)^{-(1+\frac{1}{\alpha})}))^{-(1+\frac{1}{\alpha})} < 0.$$

With the choice $x = u$ and writing $f_\alpha(u)$ in the form $A_\alpha(u)u$, we deduce the existence of the desired function A_α which satisfies

$$2u \leq A_\alpha(u)u \leq 2u + (2u)^{-(1+\frac{1}{\alpha})}.$$

□

Proof of Theorem 6.5. Let

$$\tilde{\mathcal{S}}(x,\alpha) := \{(t,u,d) \in \mathbb{Z}^3_{>0} | t^2 - du^2 = 1, t + u\sqrt{d} \leq d^{\frac{1}{2}+\alpha}, d \leq x\},$$

we observe that the following map is a bijection

$$\begin{aligned} \mathcal{S}(x,\alpha) &\longrightarrow \tilde{\mathcal{S}}(x,\alpha) \\ (d, t+u\sqrt{d}) &\longmapsto (t,u,d). \end{aligned}$$

The condition $u \geq 1$ in the right-hand side guarantees that d is nonsquare.

The first part of the proof is devoted to replace the inequalities concerning d and $\eta_d = t + u\sqrt{d}$ in terms of t, u separately. The equality $u = \frac{\eta_d - \eta_d^{-1}}{2\sqrt{d}}$ allows us to produce the bound

$$u \leq \frac{1}{2}(d^\alpha - d^{-1-\alpha}) \leq \frac{1}{2}(x^\alpha - x^{-1-\alpha}) =: X_\alpha,$$

where we may assume $X_\alpha \geq 1$ otherwise $\mathcal{S}(x,\alpha)$ is empty. Observe that, since $d \mapsto d^\alpha - d^{-1-\alpha}$ is a strictly increasing function (in particular injective), we have

$$\eta_d \leq d^{\frac{1}{2}+\alpha} \Leftrightarrow u \leq \frac{1}{2}(d^\alpha - d^{-1-\alpha}), \qquad d \leq x \Leftrightarrow \frac{1}{2}(d^\alpha - d^{-1-\alpha}) \leq X_\alpha.$$

Applying the previous lemma, we define $Y_1(u,\alpha) := (A_\alpha(u)u)^{\frac{1}{\alpha}}$ satisfying

$$u = \frac{1}{2}(Y_1(u,\alpha)^\alpha - Y_1(u,\alpha)^{-1-\alpha})$$

and so

$$u \leq \frac{1}{2}(d^\alpha - d^{-1-\alpha}) \Leftrightarrow Y_1(u,\alpha) \leq d.$$

The condition $t^2 - du^2 = 1$ implies that

$$\begin{aligned} d \geq Y_1(u,\alpha) &\Leftrightarrow t \geq (Y_1(u,\alpha)u^2 + 1)^{\frac{1}{2}} =: Y_2(u,\alpha), \\ d \leq x &\Leftrightarrow 1 = t^2 - du^2 \geq t^2 - xu^2 \Leftrightarrow t \leq (xu^2+1)^{\frac{1}{2}} =: Y_3(u). \end{aligned}$$

We've just proven that

$$\tilde{\mathcal{S}}(x,\alpha) = \{(t,u,d) \in \mathbb{Z}^3_{>0} | t^2 - du^2 = 1, Y_2(u,\alpha) \leq t \leq Y_3(u)\},$$

where the conditions on t imply that $u \leq X_\alpha$.

Now, we are ready to investigate $S(x,\alpha)$. Let $\mathcal{R}(u)$ be as at the beginning of the chapter, then

$$\begin{aligned} S(x,\alpha) &= \sum_{u\geq 1}\sum_{d \geq 1} \sum_{\substack{Y_2(u,\alpha) \leq t \leq Y_3(u) \\ t^2 - du^2 = 1}} 1 = \sum_{1 \leq u \leq X_\alpha} \sum_{\substack{Y_2(u,\alpha) \leq t \leq Y_3(u) \\ t^2 - 1 \equiv 0 \mod u^2}} 1 \\ &= \sum_{1 \leq u \leq X_\alpha} \sum_{\Omega \in \mathcal{R}(u)} \sum_{\substack{Y_2(u,\alpha) \leq t \leq Y_3(u) \\ t \equiv \Omega \mod u^2}} 1 \\ &= \sum_{1 \leq u \leq X_\alpha} \rho(u)\Big(\frac{Y_3(u) - Y_2(u,\alpha)}{u^2} + O(1)\Big). \end{aligned}$$

Lemma 6.6 gives the inequalities $2 \leq A_\alpha(u) \leq \frac{5}{2}$, hence

$$\begin{aligned} Y_3(u) - Y_2(u,\alpha) &= x^{\frac{1}{2}}u - Y_1(u,\alpha)^{\frac{1}{2}}u + O(1) \\ &= x^{\frac{1}{2}}u - (A_\alpha(u)u)^{\frac{1}{2\alpha}}u + O(1) = x^{\frac{1}{2}}u + O(u^{1+\frac{1}{2\alpha}}). \end{aligned}$$

Therefore, using the results of the previous section and recalling $\epsilon \leq \alpha \leq \frac{1}{2}$,

$$\begin{aligned} S(x,\alpha) &= x^{\frac{1}{2}} \sum_{1\leq u\leq X_\alpha} \frac{\rho(u)}{u} + O\biggl(\sum_{1\leq u\leq X_\alpha} \frac{\rho(u)}{u^{1-\frac{1}{2\alpha}}}\biggr) + O\biggl(\sum_{1\leq u\leq X_\alpha} \rho(u)\biggr) \\ &= \frac{4}{\pi^2} x^{\frac{1}{2}} \log^2 X_\alpha + O(x^{\frac{1}{2}} \log X_\alpha) + O(\alpha X_\alpha^{\frac{1}{2\alpha}} \log X_\alpha) + O(X_\alpha \log X_\alpha) \\ &= \frac{4\alpha^2}{\pi^2} x^{\frac{1}{2}} \log^2 x + O(x^{\frac{1}{2}} \log x). \end{aligned}$$

The proof is now concluded since if $\eta_d \in \mathcal{S}(x,\alpha)$ is not a fundamental solution, we necessarily have

$$\eta_d \geq \varepsilon_d^2 > 4d.$$

This implies $\mathcal{S}^f(x,\alpha) = \mathcal{S}(x,\alpha)$ because $\alpha \leq \frac{1}{2}$. □

6.2.1 The full conjecture

In [16] C. Hooley suggests an extension of Th. 6.5 which covers all possible values of the parameter α.

Conjecture 6.7. *For any given $\alpha > \frac{1}{2}$, we have*

$$S^f(x,\alpha) \sim B(\alpha) x^{\frac{1}{2}} \log^2 x, \qquad x \to \infty,$$

where

$$B(\alpha) = \begin{cases} \frac{4}{\pi^2}\Bigl(\alpha - \frac{1}{4}\Bigr) & \textit{if } \frac{1}{2} < \alpha \leq 1 \\ \frac{4}{\pi^2}\Bigl(\alpha - \frac{1}{4}\Bigr) + \frac{1}{18\pi^2}(\alpha-1)^2 & \textit{if } 1 \leq \alpha \leq \frac{5}{2} \\ \frac{4}{\pi^2}\Bigl(\alpha - \frac{1}{4}\Bigr) + \frac{1}{6\pi^2}\Bigl(\alpha - \frac{7}{4}\Bigr)^2 & \textit{if } \alpha > \frac{5}{2}. \end{cases}$$

É. Fouvry has worked on this conjecture investigating the case $\alpha \leq 1$. He has been able to produce the following lower bound, see [[6], Th. 1.1].

Theorem 6.8. *As $x \to \infty$, we have the inequalities*

$$\begin{aligned} S^f(x,\alpha) &\gtrsim \frac{1}{\pi^2}\Bigl(1 + 4\Bigl(\alpha - \frac{1}{2}\Bigr) - 4\Bigl(\alpha - \frac{1}{2}\Bigr)^2\Bigr) x^{\frac{1}{2}} \log^2 x \\ S(x,\alpha) &\gtrsim \frac{1}{\pi^2}\Bigl(1 + 4\Bigl(\alpha - \frac{1}{2}\Bigr) - 3\Bigl(\alpha - \frac{1}{2}\Bigr)^2\Bigr) x^{\frac{1}{2}} \log^2 x, \end{aligned}$$

uniformly for $\frac{1}{2} \leq \alpha \leq 1$.

This result is now improved by P. Xi , see [[25], Th. 1.1], who provides a better multiplicative constant with respects to the previous statement.

Bibliography

[1] Baker A., *Linear forms in the logarithms of algebraic numbers*, Mathematika **13**, 204-216, 1966.

[2] Cohen H., Lenstra W. J., *Heuristics on class groups of number fields*, in Jager H. (eds) Number Theory Noordwijkerhout 1983, Lecture Notes in Math. vol 1068, 33-62, Springer, 1984.

[3] Cohn H., *A Second Course in Number Theory*, Wiley, 1962.

[4] Clark P.L., *Number Theory: A Contemporary Introduction*, University of Georgia, 2018. Available at `http://math.uga.edu/~pete/4400FULL2018.pdf`.

[5] Dudley U., *Elementary Number Theory, 2nd ed.*, Dover Publications, 2008.

[6] Fouvry É., *On the size of the fundamental solution of the Pell equation*, J. reine angew. Math. **717**, 1-33, 2014.

[7] Fouvry É., Jouve F., *A positive density of fundamental discriminants with large regulator*, Pacific J. Math. **262**, 81-107, 2013.

[8] Fouvry É., Jouve F., *Size of regulators and consecutive square-free numbers*, Math. Z. **273**:3-4, 869-882, 2013.

[9] Fouvry É., Klüners J., *The parity of the period of the continued fractions of* $\sqrt{d}$, Proc. Lond. Math. Soc. (3) **101**:2, 337-391, 2010.

[10] Frölich A. and Taylor M.J., *Algebraic Number Theory*, Cambridge Studies in Advanced Mathematics **27**, Cambridge University Press, 1993.

[11] Gauss C. F., *Disquisitiones Arithmeticae*, Springer-Verlag, 1986.

[12] Hecke E., *Lectures on the Theory of Algebraic Numbers*, Graduate texts in mathematics **77**, Springer, 1981.

[13] Heilbronn H., *On the class-number in imaginary quadratic fields*, Quart. J. Math. Oxford Ser. **5**, 150-160, 1934.

[14] Heilbronn H., Linfoot H., *On the imaginary quadratic corpora of class-number one*, Quart. J. Math. Oxford Ser. **5**, 293-301, 1934.

[15] Hildebrand A.J., *Introduction to Analytic Number Theory*, University of Illinois, 2015. Available at `http://www.math.uiuc.edu/~hildebr/ant`.

[16] Hooley C., *On the Pellian equation and the class number of indefinite binary quadratic forms*, J. reine angew. Math. **353**, 98-131, 1984.

[17] Iwaniec H., Kowalski E., *Analytic Number Theory*, American Mathematical Society, Colloquium Publications **53**, 2004.

[18] Jacobson M.J., Williams H.C., *Solving the Pell Equation*, Springer, 2009.

[19] LeVeque W.J., *Topics in Number Theory, Volume II*, Dover Publications, 2002.

[20] Marcus D., *Number Fields*, Universitext, Springer, 2018.

[21] Narkiewicz W., *Elementary and Analytic Theory of Algebraic Numbers*, Springer Monographs in Mathematics, Springer, 2004.

[22] Stark H. M., *A complete determination of the complex quadratic fields of class-number one*, Michigan Math. J. **14**, 1-27, 1967.

[23] Strömbergsson A., *Analytic Number Theory - Lecture notes based on Davenport's book*, Uppsala University, 2008. Available at `http://www2.math.uu.se/~astrombe/analtalt08/www_notes.pdf`.

[24] Tenenbaum G., *Introduction to Analytic and Probabilistic Number Theory, 3rd ed.*, Graduate Studies in Mathematics **163**, American Mathematical Society, 2015.

[25] Xi P., *Counting fundamental solutions to the Pell equation with prescribed size*, Compositio Math. **154**, 2379-2402, 2018.