COUNTING EXTENSIONS OF IMAGINARY QUADRATIC FIELDS

ALEXANDR BENEŠ

Abstract. The goal is to obtain an asymptotic formula for the number of quadratic extensions with bounded discriminant of a some quadratic number field with odd class number. This extends an already known result for \( \mathbb{Q} \).

Introduction

Let \( K \) be a number field. We define the function \( a_n \) as the number of quadratic extensions of \( K \) with discriminant \( \leq n \). In [Woo14] it is shown that for \( K \) the rational numbers the function \( a_n \) has the asymptotic behaviour:

\[
a_{\mathbb{Q}}(n) = \frac{6}{\pi^2}n + o(n).
\]

We will extend this theorem for \( K \) an imaginary and real quadratic fields with odd class number. The main result for imaginary quadratic number fields is:

Theorem 1. For a quadratic imaginary number field \( K = \mathbb{Q}(\sqrt{-p}) \) with \( p \) prime \( > 3 \) that is \( 3 \) (mod 4), the function \( a_K(n) = \#\{L/K|\deg(L/K) = 2, \mathfrak{o}_L \leq n\} \) is asymptotically equal to

\[
a_K(n) = Cn + o(n)
\]

where \( C \) is given by

\[
C = \frac{1}{2\zeta_K(2)} \frac{\prod_{p|2} g_p(1)}{\left(1 + N(p)^{-1}\right)} = \frac{\mathfrak{o}_K^{-5/2}}{2\pi} \frac{\prod_{p|2} g_p(1)}{\left(1 + N(p)^{-1}\right)}
\]

where \( h_K \) is the class number, \( \mathfrak{o}_K \) is the discriminant and \( g_p \) is a simple term that will be given exactly. An analogous result for real number fields is Theorem [18].

Our method will use class field theory. Similar method can be used to count cubic or higher degree extension or count extensions with certain splitting properties at a set of primes. We will extend the proof found in [Woo14] from the rational numbers to some quadratic number fields. The book [Coh00] tells more about using class field theory to create algorithms to count extensions with certain properties. The article [Wri89] uses this method for

\[\text{The author was supported by the project PRIMUS/20/SCI/002 from Charles University.}\]

Address: Charles University, Faculty of Mathematics and Physics, Department of Algebra, Sokolovská 83, 18600 Praha 8, Czech Republic

Email: abenes970@gmail.com.
extensions of a number field with given Galois group. For more about characters on quadratic number fields see [LR20].

The main idea is to view quadratic extensions of $K$ as open index 2 subgroups of the absolute Galois group of $K$ and use the Artin reciprocity to transform them to subgroups of the group of idèles. These can also be seen as kernels of homomorphisms from idèles to $\mathbb{Z}/2\mathbb{Z}$. If $K$ has odd class number, then all such homomorphisms can be constructed as sums of homomorphisms from local fields to $\mathbb{Z}/2\mathbb{Z}$ such that they send all units of $O_K$ to 0.

If the class number is even, then there are homomorphisms from the class group $Cl_K$ to $\mathbb{Z}/2\mathbb{Z}$, which would have to be taken to account. Also there would be more homomorphisms from local fields than homomorphisms from the idèles, because the group $\text{Ext}^1(Cl_K, \mathbb{Z}/2\mathbb{Z})$ would be nonzero and to calculate it, we would need to know nontrivial information about the structure of the class group.

The discriminant of each extensions can be computed from the local homomorphisms. The information about the extension can be put into one function called the counting function. The asymptotic behaviour is then estimated from the counting function using a Tauberian theorem, if we rewrite the counting function using certain zeta and L-functions.

1. Algebraic number theory

We will denote $K$ a number field. $O_K$ its ring of integers, $d_K$ the discriminant (which will always be positive), $p$ a place of $K$ and $|\cdot|_p$ the associated norm. Then $K_p$ will be the completion of $K$ with respect to the norm, a locally compact normed field called a local field associated to $p$. A local field is non-archimedean if it is associated to a discrete valuation. For a non-archimedean local field $A$ we define the ring of integers $O_A = \{x \in A : |x| \leq 1\}$, its maximal ideal $m = \{x \in A : |x| < 1\}$ and the residue field $\kappa_A = O_A/m_A$ which is finite. The discreteness of the norm implies that the maximal ideal is principal and its generator is called uniformizer $\pi$. The absolute value is usually normalized so that the uniformizer has norm $q^{-1}$ where $q$ is the cardinality of the residue field. The units in $O_A$ are exactly the elements with $|a| = 1$.

2. Groups of units of local fields

For our main result we will need to know more about the structure of the group of units of local fields. For a local field $A$ we define the $n$-th unit group $U^{(n)} = 1 + m^n$ and $U = O^\times = U^{(0)}$.

**Theorem 2.** We have $A^\times \cong (\pi) \times U \cong (\pi) \times U/U^{(1)} \times U^{(1)}$ and the quotients $U/U^{(n)} \cong (O/m^n)^\times$ and $U^{(n)}/U^{(n+1)} \cong U/m$ for $n \geq 1$.

**Proof.** See 3.10 and 5.3 in Chapter II. in [NS99].
Theorem 3. For a non-archimedean local field $A$ of characteristic 0 there is an isomorphism
$$\exp : U^{(n)} \to m^n$$
with the inverse log for $n > \frac{1}{p}$, where $p$ is the characteristic of the residue field and $e$ is the normalized valuation of $p$. The functions are given by the power series
$$\exp(x) = \sum_{k=0}^{\infty} \frac{x^k}{k!}, \quad \log(1 + x) = \sum_{k=0}^{\infty} \frac{(-1)^k x^k}{k}$$
which converge on their domain of definition.

Proof. Proposition 5.5 in Chapter II: in [NS99]. □

We can put this together with the fact $m^n = (\pi^n)U \cong O \cong Z_p^{[A/Q_p]}$ as additive groups to get

Theorem 4. For a local field $A$ of characteristic 0 and its ring of integers $O_A$ we have:
$$A^\times \cong Z \times Z/(q - 1)Z \times Z/(p^a)Z \times Z_p^d$$
$$O_A^\times \cong Z/(q - 1)Z \times Z/(p^a)Z \times Z_p^d$$
where $p$ is the characteristic of the residue field and $q$ is its order, $d$ is the degree of $A$ over $Q_p$ and $a$ is some integer.

Proof. Proposition 5.7 in Chapter II. in [NS99]. □

3. Extensions of local fields

For an extension of number fields $L/K$ and primes $q$ of $L$ above $p$ (this means that $p = O_K \cap q$), the local fields $L_q$ and $K_p$ form an extension with properties that tells us information about the primes. For proofs of these theorems see Chapter 7 and 8 of [Mil17].

Definition 5. If $A/B$ is an extension of non-archimedean characteristic 0 local fields with normalized valuations and uniformizers $\pi_A, \pi_B$, then we define the degree of inertia as the degree of the extension of finite fields $f_{A/B} = [\kappa_A/\kappa_B] = [(O_A/(\pi_A))/(O_B/(\pi_B))]$ and the ramification index as $e_{A/B} = \nu_A(\pi_B)$. An extension is unramified if the degree of ramification is 1.

Theorem 6 (Local field extensions). For an extension of number fields $L/K$ and nonzero primes $p \subset O_K$ and $q \subset O_L$ such that $q \cap O_K = p$ we have an extension of local fields $L_q/K_p$. If $q_i$ are all the primes of $L$ above $p$, then $L \otimes_K K_p \cong \prod L_{q_i}$. Furthermore the degree of inertia of the local field extension is equal to the degree of inertia of the primes and the same for the ramification index.

Proof. See Proposition 8.2 in [Mil17]. □

Theorem 7. Finite unramified extensions $L/K$ of non-archimedean local field $K$ correspond to finite extensions of the residue field $K_K = O_K/(\pi_K)$ by sending $L \mapsto \kappa_L = O_L/(\pi_L)$ and if $\kappa_L = \kappa_K[X]/(f(X))$, then $L = K[X]/(\tilde{f}(X))$ for some lift $\tilde{f}(X)$ of $f(X)$ to $K[X]$. 
We follow Chapter VI of [NS99]. We have a number field $K$ and the set of its places $p$ and the corresponding local fields $K_p$. The group of idèles is an object $\mathbb{I}_K$ that collects all the local fields into one.

**Definition 8.** The group of idèles is defined

$$\mathbb{I}_K = \prod_{p \text{ places}} K_p^\times = \{(a_p) \in \prod_{p \text{ places}} K_p^\times \mid \text{all but finitely many } a_p \text{ are in } \mathcal{U}_p\}$$

We can put a topology on idèles by defining a system of neighborhoods of 1 to be the sets:

$$\prod_{p \in S} W_p \times \prod_{p \not\in S} \mathcal{U}_p$$

where $S$ is a finite set of places including the infinite ones and $W_p$ are systems of neighborhoods of 1 in $K_p^\times$. Systems of neighborhoods of other points are obtained by translations.

From the inclusions $K \subset K_p$ we get the diagonal embedding $K^\times \to \mathbb{I}_K$. The quotient $\mathbb{I}_K / K$ is called the idèle class group $C_K$ and it inherits the quotient topology from $\mathbb{I}_K$. There is a natural homomorphism $\mathbb{I}_K \to J_K, (a_i) \mapsto \prod_{p \text{ finite}} \mathcal{P}^\nu_p(a_p)$ to the group of fractional ideals. It is obviously surjective. This homomorphism factorizes to a surjection $C_K \to Cl_K$ since $K^\times$ maps exactly to principal fractional ideals.

For a set of places $S$ we have a subgroup of idèles $\mathbb{I}_S^K = \prod_{p \in S} K_p^\times \times \prod_{p \not\in S} \mathcal{U}_p$. If $S$ is the set of infinite places we will denote it by $\mathbb{I}_\infty^K$.

**Theorem 9.** There is an exact sequence

$$0 \to \mathbb{I}_K^\infty K^\times / K^\times \to C_K \to Cl_K \to 0$$

**Proof.** See Proposition 1.3 in Chapter VI. in [NS99]. □

Note that by the second isomorphism theorem $\mathbb{I}_K^\infty K^\times / K^\times \cong \mathbb{I}_K^\infty / (\mathbb{I}_K^\infty \cap K^\times)$.

Idèles can be used to conveniently formulate the main result of class field theory: the global Artin reciprocity.

**Theorem 10** (Artin reciprocity). There is a continuous homomorphism from the idèle class group of a number field to the abelization of its absolute Galois group

$$C_K \to \text{Gal}(K)^{ab}$$

called the Artin map. Furthermore this homomorphism is surjective and its kernel is the largest connected component of $C_K$ that includes 1.

**Proof.** Chapter V.5 of [Mil13]. □

This powerful result tells us that abelian extensions of $K$ can be described by the idèle class group.
5. Field extensions

In this section we will assume that $K$ is an imaginary quadratic number field and that the class number of $K$ is odd.

We can use the Artin reciprocity to classify all quadratic extensions of an imaginary quadratic number field $K$. All quadratic extensions are abelian. By Galois theory they correspond to index 2 (necessarily normal) closed (equivalently open) subgroups of $G(K)$, the absolute Galois group of $K$. All finite extensions of $K$ correspond to closed subgroups of $G(K)$ with finite index. Its commutator $\Gamma = [G(K), G(K)]$ is a normal subgroup which is contained in all normal subgroups $H$ such that $G(K)/H$ is abelian. So all index 2 closed subgroups correspond to index 2 closed subgroups that lie in $G(K)^{ab} = G(K)/\Gamma$ or equivalently continuous surjective homomorphisms that lie in $\text{Hom}(G(K)^{ab}, \mathbb{Z}/2\mathbb{Z})$. We will call $\text{Hom}_{\text{c}}(G(K)^{ab}, \mathbb{Z}/2\mathbb{Z})$ the subgroup of continuous homomorphisms. Now we use the Artin reciprocity to transform this to homomorphisms to $\mathbb{Z}/2\mathbb{Z}$ from the idèle class group.

**Theorem 11.** The inclusion $\mathbb{I}_K^\infty K^\times/K^\times \to C_K$ induces an isomorphism $\text{Hom}(C_K, \mathbb{Z}/2\mathbb{Z}) \to \text{Hom}(\mathbb{I}_K^\infty K^\times/K^\times, \mathbb{Z}/2\mathbb{Z})$ for $K$ with odd class number (not necessarily imaginary quadratic).

**Proof.** We have the exact sequence

$$
0 \longrightarrow \mathbb{I}_K^\infty K^\times/K^\times \longrightarrow C_K \longrightarrow Cl_K \longrightarrow 0. 
$$

We will apply the left exact functor $\text{Hom}(\_, \mathbb{Z}/2\mathbb{Z})$ to the sequence and use the property of $\text{Ext}$ functors:

$$
\text{Hom}(Cl_K, \mathbb{Z}/2\mathbb{Z}) \longrightarrow \text{Hom}(C_K, \mathbb{Z}/2\mathbb{Z}) \longrightarrow \text{Ext}^1(Cl_K, \mathbb{Z}/2\mathbb{Z}) \longrightarrow \text{Hom}(\mathbb{I}_K^\infty K^\times/K^\times, \mathbb{Z}/2\mathbb{Z}) \longrightarrow \text{Ext}^1(Cl_K, \mathbb{Z}/2\mathbb{Z})
$$

The edge terms are 0 as we will now show. Because $Cl_K$ is odd $\text{Hom}(Cl_K, \mathbb{Z}/2\mathbb{Z}) = 0$. We have $\text{Ext}^1(Cl_K, \mathbb{Z}/2\mathbb{Z}) = 0$ since $\text{Ext}^1(\mathbb{Z}/p\mathbb{Z}, A) \cong A/(p)$ for any group $A$.

We need to restrict ourselves to continuous homomorphisms. The topology on $\mathbb{I}_K$ induces the subset topology on $\mathbb{I}_K^\infty$ and the quotient topology on $\mathbb{I}_K^\infty/\mathbb{I}_K^\infty \cap K^\times$). Note that we have $\mathbb{I}_K^\infty K^\times/K^\times \cong \mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times)$.

**Theorem 12.** There is an isomorphism of continuous homomorphisms $\text{Hom}_{\text{c}}(C_K, \mathbb{Z}/2\mathbb{Z}) \to \text{Hom}_{\text{c}}(\mathbb{I}_K^\infty K^\times/K^\times, \mathbb{Z}/2\mathbb{Z})$ for $K$ with odd class number, where $\text{Hom}_{\text{c}}(A, B)$ is the group of continuous homomorphisms from $A$ to $B$.

**Proof.** From the previous theorem we have a bijection of all homomorphisms $\text{Hom}(C_K, \mathbb{Z}/2\mathbb{Z}) \to \text{Hom}(\mathbb{I}_K^\infty K^\times/K^\times, \mathbb{Z}/2\mathbb{Z}) \cong \text{Hom}(\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times), \mathbb{Z}/2\mathbb{Z})$. The inclusion map $\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times) \to C_K$ is continuous, so a continuous homomorphism maps to a continuous homomorphism. So there is a map $\text{Hom}_{\text{c}}(C_K, \mathbb{Z}/2\mathbb{Z}) \to \text{Hom}_{\text{c}}(\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times), \mathbb{Z}/2\mathbb{Z})$ and it is injective.

If the preimage of $\chi \in \text{Hom}_{\text{c}}(\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times), \mathbb{Z}/2\mathbb{Z}) \subset \text{Hom}(\mathbb{I}_K^\infty/(\mathbb{I}_K^\infty \cap K^\times), \mathbb{Z}/2\mathbb{Z})$
Lemma 13. There is a bijection between quadratic extensions of any number field $K$ and continuous surjective homomorphisms $C_K \to \mathbb{Z}/2\mathbb{Z}$ given by the Artin map.

Proof. Quadratic extensions of $K$ correspond to open index 2 subgroups of $G(K)$. If $O$ is the connected component of 1 in $C_K$, then the Artin map gives an isomorphism $C_K/O \to G(K)$. This gives correspondence of open index 2 subgroups of $G(K)$ and $C_K/O$. These subgroups of $C_K/O$ can be seen as kernels of continuous surjective homomorphisms $C_K/O \to \mathbb{Z}/2\mathbb{Z}$. These correspond to continuous surjective homomorphisms $C_K \to \mathbb{Z}/2\mathbb{Z}$ since the connected component of 1 is always mapped to 0 by continuity.

We will now look at $\text{Hom}(\mathbb{I}_K^\times, \mathbb{Z}/2\mathbb{Z})$ with $\mathbb{I}_K^\times \cap K^\times$ in the kernel. The elements of $\mathbb{I}_K^\times \cap K^\times$ all generate the unit ideal. Therefore they are exactly the units of $O_K$ which are $\{+1, -1\}$ if $K \neq \mathbb{Q}[i], \mathbb{Q}[\sqrt{2\pi}/3]$.

Lemma 14. For an imaginary quadratic number field $K$, continuous homomorphisms $\mathbb{I}_K^\times \to \mathbb{Z}/2\mathbb{Z}$ are finite sums of local homomorphisms $U_p \to \mathbb{Z}/2\mathbb{Z}$ for some distinct primes $p$ of $K$. More explicitly $\chi = \sum_p \chi_p$ where $\chi_p$ is the composition of the inclusion $U_p = (1, \ldots, U_p, \ldots, 1) \to \mathbb{I}_K^\times$.

Proof. Composition with the inclusion $U_p = (1, \ldots, U_p, \ldots, 1) \to \mathbb{I}_K^\times$ induces homomorphisms $\chi_p : U_p \to \mathbb{Z}/2\mathbb{Z}$. The kernel of the homomorphism $\chi : \mathbb{I}_K^\times \to \mathbb{Z}/2\mathbb{Z}$ is open, so there is a finite set $S$ of primes such that the kernel includes $\prod_{p \in S} W_p \times \prod_{p \not\in S} U_p$, so all but finitely many $\chi_p$ are trivial and $\chi(\ldots, a_p, \ldots) = \prod_{p \in S} \chi_p(a_p)$. The local field at the infinite place $\mathbb{C}^\times$ is always mapped to 0 (since every element in $\mathbb{C}^\times$ has a square root), so the sum only includes finite primes.

Conversely every finite sum of local homomorphisms gives a continuous homomorphism as we will show. Let $\chi = \sum_{p \in S} \chi_p$. As we will see in Lemma 17 every local homomorphism $\chi_p : U_p \to \mathbb{Z}/2\mathbb{Z}$ has some subgroup $U_p^{(n_p)}$ in the kernel and if $S$ is the set of primes in the sum, then every element $g$ in the kernel has an open neighbourhood $g \prod_{p \in S} U_p^{(n_p)} \times \prod_{p \not\in S} U_p$, so the kernel is open.

All these theorems can be summarized as:

Theorem 15. Quadratic extensions of an imaginary quadratic number field $K$ with odd class number are in bijection with finite sums $\chi : \mathbb{I}_K^\times \to \mathbb{Z}/2\mathbb{Z}$, that can be written as sums $\chi = \sum_p \chi_p$ of homomorphisms $\chi_p : U_p \to \mathbb{Z}/2\mathbb{Z}$ with $\mathbb{I}_K^\times \cap K^\times$ in the kernel of $\chi$ and $\chi_p$ is $\chi$ composed with the inclusion $U_p = (1, \ldots, U_p, \ldots, 1) \to \mathbb{I}_K^\times$.
6. Conductors

Now we need to know how can we compute the discriminant of a number field defined by such homomorphisms. We can do it using conductors.

**Definition 16.** For a homomorphism \( \chi_p : \mathcal{U}_p \to \mathbb{C}^\times \) we define the local Artin conductor to be the smallest integer \( f_\chi \) such that \( \mathcal{U}_p(f_\chi) \subset \ker \chi_p \). We define the global Artin conductor \( f_\chi \) of a homomorphism \( \chi : G(K)_{ab} \to \mathbb{C}^\times \) as \( f_\chi = \prod p^{f_\chi_p} \) where \( \chi_p \) are the homomorphisms induced from \( \chi \) by the map \( \mathcal{U}_p = (1, \ldots, U_p, \ldots, 1) \to I_K \to C_K \to G(K)_{ab} \).

We can interpret the group \( \mathbb{Z}/n\mathbb{Z} \) as a subgroup of \( \mathbb{C}^\times \) generated by the \( n \)-th roots of unity. In our case \( \chi \) is a homomorphism \( \chi : G(K)_{ab} \to \mathbb{Z}/2\mathbb{Z} \cong \{+1, -1\} \subset \mathbb{C}^\times \).

**Lemma 17.** For a character \( \chi : \mathcal{U}_p \to \mathbb{Z}/n\mathbb{Z} \) the conductor is finite.

**Proof.** We have to show that some \( \mathcal{U}_p(n) \) is in the kernel of \( \chi \). Since \( \mathbb{Z}/n\mathbb{Z} \) is finite, the power \( (\mathcal{U}_p(n))^n \) is in the kernel. From Theorem \ref{primes} there is an isomorphism \( \log : \mathcal{U}_p(k) \cong (\pi)^k \) for \( k \) larger than some constant \( l \), where \( \pi \) is the uniformizer of \( K \). We find that \( \mathcal{U}_p(k) \subset (\mathcal{U}_p(n))^n \) since every element \( \log(a) \in (\pi)^k \) has an \( n \)-th root \( \log(a)/n \in (\pi)^{k-n\nu_p(n)} \cong U_p(k-n\nu_p(n)) \) if we choose \( k \) so that \( k - n\nu_p(n) > l \). Therefore all elements in \( U_p(n) \) are \( n \)-th powers, so \( U_p(k) \subset (U_p(n))^n \). \( \square \)

If the character is a sum, the conductor is computable from the summands.

**Theorem 18.** Let \( \chi = \sum_p \chi_p \) be a sum of local characters \( \chi_p \) over distinct primes, like in Theorem \ref{sum-conductor}. The conductor of \( \chi \) is \( \prod_p f_{\chi_p} \), where \( f_{\chi_p} \) is the local conductor of \( \chi_p \).

**Proof.** The characters \( \chi_p \) are obtained from \( \chi \) by composition with the inclusion \( \mathcal{U}_p = (1, \ldots, U_p, \ldots, 1) \to I_K \), so this holds by the definition of the conductor. \( \square \)

The relationship between conductor and discriminant is given by the following formula.

**Theorem 19.** For an abelian number field extension \( L/K \) the relative discriminant \( \mathcal{d}_{L/K} \) is given by

\[
\mathcal{d}_{L/K} = \prod_{\chi \in \text{Char}(G(K))} f_\chi
\]

where \( \text{Char}(G) \) is the set of characters of \( G \), that is homomorphisms \( G \to \mathbb{C}^\times \).

**Proof.** Can be found in [NS99], VII.11.9. \( \square \)

If \( L/K \) is a quadratic extension, \( \text{Gal}(L/K) \cong \mathbb{Z}/2\mathbb{Z} \) and there are only 2 characters with one trivial. The trivial character has conductor 1. If \( \chi : G(K) \to \mathbb{Z}/2\mathbb{Z} \) is a continuous character and \( L \) is the number field
COUNTING EXTENSIONS OF IMAGINARY QUADRATIC FIELDS

corresponding to the open subgroup \( \ker(\chi) \) by the Galois correspondence, then it factors as \( G(K) \to G(K)/\ker(\chi) = \text{Gal}(L/K) \to \mathbb{Z}/2\mathbb{Z} \) and hence \( \chi \) gives the nontrivial character on \( \text{Gal}(L/K) \) so we can compute its conductor locally and thus get the relative discriminant of \( L/K \). The absolute discriminant of \( L \) is then easily computable.

**Theorem 20.** Given a tower of number fields \( L/K/S \) then the relative discriminant of \( L/S \) can be computed as

\[
\mathfrak{o}_{L/S} = N_{K/S}(\mathfrak{o}_{L/K})\mathfrak{o}_{K/S}^{\deg L/K}
\]

where \( N_{K/S}(-) \) is the ideal norm of \( K/S \).

**Proof.** See [NS99] III.2.10. \( \square \)

Let’s calculate the conductor of local fields for our quadratic imaginary number field \( K \). We will start with the odd primes.

**Lemma 21.** If \( p \) is a prime of \( K \) not above 2 (i.e. \( p \cap \mathbb{Z} = (p) \) for an odd prime \( p \)), then \( \mathcal{U}_p \cong \mathbb{Z}/(p^i - 1)\mathbb{Z} \times \mathbb{Z}/p^a\mathbb{Z} \times \mathbb{Z}_p^d \) where \( i \) is the degree of inertia of \( p \) in \( K/\mathbb{Q} \). The number \( d \) is 1 if \( p \) is split and 2 if inert or ramified and \( a \) is some integer.

**Proof.** We know from Theorem 6 that \( K_p \) is an extension of \( \mathbb{Q}_p \) and the degree of inertia and ramification is the same as for \( p \) in \( K/\mathbb{Q} \). We will use Theorem 4. From this theorem we know that \( i \) is the degree of inertia. The number \( d \) is the degree of \( K_p/\mathbb{Q}_p \) is using Theorem 6 the ramification degree times the inertia degree. \( \square \)

We can see that there are only 2 local characters for primes not above 2:

**Lemma 22.** If \( p \) is a prime not above 2, then there are two characters on \( \mathcal{U}_p \) one of which is trivial.

**Proof.** There are no nontrivial homomorphisms to \( \mathbb{Z}/2\mathbb{Z} \) from \( \mathbb{Z}/p^a\mathbb{Z} \) since it has odd size and neither from \( \mathbb{Z}_p \), since \( \frac{1}{2} \in \mathbb{Z}_p \) because \( \frac{1}{2} \in \mathbb{Q}_p \) and \( \nu_p(\frac{1}{2}) = 0 \) for odd \( p \). Finally there is a nontrivial homomorphism from \( \mathbb{Z}/(p^i - 1)\mathbb{Z} \) with kernel \( \mathbb{Z}/(p^i - 1)\mathbb{Z} \) since \( 2|(p^i - 1) \).

The conductors of these local characters are easily computable:

**Lemma 23.** If \( p \) is prime not above 2, then the local conductor of the trivial local character on \( \mathcal{U}_p \) is 0 and for the nontrivial one with kernel \( \frac{(p^i - 1)}{2}\mathbb{Z}/(p^i - 1)\mathbb{Z} \) it is 1.

**Proof.** The trivial one has kernel \( \mathcal{U}_p = \mathcal{U}_p^{(0)} \) and the nontrivial one factors through \( \mathcal{U}_p^{(1)} \) since \( \mathcal{U}_p/\mathcal{U}_p^{(1)} \equiv \mathbb{Z}/(p^i - 1)\mathbb{Z} \) by Theorem 2. \( \square \)

If \( p \) is above 2, then we have three cases depending whether 2 is split, ramified or inert in \( K \). Notice that 2 can’t be ramified if \( K \) is imaginary quadratic with odd class number unless \( K = \mathbb{Q}(i) \) or \( \mathbb{Q}(\sqrt{-2}) \).

**Theorem 24.** The prime 2 is not ramified in the extension \( K/\mathbb{Q} \), where \( K \) is quadratic imaginary with odd class number unless \( K = \mathbb{Q}(i) \) or \( \mathbb{Q}(\sqrt{-2}) \).
Proof. We will show that the ideal $2\mathcal{O}_K$ cannot be written as a principal ideal squared. If the only units in $\mathcal{O}_K$ are $+1, -1$, then $2$ is associated with a square only if $2 = x^2$ or $-2 = x^2$ for some $x \in \mathcal{O}_K$. The first case is not possible since $K$ is imaginary and the second case is possible only in $\mathbb{Q}(\sqrt{-2})$. If there are more units then $K = \mathbb{Q}(i)$ or $K = \mathbb{Q}(\sqrt{-3})$ and for $\mathbb{Q}(\sqrt{-3})$ $2$ is inert. If $(2) = q^2$ for some non-principal ideal $q$, then it has order 2 in the class group, which is a contradiction. 

Lemma 25. If $2$ is split, we have two primes $p$ and $q$ above 2 and $\mathcal{U}_I \cong \mathbb{Z}_2^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2$ for $I = p, q$. If 2 is inert, we have $\mathcal{U}_2 \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^2$.

Proof. We can use Theorem 6 to see that $K_I$ is isomorphic to $\mathbb{Q}_2$ if $I$ is split and $K_2$ is an unramified degree 2 extension of $\mathbb{Q}_2$ if it is inert.

If 2 is split, we can use Theorem 4 and the fact that $O_I$ is isomorphic to $\mathbb{Z}_2$. The exponent $a$ at $\mathbb{Z}/2^a\mathbb{Z}$ is 1 since $-1 \in \mathbb{Z}_2$, but $x^2 = -1$ has no solution in $\mathbb{Z}_2$ (it doesn’t have a solution in $\mathbb{Z}/4\mathbb{Z}$), so there is a second primitive root of unity in $\mathbb{Z}_2$, but no primitive forth root of unity.

If 2 is inert we use the same theorem, $O_2$ is the ring of units of an unramified degree 2 extension of $\mathbb{Z}_2$. From Theorem 7 it can be written as $\mathbb{Q}_2[X]/(f(X))$ where $f(X)$ is a polynomial such that $\mathbb{Z}/2\mathbb{Z}[X]/(f(X))$ is a degree two field extension of the local field $\mathbb{Z}/2\mathbb{Z}$, i.e. it is irreducible in $\mathbb{Z}/2\mathbb{Z}$. This polynomial is $f(X) = X^2 + X + 1$. So the local field is isomorphic to $\mathbb{Q}_2[X]/(X^2 + X + 1)$ and $O_2 \cong \mathbb{Z}_2[X]/(X^2 + X + 1)$ (the elements with valuation $\geq 0$). We also have $a = 1$ since $x^2 = -1$ doesn’t have a solution in $\mathbb{Z}/4\mathbb{Z}[X]/(X^2 + X + 1)$, so there is no primitive forth root of unity. 

Lemma 26. There is an isomorphism $(\mathbb{Z}/4\mathbb{Z}[X]/(X^2 + X + 1))^\times \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z})$.

Proof. The invertible elements in $\mathbb{Z}/4\mathbb{Z}[X]/(X^2 + X + 1)$ are of the form $AX + B$ where both $A, B$ are not zero divisors in $\mathbb{Z}/4\mathbb{Z}$, that is 0 or 2. Therefore there are $4 \cdot 4 - 4 = 12$ elements, so the group is isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$ or $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$. The elements $2X+1, 2X+3$ and $3$ have order 2 and so the group must be isomorphic to $\mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z}$. 

Lemma 27. There is an isomorphism $(\mathbb{Z}/8\mathbb{Z}[X]/(X^2 + X + 1))^\times \cong (\mathbb{Z}/3\mathbb{Z}) \times (\mathbb{Z}/2\mathbb{Z}) \times (\mathbb{Z}/4\mathbb{Z})$.

Proof. The invertible elements in $\mathbb{Z}/8\mathbb{Z}[X]/(X^2 + X + 1)$ are of the form $AX + B$ where both $A, B$ are not zero divisors in $\mathbb{Z}/8\mathbb{Z}$, that is 0, 2, 4 or 6. Therefore there are $8 \cdot 8 - 4 \cdot 4 = 48$ elements. Every element can be multiplied by one of $1, X, X^2$ so that it is of the form $2AX + B$. It can then be multiplied by one of $+1, -1$ so that $B$ is $1 + 4C$. These elements $2AX + 4C + 1$ form a subgroup with $4 \cdot 2 = 8$ elements and it has an element $2X + 1$ of order 4 and 3 elements $5, 4X + 1, 4X + 5$ of order 2, so it is isomorphic to $\mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z}$.

It is now possible to determine all characters for even primes.

Lemma 28. For split primes over 2 we have 3 nontrivial characters with local conductors 2, 3 and 3. If 2 is inert we have 7 nontrivial characters, 3 of them with local conductor 3 and 4 with local conductor 3.
Proof. There are two homomorphism \( \mathbb{Z}_2 \rightarrow \mathbb{Z}/2\mathbb{Z} \). One is trivial and the other one is nontrivial with kernel \( 2\mathbb{Z}_2 \) (because \( 2\mathbb{Z}_2 \) is always in the kernel and so the homomorphism is determined by the image of 1). For split primes we have \( \mathcal{U}_I \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2 \) using Lemma 25, so there are \( 2 \times 2 = 4 \) characters of which 3 are nontrivial (with kernels \((0, 2\mathbb{Z}_2), (\mathbb{Z}/2\mathbb{Z}, 0), (\mathbb{Z}/2\mathbb{Z}, 2\mathbb{Z}_2)\)). Also \( \mathcal{U}_I/\mathcal{U}_I(2) \cong (\mathbb{Z}/2\mathbb{Z})^\times \cong (\mathbb{Z}/4\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \) using Theorem 2, so one of them has conductor 2 (a character factorizes through \( \mathcal{U}/\mathcal{U}(n) \) iff it has local conductor \( \leq n \)). We also have \( \mathcal{U}_I/\mathcal{U}_I(3) \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) and so there are 3 nontrivial characters with local conductors \( \leq 3 \). One of them has local conductor 2, so the other two have local conductor 3.

From the proof of Lemma 25 for inert prime 2 the local field is isomorphic to \( \mathcal{O}_2 \cong \mathbb{Z}_2[X]/(X^2 + X + 1) \). The group of units is \( \mathcal{U}_2 \cong (\mathbb{Z}_2[X]/(X^2 + X + 1))^\times \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}_2^2 \) using Theorem 4. So there are 7 nontrivial characters total. Using Theorem 2 and 26, we can see that \( \mathcal{U}_2/\mathcal{U}_2(3) \cong (\mathbb{Z}/4\mathbb{Z}[X]/(X^2 + X + 1))^\times \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) so 3 of them have conductor 2 and \( \mathcal{U}_2/\mathcal{U}_2(3) \cong (\mathbb{Z}/8\mathbb{Z}[X]/(X^2 + X + 1))^\times \cong \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \) using Lemma 24, so all other characters factorize through \( \mathcal{U}_2(3) \) and so have conductor 3.

\[ \Box \]

7. Counting Function

We put all information about quadratic extensions of a number field \( K \) into one function. We still assume that \( K \) is imaginary quadratic with odd class number.

In this section we will assume that \( K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}), \mathbb{Q}(\sqrt{-3}) \).

**Definition 29.** The counting function \( f_K(s) \) of a number field \( K \) is a function of a complex variable \( s \) defined as the series

\[ f_K(s) = \sum_{n=0}^{\infty} a_n n^{-s} \]

where \( a_n \) is the number of quadratic field extensions of \( K \) with absolute discriminant \( n \).

We have already seen in Theorem 13 that quadratic extensions correspond to nontrivial continuous homomorphisms \( \mathbb{R}^\times_K K^\times/K^\times \cong \mathbb{R}^\times/(\mathbb{R}^\times \cap K^\times) \rightarrow \mathbb{Z}/2\mathbb{Z} \). If \( K \neq \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3}) \), we have \( \mathcal{O}_K^\times = \{+1, -1\} \). Let’s first look at homomorphisms \( \mathbb{R}^\times_K \rightarrow \mathbb{Z}/2\mathbb{Z} \).

In our case of an imaginary quadratic field we have \( \mathbb{R}^\times_K = \mathbb{C}^\times \times \prod_{p \text{ finite}} \mathcal{U}_p \).

We know from Theorem 15 that each character is a sum of a finite number of homomorphisms \( \mathcal{U}_p \rightarrow \mathbb{Z}/2\mathbb{Z} \).

We will see that the counting function can be written as a product of local factor over the primes. For convenience we will define the absolute conductor of a character as the norm of the conductor of the character, which is natural number instead of an ideal.
Definition 30. We define the local factor \( g_p(s) \) at a prime \( p \) to be the function
\[
g_p(s) = \sum_{\chi_i} N(p)^{-f_i s}
\]
where the sum is over all characters \( \chi_i \) on \( U_p \) and \( f_i \) is the local conductor of \( \chi_i \).

From Lemma 23 we get that:

Theorem 31. For primes \( p \) not above 2 the local factor is
\[
g_p(s) = (1 + N(p)^{-s})
\]

Similarly from Lemma 28 we get

Theorem 32. If 2 is inert, then the local factor \( g_2(s) \) is:
\[
g_2(s) = (1 + 3N(2)^{-2s} + 4N(2)^{-3s})
\]
and if 2 is split, then for the primes \( I \) above 2 we have
\[
g_I(s) = (1 + N(I)^{-2s} + 2N(I)^{-3s}).
\]

First we show that a simplified counting function can be written as a product of local factors.

Theorem 33. The counting function \( f_0(s) = \sum_{n \geq 1} a_n n^{-s} \) where \( a_n \) is the number of continuous characters \( \gamma : \mathbb{I}_K^\infty \to \mathbb{Z}/2\mathbb{Z} \) with absolute conductor \( n \) can be written as
\[
f_0(s) = \prod_{\text{primes of } K} g_p(s) = \prod_{p \mid 2} g(s)_p \times \prod_{p \nmid 2} (1 + N(p)^{-s}).
\]
Furthermore it converges for \( \text{Re}(s) > 1 \).

Proof. Notice that the function \( f_0(s) \) can also be written as a sum over ideals of \( \mathcal{O}_K \), that is
\[
f_0(s) = \sum_I a_I N(I)^{-s},
\]
where \( a_I \) is the number of homomorphisms with conductor \( I \). This is the same sum, we are just indexing the terms by the conductors (ideals) instead of their norms (natural numbers).

Using the theorems in Section 5 we know that every nontrivial homomorphism \( \gamma : \mathbb{I}_K^\infty \to \mathbb{Z}/2\mathbb{Z} \) can be uniquely written as a sum of finitely many homomorphisms \( \chi_p : U_p \to \mathbb{Z}/2\mathbb{Z} \) over distinct primes. Denote \( D_k \) the set of primes of \( \mathcal{O}_K \) with norm less than \( k \) and \( H_k \) the set of ideals, that can be written as products of prime ideals from \( D_k \). The set \( D_k \) is finite, because the are only finitely many ideals with norm less then some number (Theorem 4.4). Every character \( \gamma \) whose conductor is in \( H_k \) can be written as a sum of local characters over primes in \( D_k \). This is because the absolute conductor of a sum of local homomorphisms over distinct primes \( \sum_p \chi_p \) is \( \prod_p N(p)^{f_p} \), by Theorem 18.

We have
\[
\sum_{I \in H_k} a_I N(I)^{-s} = \prod_{p \in D_k} g_p(s)
\]
as we will show. The local factors \( g_p(s) \) are sums of the terms \( N(p)^{-f_p s} \) for all local characters \( \chi_p \) on \( U_p \) to the power \( -s \) (here \( f_p \) is the local conductor of \( \chi_p \)). If we multiply out all the local factors for primes in \( D_k \), we get exactly the sum of absolute conductors of all sums of local characters of primes in \( D_k \) to the power \( -s \). Therefore
the product is \( \sum_{\chi} N(I_{\chi})^{-s} = \sum_{I \in H_k} a_I N(I)^{-s} \) where the first sum is over characters with conductor in \( H_k \) and \( I_{\chi} \) is the conductor of \( \chi \).

From this and the form of the factors \( g_p(s) \), we can see that \( a_I \) is at most 4, so the sum \( f_0(s) = \sum_{I \text{ ideal of } \mathcal{O}_K} a_I N(I)^{-s} \) converges for \( \text{Re}(s) > 1 \). We get the inequality

\[
|f_0(s) - \prod_{p \in D_k} g_p(s)| \leq \sum_{I \notin H_k} a_I N(I)^{-\text{Re}(s)}.
\]

Thus on the halfplane \( \text{Re}(s) > 1 \) the product converges to \( f_0(s) \) by letting \( k \) go to infinity. \( \square \)

The counting function looks like an Euler product for the Dedekind zeta function.

In fact, we have

**Theorem 34.** The function \( f_0(s) \) can be expressed as

\[
f_0(s) = \frac{\zeta_K(s)}{\zeta_K(2s)} \times \prod_{p \mid 2} \frac{g(s)_p}{(1 + N(p)^{-s})}
\]

and therefore can be analytically extended to a holomorphic function for \( \text{Re}(s) > 1/2, s \neq 1 \) with a simple pole at 1.

**Proof.** We can write

\[
f_0(s) = \prod_{p \mid 2} g(s)_p \times \prod_{p \nmid 2} (1 + N(p)^{-s}) =
\]

\[
= \prod_{p \mid 2} \frac{g(s)_p}{(1 + N(p)^{-s})} \times \prod_{p \text{ all primes}} (1 + N(p)^{-s}) =
\]

\[
= \prod_{p \mid 2} \frac{g(s)_p}{(1 + N(p)^{-s})} \times \prod_{p \text{ all primes}} \frac{(1 - N(p)^{-2s})}{(1 - N(p)^{-s})} =
\]

\[
= \prod_{p \mid 2} \frac{g(s)_p}{(1 + N(p)^{-s})} \times \frac{\zeta_K(s)}{\zeta_K(2s)}.
\]

The function \( \zeta_K \) is holomorphic outside 1 with a simple pole at 1. It also has no zeros for \( \text{Re}(s) > 1 \) so the function \( \frac{1}{\zeta_K(2s)} \) is holomorphic on the halfplane \( \text{Re}(s) > 1/2 \). There are only 1 or 2 primes above 2, so the first factor is holomorphic on \( \mathbb{C} \). \( \square \)

From Theorem 15 we know that quadratic extensions of \( K \) correspond to homomorphisms from \( \mathbb{I}_K^\times \) to \( \mathbb{Z}/2\mathbb{Z} \) with \( \mathbb{I}_K^\times \cap K^\times \) in the kernel. So far we have only looked at homomorphisms \( \mathbb{I}_K^\times \to \mathbb{Z}/2\mathbb{Z} \), so we need to figure out which ones send \( \mathbb{I}_K^\times \cap K^\times \) to 0 in \( \mathbb{Z}/2\mathbb{Z} \). As we saw just before Lemma 15 we have \( \mathbb{I}_K^\times \cap K^\times = \{+1, -1\} \). So the characters need to send \(-1\) to 0. We will call a character even if it does send \(-1\) to 0 and odd otherwise.

**Definition 35.** We define the odd local factor \( g_-(s)_p \) at a prime \( p \) to be the function

\[
g_p(s) = \sum_{\chi_i} \sigma_i N(p)^{-f_i s}
\]
where the sum is over all characters $\chi_i$ on $\mathcal{U}_p$ and $f_i$ is the local conductor of $\chi_i$ and $\sigma_i$ is 1 if the character is even and $-1$ if it is odd.

From Lemma 23 we get that:

**Theorem 36.** For primes $p$ not above 2 the odd local factor is

$$g_-(s)_p = (1 + N(p)^{-s})$$

if $p$ is inert or the prime $p$ (where $p$ is above $p$) is 1 mod 4 and

$$g_-(s)_p = (1 - N(p)^{-s})$$

if it is not inert and $p$ is 3 (mod 4).

**Proof.** Same as for the ordinary local factor, but now we have to look where is $-1$ sent by the nontrivial character on $\mathcal{U}_p$. From Lemma 23 we get that $\mathcal{U}_K \cong \mathbb{Z}/(p^i - 1)\mathbb{Z} \times \mathbb{Z}/p^2\mathbb{Z} \times \mathbb{Z}/p^d$. The element $-1$ is mapped to $((\frac{p^i-1}{2}),0,0)$ by the isomorphism. If $p$ is inert, then $i = 2$ and $4|(p^i - 1)$, so $-1$ is mapped to 0 by the nontrivial character. This is also the case if $4|(p - 1)$. Otherwise $-1$ is sent to $1 \in \mathbb{Z}/2\mathbb{Z}$ and the nontrivial character on $\mathcal{U}_p$ is odd. \(\square\)

We will write $C$ for the set of primes that satisfy the first condition in the previous theorem.

Similarly from Lemma 23 we get

**Theorem 37.** If 2 is inert, then the odd local factor $g_-(s)_2$ is:

$$g_-(s)_2 = (1 + N(2)^{-2s} - 2N(2)^{-2s} + 2N(2)^{-3s} - 2N(2)^{-3s})$$

and is 2 s split, then for the primes $I$ above 2 we have

$$g_-(s)_I = (1 - N(I)^{-2s} - N(I)^{-3s} + N(I)^{-3s})$$

**Proof.** Same as for the ordinary local factor, but we use Lemmas 26 and 27 to figure out what characters are odd.

If 2 is split, then $-1$ maps to $1 \in \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/4\mathbb{Z})^\times \cong U/U(2)$ and to $(1,0) \in \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong (\mathbb{Z}/8\mathbb{Z})^\times \cong U/U(3)$, so one character of local conductor 2 is odd and two characters of local conductor at most 3 are odd, one of them has local conductor 2. In total there is one odd character of local conductor 2 and one odd character of local conductor 3. Thus the local factor, denoted $g_-(s)_I$, is $(1 - N(I)^{-2s} - N(I)^{-3s} + N(I)^{-3s})$.

If 2 is inert, $-1$ maps to $(0,1,0) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \cong U/U(2)$ and to $(0,1,0,0) \in \mathbb{Z}/3\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/4\mathbb{Z} \cong U/U(3)$ and we can see that two characters of conductor 2 are odd, and two characters of conductor 3 are odd, and thus the local factor is $(1 + N(2)^{-2s} - 2N(2)^{-2s} + 2N(2)^{-3s} - 2N(2)^{-3s})$. \(\square\)

**Theorem 38.** The counting function $f_-(s) = \sum_{n \geq 1} b_n n^{-s}$ where $b_n$ is the number of continuous characters $\mathbb{F}_K^\times \rightarrow \mathbb{Z}/2\mathbb{Z}$ with absolute conductor $n$ that are even minus the number characters with conductor $n$ that are odd, can be written as

$$f_-(s) = \prod_{p \text{ primes of } K} g_-(s)_p = \prod_{p|2} g_-(s)_p \prod_{p \in C, p \nmid 2} (1 + N(p)^{-s}) \prod_{p \in C} (1 - N(p)^{-s})$$
Furthermore it converges for \( \text{Re}(s) > 1 \).

Proof. The proof is similar to the one for the counting function \( f_0(s) \). If we write a character on \( I_K^\times \) as a sum of local characters on \( U_p \), then the character is even iff there is an even number of odd characters in the sum, since \(-1\) is then mapped to 0 in \( \mathbb{Z}/2\mathbb{Z} \). If we multiply out the product, the terms correspond to sums of local characters and the sign is positive if the sum has even number of odd local characters and negative if it has an odd number of odd local characters.

Finally the counting function of \( K \) is expressed as:

Theorem 39. The counting function \( f_K(s) \) can be written as

\[
f_K(s) = \frac{\varpi^{-2s}}{2}(f_0(s) + f_-(s)) - \frac{\varpi^{-2s}}{2}
\]

where \( K \) is a quadratic imaginary number field with odd class number different from \( \mathbb{Q}(i) \), \( \mathbb{Q}(\sqrt{-2}) \), \( \mathbb{Q}(\sqrt{-3}) \) and \( \varpi_K \) is the discriminant of \( K \) as a natural number.

Proof. We know from Theorem 15 that quadratic extensions of \( K \) correspond to nontrivial continuous on \( I_K^\infty \to \mathbb{Z}/2\mathbb{Z} \) with \((I_K^\infty \cap K^\times)\) in the kernel. We have \((I_K^\infty \cap K^\times) = \{+1, -1\}\) for our \( K \) and so the extensions correspond to even nontrivial continuous characters. Furthermore the absolute discriminant of the extension corresponding to the character \( \chi \) is from Theorem 20 equal to \( N(I_\chi)\varpi_K^2 \) where \( I_\chi \) is the conductor of \( \chi \).

The function \( f_0 \) counts all characters, and the function \( f_- \) counts even characters minus odd characters. Therefore adding them with a factor of one half counts only even characters. The terms in this counting function have terms \( N(I)^{-s} \), so we have to multiply it by \( \varpi^{-2s} \) to get terms with the absolute discriminant. The term \( -\varpi^{-2s} \) is the eliminate the trivial character which correspond to the extension \( K/K \) which we don’t count.

\[\square\]

8. Asymptotical distribution of number fields

We can use the counting function to get the asymptotical distribution of quadratic extensions of \( K \).

Theorem 40. Let \( f(s) = \sum_{n=1} a_n n^{-s} \) be convergent for \( \text{Re}(s) > a > 0 \). Assume that in the domain of convergence \( f(s) = g(s)(s-a)^{-w} + h(s) \) holds, where \( g(s), h(s) \) are holomorphic functions in the closed half plane \( \text{Re}(s) \geq a \), and \( g(a) \neq 0 \), and \( w > 0 \). Then

\[
\sum_{1 \leq n \leq X} a_n = \frac{g(a)}{a\Gamma(w)} X^a (\log X)^{w-1} + o(X^a (\log X)^{w-1})
\]

As a special case, if \( f(s) \) converges for \( \text{Re}(s) > 1 \) and has meromorphic continuation to \( \text{Re}(s) \geq 1 \) with a simple pole at \( s = 1 \) with residue \( r \), then

\[
\sum_{1 \leq n \leq X} a_n = rX + o(X)
\]
Proof. Corollary on page 121 of [Nar83].

We know that the function \( f_0(s) \) is up to some simple factors equal to \( \frac{\zeta_K(s)}{\zeta_K(2s)} \). This function satisfies the special case of the previous theorem, we just have to compute the residue. The residue is \( \text{Res}_{s=1} \frac{\zeta_K(s)}{\zeta_K(2s)} = \frac{\text{Res}_{s=1} \zeta_K(s)}{\zeta_K(2)} \).

The residue of the Dedekind zeta function is given by the class number formula.

**Theorem 41.** The residue of the Dedekind zeta function of the number field \( K \) is

\[
\text{Res}_{s=1} \zeta_K(s) = \frac{2r_1(2\pi)^r \text{Reg}_K h_K}{w_K \sqrt{\Delta_K}}
\]

where \( r_1 \) and \( r_2 \) is the number of real and complex places respectively, \( \text{Reg}_K \) is the regulator of \( K \), \( h_K \) is the class number and \( w_K \) is the number of roots of unity in \( K \). In particular, for an imaginary quadratic number field \( r_1 = 0, r_2 = 1 \) and \( \text{Reg}_K = 1 \)

Proof. See [NS99] VII. 5.11.

The value \( \zeta_K(2) \) for imaginary quadratic number field is calculated in [Zag86] Theorem 2.

\[
\zeta_K(2) = \frac{\pi^2}{6\sqrt{\Delta_K}} \sum_{0 < n < \Delta_K} \left\langle -\frac{\Delta_K}{n} \right\rangle A \left( \cot \left( \frac{\pi n}{\Delta_K} \right) \right)
\]

where the function \( A(x) \) is defined as

\[
A(x) = 2 \int_0^\infty \frac{t \, dt}{x \sinh^2 t + x^{-1} \cosh^2 t}
\]

and \( \langle a \rangle \) is the Kronecker symbol.

Now for the function \( f_-(s) \). We can express it using Dirichlet L-functions. A Dirichlet character is a homomorphism \( \chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times \). We can extend it to \( \mathbb{Z} \) by defining \( \chi(a) = 0 \) if \( \gcd(m, a) \neq 1 \). For example we have a character \( \chi_4 : (\mathbb{Z}/4\mathbb{Z})^\times \to \mathbb{C} \) where \( \chi_4(3) = -1 \). For an imaginary quadratic number field \( K \) there is a character (the Kronecker symbol \( \left( \frac{\cdot}{\Delta_K} \right) \)) \( \chi_K : (\mathbb{Z}/\Delta_K \mathbb{Z})^\times \to \mathbb{C} \) such that \( \chi_K(p) = 1 \) if \( p \) splits in \( K \) and -1 if \( p \) is inert in \( K \).

We will denote \( I, S, R \) the set of inert, split and ramified primes of \( K \) not above 2 and \( I_i, S_i, R_i \) \( i = 1, 3 \) the subset of primes that are \( i \mod 4 \). For every character \( \chi : (\mathbb{Z}/m\mathbb{Z})^\times \to \mathbb{C}^\times \) we have an L-function

\[
L(\chi, s) = \prod_{p \text{ prime}} \frac{1}{1 - \chi(p)p^{-s}}
\]

which converges to a holomorphic function for \( \text{Re}(s) > 1 \).
COUNTING EXTENSIONS OF IMAGINARY QUADRATIC FIELDS

If we ignore the factors from primes above 2, the function \( f_-(s) \) is equal to

\[
\prod_{p \notin C} (1 + N(p)^{-s}) \prod_{p \in C} (1 - N(p)^{-s}) = \\
\prod_{p \in I} (1 + p^{-2s}) \prod_{p \in S_1} (1 + p^{-s})^2 \prod_{p \in S_3} (1 - p^{-s})^2 \times R(s)
\]

since the norm of a prime ideal \( p \) above 2 is \( p^2 \) if it is inert and \( p \) otherwise and \( p \) is odd in all products. Here \( R(s) \) is the factor for the (finitely many) ramified primes \( R(s) = \prod_{p \in R_1} (1 + N(p)^{-s}) \times \prod_{p \in R_3} (1 - N(p)^{-s}) \).

Now we can write:

\[
\prod_{p \in I} (1 + p^{-2s}) \prod_{p \in S_1} (1 + p^{-s})^2 \prod_{p \in S_3} (1 - p^{-s})^2 R(s) = \\
\prod_{p \in I} (1 - p^{-4s}) \prod_{p \in S_1} (1 - p^{-2s})^2 \prod_{p \in S_3} (1 + p^{-s})^2 \times \\
\prod_{p \in R_1} (1 - p^{-s}) \prod_{p \in R_3} (1 + p^{-s}) = \\
\frac{B(s)/\zeta_K(2s)}{\prod_{p \in I_1} (1 - p^{-s}) \prod_{p \in I_3} (1 + p^{-s}) \prod_{p \in S_1 \cup R_1} (1 - p^{-s}) \prod_{p \in S_3 \cup R_3} (1 + p^{-s})} \\
\times \prod_{p \in I_1} (1 + p^{-s}) \prod_{p \in I_3} (1 - p^{-s}) \prod_{p \in S_1} (1 - p^{-s}) \prod_{p \in S_3} (1 + p^{-s}) = \\
\frac{L(\chi, s) L(\chi \chi_K, s)}{\zeta_K(2s)} \times B(s)
\]

where \( \chi \chi_K \) is a character on \((\mathbb{Z}/\text{lcm}(4, \mathfrak{o}_K)\mathbb{Z})^\times\) and \( B(s) = \prod_{p \mid 2} 1/(1 - N(p)^{-2s}) \) is the factor of \( \zeta_K(2s) \) at 2. For this character \( \chi \chi_K(p) = 1 \) if \( p \) is inert and 3 mod 4 or split and 1 mod 4 , \( \chi \chi_K(p) = 0 \) if \( p \) is ramified or 2 and \( \chi \chi_K(p) = -1 \) otherwise. We can summarize it in the following theorem.

**Theorem 42.** Let \( K \) be a imaginary quadratic number field with odd class number not equal to \( \mathbb{Q}[i], \mathbb{Q}[\sqrt{-3}], \mathbb{Q}[\sqrt{-2}] \). Then the function \( f_-(s) \) can be written as

\[
f_-(s) = \frac{L(\chi, s) L(\chi \chi_K, s)}{\zeta_K(2s)} \times \prod_{p \mid 2} g_-(s)_p \times B(s)
\]

In particular, it is holomorphic for \( \text{Re}(s) \geq 1 \).

**Proof.** The equation is clear from the preceding discussion we just added the factors for the primes above 2. The Dedekind zeta function \( \zeta_K(2s) \) is holomorphic and nonzero on the halfplane \( \text{Re}(s) > 1/2 \). Since the characters \( \chi_4 \) and \( \chi_4 \chi_K \) are nontrivial if \( K \neq \mathbb{Q}(i) \), the L-functions are holomorphic for all \( s \). \( \square \)

The conditions we have on the number field force it to be of the following form:
Theorem 43. If \( K \) is an imaginary quadratic number field with odd class number not equal to \( \mathbb{Q}(i), \mathbb{Q}(\sqrt{-2}) \) then it is of the form \( \mathbb{Q}(\sqrt{-p}) \) where \( p \) is a prime that is \( 3 \) (mod 4).

Proof. Because 2 is not ramified, \( K \) is of the form \( \mathbb{Q}(\sqrt{-D}) \) for some \( D = 3 \) (mod 4) squarefree. By Gauss’s genus theory (see chapter 4 and 6 in [Bue89]) the class group contains exactly \( 2^{r-1} \) elements of order \( \leq 2 \) where \( r \) is the number of primes dividing \( D \). Therefore \( D \) must be prime. □

We can put everything together to get the main result

Theorem 44. For a quadratic imaginary number field \( K = \mathbb{Q}(\sqrt{-p}) \) with \( p \) prime \( > 3 \) that is \( 3 \) (mod 4), the function \( a_K(n) = \#\{L/K|\deg(L/K) = 2, \mathfrak{d}_L \leq n\} \) is asymptotically equal to

\[
a_K(n) = Cn + o(n)
\]

where \( C \) is given by

\[
C = \frac{1}{2\mathfrak{d}_K} \mathop{\text{Res}}_{s=1} \zeta_K(s) \prod_{p|2} \frac{g_p(1)}{(1 + N(p))^{-1}} = \frac{\mathfrak{d}_K^{-5/2} \pi h_K}{2 \zeta_K(2)} \prod_{p|2} \frac{g_p(1)}{(1 + N(p))^{-1}}
\]

Proof. Apply the special case of Theorem 40 to the function

\[
f_K(s) = \mathfrak{d}_K^{-s} \left( f_0(s) + f_-(s) \right) = \mathfrak{d}_K^{-2s}.
\]

This function is holomorphic for \( \Re(s) \geq 1 \) except for a pole at 1. The functions \( f_-(s) \) and \( \mathfrak{d}_K^{-2s} \) have no pole at 1, so it doesn’t affect the asymptotic growth. The number \( C \) is the residue of \( f_K(s) \) at 1, which is thus \( \frac{1}{2\mathfrak{d}_K} \) times the residue of \( f_0(s) \). Then use Theorem 41 to get the formula for the residue. □

9. Special cases

We ignored the cases of \( K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-2}) \). We will show that the main Theorem 44 holds for these fields in this form:

Theorem 45. For a quadratic imaginary number field \( K \) with odd class number the function \( a_K(n) = \#\{L/K|\deg(L/K) = 2, \mathfrak{d}_L \leq n\} \) is asymptotically equal to

\[
a_K(n) = Cn + o(n)
\]

where \( C \) is given by

\[
C = \frac{\mathfrak{d}_K^{-5/2} \pi h_K}{w_K \zeta_K(2)} \prod_{p|2} \frac{g_p(1)}{(1 + N(p))^{-1}}
\]

where \( w_K \) is the number of roots of unity in \( K \) and \( g_p(s) \) is

\[
g_p(s) = \begin{cases} 
(1 + 2^{-2s} + 2 \cdot 2^{-3s}), & \text{if } 2 \text{ is split in } K \\
(1 + 3 \cdot 4^{-2s} + 4 \cdot 4^{-3s}), & \text{if } 2 \text{ is inert in } K \\
(1 + 2^{-2s} + 2 \cdot 2^{-4s} + 4 \cdot 2^{-5s}), & \text{if } 2 \text{ is ramified in } K
\end{cases}
\]

Proof. We only need to show this for \( K = \mathbb{Q}(i), \mathbb{Q}(\sqrt{-3}), \mathbb{Q}(\sqrt{-2}) \). The only problem with \( \mathbb{Q}(\sqrt{-3}) \) is that the unit group has six elements, \( \mathcal{O}_K^\times \cong \mathbb{Z}/6\mathbb{Z} \cong \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}/3\mathbb{Z} \). The \( \mathbb{Z}/2\mathbb{Z} \) part is generated by \(-1\) and the
The unit group has 4 elements and is generated by \( i \) and \(-1\). We also have more units, the unit group is generated by \(-1\) and the ring of integers is \( \mathbb{Z} \). The case of real number fields is similar to the function \( h_{\sqrt{-2}}(x) \) for \( x \) such that 2 is not ramified and with a unit of norm -1. Then the counting function is constructed similarly, only now the function \( f_{-}(s) \) is equal to

\[
f_{-}(s) = \prod_{p \text{ inc.}} (1+p^2) \prod_{p \text{ spl., 1 mod 8}} (1+p)^2 \prod_{p \text{ spl., 5 mod 8}} (1-p)^2 \times g_{-}(s)_{1+i} \times R(s),
\]

which can also be written as \( L(\chi_8, s)L(\chi_4\chi_8, s)\zeta_{\mathbb{Q}(i)}(2s) \times B(s) \) similarly as in Theorem 44 where the character \( \chi_8(s) = -1 \) for \( s = 5, 7 \) mod 8 and \( \chi_8(s) = 1 \) otherwise. This function is holomorphic in the region \( \text{Re}(s) \geq 1 \) and so the Theorem 44 holds even for \( \mathbb{Q}(i) \).
where \( g_p(s) \) is as in theorems 31 and 32. And the analogue of Theorem 34 holds
\[
f_0(s) = \frac{\zeta_K(s)}{\zeta_K(2s)} \prod_{p | 2} g_p(1) (1 + N(p)^{-s}).
\]

Proof. The fundamental unit \( \varepsilon \) and -1 generate the units of \( K \) by the Dirichlet unit theorem. The condition means that we have \( \nu_1(\varepsilon) > 0, \nu_2(\varepsilon) < 0 \). We also have \( \nu_1(-1) < 0, \nu_2(-1) < 0 \). This means that in this case we can choose characters on the infinite real primes to send -1 and \( \varepsilon \) to any combination of 0 and 1 in \( \mathbb{Z}/2\mathbb{Z} \). The proof is then similar to Theorem 33, since for every character on the finite primes there is a unique character on the infinite primes such that their sum sends all units to 0. Therefore all characters can be chosen to be even. \( \square \)

These number fields have the following form.

**Theorem 47.** Let \( K \) be a real quadratic number field with odd class number and with a unit of norm -1 such that 2 is not ramified. Then these fields are exactly of the form \( \mathbb{Q}(\sqrt{p}) \) where \( p \) is a prime that is \( 1 \pmod{4} \).

Proof. \( K \) must be of the form \( \mathbb{Q}(\sqrt{D}) \) for some squarefree \( D \) that is \( 1 \pmod{4} \). The Gauss’s genus theory says that the narrow class group has exactly \( 2^{r-1} \) elements of order \( \leq 2 \) where \( r \) is the number of primes dividing \( D \). Because we have a unit of order -1, the narrow class group is the same as the class group. Therefore \( D \) must be prime. Additionally the Pell equation \( x^2 - Dy^2 = -4 \) has a solution (see Theorem 9.3 in [Bue89]), so the field has a unit of norm -1. \( \square \)

From this we get the analogue of Theorem 43.

**Theorem 48.** For a real quadratic number field \( K = \mathbb{Q}(\sqrt{p}) \) with \( p \) prime that is \( 1 \pmod{4} \) the function \( a_K(n) = \#\{L/K \mid \deg(L/K) = 2, \mathfrak{o}_L \leq n \} \) is asymptotically equal to
\[
a_K(n) = Cn + o(n)
\]
where \( C \) is given by
\[
C = \frac{1}{\mathfrak{o}_K^{5/2}} \frac{\zeta_K(s)}{\zeta_K(2)} \prod_{p | 2} g_p(1) (1 + N(p)^{-1}) = \frac{2\mathfrak{o}_K^{-5/2} \log \varepsilon \cdot h_K}{\zeta_K(2)} \prod_{p | 2} \frac{g_p(1)}{(1 + N(p)^{-1})}
\]

Proof. Apply the special case of Theorem 40 to the function \( f_K(s) = \mathfrak{o}_K^{-2s} f_0(s) \) and then use the class number formula. \( \square \)

**References**

[Bue89] Duncan A Buell. *Binary quadratic forms*. Springer, 1989.
[Coh00] Henri Cohen. *Advanced topics in computational number theory*. Springer, 2000.
[LR20] Wen-Ching Winnie Li and Zeev Rudnick. Pair arithmetical equivalence for quadratic fields. [https://arxiv.org/abs/2007.13147](https://arxiv.org/abs/2007.13147), 2020.
[Mil13] James Milne. *Class field theory*, 2013.
[Mil17] James Milne. *Algebraic number theory*, 2017.
[Nar83] Władysław Narkiewicz. *Number theory*. World Scientific Publishing Co., 1983.
[NS99] Jürgen Neukirch and Norbert Schappacher. *Algebraic number theory*. Springer, 1999.
[Woo14] Melanie Matchett Wood. Asymptotics for number fields and class groups, 2014. URL: http://swc.math.arizona.edu/aws/2014/2014WoodNotes.pdf

[Wri89] David J. Wright. Distribution of discriminants of abelian extensions. Proc. London Math. Soc, 1989.

[Zag86] Don Zagier. Hyperbolic manifolds and special values of Dedekind zeta-functions. 1986.