THE IDEAL CLASS NUMBER FORMULA FOR AN IMAGINARY QUADRATIC FIELD

The factorizations

$$6 = 2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$$

show that unique factorization fails in the ring

$$\mathbb{Z}[\sqrt{-5}] = \{a + b\sqrt{-5} : a, b \in \mathbb{Z}\},$$

because 2, 3, and $1 \pm \sqrt{-5}$ are irreducible and nonassociate.

These notes present a formula, due to Dirichlet, that in some sense measures the extent to which unique factorization fails in settings such as $\mathbb{Z}[\sqrt{-5}]$. The large-scale methodology deserves immediate note, before the reader is immersed in a long succession of smaller attention-demanding specifics:

- *algebra* lets us define a group that measures the failure of unique factorization,
- *geometry* shows that the group is finite and gives an algorithm to find a set of group element representatives in any specific instance,
- and *analysis* yields the formula for the group's order.

To move forward through the main storyline without bogging down, the exposition quotes results from algebra and complex analysis even though elementary arguments are possible in this context. For a more fleshed out and elementary presentation, see Tom Weston's online notes for the 2004 Ross mathematics program,

`www.math.umass.edu/~weston/oldpapers/cnf.pdf`

The class number formula in general is discussed in many number theory books, such as the books by Marcus and by Borevich and Shafarevich.

Contents

Part 1. ALGEBRA: QUADRATIC NUMBER FIELDS 2

Part 2. GEOMETRY: COMPLEX LATTICES 17

Part 1. ALGEBRA: QUADRATIC NUMBER FIELDS

This part of these notes discusses *quadratic number fields* (fields like $\mathbb{Q}(\sqrt{-5})$) and their *rings of integers* (rings like $\mathbb{Z}[\sqrt{-5}]$). The ideals of the ring factor uniquely even though the elements of the ring may not. A group called the *ideal class group* measures the extent to which ideals fail to correspond to ring elements, thus measuring the extent to which unique factorization of elements fails.

1. Quadratic fields and their integers

Definition 1.1. *A* **quadratic number field** *is a field F (inside $\mathbb{C}$) such that F has dimension 2 as a vector space over $\mathbb{Q}$. Such a field takes the form*

$$F = \mathbb{Q}(\sqrt{n}) = \{a + b\sqrt{n} : a, b \in \mathbb{Q}\}, \quad n \in \mathbb{Z} - \{0,1\} \text{ squarefree.}$$

If n is positive then F is a **real** *quadratic number field, and if n is negative then F is an* **imaginary** *quadratic number field.*

From now on in this writeup the symbol F denotes a quadratic number field, and *quadratic number field* is freely shortened to *quadratic field*.

The **conjugation** function of F is

$$\overline{} : F \longrightarrow F, \quad \overline{a + b\sqrt{n}} = a - b\sqrt{n}.$$

Conjugation is a ring homomorphism, meaning that

$$\overline{x+y} = \overline{x} + \overline{y} \quad \text{and} \quad \overline{xy} = \overline{x}\,\overline{y} \quad \text{for all } x, y \in F.$$

And conjugation is an involution, meaning that

$$\overline{\overline{x}} = x \quad \text{for all } x \in F.$$

Thus conjugation is an automorphism of F. The only other automorphism of F is the identity map, and so the group of automorphisms of F has order 2, generated by conjugation.

The **trace** function of F is the additive homomorphism

$$\mathrm{tr} : F \longrightarrow \mathbb{Q}, \quad \mathrm{tr}(\alpha) = \alpha + \overline{\alpha}.$$

Specifically,

$$\mathrm{tr}(a + b\sqrt{n}) = a + b\sqrt{n} + \overline{a + b\sqrt{n}} = 2a.$$

The **norm** function of F is the multiplicative homomorphism

$$\mathrm{N} : F^\times \longrightarrow \mathbb{Q}^\times, \quad \mathrm{N}(\alpha) = \alpha\,\overline{\alpha}.$$

Specifically,

$$\mathrm{N}(a + b\sqrt{n}) = (a + b\sqrt{n})(\overline{a + b\sqrt{n}}) = a^2 - b^2 n.$$

If F is imaginary quadratic then the norm is positive on $F^\times$. We extend the norm to $\mathrm{N}(0) = 0\overline{0} = 0$, and this extended norm is still multiplicative.

Because conjugation is an involution, it has no effect on trace and norm, i.e., $\mathrm{tr}(\overline{\alpha}) = \overline{\alpha} + \overline{\overline{\alpha}} = \overline{\alpha} + \alpha = \alpha + \overline{\alpha} = \mathrm{tr}(\alpha)$ and similarly $\mathrm{N}(\overline{\alpha}) = \mathrm{N}(\alpha)$ for all $\alpha \in F$. Because each element α of $F - \mathbb{Q}$ has trace and norm in $\mathbb{Q}$ it satisfies a monic quadratic polynomial with rational coefficients,

$$(X - \alpha)(X - \overline{\alpha}) = X^2 - \mathrm{tr}(\alpha)X + \mathrm{N}(\alpha).$$

With $\alpha = a + b\sqrt{n}$ this polynomial has discriminant $\mathrm{tr}(\alpha)^2 - 4\mathrm{N}(\alpha) = 4a^2 - 4(a^2 - b^2 n) = 4b^2 n$, and so it is irreducible because b is nonzero and n is not 0 or 1 and is squarefree. Thus α does not satisfy a monic linear polynomial over $\mathbb{Q}$. Of course, each $\alpha \in \mathbb{Q}$ satisfies the monic linear polynomial $X - \alpha$ over $\mathbb{Q}$.

Definition 1.2. *An element of F is an* **integer** *if its minimal monic polynomial over $\mathbb{Q}$ in fact has coefficients in $\mathbb{Z}$.*

Thus the integers of $F \cap \mathbb{Q}$ (the **rational integers** of F) are $\mathbb{Z}$. An element $\alpha = a + b\sqrt{n}$ of F, where $a, b \in \mathbb{Q}$, is an algebraic integer if and only if its trace $2a$ and its norm $a^2 - b^2 n$ are rational integers. Supposing that $2a, a^2 - b^2 n \in \mathbb{Z}$, we obtain necessary conditions on a and b:

- The relation $4\mathrm{N}(\alpha) = (2a)^2 - 4b^2 n$ gives $4b^2 n \in \mathbb{Z}$.
- If $a \in \mathbb{Z}$ then it further shows that $4b^2 n \in 4\mathbb{Z}$, so that $b \in \mathbb{Z}$ because n is squarefree.
- If $a \notin \mathbb{Z}$ then $a \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$ and so $2a$ is an odd integer, and the relation $4\mathrm{N}(\alpha) = (2a)^2 - 4b^2 n$ further shows that $4b^2 n \equiv 1 \pmod 4$, so that $b \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$ and then $2b$ is an odd integer and so $4b^2 = (2b)^2 \equiv 1 \pmod 4$, giving $n \equiv 1 \pmod 4$.
- That is, the necessary conditions are that either $a, b \in \mathbb{Z}$ with no conditions on n, or $a, b \in \frac{1}{2}\mathbb{Z} - \mathbb{Z}$ and $n \equiv 1 \pmod 4$.

Now we show that the necessary conditions on a and b are also sufficient:

- If $a, b \in \mathbb{Z}$ then certainly $2a, a^2 - b^2 n \in \mathbb{Z}$.
- If $a = a_o/2, b = b_o/2$ with $a_o, b_o \in \mathbb{Z}$ odd and $n \equiv 1 \pmod 4$ then $2a = a_o \in \mathbb{Z}$, and because $a_o^2 - b_o^2 n \equiv 0 \pmod 4$ also $a^2 - b^2 n = (a_o^2 - b_o^2 n)/4 \in \mathbb{Z}$.

We have established

Proposition 1.3. *The integers of the quadratic field $F = \mathbb{Q}(\sqrt{n})$ are*

$$\mathcal{O}_F = \mathbb{Z}[g], \quad g = \begin{cases} \frac{1+\sqrt{n}}{2} & \textit{if } n = 1 \pmod 4 \\ \sqrt{n} & \textit{if } n = 2, 3 \pmod 4. \end{cases}$$

The integers of F form a ring.

The minimal monic polynomial in $\mathbb{Z}[X]$ satisfied by the $\mathcal{O}_F$ generator g in the previous proposition is quadratic,

$$f(X) = \begin{cases} X^2 - X - \frac{n-1}{4} & \text{if } n = 1 \pmod 4 \\ X^2 - n & \text{if } n = 2, 3 \pmod 4. \end{cases}$$

Thus, as an abelian group the integer ring is in fact

$$\mathcal{O}_F = g\mathbb{Z} \oplus \mathbb{Z}.$$

The discriminant of the quadratic polynomial $f(X)$ (the quantity b^2-4ac that goes under the square root in the quadratic formula) is n if $n = 1 \pmod 4$ and $4n$ if $n = 2, 3 \pmod 4$. This quantity, a *structure constant* of the quadratic field F, will appear in the class number formula.

Definition 1.4. *The* **discriminant** *of F is*

$$D_F = \begin{cases} n & \text{if } n = 1 \pmod 4 \\ 4n & \text{if } n = 2, 3 \pmod 4. \end{cases}$$

The cases built into the definition of the discriminant allow it to give a uniform description of the integers,

$$\mathcal{O}_F = \mathbb{Z}[r], \qquad r = \frac{D_F + \sqrt{D_F}}{2},$$

and similarly we will see that the discriminant gives uniform descriptions of various phenomena associated with F. The minimal polynomial of r is

$$f(X) = X^2 - D_F X + D_F(D_F - 1)/4,$$

whose coefficients are rational integers and whose discriminant is indeed D_F.

One can think of the casewise formula for the discriminant as the result of a calculation rather than as a definition. Other definitions of the discriminant are case-free in terms of g (where $\mathcal{O}_F = g\mathbb{Z} \oplus \mathbb{Z}$ as before), although g itself involves cases,

$$D_F = (\det \begin{bmatrix} 1 & g \\ 1 & \overline{g} \end{bmatrix})^2$$

and

$$D_F = \det \begin{bmatrix} \mathrm{tr}(1 \cdot 1) & \mathrm{tr}(1 \cdot g) \\ \mathrm{tr}(g \cdot 1) & \mathrm{tr}(g \cdot g) \end{bmatrix}.$$

2. The units of a quadratic field

Definition 2.1. *A* **unit** *of F is an invertible element of the integer ring $\mathcal{O}_F$. The* **unit group** *of F is the multiplicative group $\mathcal{O}_F^\times$.*

Proposition 2.2. *An element α of $\mathcal{O}_F$ is a unit if and only if* $\mathrm{N}(\alpha) = \pm 1$.

Proof. If $\alpha \in \mathcal{O}_F$ is multiplicatively invertible by $\beta \in \mathcal{O}_F$ then

$$1 = \mathrm{N}(1) = \mathrm{N}(\alpha\beta) = \mathrm{N}(\alpha)\mathrm{N}(\beta),$$

so that $\mathrm{N}(\alpha) = \pm 1$ because both norms are integers. Conversely, if $\mathrm{N}(\alpha) = \pm 1$ then α is invertible by $\pm\overline{\alpha} \in \mathcal{O}_F$ because $\pm\alpha\overline{\alpha} = \pm\mathrm{N}(\alpha) = 1$. □

If $F = \mathbb{Q}(\sqrt{n})$ is imaginary quadratic then all norms $\big((2a + bD_F)^2 - b^2 D_F\big)/4$ are nonnegative, and inspection shows that the unit group is

$$\mathcal{O}_F^\times = \begin{cases} \{\pm 1, \pm i\} & \text{if } n = -1 \\ \{\pm 1, \pm\zeta_3, \pm\zeta_3^2\} & \text{if } n = -3 \text{ (where } \zeta_3 = \frac{-1+\sqrt{-3}}{2}) \\ \{\pm 1\} & \text{otherwise.} \end{cases}$$

Further examination quickly shows that these groups are cyclic, but also we know that any finite subgroup of the multiplicative group of any field is cyclic, so this is only a confirmation. If $F = \mathbb{Q}(\sqrt{n})$ is real quadratic then nontrivially there exists a so-called **fundamental unit** $u > 1$ in $\mathcal{O}_F^\times$ such that the unit group is

$$\mathcal{O}_F^\times = \{\pm u^n : n \in \mathbb{Z}\} \approx \mathbb{Z}/2\mathbb{Z} \times \mathbb{Z}.$$

Finding the fundamental unit amounts to solving Pell's Equation, $x^2 - ny^2 = 1$.

Definition 2.3. *The symbol $w = w(F)$ denotes the number of roots of unity in F, i.e., the number of complex numbers in F having absolute value* 1. *Thus*

$$w(F) = \begin{cases} 4 & \textit{if } F = \mathbb{Q}(i) \\ 6 & \textit{if } F = \mathbb{Q}(\sqrt{-3}) \\ 2 & \textit{otherwise.} \end{cases}$$

Thus w is a second structure constant of the field F, along with the discriminant D_F. For imaginary quadratic fields F the number w completely describes the unit group. For real quadratic fields the fundamental unit u is a further structure constant necessary for a full description. The more complicated unit group structure for real quadratic fields is one reason that the class number formula is easier in the imaginary case.

3. The ideals of a quadratic field

Definition 3.1. *An* **ideal** *of $\mathcal{O}_F$ is a subset $\mathfrak{a} \subset \mathcal{O}_F$ (excluding $\mathfrak{a} = \{0\}$) that forms an abelian group and is closed under multiplication by $\mathcal{O}_F$.*

Thus an ideal is a particular kind of subring. The ideals of any ring are special among subrings similarly to how the normal subgroups of any group are special among subgroups: the quotient of the ring by an ideal again has a ring structure, whereas the quotient of the ring by a subring in general need not.

The subset $\{0\} \subset \mathcal{O}_F$ does form an abelian group and it is closed under multiplication by $\mathcal{O}_F$, so often it is considered an ideal of $\mathcal{O}_F$ as well. However, the zero ideal has aberrational properties, and our concern here is with the unique factorization of nonzero ideals, so for brevity we exclude $\{0\}$ from the discussion even though in principle we should say *nonzero ideal* throughout. The zero ideal will play a role once later in the writeup, and we will point out when that happens.

Definition 3.2. *The* **sum** *of two ideals of $\mathcal{O}_F$ is the ideal generated by the sums of the elements*

$$\mathfrak{a} + \mathfrak{a}' = \langle x + x' : x \in \mathfrak{a}, x' \in \mathfrak{a}' \rangle,$$

and similarly for the **product**,

$$\mathfrak{a}\mathfrak{a}' = \langle xx' : x \in \mathfrak{a}, x' \in \mathfrak{a}' \rangle.$$

In fact the ideal sum consists of exactly the generating element-sums, but the ideal product consists of all finite sums of the generating element-products. Note that the product $\mathfrak{a}\mathfrak{a}'$ is a subset of $\mathfrak{a}$ and of $\mathfrak{a}'$. The addition and multiplication of ideals is commutative and associative and distributive. If the zero ideal $\{0\}$ were allowed then it would be the additive identity, and the integer ring $\mathcal{O}_F$ is the multiplicative identity. However, nonzero ideals do not have additive inverses. Again, our concern here is with the multiplicative structure of ideals, so the absence of an additive identity or additive inverses is of no concern. Before long we will remedy the absence of multiplicative inverses by enlarging our notion of an ideal.

Definition 3.3. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_F$, and let $\overline{\mathfrak{a}} = \{\overline{x} : x \in \mathfrak{a}\}$, another ideal of $\mathcal{O}_F$. The* **norm** *of $\mathfrak{a}$, denoted $\mathrm{N}(\mathfrak{a})$, is characterized by the conditions*

$$\mathfrak{a}\overline{\mathfrak{a}} = \mathrm{N}(\mathfrak{a})\mathcal{O}_F, \quad \mathrm{N}(\mathfrak{a}) \in \mathbb{Z}^+.$$

For example, in the integer ring $\mathcal{O}_F = \mathbb{Z}[\sqrt{-5}]$ of the quadratic field $F = \mathbb{Q}(\sqrt{-5})$, the ideal $\mathfrak{p} = (1+\sqrt{-5})\mathcal{O}_F + 2\mathcal{O}_F$ satisfies

$$\mathfrak{p}\overline{\mathfrak{p}} = 6\mathcal{O}_F + 2(1+\sqrt{-5})\mathcal{O}_F + 2(1-\sqrt{-5})\mathcal{O}_F + 4\mathcal{O}_F = 2\mathcal{O}_F,$$

showing that $\mathrm{N}(\mathfrak{p}) = 2$.

The existence of the ideal norm in general is not immediate, but we will establish it soon. Granting the ideal norm's existence, its characterizing conditions show that it is a multiplicative function of ideals,

$$\mathrm{N}(\mathfrak{a}\mathfrak{a}') = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{a}') \quad \text{for all ideals } \mathfrak{a}, \mathfrak{a}' \text{ of } \mathcal{O}_F.$$

Indeed, $\mathrm{N}(\mathfrak{a}\mathfrak{a}')\mathcal{O}_F = \mathfrak{a}\mathfrak{a}'\overline{\mathfrak{a}\mathfrak{a}'} = \mathfrak{a}\overline{\mathfrak{a}}\mathfrak{a}'\overline{\mathfrak{a}'} = \mathrm{N}(\mathfrak{a})\mathcal{O}_F\mathrm{N}(\mathfrak{a}')\mathcal{O}_F = \mathrm{N}(\mathfrak{a})\mathrm{N}(\mathfrak{a}')\mathcal{O}_F$, giving the result.

Continuing to grant its existence, the ideal norm lets us prove a cancellation law for ideals of $\mathcal{O}_F$. Suppose that

$$\mathfrak{a}\mathfrak{a}' = \mathfrak{a}\mathfrak{a}''.$$

Then

$$\mathrm{N}(\mathfrak{a})\mathfrak{a}' = \mathfrak{a}\overline{\mathfrak{a}}\mathfrak{a}' = \mathfrak{a}\overline{\mathfrak{a}}\mathfrak{a}'' = \mathrm{N}(\mathfrak{a})\mathfrak{a}'',$$

so that by the elementwise cancellation law applied to each relation $\mathrm{N}(\mathfrak{a})a' = \mathrm{N}(\mathfrak{a})a''$ with $a' \in \mathfrak{a}$ and $a'' \in \mathfrak{a}''$,

$$\mathfrak{a}' = \mathfrak{a}''.$$

Definition 3.4. *An ideal is* **principal** *if it takes the form*

$$\mathfrak{a} = x\mathcal{O}_F \quad \textit{for some } x \in \mathcal{O}_F.$$

A principal ideal is denoted by its generator in angle brackets,

$$\langle x \rangle = x\mathcal{O}_F.$$

The relation between the element norm from earlier and the ideal norm just introduced is:

$$\textit{For a principal ideal } \mathfrak{a} = \langle x \rangle, \quad \mathrm{N}(\mathfrak{a}) = |\mathrm{N}(x)|.$$

If all ideals were principal then the theory of ideals would introduce nothing new to the study of quadratic integer rings. We will see in the next section that the ideals of a quadratic integer ring factor uniquely, whereas we know by example that the elements of the ring may not. Thus the possible failure of all ideals to be principal is related to the possible failure of unique factorization of elements.

We end the section by showing that the ideal norm exists.

Proposition 3.5. *Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_F$. Then $\mathfrak{a}\overline{\mathfrak{a}} = d\mathcal{O}_F$ for some $d \in \mathbb{Z}^+$.*

Proof. The product $\mathfrak{a}\overline{\mathfrak{a}}$ contains elements $x\overline{x} = \mathrm{N}(x)$ where $x \in \mathfrak{a}$ is nonzero, and these elements are nonzero rational integers. The product is closed under negation, so it contains positive rational integers. Let d be the smallest such positive rational integer. The ideal properties of $\mathfrak{a}\overline{\mathfrak{a}}$ show that $\mathfrak{a}\overline{\mathfrak{a}} \cap \mathbb{Z} = d\mathbb{Z}$.

Because the product $\mathfrak{a}\overline{\mathfrak{a}}$ is an ideal, it contains $d\mathcal{O}_F$. That is, we have the containment $\mathfrak{a}\overline{\mathfrak{a}} \supset d\mathcal{O}_F$, and to complete the proof we need the other containment. It suffices to show that for any $x, y \in \mathfrak{a}$ the product $x\overline{y}$ lies in $d\mathcal{O}_F$. The quantities

$$\mathrm{tr}(x\overline{y}) = x\overline{y} + \overline{x}y, \qquad \mathrm{N}(x) = x\overline{x}, \qquad \mathrm{N}(\overline{y}) = y\overline{y}$$

all lie in $\mathfrak{a}\overline{\mathfrak{a}} \cap \mathbb{Z} = d\mathbb{Z}$, and so it follows that

$$\mathrm{tr}(x\overline{y}/d) = \mathrm{tr}(x\overline{y})/d \in \mathbb{Z} \qquad \text{and} \qquad \mathrm{N}(x\overline{y}/d) = \mathrm{N}(x)/d \cdot \mathrm{N}(\overline{y})/d \in \mathbb{Z}.$$

Thus $x\overline{y}/d \in \mathcal{O}_F$, i.e., $x\overline{y} \in d\mathcal{O}_F$. This completes the proof. □

The argument that the norm exists made heavy use of the particulars of the ring $\mathcal{O}_F$. In fact, any number ring has an ideal norm, where a *number ring* is the ring of integers in any *number field*, which in turn is any subfield K of $\mathbb{C}$ that has finite dimension as a vector space over $\mathbb{Q}$. However, a norm does not exist for a general commutative ring.

4. Unique factorization of ideals

Proposition 4.1 ("To contain is to divide")**.** *Let $\mathfrak{a}$ and $\mathfrak{a}'$ be ideals of $\mathcal{O}_F$. Then*

$$\mathfrak{a}' \mid \mathfrak{a} \iff \mathfrak{a} \subset \mathfrak{a}'.$$

The implication $\mathfrak{a}' \mid \mathfrak{a} \implies \mathfrak{a} \subset \mathfrak{a}'$ in this proposition is general, but the ideal norm will be needed to prove that $\mathfrak{a} \subset \mathfrak{a}' \implies \mathfrak{a}' \mid \mathfrak{a}$. Thus, arguments that use the latter implication are particular to rings having an ideal norm. Another way to say this is that *to contain is to divide* is substantive but *to divide is to contain* is not.

Proof. If $\mathfrak{a}' \mid \mathfrak{a}$ then $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}''$ for some $\mathfrak{a}''$ and so $\mathfrak{a} \subset \mathfrak{a}'$. Conversely, if $\mathfrak{a} \subset \mathfrak{a}'$ then $\mathfrak{a}\overline{\mathfrak{a}'} \subset \mathfrak{a}'\overline{\mathfrak{a}'} = \mathrm{N}(\mathfrak{a}')\mathcal{O}_F$ and thus $\mathfrak{a}\overline{\mathfrak{a}'}/\mathrm{N}(\mathfrak{a}')$ is an ideal of $\mathcal{O}_F$. Because $\mathfrak{a}' \cdot \mathfrak{a}\overline{\mathfrak{a}'}/\mathrm{N}(\mathfrak{a}') = \mathfrak{a}$, indeed $\mathfrak{a}' \mid \mathfrak{a}$. □

Definition 4.2. *An ideal $\mathfrak{a}$ of $\mathcal{O}_F$ that is a proper subset of $\mathcal{O}_F$ is* **prime** *if:*

$$\textit{For all ideals } \mathfrak{a}', \mathfrak{a}'' \textit{ of } \mathcal{O}_F, \quad \mathfrak{a} \mid \mathfrak{a}'\mathfrak{a}'' \implies \mathfrak{a} \mid \mathfrak{a}' \textit{ or } \mathfrak{a} \mid \mathfrak{a}''.$$

An ideal $\mathfrak{a}$ of $\mathcal{O}_F$ that is a proper subset of $\mathcal{O}_F$ is **irreducible** *if:*

$$\textit{For all ideals } \mathfrak{a}', \mathfrak{a}'' \textit{ of } \mathcal{O}_F, \quad \mathfrak{a}'\mathfrak{a}'' = \mathfrak{a} \implies \mathfrak{a}' = \mathfrak{a} \textit{ or } \mathfrak{a}'' = \mathfrak{a}.$$

An ideal $\mathfrak{a}$ of $\mathcal{O}_F$ that is a proper subset of $\mathcal{O}_F$ is **maximal** *if:*

$$\textit{For all ideals } \mathfrak{a}' \textit{ of } \mathcal{O}_F, \quad \mathfrak{a} \subset \mathfrak{a}' \implies \mathfrak{a}' = \mathfrak{a} \textit{ or } \mathfrak{a}' = \mathcal{O}_F.$$

So

prime means *doesn't decompose as a divisor,*

and

irreducible means *doesn't decompose as a product,*

and

maximal means *there is no bigger proper ideal.*

(*Maximal* does not mean *bigger than all other ideals.*) An exercise shows that the definition of prime ideal given here is equivalent to:

$$\text{For all nonzero elements } a', a'' \text{ of } \mathcal{O}_F, \quad a'a'' \in \mathfrak{a} \implies a' \in \mathfrak{a} \text{ or } a'' \in \mathfrak{a},$$

and furthermore, because every ideal contains 0, the word "nonzero" can be removed from the previous display. This reproduces the usual definition of a prime ideal in terms of elements rather than in terms of ideals.

Proposition 4.3. *Prime ideals of $\mathcal{O}_F$ are irreducible. Irreducible ideals of $\mathcal{O}_F$ are maximal. Maximal ideals of $\mathcal{O}_F$ are prime.*

Proof. Consider any prime ideal $\mathfrak{a}$ of $\mathcal{O}_F$. If $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}''$ then $\mathfrak{a} \mid \mathfrak{a}'\mathfrak{a}''$ and so without loss of generality $\mathfrak{a} \mid \mathfrak{a}'$. Also, if $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}''$ then $\mathfrak{a}' \mid \mathfrak{a}$. Because to divide is to contain, $\mathfrak{a}' \subset \mathfrak{a}$ and $\mathfrak{a} \subset \mathfrak{a}'$, and so $\mathfrak{a}' = \mathfrak{a}$.

Let $\mathfrak{a}$ be irreducible, and suppose that $\mathfrak{a} \subset \mathfrak{a}'$. Because to contain is to divide, $\mathfrak{a}' \mid \mathfrak{a}$, i.e., $\mathfrak{a}'\mathfrak{a}'' = \mathfrak{a}$ for some $\mathfrak{a}''$, and so $\mathfrak{a}' = \mathfrak{a}$ or $\mathfrak{a}'' = \mathfrak{a}$, but in the latter case $\mathfrak{a}' = \mathcal{O}_F$ by the cancellation law.

Maximal ideals are prime in any commutative ring with 1, because essentially by definition the quotient of the ring by an ideal is a field precisely when the ideal is maximal, and the quotient is an integral domain precisely when the ideal is prime. The reader may work out a more elementary proof here if desired. □

In the proof just given, the argument that irreducible ideals are maximal uses the *to contain is to divide* principle that relies on the ideal norm, and it is the substance of the proposition. The other two statements are basic. With the proposition established, the proof of unique factorization is prepared.

Theorem 4.4. *Any ideal $\mathfrak{a}$ of $\mathcal{O}_F$ factors uniquely into prime ideals.*

Proof. Let $\mathfrak{a}$ be an ideal of $\mathcal{O}_F$. Then $\mathfrak{a}$ factors as a finite product of irreducibles via a process that must terminate by induction on $\mathrm{N}(\mathfrak{a})$. The fact that irreducibles are prime makes the factorization unique, because if

$$\mathfrak{a} = \mathfrak{p}_1 \cdots \mathfrak{p}_s = \mathfrak{q}_1 \cdots \mathfrak{q}_t$$

where the $\mathfrak{p}_i$ are irreducible but not necessarily distinct, and similarly for the $\mathfrak{q}_j$, then

$$\mathfrak{p}_s \mid \mathfrak{q}_1 \cdots \mathfrak{q}_t$$

so that because $\mathfrak{p}_s$ is prime we have $\mathfrak{p}_s \mid \mathfrak{q}_t$ after reindexing if necessary, and thus, because $\mathfrak{q}_t$ is irreducible,

$$\mathfrak{p}_s = \mathfrak{q}_t.$$

By cancellation,

$$\mathfrak{p}_1 \cdots \mathfrak{p}_{s-1} = \mathfrak{q}_1 \cdots \mathfrak{q}_{t-1}.$$

By induction on the norm, the two factorizations in the previous display are equal, and hence so are the two factorizations of $\mathfrak{a}$. □

5. The character of a quadratic field

We review the completion of the quadratic reciprocity law at 2. The four characters of $(\mathbb{Z}/8\mathbb{Z})^\times$ are shown in the following table:

	1	3	5	7	conductor
χ_1	1	1	1	1	1
χ_{-1}	1	−1	1	−1	4
χ_2	1	−1	−1	1	8
χ_{-2}	1	1	−1	−1	8

The character group is the $(2, 2)$ abelian group, so for example $\chi_{-1}\chi_2 = \chi_{-2}$ and $\chi_i^2 = \chi_1$ for all i. Note that χ_{-1} has conductor 4 but χ_2 and χ_{-2} are primitive modulo 8. The characters χ_i are named to indicate that $\chi_{-1}(p) = (-1/p)$ and

$\chi_2(p) = (2/p)$ and $\chi_{-2}(p) = (-2/p)$ for odd primes p, and trivially so for χ_1 as well.

Define

$$\left(\frac{m}{2}\right) = \chi_2(m), \quad m \text{ odd},$$

with χ_2 understood to be lifted from $(\mathbb{Z}/8\mathbb{Z})^\times$ to $\mathbb{Z}$. Recall also the definition

$$\left(\frac{m}{-1}\right) = \operatorname{sgn} m, \quad m \text{ nonzero}.$$

For any odd prime p we have $(p/2)(2/p) = 1$ because $(p/2) = (2/p)$. Also we have $(-1/2)(2/-1) = 1$ because both $(-1/2)$ and $(2/-1)$ are 1. It follows that $(m/2)(2/m) = 1$ for all odd integers m.

The Jacobi/Kronecker symbol (P/Q) for coprime nonzero integers now can be defined totally multiplicatively in its numerator and denominator. Consider two coprime nonzero integers,

$$\begin{Bmatrix} P = 2^a P', & P' \text{ odd} \\ Q = 2^b Q', & Q' \text{ odd} \end{Bmatrix}.$$

Thus $a, b \in \mathbb{Z}_{\geq 0}$ with $\min\{a, b\} = 0$, and P', Q' are coprime. The general Jacobi/Kronecker symbol reciprocity formula is

$$\boxed{(P/Q) \cdot (Q/P) = (-1)^{\frac{P'-1}{2} \cdot \frac{Q'-1}{2}} \cdot \begin{Bmatrix} 1 & \text{if at least one of } P, Q \text{ is positive} \\ -1 & \text{if both } P, Q \text{ are negative} \end{Bmatrix}.}$$

It follows that uniformly across the four cases of $(\operatorname{sgn} P, \operatorname{sgn} Q)$,

$$(P/Q) = (-1)^{\frac{P'-1}{2} \cdot \frac{Q'-1}{2}} (Q/|P|), \quad P,\ Q \text{ coprime and nonzero.} \tag{1}$$

We will use this formula (1) several times below, rather than the boxed formula immediately preceding it.

Now return to a quadratic field $F = \mathbb{Q}(\sqrt{n})$ where $n \neq 0, 1$ is squarefree. Recall that the field's discriminant is defined as

$$D_F = \begin{cases} n & \text{if } n = 1 \pmod 4 \\ 4n & \text{if } n = -1, 2 \pmod 4). \end{cases}$$

Definition 5.1. *Let F be a quadratic field with discriminant D_F. The* **quadratic character** *of F is*

$$\chi_F : \mathbb{Z}_{\neq 0} \longrightarrow \mathbb{C}, \quad \chi_F(m) = \left(\frac{D_F}{m}\right).$$

Especially, $\chi_F(-1) = \operatorname{sgn}(D_F)$.

Theorem 5.2. *Let $F = \mathbb{Q}(\sqrt{n})$ be a quadratic field with discriminant D_F. Then the quadratic character χ_F has period $|D_F|$.*

Proof. Introduce the notation

$$D_F = 2^a \delta, \quad m = 2^b \mu \quad (\delta \text{ and } \mu \text{ odd}).$$

As in (1) above, the Jacobi/Kronecker symbol reciprocity formula gives, recalling that $(\cdot/2) = \chi_2$ for the second step,

$$\chi_F(m) = (-1)^{\frac{\delta-1}{2} \cdot \frac{\mu-1}{2}} \left(\frac{m}{|D_F|}\right) = (-1)^{\frac{\delta-1}{2} \cdot \frac{\mu-1}{2}} \chi_2(m)^a \left(\frac{m}{|\delta|}\right) \quad \text{if } \gcd(m, D_F) = 1.$$

To show that this has period $|D_F|$, inspect D_F in terms of n for $n = 1, -1 \pmod 4$ and $n = 2, -2, \pmod 8$ (these cases cover all possibilities of $n \pmod 8$ because n is squarefree) to get the following possibilities:

n	D_F	δ	$(-1)^{(\delta-1)/2}$	a
$n = \ \ 1 \pmod 4$	n	$n = \ \ 1 \pmod 4$	1	0
$n = -1 \pmod 4$	$4n$	$n = -1 \pmod 4$	-1	2
$n = \ \ 2 \pmod 8$	$4n = 8\frac{n}{2}$	$\frac{n}{2} = \ \ 1 \pmod 4$	1	3
$n = -2 \pmod 8$	$4n = 8\frac{n}{2}$	$\frac{n}{2} = -1 \pmod 4$	-1	3

Again with $\gcd(m, D_F) = 1$, in the first and third cases $(-1)^{\frac{\delta-1}{2}\cdot\frac{\mu-1}{2}} = 1$; in the second and fourth cases D_F is even and so $\mu = m$ and $(-1)^{\frac{\delta-1}{2}\cdot\frac{\mu-1}{2}} = \chi_{-1}(m)$. Also $\chi_2^2 = 1$. So overall $\chi_F(m) = (-1)^{\frac{\delta-1}{2}\frac{m-1}{2}}\chi_2(m)^a(m/|\delta|)$ is

$$\chi_F(m) = \begin{cases} \chi_1(m)\cdot(m/|n|) & \text{if } n = \ \ 1 \pmod 4 \\ \chi_{-1}(m)\cdot(m/|n|) & \text{if } n = -1 \pmod 4 \\ \chi_2(m)\cdot(m/|n/2|) & \text{if } n = \ \ 2 \pmod 8 \\ \chi_{-2}(m)\cdot(m/|n/2|) & \text{if } n = -2 \pmod 8 \end{cases} \qquad \text{if } \gcd(m, D_F) = 1.$$

There is no need to write the trivial term $\chi_1(m)$ in the first case of this formula, but we did so for uniformity. Because χ_1 is trivial and χ_{-1} has conductor 4 while $\chi_{\pm 2}$ are primitive modulo 8, and because $(\cdot/N)$ has period N for squarefree odd positive N, the period is

$$\left\{ \begin{array}{rl} |n| & \text{if } n = \ \ 1 \pmod 4 \\ 4|n| & \text{if } n = -1 \pmod 4 \\ 8|n/2| & \text{if } n = \pm 2 \pmod 8 \end{array} \right\} = |D_F| \text{ in all cases,}$$

as was to be proved. □

In light of Theorem 5.2 we may view the quadratic character of $F = \mathbb{Q}(\sqrt{n})$ as a true **Dirichlet character**, a homomorphism

$$\chi_F : (\mathbb{Z}/D_F\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times,$$

defined by

$$\chi_F(m + D_F\mathbb{Z}) = \begin{cases} \chi_1(m)\cdot(m/|n|) & \text{if } n = \ \ 1 \pmod 4 \\ \chi_{-1}(m)\cdot(m/|n|) & \text{if } n = -1 \pmod 4 \\ \chi_2(m)\cdot(m/|n/2|) & \text{if } n = \ \ 2 \pmod 8 \\ \chi_{-2}(m)\cdot(m/|n/2|) & \text{if } n = -2 \pmod 8). \end{cases}$$

As usual, we extend the definition to $\mathbb{Z}/D_F\mathbb{Z}$,

$$\chi_F(m + D_F\mathbb{Z}) = 0 \quad \text{if } \gcd(m, |D_F|) > 1.$$

Because $\chi_F(-1) = \operatorname{sgn}(D_F)$, we have

$$\chi_F(-1 + D_F\mathbb{Z}) = \begin{cases} 1 & \text{if } F \text{ is real quadratic} \\ -1 & \text{if } F \text{ is imaginary quadratic.} \end{cases}$$

In general, a Dirichlet character that takes -1 to 1 is called *even*, and a Dirichlet character that takes -1 to -1 is called *odd*. That is, the character of a real quadratic field is even and the character of an imaginary quadratic field is odd.

For example, if $F = \mathbb{Q}(i)$, so that $\mathcal{O}_F = \mathbb{Z}[i]$ is the ring of Gaussian integers, then the quadratic character is the odd character $\chi_F : (\mathbb{Z}/4\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ given by

$$\chi_F(m) = (-4/m) = (-1/m) = \chi_{-1}(m) = (-1)^{(m-1)/2}.$$

If $F = \mathbb{Q}(\sqrt{2})$, so that $\mathcal{O}_F = \mathbb{Z}[\sqrt{2}]$, then the quadratic character is the even character $\chi_F : (\mathbb{Z}/8\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ given by

$$\chi_F(m) = (8/m) = (2/m) = \chi_2(m) = (-1)^{(m^2-1)/8}.$$

If $F = \mathbb{Q}(\sqrt{-3})$, so that $\mathcal{O}_F = \mathbb{Z}[\zeta_3]$ is the ring of Eisenstein integers, then the quadratic character is $\chi_F : (\mathbb{Z}/3\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ given by

$$\chi_F(m) = (-3/m) = (m/3).$$

If $F = \mathbb{Q}(\sqrt{-5})$, so that $\mathcal{O}_F = \mathbb{Z}[\sqrt{-5}]$, then the quadratic character is $\chi_F : (\mathbb{Z}/20\mathbb{Z})^\times \longrightarrow \mathbb{C}^\times$ given by

$$\chi_F(m) = (-20/m) = (-1/m)(5/m) = (-1)^{(m-1)/2}(m/5).$$

As a remark here, though it is not necessary for the purposes of this writeup, we state that for any nonzero integer $D = 0, 1 \pmod 4$,

> *D uniquely takes the form $f^2 D_F$ where D_F is a quadratic number field discriminant or $D_F = 1$.*

The resulting character $m \mapsto (D/m)$ for nonzero integers m therefore has period $|D_F|$. To establish the statement first write $D = 2^{e_2}\delta$ where $\delta = \operatorname{sgn}(D)\prod_p p^{e_p}$, the product taken over odd prime divisors p of D; note that $e_2 \neq 1$ and if $e_2 = 0$ then $\delta = 1 \pmod 4$. Let $f_o = \prod_p p^{\lfloor e_p/2 \rfloor}$ and let $\delta_o = \operatorname{sgn}(D)\prod_{p:e_p \text{ odd}} p$, so that $\delta = f_o^2\delta_o$ and δ_o is squarefree and $\delta_o = \delta \pmod 4$. Now,

- for $e_2 \geq 0$ even and $\delta = 1 \pmod 4$ set $f = 2^{e_2/2} f_o$ and $D_F = \delta_o$,
- for $e_2 \geq 2$ even and $\delta = 3 \pmod 4$ set $f = 2^{(e_2-2)/2} f_o$ and $D_F = 4\delta_o$,
- for $e_2 \geq 3$ odd set $f = 2^{(e_2-3)/2} f_o$ and $D_F = 8\delta_o = 4 \cdot 2\delta_o$, noting that $2\delta_o$ is squarefree and $2\delta_o = 2 \pmod 4$.

As for uniqueness, one can see that every step of the decomposition $D = f^2 D_F$ is forced, including the allocation of powers of 2 between f and D_F.

Finally we explain that when the discriminant is even, the quadratic character has half-period skew periodicity. Specifically, suppose as usual that $n \neq 0, 1$ is squarefree, and suppose further that $n \neq 1 \pmod 4$. Thus the quadratic field $F = \mathbb{Q}(\sqrt{n})$ has even discriminant $D_F = 4n$, and the quadratic character has period $|D_F|$. As an example, for $n = -5$ the values of the quadratic character $(-20/\cdot)$ on 0 through 9 and then 10 through 19 are (as we have seen before in the quadratic reciprocity writeup)

$$0, 1, 0, 1, 0, 0, 0, 1, 0, 1 \quad \text{and then} \quad 0, -1, 0, -1, 0, 0, 0, -1, 0, -1.$$

Two phenomena are notable here. First, the quadratic residues are concentrated in the left half of 0 through 19. Generally, not just for $n = -5$, there are more residues in the left half than in the right, but the extreme case of all the residues in the left half is not general. The second notable phenomenon in the previous display is that the quadratic character on the second half is the negative of the quadratic character on the first half,

$$\chi_F(r + |D_F|/2) = -\chi(r), \quad 0 \leq r < |D_F|/2.$$

We establish the half-period skew periodicity, to be used later in this writeup. The decomposition

$$(\mathbb{Z}/|D_F|\mathbb{Z})^\times = \begin{cases} (\mathbb{Z}/4\mathbb{Z})^\times \times (\mathbb{Z}/|n|\mathbb{Z})^\times & \text{if } n = 3 \pmod 4, \\ (\mathbb{Z}/8\mathbb{Z})^\times \times (\mathbb{Z}/(|n|/2)\mathbb{Z})^\times & \text{if } n = 2 \pmod 4) \end{cases}$$

shows via the Sun Ze theorem that a Dirichlet character of full period modulo $|D_F|$ is naturally viewed as the product of a pair of Dirichlet characters of full period modulo 4 and $|n|$, or modulo 8 and $|n|/2$. (We leave the specifics of showing this to the reader.) For $n = 3 \pmod 4$, $r + |D_F|/2 = r + 2|n| = r + 2 \pmod 4$. The Dirichlet character of full period modulo 4 satisfies $\chi(r + |D_F|/2) = \chi(r+2) = -\chi(r)$, and every Dirichlet character modulo $|n| = |D_F|/4$ satisfies $\chi(r + |D_F|/2) = \chi(r)$; together these give $\chi_F(r + |D_F|/2) = -\chi_F(r)$. Similarly for $n = 2 \pmod 4$, $r + |D_F|/2 = r + 2|n| = r + 4 \pmod 8$, and because the two Dirichlet characters of full period modulo 8 (these are $\chi_{\pm 2}$ from the beginning of this section) satisfy $\chi(r+4) = -\chi(r)$ it follows again that $\chi_F(r + |D_F|/2) = -\chi_F(r)$.

6. Decomposition of rational primes

Now we can see the importance of the discriminant. It is the crux of the quadratic character, which in turn describes the decomposition of rational primes in F as follows:

Theorem 6.1. *Let p be a rational prime. The decomposition of p in $\mathcal{O}_F$ is*

$$p\mathcal{O}_F = \begin{cases} \mathfrak{p}\mathfrak{q} \ \textit{where } \mathrm{N}(\mathfrak{p}) = \mathrm{N}(\mathfrak{q}) = p & \textit{if } \chi_F(p) = 1 \\ \mathfrak{p} \ \ \textit{where } \mathrm{N}(\mathfrak{p}) = p^2 & \textit{if } \chi_F(p) = -1 \\ \mathfrak{p}^2 \ \textit{where } \mathrm{N}(\mathfrak{p}) = p & \textit{if } \chi_F(p) = 0. \end{cases}$$

Thus the decomposition of p in $\mathcal{O}_F$ depends only on p $\pmod{|D_F|}$.

Proof. (Sketch.) Recall that

$$\mathcal{O}_F = \mathbb{Z}[r] \quad \text{where} \quad r = \frac{D_F + \sqrt{D_F}}{2},$$

and that the polynomial of r is

$$f(X) = X^2 - D_F X + \frac{D_F(D_F - 1)}{4}, \quad \text{with discriminant } D_F.$$

Let $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ and let an overbar denote reduction modulo p. There is a natural isomorphism of quotient rings, whose details will be reviewed below,

$$\mathbb{Z}[r]/p\mathbb{Z}[r] \approx \mathbb{F}_p[X]/\langle \overline{f}(X) \rangle, \qquad \varphi(r) + p\mathbb{Z}[r] \longleftrightarrow \overline{\varphi}(X) + \langle \overline{f}(X) \rangle,$$

the basic idea being that both sides are the quotient of $\mathbb{Z}[X]$ by p and by $f(X)$. The quotient rings have overrings $\mathbb{Z}[r]$ and $\mathbb{F}_p[X]$, giving a diagram is as follows:

$$\begin{tikzcd}
\mathbb{Z}[r] \arrow[d] & \mathbb{F}_p[X] \arrow[d] \\
\mathbb{Z}[r]/p\mathbb{Z}[r] \arrow[r, leftrightarrow] & \mathbb{F}_p[X]/\langle \overline{f}(X) \rangle
\end{tikzcd}$$

We seek the prime ideals of $\mathbb{Z}[r]$ that contain $p\mathbb{Z}[r]$. Meanwhile, $\mathbb{F}_p[X]$ is a Euclidean ring, hence a PID, so working there is easy. Thus the idea of the proof is to move the question from the upper left corner $\mathbb{Z}[r]$ of the diagram to the upper right corner $\mathbb{F}_p[X]$.

A basic fact from commutative ring theory is that the prime ideals of a ring R that contain a given ideal J correspond bijectively in the natural way with the prime ideals of the quotient R/J; here if J is prime in R then the corresponding prime ideal of R/J is the zero ideal, so we must admit the zero ideal into consideration. Thus, finding the prime ideals of $\mathbb{Z}[r]$ that contain $p\mathbb{Z}[r]$, in the upper left corner of the diagram, reduces to finding the prime ideals of $\mathbb{Z}[r]/p\mathbb{Z}[r]$, in the lower left corner of the diagram, which in turn reduces to finding the prime ideals of $\mathbb{F}_p[X]/\langle\overline{f}(X)\rangle$, in the lower right corner of the diagram, which reduces to finding the prime ideals of $\mathbb{F}_p[X]$ that contain $\langle\overline{f}(X)\rangle$, in the upper right corner of the diagram. Because $\mathbb{F}_p[X]$ is a PID this amounts to factoring $\overline{f}(X)$ in $\mathbb{F}_p[X]$, and the quadratic character value $\chi_F(p) = (D_F/p)$ describes the factorization; here the case $p = 2$ needs to be checked separately, its three subcases $D_F = 1 \bmod 8$, $D_F = 5 \bmod 8$, $D_F = 0 \bmod 4$ giving quadratic character values $\chi_F(2) = 1, -1, 0$ and giving $\overline{f}(X) \in \mathbb{F}_2$ with $2, 0, 1$ roots. So we are done other than writing the specifics.

To do so, start from

$$\overline{f}(X) = \begin{cases} (X-\overline{\alpha})(X-\overline{\beta}) & \text{if } \chi_F(p) = 1 \\ \overline{f}(X) & \text{if } \chi_F(p) = -1 \\ (X-\overline{\alpha})^2 & \text{if } \chi_F(p) = 0. \end{cases}$$

Here $\alpha, \beta \in \mathbb{Z}$ and $\overline{\alpha} \neq \overline{\beta}$. Thus the prime ideal factorization of $\langle\overline{f}(X)\rangle$ in $\mathbb{F}_p[X]$ is

$$\langle\overline{f}(X)\rangle = \begin{cases} \langle X-\overline{\alpha}\rangle\langle X-\overline{\beta}\rangle & \text{if } \chi_F(p) = 1 \\ \langle\overline{f}(X)\rangle & \text{if } \chi_F(p) = -1 \\ \langle X-\overline{\alpha}\rangle^2 & \text{if } \chi_F(p) = 0. \end{cases}$$

The prime ideals of $\mathbb{F}_p[X]/\langle\overline{f}(X)\rangle$ are correspondingly

$$\begin{cases} \langle X-\overline{\alpha}+\langle\overline{f}(X)\rangle\rangle, \langle X-\overline{\beta}+\langle\overline{f}(X)\rangle\rangle & \text{if } \chi_F(p) = 1 \\ \langle\overline{f}(X)\rangle \text{ (the zero ideal)} & \text{if } \chi_F(p) = -1 \\ \langle X-\overline{\alpha}+\langle\overline{f}(X)\rangle\rangle & \text{if } \chi_F(p) = 0. \end{cases}$$

Pass the ideal generators back through the isomorphism $\mathbb{Z}[r]/p\mathbb{Z}[r] \approx \mathbb{F}_p[X]/\langle\overline{f}(X)\rangle$ given by $\varphi(r) + p\mathbb{Z}[r] \longleftrightarrow \overline{\varphi}(X) + \langle\overline{f}(X)\rangle$ to get that the prime ideals of $\mathbb{Z}[r]/p\mathbb{Z}[r]$ are

$$\begin{cases} \langle r-\alpha+p\mathbb{Z}[r]\rangle, \langle r-\beta+p\mathbb{Z}[r]\rangle & \text{if } \chi_F(p) = 1 \\ p\mathbb{Z}[r] \text{ (the zero ideal)} & \text{if } \chi_F(p) = -1 \\ \langle r-\alpha+p\mathbb{Z}[r]\rangle & \text{if } \chi_F(p) = 0. \end{cases}$$

So finally the prime ideal factorization of $p\mathbb{Z}[r]$ in $\mathbb{Z}[r]$ is

$$p\mathbb{Z}[r] = \begin{cases} \mathfrak{p}\mathfrak{q}, \quad \mathfrak{p} = \langle r-\alpha, p\rangle, \ \mathfrak{q} = \langle r-\beta, p\rangle & \text{if } \chi_F(p) = 1 \\ \mathfrak{p}, \quad \mathfrak{p} = \langle p\rangle & \text{if } \chi_F(p) = -1 \\ \mathfrak{p}^2, \quad \mathfrak{p} = \langle r-\alpha, p\rangle & \text{if } \chi_F(p) = 0. \end{cases}$$

The ideals $\mathfrak{p}$ and $\mathfrak{q}$ in the first and third cases have norm p because $p\mathbb{Z}[r]$ has norm p^2. □

As for the natural isomorphism in the proof, the idea is that we may quotient by $f(X)$ and p in either order because we are quotienting by them both. The general isomorphism that captures this idea is

$$(A/C)\,/\,((B+C)/C) \approx A/(B+C) \approx (A/B)\,/\,((C+B)/B).$$

Now start from the isomorphisms that show that the upper two rings in the proof's u-shaped diagram are quotients, one by $f(X)$ and the other by p,

$$\mathbb{Z}[r] \approx \mathbb{Z}[X]/\langle f(X)\rangle, \qquad \varphi(r) \longleftrightarrow \varphi(X) + \langle f(X)\rangle$$

and

$$\mathbb{Z}[X]/p\mathbb{Z}[X] \approx \mathbb{F}_p[X], \qquad \varphi(X) + p\mathbb{Z}[X] \longleftrightarrow \overline{\varphi}(X).$$

This makes the lower two rings of the diagram isomorphic because they are quotients by both $f(X)$ and p. More specifically, from the first of these isomorphisms, then the general isomorphism, and then the second of these isomorphisms,

$$\begin{aligned}\mathbb{Z}[r]/p\mathbb{Z}[r] &\approx \big(\mathbb{Z}[X]/\langle f(X)\rangle\big)\,/\,\big((p\mathbb{Z}[X] + \langle f(X)\rangle)/\langle f(X)\rangle\big)\\ &\approx \big(\mathbb{Z}[X]/p\mathbb{Z}[X]\big)\,/\,\big((\langle f(X)\rangle + p\mathbb{Z}[X])/p\mathbb{Z}[X]\big)\\ &\approx \mathbb{F}_p[X]/\langle \overline{f}(X)\rangle,\end{aligned}$$

where explicitly the maps are

$$\begin{aligned}\varphi(r) + p\mathbb{Z}[r] &\longleftrightarrow \varphi(X) + \langle f(X)\rangle + (p\mathbb{Z}[X] + \langle f(X)\rangle)\\ &\longleftrightarrow \varphi(X) + p\mathbb{Z}[X] + (\langle f(X)\rangle + p\mathbb{Z}[X])\\ &\longleftrightarrow \overline{\varphi}(X) + \langle \overline{f}(X)\rangle.\end{aligned}$$

Thus we have the isomorphism in the proof,

$$\mathbb{Z}[r]/p\mathbb{Z}[r] \approx \mathbb{F}_p[X]/\langle \overline{f}(X)\rangle, \qquad \varphi(r) + p\mathbb{Z}[r] \longleftrightarrow \overline{\varphi}(X) + \langle \overline{f}(X)\rangle.$$

7. More on decomposing primes by factoring polynomials

This section consists of comments about Theorem 6.1 beyond what we need for this writeup, and so it is optional reading.

Other than the use of the quadratic character to determine the factorization of $\overline{f}(X)$ in $\mathbb{F}_p[X]$, nothing in the proof of Theorem 6.1 is limited to quadratic fields. The rest of the argument applies to any number ring of the form $\mathbb{Z}[r]$ where r has polynomial $f(X)$. That is, the decomposition of p as an ideal of $\mathcal{O}_F = \mathbb{Z}[r]$ is described by the factorization of $\overline{f}(X)$ in $\mathbb{F}_p[X]$: if

$$\overline{f}(X) = \prod_{i=1}^{g} \overline{\varphi}_i(X)^{e_i}, \quad \deg(\overline{\varphi}_i) = f_i \text{ for each } i$$

with $\sum_{i=1}^{g} e_i f_i = \deg(f)$, then

$$p\mathcal{O}_F = \prod_{i=1}^{g} \mathfrak{p}_i^{e_i}, \qquad \mathfrak{p}_i = \langle \varphi_i(r), p\rangle,\ \mathrm{N}(\mathfrak{p}_i) = p^{f_i} \text{ for each } i$$

and $\sum_{i=1}^{g} e_i f_i = [F:\mathbb{Q}]$. Further we might hope for this factorization to be determined at least sometimes by a general reciprocity law, e.g., congruence condition on p.

For example, with the complex fifth root of unity $\zeta_5 = e^{2\pi i/5}$, let $F = \mathbb{Q}(\zeta_5)$ be the fifth cyclotomic field, whose integer ring is known to be $\mathcal{O}_F = \mathbb{Z}[\zeta_5]$. The fifth cycltomic polynomial,

$$\Phi_5(X) = X^4 + X^3 + X^2 + X^1 + 1,$$

factors as follows modulo primes p.

$$\Phi_5(X) \equiv_{p\mathbb{Z}[X]} \begin{cases} \prod_{j=1}^4 (X - g^{j(p-1)/5}) \text{ where } (\mathbb{Z}/p\mathbb{Z})^\times = \langle g \rangle & \text{if } p \equiv 1 \pmod 5 \\ Q_1(X)Q_2(X) \text{ where } Q_1, Q_2 \text{ are quadratic} & \text{if } p \equiv 4 \pmod 5 \\ \Phi_5(X) & \text{if } p \equiv 2,3 \pmod 5 \\ (X-1)^4 & \text{if } p = 5. \end{cases}$$

In the second case the quadratic polynomials are $X^2 + rX + 1$ and $X^2 + (1-r)X + 1$ where $r^2 - r - 1 \equiv 0 \pmod p$; such r exists because the discriminant of $Y^2 - Y - 1$ is 5, a square modulo p because $(5/p) = (p/5) = (4/5) = 1$. Similarly $\Phi_5(X)$ is irreducible modulo p if $p \equiv 2,3 \pmod 5$ because $(5/p) = -1$. The vectors (e, f, g) from the previous paragraph corresponding to the four cases of the previous display are $(1,1,4)$, $(1,2,2)$, $(1,4,1)$, and $(4,1,1)$. In each case, e is $\phi(p^d)$ where p^d is the largest power of p dividing 5, and f is the smallest positive integer such that $p^f \equiv 1 \pmod{5_p}$ where $5_p = 5/p^d$, and g is $\phi(5_p)/f$, so that altogether $efg = \phi(5)$. These are the values of e, f, g for $N = 5$ in our writeup on primes in arithmetic progression. This example suggests that the result, from that writeup, that $\prod_\chi (1 - \chi(p)p^{-s})^{-1}$ (the product taken over all characters modulo N) equals $(1 - p^{-fs})^{-g}$ relates the pth factor of the Nth zeta function $\zeta_N(s) = \prod_\chi L(\chi, s)$ to the factorization of p in the integer ring of the Nth cyclotomic field $\mathcal{O}_F = \mathbb{Z}[\zeta_N]$. The reader could check that similarly to $N = 5$, this holds for $N = 8$ with $\Phi_8(X) = X^4 + 1$, and for $N = 12$ with $\Phi_{12}(X) = X^4 - X^2 + 1$.

In situations where a number ring $\mathcal{O}_F$ does not take the form $\mathbb{Z}[r]$, or where it does but the polynomial of r is complicated, a simple polynomial may still describe the decomposition of all but finitely many rational primes p in $\mathcal{O}_F$. To illustrate this, recall that our quadratic field is $F = \mathbb{Q}(\sqrt{n})$ where $n \in \mathbb{Z} - \{0, 1\}$ is squarefree, that its discriminant D_F is n if $n = 1 \pmod 4$ and is $4n$ if $n = 2, 3 \pmod 4$, and that its integer ring is $\mathcal{O}_F = \mathbb{Z}[(D_F + \sqrt{D_F})/2]$, properly containing $\mathbb{Z}[\sqrt{n}]$ when $n = 1 \pmod 4$ and equal to $\mathbb{Z}[\sqrt{n}]$ when $n = 2, 3 \pmod 4$. The polynomial

$$f_2(X) = X^2 - n$$

satisfied by $\sqrt{n}$ has discriminant $4n$, which is $4D_F$ if $n = 1 \pmod 4$ and is D_F if $n = 2, 3 \pmod 4$. The reader can check that the factorization of $f_2(X)$ modulo p describes the decomposition of p in $\mathcal{O}_F$ for any odd prime p, but not necessarily for $p = 2$. For example, the reduction $X^2 - 5 = (X-1)^2$ modulo 2 seems to suggest that 2 ramifies in $\mathbb{Q}(\sqrt{5})$, but in fact 2 is inert because $X^2 - 5X + 5$ is irreducible modulo 2. In general, when r lies in $\mathcal{O}_F$ and $f(X)$ is the polynomial of r, the factorization of $f(X)$ modulo p describes the decomposition of p as a product of ideals in $\mathcal{O}_F$ if p does not divide the index $[\mathcal{O}_F : \mathbb{Z}[r]]$. A sufficient condition for this is that p^2 not divide the discriminant of $f(X)$, and so even when we don't know how much bigger $\mathcal{O}_F$ is than $\mathbb{Z}[r]$, we do know that the factorization describes the decomposition for all p whose squares don't divide the discriminant. For example, if $F = \mathbb{Q}(\sqrt[3]{n})$ where $n > 1$ is a cubefree integer then the factorization of $X^3 - n$

modulo p determines the decomposition of p in $\mathcal{O}_F$ for all $p \nmid 3n$, because $X^3 - n$ has discriminant $-27n^2$.

8. Fractional ideals and the ideal class group

Definition 8.1. *A* **fractional ideal** *of F is*

$$\mathfrak{b} = \alpha\mathfrak{a}, \quad \alpha \in F^\times,\ \mathfrak{a} \text{ is an ideal of } \mathcal{O}_F.$$

Sometimes ordinary ideals are called **integral** *ideals to distinguish them from properly fractional ideals.*

Any fractional ideal forms an abelian group and is closed under multiplication by elements of $\mathcal{O}_F$, but a fractional ideal is not closed under multiplication by elements of F.

Because multiplication is defined for ideals of $\mathcal{O}_F$, it is also defined for fractional ideals of F,

$$\alpha\mathfrak{a} \cdot \alpha'\mathfrak{a}' = \alpha\alpha'\mathfrak{a}\mathfrak{a}'.$$

The multiplication of fractional ideals is commutative and associative. The integer ring $\mathcal{O}_F$ is the multiplicative identity. And unlike ordinary ideals, fractional ideals are invertible. Specifically, if

$$\mathfrak{b} = \alpha\mathfrak{a}$$

then the calculation $\alpha\mathfrak{a} \cdot (\alpha \mathrm{N}(\mathfrak{a}))^{-1}\overline{\mathfrak{a}} = \mathcal{O}_F$ shows that

$$\mathfrak{b}^{-1} = (\alpha \mathrm{N}(\mathfrak{a}))^{-1}\overline{\mathfrak{a}}.$$

A fractional ideal is **principal** if it takes the form

$$\mathfrak{b} = \alpha\langle x\rangle, \quad \langle x\rangle \text{ is a principal ideal of } \mathcal{O}_F.$$

Equivalently, $\mathfrak{b} = \beta\mathcal{O}_F$ where $\beta \in F^\times$. The product of principal fractional ideals is again principal, and the inverse of a principal fractional ideal is again principal. Thus the principal fractional ideals form a subgroup of the multiplicative group of fractional ideals of the quadratic field F.

Definition 8.2. *The* **ideal class group** *of F is the quotient group*

$$\mathrm{Cl}(F) = \{\textit{fractional ideals of } F\}/\{\textit{principal fractional ideals of } F\}.$$

The order of the ideal class group is the **ideal class number***, denoted $h(F)$.*

Thus an element of the ideal class group is an ideal class, a set of ideals,

$$\mathcal{C}(\mathfrak{b}) = \{\alpha\mathfrak{b} : \alpha \in F^\times/\mathcal{O}_F^\times\}$$

and the multiplication of the ideal class group is

$$\mathcal{C}(\mathfrak{b})\mathcal{C}(\mathfrak{b}') = \mathcal{C}(\mathfrak{b}\mathfrak{b}').$$

We will see that the ideal class number is finite. The point here is that

> *All fractional ideals are principal if and only if all integral ideals are principal, in which case nonzero elements of $\mathcal{O}_F$ factor uniquely up to units. Thus unique factorization of elements holds if the ideal class group is trivial, i.e., if the ideal class number is* 1.

In fact unique factorization of elements holds *only* if the ideal class group is trivial, but this result is beyond our scope.

The ideal class group and the ideal class number can be constructed with reference only to integral ideals. Define two integral ideals $\mathfrak{a}$ and $\mathfrak{a}'$ to be equivalent if $\alpha\mathfrak{a} = \alpha'\mathfrak{a}'$ for some nonzero $\alpha, \alpha' \in \mathcal{O}_F$. Then the ideal class group is the set of equivalence classes. However, the benefits of introducing fractional ideals are the more naturally-motivated group structure of the ideal class group as a true quotient group, and the greater immediacy of the fact that the class group measures the failure of unique factorization.

The ideal class number h is another structure constant of the field F.

9. Abelian group structure of ideals

The next result is preparation for the pending transition from algebra to geometry in the second part of these notes.

Proposition 9.1. *Let $\mathfrak{b}$ be a fractional ideal of F. Then $\mathfrak{b}$ takes the form*

$$\mathfrak{b} = \alpha\mathbb{Z} \oplus \beta\mathbb{Z},$$

where α and β are nonzero elements of F and $\alpha/\beta \notin \mathbb{Q}$.

Proof. Because the fractional ideal takes the form $\mathfrak{b} = \alpha\mathfrak{a}$ where $\alpha \in F^\times$ and $\mathfrak{a}$ is an ideal of $\mathcal{O}_F$, it suffices to prove the result for integral ideals $\mathfrak{a}$. Because $\mathfrak{a}\overline{\mathfrak{a}} = \mathrm{N}(\mathfrak{a})\mathcal{O}_F$, we have

$$\mathrm{N}(\mathfrak{a})\mathcal{O}_F \subset \mathfrak{a} \subset \mathcal{O}_F.$$

Recall that $F = \mathbb{Q}(\sqrt{n})$ where $n \in \mathbb{Z}$ is squarefree, and that $\mathcal{O}_F = r\mathbb{Z} \oplus \mathbb{Z}$ where $r = \frac{D_F + \sqrt{D_F}}{2}$. The previously displayed containments are

$$\mathrm{N}(\mathfrak{a})r\mathbb{Z} \oplus \mathrm{N}(\mathfrak{a})\mathbb{Z} \subset \mathfrak{a} \subset r\mathbb{Z} \oplus \mathbb{Z}.$$

Because the abelian group $\mathfrak{a}$ sits between two free abelian groups of rank 2, it is free of rank 2 as well. This point is just a matter of linear algebra over $\mathbb{Q}$. □

Part 2. GEOMETRY: COMPLEX LATTICES

If the quadratic field F is imaginary then its ideals can be interpreted as lattices in the complex plane having a special property called *complex multiplication*. Complex geometry shows that the ideal class group of F is finite. Its order, denoted h, is the *ideal class number* of F. The goal of these notes is a formula for h.

10. Complex lattices and homothety

Definition 10.1. *A* **complex lattice** *is a rank-2 abelian subgroup of $\mathbb{C}$,*

$$\Lambda = \lambda_1\mathbb{Z} \oplus \lambda_2\mathbb{Z}, \quad \lambda_1, \lambda_2 \in \mathbb{C}^\times,\ \lambda_1/\lambda_2 \notin \mathbb{R}.$$

Note that in particular, any fractional ideal of an imaginary quadratic field is a complex lattice. (Proposition 9.1 does the bulk of the work of supporting this observation—the only loose end is that an imaginary quadratic field contains no irrational real numbers.)

In the previous definition, the $\mathbb{Z}$-basis $\{\lambda_1, \lambda_2\}$ determines the lattice Λ, but not conversely. We adopt the convention that lattice bases are *ordered* and that furthermore they are always ordered so that $\mathrm{Im}(\lambda_1/\lambda_2) > 0$. Then (exercise, facilitated by the formula $\mathrm{Im}\left(\frac{az+b}{cz+d}\right) = \det(\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right])\mathrm{Im}(z)/|cz+d|^2$ for $\left[\begin{smallmatrix} a & b \\ c & d \end{smallmatrix}\right]$ invertible with real entries and z a complex number that isn't real)

Proposition 10.2. *The ordered pairs of nonzero complex numbers* (λ_1, λ_2) *and* (λ_1', λ_2') *are bases for the same lattice* Λ *if and only if*

$$\begin{bmatrix} \lambda_1' \\ \lambda_2' \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \end{bmatrix} \quad \text{for some } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{SL}_2(\mathbb{Z}).$$

(*Here* $\mathrm{SL}_2(\mathbb{Z})$ *is the group of 2-by-2 matrices having integer entries and determinant* 1.)

It follows that if Λ is a lattice and (λ_1, λ_2) is a basis of Λ then the area of the parallelogram

$$P(\lambda_1, \lambda_2) = \{t_1\lambda_1 + t_2\lambda_2 : t_1, t_2 \in [0,1]\} \quad \text{where } (\lambda_1, \lambda_2) \text{ is a basis of } \Lambda$$

depends only Λ, not on the choice of basis. This is because if (λ_1, λ_2) and (λ_1', λ_2') are bases then the linear map taking λ_i to λ_i' for $i = 1, 2$ preserves area because it has determinant 1.

Definition 10.3. *Two lattices* Λ *and* Λ' *are* **homothetic** *if*

$$\Lambda' = c\Lambda \quad \textit{for some } c \in \mathbb{C}^\times.$$

Homothety is clearly an equivalence relation. It preserves the geometry of any lattice up to dilation and rotation. We now find a canonical representative of any equivalence class of lattices under homothety.

Lemma 10.4. *Let* Λ *be a complex lattice. Then* Λ *has nonzero elements of least modulus.*

Proof. First we show that the lattice point 0 is isolated, meaning that it has a $\mathbb{C}$-neighborhood containing no other lattice point. This property is preserved under homothety, so we may assume that our lattice is $\Lambda = \tau\mathbb{Z} \oplus \mathbb{Z}$ where $\mathrm{Im}(\tau) > 0$. The ball about 0 of radius $r = \min\{\mathrm{Im}(\tau), 1\}$ contains no other lattice point.

The group structure of the lattice shows that same radius works for a similar ball about any lattice point. Consequently any bounded subset of the lattice is finite. The result follows. □

Now let a lattice Λ be given. After applying a homothety, we may assume that one of its nonzero elements of least modulus is 1. Let $\tau \in \Lambda$ be an element of $\Lambda - \mathbb{Z}$ having least modulus; we may assume that $\mathrm{Im}(\tau) > 0$. Then $|\tau| \geq 1$, and also $|\mathrm{Re}(\tau)| \leq 1/2$, else some $\tau + n$ (where $n \in \mathbb{Z}$) has smaller modulus. Thus τ lies in the **fundamental domain**,

$$D = \{\tau \in \mathbb{C} : \mathrm{Im}(\tau) > 0,\ |\mathrm{Re}(\tau)| \leq 1/2,\ |\tau| \geq 1\}$$

(see figure 1). And so every lattice is homothetic to a lattice

$$\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z}, \quad \tau \in D.$$

Furthermore, τ is essentially unique. One type of exception to uniqueness is easy to find: if $\mathrm{Re}(\tau) = -1/2$ then also $\Lambda = (\tau + 1)\mathbb{Z} \oplus \mathbb{Z}$ with $\tau + 1 \in D$. That is, the two vertical sides of the fundamental domain should be identified. A second kind of uniqueness is slightly more subtle: if $|\tau| = 1$ then (writing "$\sim$" for homothety)

$$\Lambda_\tau = \tau\mathbb{Z} \oplus \mathbb{Z} \sim \mathbb{Z} \oplus \tau^{-1}\mathbb{Z} = -\tau^{-1}\mathbb{Z} \oplus \mathbb{Z}.$$

But $-\tau^{-1}$ is also on the circular arc of the boundary of D, being the horizontal reflection of τ. And so the left and right halves of the semicircular boundary arc of D should be identified as well. Otherwise, τ is uniquely determined by the process just described of finding it. To specify unique representatives, we may keep only the right half of the boundary of D,

- $\mathrm{Im}(\tau) \geq \sqrt{3}/2$,
- $-1/2 < \mathrm{Re}(\tau) \leq 1/2$,
- $|\tau| > 1$ if $\mathrm{Re}(\tau) < 0$, and $|\tau| \geq 1$ if $\mathrm{Re}(\tau) \geq 0$.

A lattice Λ_τ where τ satisfies the three previous conditions is **normalized**.

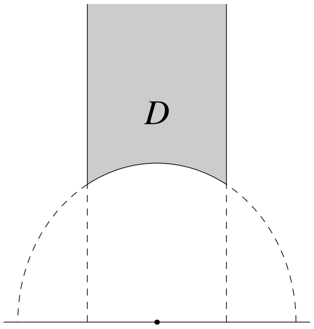

Figure 1. The fundamental domain

Especially, we show that each ideal class in an imaginary quadratic field has a unique normalized element. Indeed, let $\mathfrak{b}$ be a fractional ideal of the imaginary quadratic field F. Let $\alpha \in F^\times$ be a least-norm nonzero element of $\mathfrak{b}$. The ideal $\alpha^{-1}\mathfrak{b}$ lies in the class of $\mathfrak{b}$ and it contains 1 as a least-norm nonzero element. Hence it is normalized. Any other $\alpha' \in F^\times$ that is a least-norm nonzero element of $\mathfrak{b}$ differs multiplicatively from α by a unit, and so $\alpha^{-1}\mathfrak{b}$ is unique. The next section will show that the normalized ideal $\alpha^{-1}\mathfrak{b}$ in the ideal class of $\mathfrak{b}$ has a further property that allows only finitely many ideal classes altogether.

11. Complex multiplication

For any lattice Λ and any integer m we have $m\Lambda \subset \Lambda$, the lattice dilating back into itself or collapsing to 0. But further, some lattices *spiral* back into themselves under other multiplications.

Definition 11.1. *Let Λ be a lattice. If*

$$m\Lambda \subset \Lambda \quad \textit{for some } m \in \mathbb{C} - \mathbb{Z}$$

then Λ has **complex multiplication (CM)** *by m.*

The property of having complex multiplication by m is preserved by homothety, so we may restrict our attention to lattices Λ_τ.

To study which such CM-values m are possible for which lattices Λ_τ, assume that Λ_τ has CM by m. Thus

$$m\begin{bmatrix} \tau \\ 1 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix}\begin{bmatrix} \tau \\ 1 \end{bmatrix} \quad \text{for some } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}).$$

Thus m is an eigenvalue of the matrix, and $\left[\begin{smallmatrix}\tau\\1\end{smallmatrix}\right]$ is an eigenvector. Because we are assuming that $m \notin \mathbb{Z}$, the condition $m \in \mathbb{R}$ is impossible, e.g., it would force $m = d$. So m is an imaginary quadratic algebraic integer. Furthermore, because $m = c\tau + d$ (with $c \neq 0$), the lattice basis element

$$\tau = \frac{m-d}{c}$$

lies in the same imaginary quadratic field as m. The field takes the form $F = \mathbb{Q}(\sqrt{n})$ where $n \in \mathbb{Z}_{<0}$ is squarefree. Recall that the integer ring $\mathcal{O}_F$ is

$$\mathcal{O}_F = \mathbb{Z}[r], \quad r = \frac{D_F + \sqrt{D_F}}{2}, \quad D_F = \begin{cases} n & \text{if } n = 1 \pmod 4 \\ 4n & \text{if } n = 2, 3 \pmod 4). \end{cases}$$

The key ideas connecting the previous part of this writeup to the present part are:

> *Fractional ideals of F are complex lattices with CM by the generator r of the integer ring $\mathcal{O}_F$. To find all normalized lattices $\Lambda_\tau \subset F$ having complex multiplication by r is precisely to find a set of representatives of the ideal class group of F.*

Recall that *normalized* means that τ satisfies the three bullets at the end of the previous section.

The condition for CM by r is

$$r\begin{bmatrix}\tau\\1\end{bmatrix} = \begin{bmatrix}a & b\\c & d\end{bmatrix}\begin{bmatrix}\tau\\1\end{bmatrix} \quad \text{for some } \begin{bmatrix}a & b\\c & d\end{bmatrix} \in \mathrm{M}_2(\mathbb{Z}).$$

Thus

$$\tau = \frac{r-d}{c} = \frac{D_F - 2d + \sqrt{D_F}}{2c}, \quad c, d \in \mathbb{Z},$$

subject to four conditions on c and d, three of them rephrasing the three bullets in the previous section ($\mathrm{Im}(\tau) \geq \sqrt{3}/2$, $-1/2 < \mathrm{Re}(\tau) \leq 1/2$, $|\tau| > 1$ if $\mathrm{Re}(\tau) < 0$ and $|\tau| \geq 1$ if $\mathrm{Re}(\tau) \geq 0$), and the fourth to be explained below,

- $0 < c \leq \sqrt{|D_F|/3}$,
- $(D_F - c)/2 \leq d < (D_F + c)/2$,
- $4c^2 < (D_F - 2d)^2 - D_F$ if $D_F < 2d$, $4c^2 \leq (D_F - 2d)^2 - D_F$ if $D_F \geq 2d$,
- $c \mid \mathrm{N}(r-d)$.

For the fourth condition, r satisfies the characteristic polynomial of $\left[\begin{smallmatrix}a & b\\c & d\end{smallmatrix}\right]$, *i.e.*, $r^2 - (a+d)r + ad - bc = 0$, but also r satisfies the unique minimal polynomial relation $r^2 - \mathrm{tr}(r)r + \mathrm{N}(r) = 0$; so $\mathrm{tr}(r) = a + d$, which is to say $r - a = -(\overline{r} - d)$. Thus the characteristic polynomial condition $(r-a)(r-d) - bc = 0$ is $\mathrm{N}(r-d) = -bc$. Conversely, if $\mathrm{N}(r-d) = -bc$ for some b, then let $a = \mathrm{tr}(r-d)+d$; it is easy to verify that $\mathrm{tr}(r) = a + d$ and $\mathrm{N}(r) = ad - bc$, so r satisfies the characteristic polynomial of $\left[\begin{smallmatrix}a & b\\c & d\end{smallmatrix}\right]$.

The four conditions in the bullet list just above show that for a given imaginary quadratic field F, with its discriminant D_F and its integer ring generator r, there exist only finitely many values $\tau = (r-d)/c$ that describe lattices with complex multiplication. This shows that the class number of F is finite. The τ-values are easy to find by hand if $|D_F|$ is small, and easy to find by algorithm in any case. Because ideal class representatives are $\mathfrak{b} = \langle \tau, 1 \rangle$ where $\tau = (r-d)/c$ with c and d satisfying the four conditions, integral representatives are $\mathfrak{a} = \langle r - d, c \rangle$. We have proved

Theorem 11.2. *Let F be an imaginary quadratic field. The ideal class number $h(F)$ is finite.*

We know that there must exist at least one normalized lattice with CM by r, corresponding to the identity element of the ideal class group. And indeed, the lattice $\mathcal{O}_F = \Lambda_r$ works. But there may be others.

For example, the reader can use these ideas to show that the integer ring $\mathcal{O}_F = \mathbb{Z}[\frac{-39+\sqrt{-39}}{2}]$ of the imaginary quadratic field $F = \mathbb{Q}(\sqrt{-39})$ gives four pairs $(c,d) = (1,-20),(2,-20),(2,-19),(3,-21)$, and so its four ideal class representatives $\langle r-d, c\rangle$ are $\mathcal{O}_F = \langle \frac{1+\sqrt{-39}}{2}, 1\rangle$, $\mathfrak{p}_1 = \langle \frac{1+\sqrt{-39}}{2}, 2\rangle$, $\mathfrak{p}_2 = \langle \frac{-1+\sqrt{-39}}{2}, 2\rangle$, and $\mathfrak{q} = \langle \frac{-3+\sqrt{-39}}{2}, 3\rangle$. Because $\mathcal{O}_F = \mathbb{Z}[\frac{1+\sqrt{-39}}{2}]$ and the polynomial of $\frac{1+\sqrt{-39}}{2}$ is $X^2 - X + 10$, the proof of Theorem 6.1 shows that $2\mathcal{O}_F = \mathfrak{p}_1\mathfrak{p}_2$ and $3\mathcal{O}_F = \mathfrak{q}^2$. Because the classes of $\mathfrak{p}_1$ and $\mathfrak{p}_2$ are distinct and each is the other's inverse, so that neither class is its own inverse, the ideal class group is cyclic of order 4 rather than the product of two cyclic groups of order 2 (these are the only possibilities for a four-element abelian group).

Our goal is a *formula* for $h(F)$ to complement the *algorithm* that we now have for it. The formula requires elements of analytic number theory, to be presented in the third part of this writeup, in addition to the algebra of the first part and the geometry of this part. Its conceptual content beyond the ideal class number algorithm is that it relates the algebraic structure constants of our quadratic number field—its discriminant, descriptors of its unit group, and its ideal class number—to an analytic datum, a *special value* of the *quadratic L-function* of the field, to be explained. The following proposition will be cited in the course of the analysis to follow.

Proposition 11.3. *Let F be an imaginary quadratic field, let D_F be the discriminant of F, and let $r = \frac{D_F+\sqrt{D_F}}{2}$. Consider an integral ideal class representative*

$$\mathfrak{a} = \langle r-d, c\rangle \quad \textit{with } c \textit{ and } d \textit{ as just above},$$

and let α denote the area of the parallelogram spanned by $r-d$ and c. Then

$$\frac{\mathrm{N}(\mathfrak{a})}{\alpha} = \frac{2}{\sqrt{|D_F|}}\,.$$

Note that the right side is independent of c and d. That is, the ideal norm (an algebraic quantity) is the parallelogram area (a geometric quantity) times a constant that depends only on the field F. Especially the proposition with $\mathfrak{a} = \mathcal{O}_F$ says that the area of a fundamental parallelogram of the full integer ring of F is $\sqrt{|D_F|}/2$; that is, the absolute discriminant is roughly a measure of the sparseness of $\mathcal{O}_F$ as a lattice in $\mathbb{C}$.

Proof. The parallelogram area is $\alpha = c\sqrt{|D_F|}/2$, so we need to show that $\mathrm{N}(\mathfrak{a}) = c$. Let $b = -\mathrm{N}(r-d)/c$. Because $\mathfrak{a}\overline{\mathfrak{a}} = \mathrm{N}(\mathfrak{a})\mathcal{O}_F$ and

$$\mathfrak{a}\overline{\mathfrak{a}} = \langle \mathrm{N}(r-d), (r-d)c, (\overline{r}-d)c, c^2\rangle = c\langle b, r-d, \overline{r}-d, c\rangle,$$

it suffices to show that $\langle b, r-d, \overline{r}-d, c\rangle$ contains 1. It contains the element

$$g = \gcd(b, \mathrm{tr}(r) - 2d, c).$$

To show that $g = 1$, note that the quantities $\mathrm{tr}(r) - 2d = \mathrm{tr}(r-d)$ and $-bc = \mathrm{N}(r-d)$ are the coefficients of the polynomial of $r-d$, which has the same discriminant

D_F as the polynomial of r because d is real. Also, g^2 divides both terms of this discriminant and hence divides the discriminant altogether. In symbols,

$$\begin{aligned} g^2 \mid (\mathrm{tr}(r)-2d)^2+4bc &= (\mathrm{tr}(r)-2d)^2-4\mathrm{N}(r-d) \\ &= \mathrm{tr}(r)^2-4\mathrm{tr}(r)d+4d^2-4\mathrm{N}(r)+4\mathrm{tr}(r)d-4d^2 \\ &= \mathrm{tr}(r)^2-4\mathrm{N}(r) = D_F^2-D_F(D_F-1)=D_F. \end{aligned}$$

Recall that our quadratic field is $F=\mathbb{Q}(\sqrt{n})$ with n a squarefree negative integer. If $n=1 \pmod 4$ then $D_F=n$ is squarefree, and so $g=1$ and we are done. On the other hand, if $n=2,3 \pmod 4$ then $D_F=4n$ and so g could equal 1 or 2. To show that $g=1$ in this case as well, note that the equality $bc=-\mathrm{N}(r)+\mathrm{tr}(r)d-d^2$ in the calculation just carried out is now

$$bc=-\frac{D_F(D_F-1)}{4}+D_Fd-d^2=-n(4n-1)+4nd-d^2=n-d^2 \pmod 4.$$

Thus $bc\neq 0 \pmod 4$ because $n=2,3 \pmod 4$ and $d^2=0,1 \pmod 4$. So at least one of b,c is odd, disallowing the possibility that $g=\gcd(b,\mathrm{tr}(r)-2d,c)$ is 2. □

Part 3. ANALYSIS: ZETA AND L-FUNCTIONS OF AN IMAGINARY QUADRATIC FIELD

To obtain the class number formula, we encode information about the imaginary quadratic field F in *Dirichlet series*, series of the form

$$f(s)=\sum_{n\in\mathbb{Z}^+}\frac{a_n}{n^s}, \quad s\in\mathbb{C}.$$

The various Dirichlet series in question—the Euler–Riemann zeta function, the quadratic L-function of F, and the Dedekind zeta function of F—have useful complex analytic properties that combine with the number theoretic information that they encode to give the class number formula.

12. Summation by parts and Dirichlet series convergence

Let $\{a_n\}_{n\geq 1}$ and $\{b_n\}_{n\geq 1}$ be complex sequences. Define

$$A_n=\sum_{k=1}^{n}a_k \quad \text{for } n\geq 0 \text{ (including } A_0=0),$$

so that

$$a_n=A_n-A_{n-1} \quad \text{for } n\geq 1.$$

Also define

$$\Delta b_n=b_{n+1}-b_n \quad \text{for } n\geq 1,$$

so that, with b_0 understood to be 0,

$$b_n=\sum_{k=0}^{n-1}\Delta b_k.$$

Then for any $1\leq m\leq n$, the **summation by parts** formula is

$$\sum_{k=m}^{n-1}a_kb_k=A_{n-1}b_n-A_{m-1}b_m-\sum_{k=m}^{n-1}A_k\Delta b_k.$$

The formula is easy to verify in consequence of

$$a_k b_k = A_k b_{k+1} - A_{k-1} b_k - A_k \Delta b_k, \quad k \geq 1,$$

noting that the first two terms on the right side telescope when summed.

Proposition 12.1. *Let $\{a_n\}_{n\geq 1}$ be a complex sequence such that for some positive numbers C and r,*

$$\left|\sum_{k=1}^{n} a_k\right| \leq Cn^r \quad \textit{for all large enough } n.$$

Then the Dirichlet series

$$f(s) = \sum_{n\in\mathbb{Z}^+} \frac{a_n}{n^s}, \quad s \in \mathbb{C}$$

is complex analytic on the open right half plane $\{\mathrm{Re}(s) > r\}$. If furthermore $\{a_n\}$ is a nonnegative real sequence then $f(s)$ converges absolutely on $\{\mathrm{Re}(s) > r\}$.

Proof. Let

$$\{b_n\} = \{n^{-s}\}.$$

Then summation by parts gives for $1 \leq m \leq n$,

$$\sum_{k=m}^{n-1} \frac{a_k}{k^s} = \frac{A_{n-1}}{n^s} - \frac{A_{m-1}}{m^s} - \sum_{k=m}^{n-1} A_k \left(\frac{1}{(k+1)^s} - \frac{1}{k^s}\right).$$

Introduce the notation

$$s = \sigma + it, \quad \sigma > r,$$

so that $|x^s| = x^\sigma$ for all $x \in \mathbb{R}^+$, and estimate that

$$\left|\frac{1}{(k+1)^s} - \frac{1}{k^s}\right| = \left|-s\int_k^{k+1} t^{-s-1}\,dt\right| \leq |s|\int_k^{k+1} t^{-\sigma-1}\,dt < |s|k^{-\sigma-1}.$$

We are given that $|A_k| \leq Ck^r$ for all large enough k, and so the summation by parts from a moment ago says that for all large enough $1 \leq m \leq n$,

$$\left|\sum_{k=m}^{n-1} \frac{a_k}{k^s}\right| \leq C\left(\frac{1}{n^{\sigma-r}} + \frac{1}{m^{\sigma-r}} + |s|\sum_{k=m}^{n-1} \frac{1}{k^{\sigma-r+1}}\right).$$

Recall that $\sigma > r$. Let $n \to \infty$ to see that for all large enough $m \geq 1$,

$$\left|\sum_{k=m}^{\infty} \frac{a_k}{k^s}\right| \leq C\left(\frac{1}{m^{\sigma-r}} + |s|\sum_{k=m}^{\infty} \frac{1}{k^{\sigma-r+1}}\right).$$

Because $\sigma > r$, the right side goes to 0 as $m \to \infty$. As s varies through a compact subset K of the open right half plane $\{\sigma > r\}$, the right side goes to 0 at a rate that depends only on $\min\{\sigma : \sigma + it \in K\}$ and $\max\{|s| : s \in K\}$, and thus the Dirichlet series $f(s) = \sum_{n\in\mathbb{Z}^+} a_n n^{-s}$ converges uniformly on K. Because the partial sums of $f(s)$ are analytic on $\{\mathrm{Re}(s) > r\}$, their uniform convergence on compacta is the hypothesis for a standard theorem of complex analysis that then says that $f(s)$ is analytic on $\{\mathrm{Re}(s) > r\}$ as well.

Now assume that $a_n \in \mathbb{R}_{\geq 0}$ for all n. Because $f(s)$ converges on $\{\mathrm{Re}(s) > r\}$, it converges for any $s = \sigma > r$. But for general $s = \sigma + it$ where $\sigma > r$ we have

$$\left|\frac{a_n}{n^s}\right| = \frac{a_n}{n^\sigma},$$

And so $f(s)$ converges absolutely because $f(\sigma)$ converges. □

A slogan-encapsulation of Proposition 12.1 is

$$|\sum^{n} a_k| = \mathcal{O}(n^r) \implies \sum \frac{a_n}{n^s} \text{ is well-behaved on } \{\mathrm{Re}(s) > r\}.$$

13. The Euler–Riemann zeta function

Definition 13.1. *The* **Euler–Riemann zeta function** *is formally*

$$\zeta(s) = \sum_{n \in \mathbb{Z}^+} n^{-s} = \prod_{p \in \mathcal{P}} (1 - p^{-s})^{-1}.$$

The formal equality of the sum and the product follows from the geometric series formula and then the unique factorization of positive integers,

$$\prod_{p \in \mathcal{P}} (1 - p^{-s})^{-1} = \prod_{p \in \mathcal{P}} \sum_{e_p \geq 0} (p^{e_p})^s = \sum_{n \in \mathbb{Z}^+} n^{-s}.$$

Proposition 13.2 (Properties of the Euler–Riemann Zeta Function)**.** *The function $\zeta(s)$ is complex analytic on the open right half plane $\{\mathrm{Re}(s) > 1\}$, where the formal equality of the sum and product expressions of $\zeta(s)$ is analytically valid. The function $\zeta(s)$ extends meromorphically to the open right half plane $\{\mathrm{Re}(s) > 0\}$, and the extension has only a simple pole at $s = 1$ with residue 1. That is,*

$$\zeta(s) = \frac{1}{s-1} + \psi(s), \quad \mathrm{Re}(s) > 0$$

where ψ is analytic.

Proof. The fact that $\zeta(s)$ is complex analytic on $\mathrm{Re}(s) > 1$ follows from Proposition 12.1 with $C = r = 1$ because $\{a_i\}$ is the sequence $\{1, 1, 1, \dots\}$. For any bound $B > 0$ we have the identity

$$\sum_{n = \prod_{p<B} p^{e_p}} n^{-s} = \prod_{p<B} (1 - p^{-s})^{-1},$$

using the condition $\mathrm{Re}(s) > 1$ to rearrange the terms because the sum converges absolutely. As $B \to \infty$ the sum converges to $\zeta(s)$ because it converges absolutely and thus the order of summation is irrelevant. Consequently the product converges to $\zeta(s)$ as well. For the last statement, compute that

$$\frac{1}{s-1} = \int_1^\infty t^{-s}\, dt = \sum_{n=1}^{\infty} \int_n^{n+1} t^{-s}\, dt = \zeta(s) + \sum_{n=1}^{\infty} \int_n^{n+1} (t^{-s} - n^{-s})\, dt.$$

Call the sum $-\psi(s)$. Because for all $t \in [n, n+1]$ we have

$$|t^{-s} - n^{-s}| = |s \int_n^t x^{-s-1}\, dx| \leq |s| \int_n^t x^{-\sigma-1}\, dx \leq |s| n^{-\sigma-1}(t-n) \leq |s| n^{-\sigma-1},$$

it follows that

$$\left| \int_n^{n+1} (t^{-s} - n^{-s})\, dt \right| \leq \frac{|s|}{n^{\sigma+1}}\,,$$

and so $-\psi(s)$ converges to an analytic function on $\{\mathrm{Re}(s) > 0\}$ by the convergence properties of $|s| \sum_n n^{-\sigma-1}$. □

14. The L-function of a quadratic field

Recall the quadratic character of a quadratic field F, defined using the discriminant of F and the extended Jacobi symbol,

$$\chi_F : \mathbb{Z}^+ \longrightarrow \mathbb{Z}, \quad \chi_F(n) = \left(\frac{D_F}{n}\right).$$

Because the symbol D_F subsumes the information formerly contained in the symbol n for describing the quadratic field F, we have liberated n for the previous display and the sequel.

Definition 14.1. *Let F be a quadratic field with discriminant D_F. The* **quadratic L-function** *of F is formally*

$$L(\chi_F, s) = \sum_{n \in \mathbb{Z}^+} \chi_F(n) n^{-s} = \prod_{p \in \mathcal{P}} (1 - \chi_F(p) p^{-s})^{-1}.$$

The formal equality of the sum and the product follows similarly to the Euler–Riemann zeta function because χ is multiplicative. Because the quadratic character encodes the decomposition of rational primes in $\mathcal{O}_F$ (Theorem 6.1), so does the quadratic L-function.

Proposition 14.2 (Properties of the Quadratic L-Function)**.** *The quadratic L-function $L(\chi_F, s)$ is complex analytic on $\{\mathrm{Re}(s) > 0\}$. The formal equality of the sum and product expressions of $L(\chi_F, s)$ is analytically valid for* $\mathrm{Re}(s) > 1$*.*

Proof. By Theorem 5.2, $\chi_F(n)$ depends only on $n \pmod{|D_F|}$. So for any $n_o \in \mathbb{Z}^+$,

$$\sum_{n=n_o}^{n_o+|D_F|-1} \chi_F(n) = 0,$$

because we are summing the nontrivial character χ_F over the group $(\mathbb{Z}/D_F\mathbb{Z})^\times$. It follows that for all $n \geq 1$,

$$\left| \sum_{k=1}^{n} \chi_F(k) \right| \leq |D_F|.$$

Now Proposition 12.1 shows that $L(\chi_F, s)$ is analytic on $\{\mathrm{Re}(s) > 0\}$. The argument that the sum and the product are equal is essentially the same as for the Euler–Riemann zeta function, requiring $\mathrm{Re}(s) > 1$ for absolute convergence so that terms can be rearranged. □

The next result evaluates $L(\chi_F, 1)$ as a constant factor times a roughly $|D_F|/2$-fold sum of values weighted by the quadratic character. The values are logarithms of sines if F is real quadratic and they are simply 1 if F is imaginary quadratic. The value $L(\chi_F, 1)$ will figure in the class number formula.

Proposition 14.3 (Special Value of the Quadratic L-Function)**.** *For a real quadratic field F,*

$$L(\chi_F, 1) = -\frac{2}{\sqrt{D_F}} \sum_{1 \leq r < D_F/2} \chi_F(r) \log(\sin(\pi r / D_F)).$$

For an imaginary quadratic field F,

$$L(\chi_F, 1) = -\frac{\pi}{|D_F|^{3/2}} \sum_{r=1}^{|D_F|-1} \chi_F(r) r, \tag{2}$$

and further this formula simplifies to

$$L(\chi_F,1)=\frac{\pi}{(2-\chi(2))\sqrt{|D_F|}}\sum_{1\le r<|D_F|/2}\chi_F(r). \tag{3}$$

Before proving the proposition, we make two comments. First, the quantity $\sum_{r=1}^{|D_F|-1}\chi_F(r)r$ that arises in the imaginary quadratic case is the first so-called χ_F-*Bernoulli number*, B_{1,χ_F}, where the χ_F-Bernoulli numbers in general are defined by a generating function,

$$\sum_{r=1}^{|D_F|-1}\frac{\chi_F(r)te^{rt}}{e^t-1}=\sum_{k\ge 0}B_{k,\chi_F}\frac{t^k}{k!}\,.$$

Indeed, from the definition of the Bernoulli polynomials, $\frac{te^{xt}}{e^t-1}=\sum_{k\ge 0}B_k(x)t^k/k!$, the left side of the previous display is, after reversing a double sum,

$$\sum_{r=1}^{|D_F|-1}\frac{\chi_F(r)te^{rt}}{e^t-1}=\sum_{k\ge 0}\sum_{r=1}^{|D_F|-1}\chi_F(r)B_k(r)\frac{t^k}{k!}\,,$$

so that $B_{k,\chi_F}=\sum_{r=1}^{|D_F|-1}\chi_F(r)B_k(r)$. In particular, because $B_1(r)=r-1/2$ and $\sum_r\chi_F(r)=0$, we have $B_{1,\chi_F}=\sum_{r=1}^{|D_F|-1}\chi_F(r)r$ as claimed. Of course there are χ-Bernoulli numbers for any Dirichlet character χ, not only for our particular character χ_F.

Second, to get (3) from (2) in the imaginary quadratic case, introduce the notation

$$S=\sum_{1\le r<|D_F|}\chi_F(r)r,\qquad S_1=\sum_{1\le r<|D_F|/2}\chi_F(r)r,\qquad S_0=\sum_{1\le r<|D_F|/2}\chi_F(r);$$

what needs to be shown is that $S=(|D_F|/(\chi(2)-2))S_0$. If the imaginary quadratic field is $F=\mathbb{Q}(\sqrt{n})$ for negative squarefree $n=1 \pmod 4$, so that $D_F=n$, the relations

$$S=\begin{cases}\displaystyle\sum_{1\le r<|D_F|/2}\big(\chi_F(r)r+\chi(|D_F|-r)(|D_F|-r)\big)\\ \displaystyle\sum_{1\le r<|D_F|/2}\big(\chi_F(2r)2r+\chi(|D_F|-2r)(|D_F|-2r)\big)\end{cases}$$

and the fact that χ_F is odd and quadratic give $S=2S_1-|D_F|S_0$ and $\chi(2)S=4S_1-|D_F|S_0$. These two relations give $S=(|D_F|/(\chi(2)-2))S_0$ as desired. If instead $F=\mathbb{Q}(\sqrt{n})$ for negative squarefree $n=2,3 \pmod 4$, so that $D_F=-4n$ and now $\chi_F(2)=0$, then recall from the end of section 5 that $\chi_F(r+|D_F|/2)=-\chi_F(r)$. Consequently,

$$S=\sum_{1\le r<|D_F|/2}\big(\chi_F(r)r+\chi_F(r+|D_F|/2)(r+|D_F|/2)\big)=(-|D_F|/2)S_0,$$

and again we have $S=(|D_F|/(\chi(2)-2))S_0$ as desired, now with $\chi(2)=0$. Now we proceed to the proof of Proposition 14.3, needing to establish only (2) in the imaginary quadratic case.

Proof. Recall that χ_F has period $|D_F|$. Compute that for $\mathrm{Re}(s) > 1$ (so that we may rearrange the terms),

$$L(\chi_F, s) = \sum_{n \in \mathbb{Z}^+} \chi_F(n) n^{-s} = \sum_{t=0}^{|D_F|-1} \chi_F(t) \sum_{\substack{n \in \mathbb{Z}^+ \\ n = t\ (|D_F|)}} n^{-s}.$$

The inner sum is

$$\sum_{\substack{n \in \mathbb{Z}^+ \\ n = t\ (|D_F|)}} n^{-s} = \sum_{n \in \mathbb{Z}^+} a_n(t) n^{-s} \quad \text{where } a_n(t) = \begin{cases} 1 & \text{if } n = t \pmod{|D_F|} \\ 0 & \text{if } n \neq t \pmod{|D_F|}, \end{cases}$$

and the casewise coefficient has a uniform description as a character sum,

$$a_n(t) = \frac{1}{|D_F|} \sum_{r=0}^{|D_F|-1} \zeta_{|D_F|}^{(t-n)r}, \quad \text{where} \quad \zeta_{|D_F|} = e^{2\pi i/|D_F|}.$$

Thus we have for $\mathrm{Re}(s) > 1$,

$$\begin{aligned} L(\chi_F, s) &= \sum_{t=0}^{|D_F|-1} \chi_F(t) \sum_{n \in \mathbb{Z}^+} \frac{1}{|D_F|} \sum_{r=0}^{|D_F|-1} \zeta_{|D_F|}^{(t-n)r} n^{-s} \\ &= \frac{1}{|D_F|} \sum_{r=0}^{|D_F|-1} \sum_{t=0}^{|D_F|-1} \chi_F(t) \zeta_{|D_F|}^{rt} \sum_{n \in \mathbb{Z}^+} \zeta_{|D_F|}^{-nr} n^{-s}. \end{aligned}$$

Let $\tau_r(\chi_F)$ and $\tau(\chi_F)$ respectively denote the variant Gauss sum of χ_F that has appeared in the calculation and the basic Gauss sum of χ_F,

$$\tau_r(\chi_F) = \sum_{t=0}^{|D_F|-1} \chi_F(t) \zeta_{|D_F|}^{rt}, \qquad \tau(\chi_F) = \tau_1(\chi_F).$$

The rth variant Gauss sum is the character value at r times the basic Gauss sum,

$$\tau_r(\chi_F) = \chi_F(r) \tau(\chi_F).$$

When $\gcd(r, |D_F|) = 1$ this equality follows from a quick substitution, but when $\gcd(r, |D_F|) > 1$ the equality (which says in this case that $\tau_r(\chi_F) = 0$; in particular $\tau_0(\chi) = 0$ and so there is no need to sum over $r = 0$) relies on the fact that χ_F has no period smaller than $|D_F|$. See the handout on continuations and functional equations for the argument. Furthermore, as shown at the end of the ninth online lecture for this course, if we set $\delta = 0$ for an even quadratic character, such as arises from a real quadratic field, and if we set $\delta = 1$ for an odd quadratic character, such as arises from an imaginary quadratic field, then the basic Gauss sum of a quadratic character is

$$\tau(\chi_F) = i^\delta |D_F|^{1/2}.$$

Returning to our computed value, no longer bothering to sum over $r = 0$,

$$\begin{aligned}
L(\chi_F, s) &= \frac{1}{|D_F|} \sum_{r=1}^{|D_F|-1} \tau_r(\chi) \sum_{n\in\mathbb{Z}^+} \zeta_{|D_F|}^{-nr} n^{-s} \\
&= \frac{\tau(\chi_F)}{|D_F|} \sum_{r=1}^{|D_F|-1} \chi_F(r) \sum_{n\in\mathbb{Z}^+} \zeta_{|D_F|}^{-nr} n^{-s} \\
&= \frac{i^\delta}{|D_F|^{1/2}} \sum_{r=1}^{|D_F|-1} \chi_F(r) \sum_{n\in\mathbb{Z}^+} \zeta_{|D_F|}^{-nr} n^{-s},
\end{aligned}$$

let $s \to 1^+$ to get

$$L(\chi_F, 1) = \frac{i^\delta}{|D_F|^{1/2}} \sum_{r=1}^{|D_F|-1} \chi_F(r) \log(1 - \zeta_{|D_F|}^{-r})^{-1}.$$

Let S denote the sum in the previous display,

$$S = -\sum_{r=1}^{|D_F|-1} \chi_F(r) \log(1 - \zeta_{|D_F|}^{-r}). \tag{4}$$

A little algebraic manipulation, or a small exercise in geometry, gives the polar decomposition

$$1 - \zeta_{|D_F|}^{-r} = 2\sin(\pi r/|D_F|) e^{i(\pi/2 - \pi r/|D_F|)}.$$

Also $1-\zeta_{|D_F|}^{r}$ is the complex conjugate of $1-\zeta_{|D_F|}^{-r}$. Thus, from the general formula $\log(re^{i\theta}) = \log(r) + i\theta$,

$$\log(1 - \zeta_{|D_F|}^{\mp r}) = \log(2\sin(\pi r/|D_F|)) \pm i(\pi/2 - \pi r/|D_F|).$$

Consequently,

$$\log(1 - \zeta_{|D_F|}^{-r}) \pm \log(1 - \zeta_{|D_F|}^{r}) = \begin{cases} 2\log(2\sin(\pi r/|D_F|)) & \text{for “+”} \\ 2i(\pi/2 - \pi r/|D_F|) & \text{for “−”.} \end{cases}$$

If F is real quadratic then χ_F is even and D_F is positive, and so substituting $D_F - r$ for r in (4) gives that also (repeating (4) in the next display and also giving a second expression for S)

$$S = -\sum_{r=1}^{D_F-1} \chi_F(r) \log(1 - \zeta_{D_F}^{-r}) = -\sum_{r=1}^{D_F-1} \chi_F(r) \log(1 - \zeta_{D_F}^{r}).$$

Add the values of S shown in the previous display, making reference to the penultimate display, to get

$$S = -\sum_{r=1}^{D_F-1} \chi_F(r) \log(2\sin(\pi r/D_F)).$$

We may drop the 2 from the input to the logarithm because $\sum_r \chi_F(r) = 0$. And so in the real quadratic case, we get the claimed result upon multiplying S

by $1/\sqrt{D_F}$ and then using the symmetry of the sine function about $\pi/2$ and the value $\sin(\pi/2) = 1$,

$$\begin{aligned} L(\chi_F, 1) &= -\frac{1}{\sqrt{D_F}} \sum_{r=1}^{D_F-1} \chi_F(r) \log(\sin(\pi r/D_F)) \\ &= -\frac{2}{\sqrt{D_F}} \sum_{1 \le r < D_F/2} \chi_F(r) \log(\sin(\pi r/D_F)). \end{aligned}$$

If F is imaginary quadratic then still we have

$$\log(1-\zeta_{|D_F|}^{-r}) \pm \log(1-\zeta_{|D_F|}^{r}) = \begin{cases} 2\log(2\sin(\pi r/|D_F|)) & \text{for “+”} \\ 2i(\pi/2 - \pi r/|D_F|) & \text{for “−”}, \end{cases}$$

but now χ_F is odd, and so substituting $|D_F| - r$ for r in (4) gives that also (repeating (4) in the next display and also giving a second expression for S)

$$S = -\sum_{r=1}^{|D_F|-1} \chi_F(r) \log(1-\zeta_{|D_F|}^{-r}) = \sum_{r=1}^{|D_F|-1} \chi_F(r) \log(1-\zeta_{|D_F|}^{r}).$$

Add the values of S shown in the previous display, making reference to the penultimate display, to get

$$S = \sum_{r=1}^{|D_F|-1} \chi_F(r) i(\pi r/|D_F| - \pi/2) = \frac{\pi i}{|D_F|} \sum_{r=1}^{|D_F|-1} \chi_F(r) r.$$

And so in the imaginary quadratic case, we get the claimed result upon multiplying S by $i/|D_F|^{1/2}$,

$$L(\chi_F, 1) = -\frac{\pi}{|D_F|^{3/2}} \sum_{r=1}^{|D_F|-1} \chi_F(r) r.$$

□

15. The Dedekind zeta function of a quadratic field

The symbol $\mathfrak{a}$ denotes an integral ideal throughout this section, as compared to a nonintegral fractional ideal.

Definition 15.1. *Let F be a quadratic field. The* **Dedekind zeta function** *of F is formally (summing over ideals of $\mathcal{O}_F$ and multiplying over irreducible ideals of $\mathcal{O}_F$)*

$$\zeta_F(s) = \sum_{\mathfrak{a}} \mathrm{N}(\mathfrak{a})^{-s} = \prod_{\mathfrak{p}} (1 - \mathrm{N}(\mathfrak{p})^{-s})^{-1}.$$

The formal equality of the sum and the product follows similarly to the Euler–Riemann zeta function, this time because integral ideals factor uniquely and because the norm is multiplicative.

The Dedekind zeta function rearranges as a Dirichlet series,

$$\zeta_F(s) = \sum_{n \in \mathbb{Z}^+} \frac{a_n}{n^s} \quad \text{where } a_n = \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) = n\}.$$

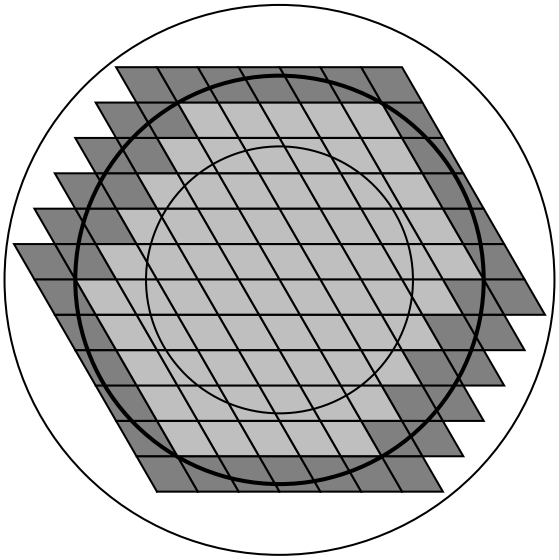

FIGURE 2. Parallelogram-tessellation approximations of a complex ball; inner, outer balls of the approximations

To analyze $\zeta_F(s)$ using summation by parts, we need to introduce

$$A_n = \sum_{k=1}^{n} a_k = \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) \le n\}, \quad n \ge 1,$$

and estimate A_n. To carry out the estimate, we will define for each of the finitely many ideal classes $\mathcal{C}$ of F

$$A_n(\mathcal{C}) = \#\{\mathfrak{a} \in \mathcal{C} : \mathrm{N}(\mathfrak{a}) \le n\}, \quad n \ge 1,$$

so that $A_n = \sum_{\mathcal{C}} A_n(\mathcal{C})$. The problem of estimating each $A_n(\mathcal{C})$ can be reduced to an estimation problem in the principal class. The principal class estimation problem is a matter of estimating the number of lattice points in a disk. Thus the following lemma will provide the key result that we need.

Lemma 15.2. *Let Λ be a complex lattice, and let α denote the area of any of its fundamental parallelograms,*

$$P(\lambda_1, \lambda_2) = \{t_1\lambda_1 + t_2\lambda_2 : t_1, t_2 \in [0, 1]\} \quad \textit{where } (\lambda_1, \lambda_2) \textit{ is a basis of } \Lambda.$$

As noted just after Proposition 10.2, α is well defined. For any $r > 0$ let B_r denote the closed complex ball of radius r. Then for some positive constant C,

$$\left| \#((\Lambda - 0) \cap B_r) - \frac{\pi r^2}{\alpha} \right| \le Cr \quad \textit{for all } r \ge 1.$$

Proof. The geometric objects in this proof are shown in figure 2. The thick circle is the boundary of B_r. Both $\#(\Lambda \cap B_r)$ and $\pi r^2/\alpha$ lie between the number of light parallelograms and the number of parallelograms altogether. The light parallelograms have more area than the inner circle, all the parallelograms less area than the outer circle. Consecutive circle radii differ by the longer diagonal of the parallelograms.

Fix a fundamental parallelogram P, and for any $\lambda \in \mathbb{C}$ let P_λ denote the λ-translate of P. For any $r \geq 0$ let

$$\begin{aligned} n_1(r) &= \#\{\lambda \in \Lambda : P_\lambda \subset B_r\}, \\ n_2(r) &= \#\{\lambda \in \Lambda : P_\lambda \cap B_r \neq \emptyset\}. \end{aligned}$$

Then

$$n_1(r) \leq \#(\Lambda \cap B_r) \leq n_2(r).$$

Let $\delta > 0$ be the length of the longer diagonal of P. Then for any $r \geq \delta$,

$$\pi(r-\delta)^2 \leq n_1(r)\alpha \leq \pi r^2 \leq n_2(r)\alpha \leq \pi(r+\delta)^2,$$

and dividing by α gives

$$\frac{\pi(r-\delta)^2}{\alpha} \leq n_1(r) \leq \frac{\pi r^2}{\alpha} \leq n_2(r) \leq \frac{\pi(r+\delta)^2}{\alpha}.$$

Thus $\#(\Lambda \cap B_r)$ and $\pi r^2/\alpha$ both lie in $[\pi(r-\delta)^2/\alpha, \pi(r+\delta)^2/\alpha]$. Consequently the absolute value of their difference is at most the interval length,

$$\left|\#(\Lambda \cap B_r) - \frac{\pi r^2}{\alpha}\right| \leq \left(\frac{4\pi\delta}{\alpha}\right) r \quad \text{for all } r \geq \delta.$$

The function $f(r) = |\#(\Lambda \cap B_r) - \pi r^2/\alpha|/r$ is bounded on $[1, \delta]$, and so in fact

$$\left|\#(\Lambda \cap B_r) - \frac{\pi r^2}{\alpha}\right| \leq Cr \quad \text{for all } r \geq 1.$$

Finally, excluding 0 from $\Lambda \cap B_r$ changes the left side by at most r because $r \geq 1$. The result follows. □

Recall that we are interested in the Dedekind zeta function of the imaginary quadratic field F, whose Dirichlet series is

$$\zeta_F(s) = \sum_{n \in \mathbb{Z}^+} \frac{a_n}{n^s} \quad \text{where } a_n = \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) = n\}.$$

As we did for the Euler–Riemann zeta function and for the quadratic field L-function, we want to estimate the absolute values of the sums

$$A_n = \sum_{k=1}^{n} a_k = \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) \leq n\}.$$

Because the a_n are nonnegative, so are the A_n. We show that A_n is roughly a certain constant multiple of n, within a multiple of $\sqrt{n}$. The constant contains the ideal class number.

Proposition 15.3. *Let F be an imaginary quadratic field. Let D_F denote the discriminant of F, let w denote the number of roots of unity in F, and let h denote the ideal class number of F. Then*

$$\left|A_n - \frac{2\pi h n}{w\sqrt{|D_F|}}\right| < C\sqrt{n}, \quad n \geq 1.$$

Proof. Let $\mathcal{C}$ be any ideal class of F, and let $\mathfrak{a}_o \in \mathcal{C}^{-1}$ be any integral ideal in the inverse class of $\mathcal{C}$. Then the map

$$\mathfrak{b} \longmapsto \mathfrak{a}_o \mathfrak{b}$$

is a bijection of the fractional ideals of F. In particular, it restricts to a bijection between two sets of integral ideals,

$$\{\mathfrak{a} \in \mathcal{C} : \mathrm{N}(\mathfrak{a}) \leq n\} \xrightarrow{\sim} \{\text{principal } \mathfrak{a}' : \mathfrak{a}_o \mid \mathfrak{a}' \text{ and } \mathrm{N}(\mathfrak{a}') \leq n\,\mathrm{N}(\mathfrak{a}_o)\}.$$

Equivalently, because to contain is to divide and because the ideal norm is the absolute value of the element norm, which is the square of the element absolute value,

$$\{\mathfrak{a} \in \mathcal{C} : \mathrm{N}(\mathfrak{a}) \leq n\} \xrightarrow{\sim} \{\langle x\rangle \subset \mathfrak{a}_o : x \neq 0,\ |x| \leq \sqrt{n\,\mathrm{N}(\mathfrak{a}_o)}\}.$$

As in the discussion leading into Lemma 15.2, define

$$A_n(\mathcal{C}) = \#\{\mathfrak{a} \in \mathcal{C} : \mathrm{N}(\mathfrak{a}) \leq n\}, \quad n \geq 1.$$

Because associate elements generate the same ideal, and because all units of $\mathcal{O}_F$ are roots of unity because F is imaginary quadratic, the previous set bijection gives

$$A_n(\mathcal{C}) = \frac{\#\left((\mathfrak{a}_o - 0) \cap B_{\sqrt{n\,\mathrm{N}(\mathfrak{a}_o)}}\right)}{w}. \tag{5}$$

Now specifically take $\mathfrak{a}_o = \langle r - d, c\rangle$ as in Proposition 11.3, and let α_o denote the area of the parallelogram spanned by c and $r - d$. By (5) and by the relation $2/\sqrt{|D_F|} = \mathrm{N}(\mathfrak{a}_o)/\alpha_o$ from Proposition 11.3, and then by Lemma 15.2,

$$\left| A_n(\mathcal{C}) - \frac{2\pi n}{w\sqrt{|D_F|}} \right| = \frac{1}{w} \left| \#\left((\mathfrak{a}_o - 0) \cap B_{\sqrt{n\,\mathrm{N}(\mathfrak{a}_o)}}\right) - \frac{\pi n\,\mathrm{N}(\mathfrak{a}_o)}{\alpha_o} \right| < C\sqrt{n}.$$

The constant C in the previous display depends on the ideal class $\mathcal{C}$. Finally, because

$$A_n = \sum_{\mathcal{C} \in \mathrm{Cl}(F)} A_n(\mathcal{C}), \quad n \geq 1,$$

sum over ideal classes and use the triangle inequality to get

$$\left| A_n - \frac{2\pi h n}{w\sqrt{|D_F|}} \right| \leq C\sqrt{n},$$

where now the constant C is independent of ideal classes. □

Proposition 15.4 (Properties of the Dedekind Zeta Function)**.** *Let F be an imaginary quadratic field. The Dedekind zeta function $\zeta_F(s)$ is analytic on $\{\mathrm{Re}(s) > 1\}$, where the formal equality of the sum and product expressions of $\zeta_F(s)$ is analytically valid. Furthermore, the Dedekind zeta function of F is the product of the Euler–Riemann zeta function and the quadratic L-function of F.*

$$\zeta_F(s) = \zeta(s)L(\chi_F, s), \quad \mathrm{Re}(s) > 1.$$

The function $\zeta_F(s)$ extends meromorphically to the open right half plane $\{s > 0\}$, and the extension has only a simple pole at $s = 1$ with residue $L(\chi_F, 1)$. That is,

$$\zeta_F(s) = \frac{L(\chi_F, 1)}{s - 1} + \psi(s), \quad \mathrm{Re}(s) > 0$$

where ψ is analytic. Thus

$$\lim_{s\to 1}(s-1)\zeta_F(s) = L(\chi_F, 1).$$

Proof. Recall that $A_n \geq 0$. Compute that by Proposition 15.3,

$$A_n - \frac{2\pi h n}{w\sqrt{|D_F|}} \leq \left| A_n - \frac{2\pi h n}{w\sqrt{|D_F|}} \right| \leq C\sqrt{n},$$

so that $A_n \leq Cn$. The analyticity of $\zeta_F(s)$ on $\{\mathrm{Re}(s) > 1\}$ follows from Proposition 12.1.

For the equality of the sum and product expressions of $\zeta_F(s)$, recall yet again that the terms of the sum rearrange as the Dirichlet series

$$\zeta_F(s) = \sum_{n\in\mathbb{Z}^+} \frac{a_n}{n^s}\,, \quad \text{where } a_n = \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) = n\}.$$

By the last statement of Proposition 12.1, the Dirichlet series converges absolutely on $\{\mathrm{Re}(s) > 1\}$. Hence so does its rearrangement $\sum_{\mathfrak{a}} \mathrm{N}(\mathfrak{a})^{-s}$, and now an argument similar to the argument for the Euler–Riemann zeta function shows the equality of this last sum and the product $\prod_{\mathfrak{p}}(1-\mathrm{N}(\mathfrak{p})^{-s})^{-1}$ on $\{\mathrm{Re}(s) > 1\}$.

As for the factorization of $\zeta_F(s)$, because

$$\left\{ \begin{aligned} \zeta_F(s) &= \prod_p \prod_{\mathfrak{p}|p\mathcal{O}_F} (1-\mathrm{N}(\mathfrak{p})^{-s})^{-1} \\ \zeta(s)\,L(\chi_F, s) &= \prod_p (1-p^{-s})^{-1}(1-\chi_F(p)p^{-s})^{-1} \end{aligned} \right\}, \quad \mathrm{Re}(s) > 1,$$

it suffices to show that for each rational prime p,

$$\prod_{\mathfrak{p}|p\mathcal{O}_F} (1-\mathrm{N}(\mathfrak{p})^{-s}) = (1-p^{-s})(1-\chi_F(p)p^{-s}).$$

But by Theorem 6.1, the decomposition of a rational prime in $\mathcal{O}_F$ is

$$p\mathcal{O}_F = \begin{cases} \mathfrak{p}\mathfrak{q} \text{ where } \mathrm{N}(\mathfrak{p}) = \mathrm{N}(\mathfrak{q}) = p & \text{if } \chi_F(p) = 1 \\ \mathfrak{p} \;\;\text{ where } \mathrm{N}(\mathfrak{p}) = p^2 & \text{if } \chi_F(p) = -1 \\ \mathfrak{p}^2 \text{ where } \mathrm{N}(\mathfrak{p}) = p & \text{if } \chi_F(p) = 0, \end{cases}$$

and so

- if $\chi_F(p) = 1$ then both sides are $(1-p^{-s})^2$,
- if $\chi_F(p) = -1$ then both sides are $1-p^{-2s}$,
- and if $\chi_F(p) = 0$ then both sides are $1-p^{-s}$.

Finally, the meromorphic continuation of $\zeta_F(s)$ follows from the properties of $\zeta(s)$ and of $L(\chi_F, s)$ because $\zeta_F(s) = \zeta(s)L(\chi_F, s)$ for $\mathrm{Re}(s) > 1$. □

Thus the equality $\zeta_F(s) = \zeta(s)L(\chi_F, s)$ is an analytic encoding of the arithmetic of $\mathcal{O}_F$.

16. The class number formula

We have not yet used the full strength of Proposition 15.3. Recall its statement that if

$$a_n = \#\{\mathfrak{a} : \mathrm{N}(\mathfrak{a}) = n\} \quad \text{and} \quad A_n = \sum_{k=1}^{n} a_k, \quad n \geq 1$$

then

$$\left| A_n - \frac{2\pi h n}{w\sqrt{|D_F|}} \right| < C\sqrt{n}, \quad n \geq 1.$$

So far we have used this only to show that A_n is $\mathcal{O}(n)$. To use the estimate in the previous display incisively, let

$$\tilde{a}_n = a_n - \frac{2\pi h}{w\sqrt{|D_F|}}, \quad n \geq 1,$$

so that the partial sums of the $\tilde{a}_n$ are

$$\widetilde{A}_n = A_n - \frac{2\pi h n}{w\sqrt{|D_F|}}, \quad n \geq 1.$$

Thus the estimate is $|\widetilde{A}_n| \leq C\sqrt{n}$ for $n \geq 1$, with the power of n now $1/2$ rather than 1, and so Proposition 12.1 says that the Dirichlet series

$$f(s) = \sum_{n \in \mathbb{Z}^+} \frac{\tilde{a}_n}{n^s} = \zeta_F(s) - \frac{2\pi h}{w\sqrt{|D_F|}}\zeta(s)$$

is analytic on $\{\mathrm{Re}(s) > 1/2\}$. In particular it is analytic at $s = 1$. Because

$$f(s) = \zeta_F(s) - \frac{2\pi h}{w\sqrt{|D_F|}}\zeta(s) \quad \text{is analytic at } s = 1,$$

and because

$$\zeta_F(s) \sim \frac{L(\chi_F, 1)}{s-1} \quad \text{and} \quad \zeta(s) \sim \frac{1}{s-1},$$

it follows that

$$L(\chi_F, 1) = \frac{2\pi h}{w\sqrt{|D_F|}}.$$

That is,

> *The tight estimate of Proposition 15.3 shows that the ideal class number of F appears in the residue of the Dedekind zeta function $\zeta_F(s)$ at $s = 1$. By Proposition 15.4, the residue is $L(\chi_F, 1)$, for which Proposition 14.3 gives a formula.*

In sum,

Theorem 16.1 (Dirichlet Class Number Formula for Imaginary Quadratic Fields)**.** *Let F be an imaginary quadratic field. Let D_F denote the discriminant of F, let w denote the number of roots of unity in F, and let h denote the ideal class number of F. Let $L(\chi_F, s)$ be the quadratic L-function of F. Then*

$$\boxed{\frac{2\pi h}{w\sqrt{|D_F|}} = L(\chi_F, 1).}$$

Conceptually the boxed formula is best left as it is, with the field structure constants h and w and D_F on one side and with the analytic quantity $L(\chi_F, 1)$ on the other. However, because we have formula (3) (page 26) from Proposition 14.3, stating that $L(\chi, 1) = \frac{\pi}{(2-\chi(2))\sqrt{|D_F|}} \sum_{1\leq r<|D_F|/2} \chi_F(r)$, the class number is

$$\boxed{h = \frac{w/2}{2-\chi(2)} \sum_{1\leq r<|D_F|/2} \chi_F(r).}$$

As an example, let $F = \mathbb{Q}(\sqrt{-5})$, so that $D_F = -20$. We have seen that the corresponding quadratic character is

$$\chi_F : (\mathbb{Z}/20\mathbb{Z})^\times \longrightarrow \{\pm 1\}, \quad \chi_F(t) = \begin{cases} 1 & \text{if } t = 1, 3, 7, 9 \\ -1 & \text{if } t = 11, 13, 17, 19, \end{cases}$$

and so the sum in the boxed formula for h is 4 and the formua gives

$$h = \frac{1}{2-0}4,$$

which is to say,

The class number of $\mathbb{Q}(\sqrt{-5})$ *is* 2.

As a second example, let $F = \mathbb{Q}(\sqrt{-39})$. The quadratic character on $(\mathbb{Z}/39\mathbb{Z})^\times$ is $(\cdot/3)(\cdot/13)$, giving

$$\chi_F(t) = \begin{cases} 1 & \text{if } t = 1, 2, 4, 5, 8, 10, 11, 16 \text{ (and } 20, 22, 25, 32) \\ -1 & \text{if } t = 7, 14, 17, 19 \text{ (and } 23, 28, 29, 31, 34, 35, 37, 38) \end{cases}$$

(as noted earlier in this writeup, the squares are concentrated more in the left half), and so the ideal class number is

$$h = \frac{1}{2-1}(8-4),$$

which is to say,

The class number of $\mathbb{Q}(\sqrt{-39})$ *is* 4.

In fact, we have already seen on page 21 that the ideal class group is cyclic of order 4.

As a third example, let $F = \mathbb{Q}(\sqrt{-163})$, noting that 163 is prime. The quadratic character is

$$\chi_F(r) = \left(\frac{-163}{r}\right) = \left(\frac{r}{163}\right).$$

One readily checks that 2 is a generator modulo 163 by using fast modular exponentiation or a machine to compute that $2^{81} = -1 \pmod{163}$ and $2^{54} = 104 \pmod{163}$. Thus the squares modulo 163 are the even powers of 2 reduced modulo 163, and similarly for the nonsquares. In particular $\chi_F(2) = -1$, and one can compute by hand or by machine that $\sum_{r=1}^{81} \chi_F(r) = 3$. So the class number formula gives

$$h = \frac{1}{2+1}3,$$

which is say,

The class number of $\mathbb{Q}(\sqrt{-163})$ *is* 1.

It is for reasons related to the class number being 1 that the number

$$e^{\pi\sqrt{163}/3} = 640320.0000000006\dots$$

is so nearly an integer.

Recall that for a *real* quadratic number field F, there is a unique smallest *fundamental unit* $u > 1$ in the unit group $\mathcal{O}_F^\times$. We end by stating that in this case the class number theorem is similar to Theorem 16.1 but incorporates the fundamental unit,

$$\boxed{\frac{2\log(u)h}{\sqrt{D_F}} = L(\chi_F, 1).}$$

Much of the argument is similar to the work in this writeup. The main difference is that the counterpart of Proposition 15.3 requires a different approach.