

## THE DIRICHLET CLASS NUMBER FORMULA FOR IMAGINARY QUADRATIC FIELDS

The factorizations

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

show that unique factorization fails in the ring

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

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

These notes present a formula that in some sense measures the extent to which unique factorization fails in environments such as  $\mathbf{Z}[\sqrt{-5}]$ . Algebra lets us define a group that measures the failure, geometry shows that the group is finite, and analysis yields the formula for its 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

[www.math.umass.edu/~weston/oldpapers/cnf.pdf](http://www.math.umass.edu/~weston/oldpapers/cnf.pdf)

for the 2004 Ross mathematics program. The class number formula in general is discussed in many number theory books, for example the books by Marcus and by Borevich and Shafarevich.

### Part 1. ALGEBRA: QUADRATIC NUMBER FIELDS

This part of these notes discusses *quadratic number fields* (fields like  $\mathbf{Q}(\sqrt{-5})$ ) and their *rings of integers* (rings like  $\mathbf{Z}[\sqrt{-5}]$ ). 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  $\mathbf{C}$ ) such that  $F$  has dimension 2 as a vector space over  $\mathbf{Q}$ . Such a field takes the form

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

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

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

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

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

Specifically,

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

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

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

Specifically,

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

If  $F$  is imaginary quadratic then the norm is positive on  $F^\times$ .

Because convolution is an involution, it has no effect on trace and norm, i.e.,  $\text{tr}(\overline{\alpha}) = \text{tr}(\alpha)$  for all  $\alpha \in F$  and  $\text{N}(\overline{\alpha}) = \text{N}(\alpha)$  for all  $\alpha \in F^\times$ .

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

Thus the integers of  $F \cap \mathbf{Q}$  (the **rational integers** of  $F$ ) are  $\mathbf{Z}$ . An element  $\alpha$  of  $F - \mathbf{Q}$  has quadratic minimal polynomial

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

and so  $\alpha = a + b\sqrt{n}$  is an algebraic integer if and only if its trace  $2a$  and its norm  $a^2 - b^2n$  are rational integers. Inspection shows that consequently,

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

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

*The integers of  $F$  form a ring.*

The minimal monic polynomial in  $\mathbf{Z}[X]$  satisfied by the generator  $g$  of the integers (see the previous proposition) is quadratic,

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

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

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

The discriminant of the quadratic polynomial (the quantity  $b^2 - 4ac$  that goes under the square root in the quadratic formula) is therefore  $n$  if  $n \equiv 1 \pmod{4}$  and  $4n$  if  $n \equiv 2, 3 \pmod{4}$ . This quantity, an *invariant* of the quadratic field  $F$ , plays a significant role in the structure of  $F$ ; in the present writeup it will manifest itself in the class number formula.

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

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

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

$$\mathcal{O}_F = \mathbf{Z} \left[ \frac{D_F + \sqrt{D_F}}{2} \right],$$

and similarly we will see that the discriminant gives uniform descriptions of various phenomena associated with  $F$ .

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  $\mathcal{O}_F = g\mathbf{Z} \oplus \mathbf{Z}$  as before), although  $g$  itself involves cases,

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

and

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

## 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  $\alpha$  of  $F^\times$  is a unit if and only if  $N(\alpha) = \pm 1$ .*

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

$$1 = N(1) = N(\alpha\beta) = N(\alpha)N(\beta),$$

so that  $N(\alpha) = \pm 1$  since both norms are integers. Conversely, if  $N(\alpha) = \pm 1$  then  $\alpha$  is invertible by  $\pm\bar{\alpha} \in \mathcal{O}_F$  since  $\pm\alpha\bar{\alpha} = \pm N(\alpha) = 1$ .  $\square$

If  $K = \mathbf{Q}(\sqrt{n})$  is imaginary quadratic then all norms  $a^2 - b^2n$  are nonnegative, and inspection shows that the unit group is

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

If  $K = \mathbf{Q}(\sqrt{n})$  is real quadratic then the unit group takes the form

$$\mathcal{O}_F^\times = \{\pm u^n : n \in \mathbf{Z}\} \approx (\mathbf{Z}/2\mathbf{Z}) \times \mathbf{Z}$$

where  $u > 1$  is the so-called **fundamental unit**. Finding the fundamental unit is the not-immediate matter of solving (the misnamed) Pell's Equation,  $x^2 - ny^2 = 1$ .

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

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

For imaginary quadratic fields  $F$  the number  $w(F)$  completely describes the unit group. For real quadratic fields the fundamental unit  $u$  is necessary for a full description. The more complicated unit group structure for real quadratic fields is the 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 qualities, and our concern here is with the unique factorization of nonzero ideals, so it is tidier to exclude  $\{0\}$  from the discussion.

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

$$\mathfrak{a} + \mathfrak{a}' = (x + x' : x \in \mathfrak{a}, x' \in \mathfrak{a}'),$$

and similarly for the product,

$$\mathfrak{a}\mathfrak{a}' = (xx' : x \in \mathfrak{a}, x' \in \mathfrak{a}').$$

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 ideal.

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

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

The existence of the ideal norm 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,

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

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

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

so that

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

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

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

A principal ideal is denoted by its generator in parentheses,

$$(x) = x\mathcal{O}_F.$$

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

$$\text{For a principal ideal } \mathfrak{a} = (x), \quad N(\mathfrak{a}) = |N(x)|.$$

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  $\mathfrak{a}\bar{\mathfrak{a}} = d\mathcal{O}_F$  for some  $d \in \mathbf{Z}^+$ .

*Proof.* The product  $\mathfrak{a}\bar{\mathfrak{a}}$  contains elements  $x\bar{x} = N(x)$  where  $x \in \mathfrak{a}$ , 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  $\mathfrak{a}\bar{\mathfrak{a}}$  show that  $\mathfrak{a}\bar{\mathfrak{a}} \cap \mathbf{Z} = d\mathbf{Z}$ .

Since the product  $\mathfrak{a}\bar{\mathfrak{a}}$  is an ideal, it contains  $d\mathcal{O}_F$ . That is,  $\mathfrak{a}\bar{\mathfrak{a}} \supset d\mathcal{O}_F$ . For the other containment, it suffices to show that for any  $x, y \in \mathfrak{a}$  the product  $x\bar{y}$  lies in  $d\mathcal{O}_F$ . The quantities

$$\text{tr}(x\bar{y}) = x\bar{y} + \bar{x}y, \quad N(x) = x\bar{x}, \quad N(\bar{y}) = y\bar{y}$$

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

$$\text{tr}(x\bar{y}/d) = \text{tr}(x\bar{y})/d \in \mathbf{Z} \quad \text{and} \quad N(x\bar{y}/d) = N(x)/d \cdot N(\bar{y})/d \in \mathbf{Z}.$$

Thus  $x\bar{y}/d \in \mathcal{O}_F$ , i.e.,  $x\bar{y} \in d\mathcal{O}_F$ . This gives the other containment  $\mathfrak{a}\bar{\mathfrak{a}} \subset d\mathcal{O}_F$ , completing the proof.  $\square$

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  $\mathbf{C}$  that has finite dimension as a vector space over  $\mathbf{Q}$ . 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

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

*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  $\mathfrak{a}\bar{\mathfrak{a}} \subset \mathfrak{a}'\bar{\mathfrak{a}} = N(\mathfrak{a}')\mathcal{O}_F$  and thus  $\mathfrak{a}\bar{\mathfrak{a}}/N(\mathfrak{a}')$  is an ideal of  $\mathcal{O}_F$ . Since  $\mathfrak{a}' \cdot \mathfrak{a}\bar{\mathfrak{a}}/N(\mathfrak{a}') = \mathfrak{a}$ , indeed  $\mathfrak{a}' \mid \mathfrak{a}$ .  $\square$

One direction in the preceding proof made use of the ideal norm, although the other direction was general. Thus the ensuing arguments that use the *to contain is to divide* principle are particular to rings having an ideal norm.

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

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

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

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

So *prime* means *doesn't decompose as a divisor* and *irreducible* means *doesn't decompose as a product*.

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

*Proof.* Consider any prime ideal  $\mathfrak{a}$  of  $\mathcal{O}_F$ . If  $\mathfrak{a} = \mathfrak{a}'\mathfrak{a}''$  then  $\mathfrak{a}' \mid \mathfrak{a}$  and (without loss of generality)  $\mathfrak{a} \mid \mathfrak{a}'$ . Thus  $\mathfrak{a} \subset \mathfrak{a}'$  and  $\mathfrak{a}' \subset \mathfrak{a}$ , and so  $\mathfrak{a}' = \mathfrak{a}$ .  $\square$

Since to contain is to divide, irreducible ideals are maximal. Thus the previous proposition has shown that prime ideals of  $\mathcal{O}_F$  are maximal. In a general commutative ring with 1, prime ideals certainly need not be maximal, since essentially by definition the quotient of a ring by a prime ideal is an integral domain whereas the quotient of a ring by a maximal ideal is a field. The previous sentence proves the next proposition immediately, but we prove it in more elementary terms as well. To streamline the proof, use the fact that in the quadratic field context, since to contain is to divide, the definition of irreducibility rephrases for ideals (with help from the cancellation law) as maximality:

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

**Proposition 4.4.** Irreducible ideals of  $\mathcal{O}_F$  are prime.

*Proof.* Consider any irreducible ideal  $\mathfrak{a}$  of  $\mathcal{O}_F$ . Suppose that  $\mathfrak{a} \mid \mathfrak{a}'\mathfrak{a}''$  and  $\mathfrak{a} \nmid \mathfrak{a}'$ . The containment  $\mathfrak{a} + \mathfrak{a}' \supset \mathfrak{a}$  is proper, so  $\mathfrak{a} + \mathfrak{a}' = \mathcal{O}_F$ , and so  $x + x' = 1$  for some  $x \in \mathfrak{a}$  and  $x' \in \mathfrak{a}'$ . For any  $x'' \in \mathfrak{a}''$ ,

$$x'' = (x + x')x'' = xx'' + x'x'' \in \mathfrak{a} + \mathfrak{a}'\mathfrak{a}'' = \mathfrak{a}.$$

Thus  $\mathfrak{a}'' \subset \mathfrak{a}$ , i.e.,  $\mathfrak{a} \mid \mathfrak{a}''$  and we are done.  $\square$

**Theorem 4.5.** 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  $N(\mathfrak{a})$ . The fact that irreducibles are prime makes the factorization unique, since if

$$\mathfrak{a} = \mathfrak{p}_1^{e_1} \cdots \mathfrak{p}_s^{e_s} = \tilde{\mathfrak{p}}_1^{f_1} \cdots \tilde{\mathfrak{p}}_t^{f_t}$$

where all  $\mathfrak{p}_i$  and  $\tilde{\mathfrak{p}}_j$  are irreducible, then

$$\mathfrak{p}_1 \mid \tilde{\mathfrak{p}}_1^{f_1} \cdots \tilde{\mathfrak{p}}_s^{f_s}$$

so that since  $\mathfrak{p}_1$  is prime we have (after reindexing if necessary)  $\mathfrak{p}_1 \mid \tilde{\mathfrak{p}}_1$ , and thus

$$\mathfrak{p}_1 = \tilde{\mathfrak{p}}_1.$$

Repeat the argument from here starting from (by cancellation)

$$\mathfrak{p}_1^{e_1-1} \cdots \mathfrak{p}_s^{e_s} = \tilde{\mathfrak{p}}_1^{f_1-1} \cdots \tilde{\mathfrak{p}}_t^{f_t}.$$

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

## 5. THE CHARACTER OF A QUADRATIC FIELD

We continue to consider a quadratic field  $F = \mathbf{Q}(\sqrt{n})$  where  $n$  is squarefree. Recall that the field's discriminant is defined as

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

Extend the Legendre symbol to allow denominator 2 as follows:

$$\begin{aligned} \left(\frac{a}{2}\right) &= \begin{cases} (2/|a|) & \text{if } a \equiv 1 \pmod{2}, \\ 0 & \text{if } a \equiv 0 \pmod{2} \end{cases} \\ &= \begin{cases} 1 & \text{if } a \equiv 1, 7 \pmod{8}, \\ -1 & \text{if } a \equiv 3, 5 \pmod{8}, \\ 0 & \text{if } a \equiv 0 \pmod{2}. \end{cases} \end{aligned}$$

Thus  $(a/2)$  depends on  $a \pmod{8}$ . The Jacobi symbol extends correspondingly to arbitrary positive integer denominator,

$$\text{if } m = \prod_{p \in \mathcal{P}} p^{e_p} \text{ then } \left(\frac{a}{m}\right) = \prod_{p \in \mathcal{P}} \left(\frac{a}{p}\right)^{e_p}.$$

If  $m$  is even then  $(a/m)$  as a function of its numerator no longer need depend only on  $a \pmod{m}$ .

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

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

**Proposition 5.2.** Let  $F$  be a quadratic field with discriminant  $D_F$ . Then the quadratic character  $\chi_F$  has period  $|D_F|$ .

*Proof.* Other than the presence of powers of 2 in  $D_F$ , the proposition is merely a matter of quadratic reciprocity. To handle the powers of 2 gracefully, recall that the function of odd positive integers  $m$

$$\left(\frac{-1}{m}\right) = \begin{cases} 1 & \text{if } m \equiv 1 \pmod{4}, \\ -1 & \text{if } m \equiv 3 \pmod{4} \end{cases}$$

has period 4, and the function of odd positive integers  $m$

$$\left(\frac{2}{m}\right) = \begin{cases} 1 & \text{if } m \equiv 1, 7 \pmod{8}, \\ -1 & \text{if } m \equiv 3, 5 \pmod{8} \end{cases}$$

has period 8, so that their product

$$\left(\frac{-2}{m}\right) = \begin{cases} 1 & \text{if } m \equiv 1, 3 \pmod{8}, \\ -1 & \text{if } m \equiv 5, 7 \pmod{8} \end{cases}$$

again has period 8.

Let  $F = \mathbf{Q}(\sqrt{n})$ .

If  $n \equiv 1 \pmod{4}$  then  $D_F = n$ . For  $m = 2^e m'$  with  $e \geq 0$  and  $m'$  odd,

$$\chi_F(m) = \left(\frac{D_F}{m}\right) = \left(\frac{n}{2^e m'}\right) = \left(\frac{n}{2}\right)^e \left(\frac{n}{m'}\right) = \left(\frac{2}{|n|}\right)^e \left(\frac{m'}{|n|}\right) = \left(\frac{m}{|n|}\right),$$

which has period  $|n| = |D_F|$ .

If  $n = 3 \pmod{4}$  then  $D_F = 4n$  and  $n$  is odd. For  $m$  odd,

$$\chi_F(m) = \left(\frac{D_F}{m}\right) = \left(\frac{n}{m}\right) = (-1)^{\frac{m-1}{2}} \left(\frac{m}{|n|}\right) = \left(\frac{-1}{m}\right) \left(\frac{m}{|n|}\right).$$

Since  $(-1/m)$  has period 4 and  $(m/|n|)$  has period  $|n|$ , it follows that  $\chi_F(m)$  has period  $4|n| = |D_F|$ . For  $m$  even,  $\chi_F(m) = 0$ , which certainly depends only on  $m \pmod{|D_F|}$ . The parity of  $m$  also depends only on  $m \pmod{|D_F|}$ , so that the two cases don't somehow intertwine.

If  $n = 2 \pmod{4}$  then  $D_F = 4n = 8n'$  where  $n'$  is odd. For  $m$  odd,

$$\begin{aligned} \chi_F(m) &= \left(\frac{D_F}{m}\right) = \left(\frac{2n'}{m}\right) = \left(\frac{2}{m}\right) (-1)^{\frac{n'-1}{2} \cdot \frac{m-1}{2}} \left(\frac{m}{|n'|}\right) \\ &= \begin{cases} \left(\frac{2}{m}\right) \left(\frac{m}{|n'|}\right) & \text{if } n' = 1 \pmod{4}, \\ \left(\frac{-2}{m}\right) \left(\frac{m}{|n'|}\right) & \text{if } n' = 3 \pmod{4}. \end{cases} \end{aligned}$$

Since  $(2/m)$  and  $(-2/m)$  have period 8 and  $(m/|n'|)$  has period  $|n'|$ , it follows that  $\chi_F(m)$  has period  $8|n'| = |D_F|$ . And again  $\chi_F(m) = 0$  for  $m$  even.  $\square$

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

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

defined by

$$\chi_F(m + |D_F|\mathbf{Z}) = \begin{cases} (m/|n|) & \text{if } n = 1 \pmod{4}, \\ (-1)^{(m-1)/2} (m/|n|) & \text{if } n = 3 \pmod{4}, \\ (m/2)(m/|n/2|) & \text{if } n = 2 \pmod{8}, \\ (-1)^{(m-1)/2} (m/2)(m/|n/2|) & \text{if } n = 6 \pmod{8}. \end{cases}$$

(In the preceding formula we can no longer write  $(-1/m)$  or  $(\pm 2/m)$  because  $m$  is no longer assumed to be positive.) As usual, we extend the definition to  $\mathbf{Z}/|D_F|\mathbf{Z}$ ,

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

It is an exercise to check that

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

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.

## 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*

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

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

(Proof to be added. For now, see Ireland and Rosen pp.190–191.)

For one example, note that if  $F = \mathbf{Q}(i)$ , so that  $\mathcal{O}_F = \mathbf{Z}[i]$  is the ring of Gaussian integers, then the quadratic character is

$$\chi_F : (\mathbf{Z}/4\mathbf{Z})^\times \longrightarrow \mathbf{C}^\times, \quad \chi_F(m) = (-1)^{(m-1)/2}.$$

Similarly, if  $F = \mathbf{Q}(\sqrt{-3})$ , so that  $\mathcal{O}_F = \mathbf{Z}[\zeta_3]$  is the ring of Eisenstein integers, then the quadratic character is

$$\chi_F : (\mathbf{Z}/3\mathbf{Z})^\times \longrightarrow \mathbf{C}^\times, \quad \chi_F(m) = (m/3).$$

If  $F = \mathbf{Q}(\sqrt{-5})$ , so that  $\mathcal{O}_F = \mathbf{Z}[\sqrt{-5}]$ , then the quadratic character is

$$\chi_F : (\mathbf{Z}/20\mathbf{Z})^\times \longrightarrow \mathbf{C}^\times, \quad \chi_F(m) = (-1)^{(m-1)/2}(m/5).$$

## 7. FRACTIONAL IDEALS AND THE IDEAL CLASS GROUP

**Definition 7.1.** *A fractional ideal of  $F$  is*

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

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  $F$ .

Since 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  $\alpha\mathfrak{a} \cdot (\alpha N(\mathfrak{a}))^{-1}\bar{\mathfrak{a}} = \mathcal{O}_F$  shows that

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

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

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

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 7.2.** *The ideal class group of  $F$  is the quotient group*

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

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.

## 8. 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 8.1.** *Let  $\mathfrak{b}$  be a fractional ideal of  $F$ . Then  $\mathfrak{b}$  takes the form*

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

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

*Proof.* Since 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  $\mathfrak{a}$ . Since  $\mathfrak{a}\bar{\mathfrak{a}} = N(\mathfrak{a})\mathcal{O}_F$ , we have

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

Recall that  $F = \mathbf{Q}(\sqrt{n})$  where  $n \in \mathbf{Z}$  is squarefree, and that  $\mathcal{O}_F = g\mathbf{Z} \oplus \mathbf{Z}$  where

$$g = \begin{cases} \frac{1+\sqrt{n}}{2} & \text{if } n \equiv 1 \pmod{4}, \\ \sqrt{n} & \text{if } n \equiv 2, 3 \pmod{4}. \end{cases}$$

The previously displayed containments are

$$N(\mathfrak{a})g\mathbf{Z} \oplus N(\mathfrak{a})\mathbf{Z} \subset \mathfrak{a} \subset g\mathbf{Z} \oplus \mathbf{Z}.$$

Since 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 not trivial, but it is a matter of algebra rather than number theory.)  $\square$

**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  $h$ .

## 9. COMPLEX LATTICES AND HOMOTHETY

**Definition 9.1.** A **complex lattice** is a rank-2 abelian subgroup of  $\mathbf{C}$ ,

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

Note that in particular, any fractional ideal of an imaginary quadratic field is a complex lattice. (Proposition 8.1 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  $\mathbf{Z}$ -basis  $\{\lambda_1, \lambda_2\}$  determines the lattice  $\Lambda$ , but not conversely. We adopt the convention that lattice bases are *ordered* and that furthermore they are always ordered so that  $\text{Im}(\lambda_1/\lambda_2) > 0$ . Then (exercise)

**Proposition 9.2.** *The ordered pairs of nonzero complex numbers  $(\lambda_1, \lambda_2)$  and  $(\lambda'_1, \lambda'_2)$  are bases for the same lattice  $\Lambda$  if and only if*

$$\begin{bmatrix} \lambda'_1 \\ \lambda'_2 \end{bmatrix} = \begin{bmatrix} a & b \\ c & d \end{bmatrix} \begin{bmatrix} \lambda_1 \\ \lambda_2 \end{bmatrix} \quad \text{for some } \begin{bmatrix} a & b \\ c & d \end{bmatrix} \in \text{SL}_2(\mathbf{Z}).$$

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

It follows that if  $\Lambda$  is a lattice and  $(\lambda_1, \lambda_2)$  is a basis of  $\Lambda$  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 on  $\Lambda$ , not on the choice of basis. This is because if  $(\lambda_1, \lambda_2)$  and  $(\lambda'_1, \lambda'_2)$  are bases then the linear map taking  $\lambda_i$  to  $\lambda'_i$  for  $i = 1, 2$  preserves area because it has determinant 1.

**Definition 9.3.** Two lattices  $\Lambda$  and  $\Lambda'$  are **homothetic** if

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

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 9.4.** *Let  $\Lambda$  be a complex lattice. Then  $\Lambda$  has nonzero elements of least modulus.*

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

Now let a lattice  $\Lambda$  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  $\Lambda - \mathbf{Z}$  having least modulus; we may assume that  $\text{Im}(\tau) > 0$ . Then  $|\tau| \geq 1$ , and also  $|\text{Re}(\tau)| \leq 1/2$ , else some  $\tau + n$  (where  $n \in \mathbf{Z}$ ) has smaller modulus. Thus  $\tau$  lies in the **fundamental domain**,

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

And so every lattice is homothetic to a lattice

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

Furthermore,  $\tau$  is essentially unique. One type of exception to uniqueness is easy to find: if  $\text{Re}(\tau) = -1/2$  then also  $\Lambda = (\tau + 1)\mathbf{Z} \oplus \mathbf{Z}$  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)

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

But  $-\tau^{-1}$  is also on the circular arc of the boundary of  $D$ , being the horizontal reflection of  $\tau$ . And so the left and right halves of the semicircular boundary arc of  $D$  should be identified as well. Otherwise,  $\tau$  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  $D$ ,

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

A lattice  $\Lambda_\tau$  where  $\tau$  satisfies the three previous conditions is **normalized**.

## 10. COMPLEX MULTIPLICATION

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

**Definition 10.1.** *Let  $\Lambda$  be a lattice. If*

$$m\Lambda \subset \Lambda \quad \text{for some } m \in \mathbf{C} - \mathbf{Z}$$

*then  $\Lambda$  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  $\Lambda_\tau$ .

To study which such CM-values  $m$  are possible for which lattices  $\Lambda_\tau$ , assume that  $\Lambda_\tau$  has CM by  $m$ . Thus

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

Thus  $m$  is an eigenvalue of the matrix. Since we are assuming that  $m \notin \mathbf{Z}$ , the condition  $m \in \mathbf{R}$  is impossible, e.g., it would force  $m = d$ . So  $m$  is an imaginary quadratic algebraic integer. Furthermore, since  $m = c\tau + d$  (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  $F = \mathbf{Q}(\sqrt{n})$  where  $n \in \mathbf{Z}_{<0}$  is squarefree. Recall that the generator of the integer ring  $\mathcal{O}_F$  is

$$g = \begin{cases} \frac{1+\sqrt{n}}{2} & \text{if } n \equiv 1 \pmod{4}, \\ \sqrt{n} & \text{if } n \equiv 2, 3 \pmod{4}. \end{cases}$$

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  $g$  of the integer ring  $\mathcal{O}_F$ . To find all normalized lattices  $\Lambda_\tau \subset F$  having complex multiplication by  $g$  is precisely to find a set of representatives of the ideal class group of  $F$ .*

Recall that *normalized* means that  $\tau$  satisfies the three conditions at the end of the previous section.

Consider the case  $n \equiv 2, 3 \pmod{4}$ . The condition for CM by  $\sqrt{n}$  is

$$\begin{bmatrix} \tau \\ 1 \end{bmatrix} \in \ker \begin{bmatrix} a - \sqrt{n} & b \\ c & d - \sqrt{n} \end{bmatrix} \neq \{0\} \quad \text{for some } a, b, c, d \in \mathbf{Z}.$$

A bit of algebra, including the fact that the kernel is nonzero exactly when the determinant vanishes, shows that

$$\tau = \frac{-d + \sqrt{n}}{c}, \quad c, d \in \mathbf{Z},$$

satisfying the conditions

- $0 < c \leq 2\sqrt{-n/3}$ ,
- $-c \leq 2d < c$ ,
- $c^2 < d^2 - n$  if  $d > 0$ ,  $c^2 \leq d^2 - n$  if  $d \leq 0$ ,
- $c \mid d^2 - n$ .

Thus there exist only finitely such  $\tau$ -values, easy to find by hand if  $|n|$  is small and easy to find by algorithm in any case. The analysis for  $n \equiv 1 \pmod{4}$  is similar, leading to

$$\tau = \frac{-d + \sqrt{n}}{c}, \quad c, d \in \mathbf{Z}, \quad c \text{ even and } d \text{ odd}$$

satisfying the conditions

- $0 < c \leq 2\sqrt{-n/3}$ ,
- $-c \leq 2d < c$ ,
- $c^2 < d^2 - n$  if  $d > 0$ ,  $c^2 \leq d^2 - n$  if  $d \leq 0$ ,
- $2c \mid d^2 - n$ .

We have shown

**Theorem 10.2.** *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  $g$ , corresponding to the identity element of the ideal class group. And indeed, the lattice  $\mathcal{O}_F = \Lambda_g$  works.

Our goal is a formula for  $h(F)$ . The formula requires elements of analytic number theory, to be presented in the third part of these notes, in addition to the algebra of the first part and the geometry of the second. The following proposition will be cited in the course of the analysis.

**Proposition 10.3.** *Let  $F$  be an imaginary quadratic field, and let  $D_F$  be the discriminant of  $F$ . Let*

$$\mathfrak{a} = (c, -d + \sqrt{n}) \quad \text{with } c \text{ and } d \text{ as just above,}$$

and let  $\alpha$  denote the area of the parallelogram spanned by  $c$  and  $-d + \sqrt{n}$ . Then

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

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  $F$ .

*Proof.* We will compute that

$$N(\mathfrak{a}) = \begin{cases} 2c & \text{if } n \equiv 1 \pmod{4}, \\ c & \text{if } n \equiv 2, 3 \pmod{4}. \end{cases}$$

The desired result follows,

$$\begin{aligned} \frac{N(\mathfrak{a})}{\alpha} &= \begin{cases} 2c/(c\sqrt{-n}) = 2/\sqrt{-n} & \text{if } n \equiv 1 \pmod{4}, \\ c/(c\sqrt{-n}) = 1/\sqrt{-n} & \text{if } n \equiv 2, 3 \pmod{4} \end{cases} \\ &= \frac{2}{\sqrt{|D_F|}} \quad \text{in all cases.} \end{aligned}$$

For the norm computation, let  $q = (d^2 - n)/c$ . Since

$$\mathfrak{a}\bar{\mathfrak{a}} = (c^2, c(d + \sqrt{n}), c(d - \sqrt{n}), d^2 - n) = c(c, d + \sqrt{n}, d - \sqrt{n}, q),$$

and since  $\mathfrak{a}\bar{\mathfrak{a}} \cap \mathbf{Z} = N(\mathfrak{a})\mathbf{Z}$ , it suffices to show that

$$(c, d + \sqrt{n}, d - \sqrt{n}, q) \cap \mathbf{Z} = \begin{cases} 2\mathbf{Z} & \text{if } n \equiv 1 \pmod{4}, \\ \mathbf{Z} & \text{if } n \equiv 2, 3 \pmod{4}. \end{cases}$$

The left side contains  $\gcd(c, 2d, q)\mathbf{Z}$ . Let  $g = \gcd(c, d, q)$  (yes, with  $d$  rather than  $2d$  here). Then  $(d^2 - n)/c = q = q'g$  for some  $q'$ , and  $c = c'g$  for some  $c'$ , and so  $g^2 \mid qc = d^2 - n$ . Since also  $g^2 \mid d^2$ , it follows that  $g^2 \mid n$ . But  $n$  is squarefree, so  $g = 1$ . Thus

$$\gcd(c, 2d, q) \in \{1, 2\}.$$

The gcd in the previous display is 2 exactly when  $c$  is even,  $d$  is odd, and  $q$  is even; since  $q = (d^2 - n)/c$  this forces  $n \equiv 1 \pmod{4}$ . Conversely, if  $n \equiv 1 \pmod{4}$  then the normalizing conditions on  $c$  and  $d$  show that the gcd in the previous display is 2.

So if  $n \not\equiv 1 \pmod{4}$  then  $(c, 2d, q) \cap \mathbf{Z} = \mathbf{Z}$  and thus in this case the superset  $(c, d + \sqrt{n}, d - \sqrt{n}, q) \cap \mathbf{Z}$  is also  $\mathbf{Z}$  as desired.

If  $n \equiv 1 \pmod{4}$ , then we have shown that  $(c, 2d, q) \cap \mathbf{Z} = 2\mathbf{Z}$ , but what we need to show is that the superset  $(c, d + \sqrt{n}, d - \sqrt{n}, q) \cap \mathbf{Z}$  is  $2\mathbf{Z}$ , and so the final nagging point is that conceivably the superset is all of  $\mathbf{Z}$  instead. But this can not happen: the calculations

$$\frac{1 + \sqrt{n}}{2} \cdot 2d = d + \sqrt{n}, \quad 2d - (d + \sqrt{n}) = d - \sqrt{n}$$

show that in fact  $(c, d + \sqrt{n}, d - \sqrt{n}, q) = (c, 2d, q)$ , and so their intersections with  $\mathbf{Z}$  are equal as well.  $\square$

**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

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

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.

11. SUMMATION BY PARTS

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

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

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

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

The formula is easy to verify since

$$a_k b_k + A_k \Delta b_k = A_k b_{k+1} - A_{k-1} b_k.$$

**Proposition 11.1.** *Let  $\{a_n\}_{n \geq 1}$  be a complex sequence such that for some positive numbers  $C$  and  $r$ ,*

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

*Then the Dirichlet series*

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

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

*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

$$s = \sigma + it$$

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

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

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  $1 \leq m \leq n$ ,

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

Let  $n \rightarrow \infty$  to see that for all large enough  $m \geq 1$ ,

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

If  $\sigma > r$  then the right side goes to 0 as  $m \rightarrow \infty$ . 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  $f(s) = \sum_{n \in \mathbf{Z}^+} a_n n^{-s}$  converges uniformly on  $K$ . Since the partial sums of  $f(s)$  are analytic on  $\{\operatorname{Re}(s) > r\}$ , their uniform convergence on compacta is the hypothesis for a standard theorem of complex analysis that then says that  $f(s)$  is analytic on  $\{\operatorname{Re}(s) > r\}$  as well.

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

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

And so  $f(s)$  converges absolutely since  $f(\sigma)$  converges.  $\square$

A slogan-encapsulation of Proposition 11.1 is

$$\left| \sum_{k=1}^n a_k \right| = \mathcal{O}(n^r) \implies \sum \frac{a_n}{n^s} \text{ is well-behaved on } \{\operatorname{Re}(s) > r\}.$$

## 12. THE EULER-RIEMANN ZETA FUNCTION

**Definition 12.1.** *The Euler–Riemann zeta function is formally*

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

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

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

**Proposition 12.2** (Properties of the Euler–Riemann Zeta Function). *The function  $\zeta(s)$  is complex analytic on the open right half plane  $\{\operatorname{Re}(s) > 1\}$ , 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  $\{\operatorname{Re}(s) > 0\}$ , and the extension has only a simple pole at  $s = 1$  with residue 1. That is,*

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

where  $\psi$  is analytic.

*Proof.* The fact that  $\zeta(s)$  is complex analytic on  $\operatorname{Re}(s) > 1$  follows from Proposition 11.1 with  $C = r = 1$  since  $\{a_i\}$  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  $\operatorname{Re}(s) > 1$  to rearrange the terms since the sum converges absolutely. As  $B \rightarrow \infty$  the sum converges to  $\zeta(s)$  since 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  $-\psi(s)$ . Since 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  $\{\operatorname{Re}(s) > 0\}$  by the convergence properties of  $|s| \sum_n n^{-\sigma-1}$ .  $\square$

### 13. 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,

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

(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 13.1.** *Let  $F$  be a quadratic field with discriminant  $D_F$ . The **quadratic  $L$ -function** of  $F$  is formally*

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

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

**Proposition 13.2** (Properties of the Quadratic  $L$ -Function). *The quadratic  $L$ -function  $L(\chi_F, s)$  is complex analytic on  $\{\operatorname{Re}(s) > 0\}$ . The formal equality of the sum and product expressions of  $L(\chi_F, s)$  is analytically valid for  $\operatorname{Re}(s) > 1$ .*

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

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

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

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

Now Proposition 11.1 shows that  $L(\chi_F, s)$  is analytic on  $\{\operatorname{Re}(s) > 0\}$ . The argument that the sum and the product are equal is essentially the same as for the Euler–Riemann zeta function, requiring  $\operatorname{Re}(s) > 1$  for absolute convergence so that terms can be rearranged.  $\square$

In particular,  $L(\chi_F, 1)$  can be evaluated as a finite sum of Gauss sums times factors, where the factors are logarithms of sines if  $F$  is real quadratic and the factors are finite sums if  $F$  is imaginary quadratic. The value  $L(\chi_F, 1)$  will figure in the class number formula.

**Proposition 13.3** (Special Value of the Quadratic  $L$ -Function). *Let  $F$  be a quadratic field. Let  $\tau(\chi_F)$  denote its Gauss sum,*

$$\tau(\chi_F) = \sum_{t=0}^{|D_F|-1} \chi_F(t) \zeta_{|D_F|}^t \quad \text{where} \quad \zeta_{|D_F|} = e^{2\pi i/|D_F|}.$$

*If  $F$  is real quadratic then*

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

*If  $F$  is imaginary quadratic then*

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

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

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

The inner sum is

$$\sum_{\substack{n \in \mathbf{Z}^+ \\ n \equiv t \pmod{|D_F|}}} n^{-s} = \sum_{n \in \mathbf{Z}^+} a_n(t) n^{-s} \quad \text{where} \quad a_n(t) = \begin{cases} 1 & \text{if } n \equiv t \pmod{|D_F|}, \\ 0 & \text{if } n \not\equiv t \pmod{|D_F|}, \end{cases}$$

and the casewise coefficient has a uniform description as a finite geometric sum,

$$a_n(t) = \frac{1}{|D_F|} \sum_{r=0}^{|D_F|-1} \zeta_{|D_F|}^{(t-n)r}.$$

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

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

Let  $\tau_r(\chi_F)$  denote the variant Gauss sum that has appeared in the calculation,

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

and let  $s \rightarrow 1^+$  to get

$$L(\chi_F, 1) = \frac{1}{|D_F|} \sum_{r=0}^{|D_F|-1} \tau_r(\chi_F) \sum_{n \in \mathbf{Z}^+} \zeta_{|D_F|}^{-nr} n^{-1}.$$

The inner sum is  $\log(1 - \zeta_{|D_F|}^{-r})^{-1}$ . Also, the variant Gauss sum works out to

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

where  $\tau(\chi_F)$  is the basic Gauss sum. When  $\gcd(r, |D_F|) = 1$  the 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  $r = 0$ ) is more painstaking to prove, relying on the fact that  $\chi_F$  has no period smaller than  $|D_F|$ . See the handout on Gauss sums for the argument. So now we have

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

Let  $S$  denote the inner sum,

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

A small exercise in geometry shows that

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

Also  $1 - \zeta_{|D_F|}^r$  is the complex conjugate of  $1 - \zeta_{|D_F|}^{-r}$ . Thus

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

If  $F$  is real quadratic then  $\chi_F$  is even, and so substituting  $|D_F| - r$  for  $r$  in (1) gives that also

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

Add the values of  $S$  shown in (1) and in the previous 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 finally in the real quadratic case, we have

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

If  $F$  is imaginary quadratic then  $\chi_F$  is odd, and so substituting  $|D_F| - r$  for  $r$  in (1) gives that also

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

Add the values of  $S$  shown in (1) and in the previous 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 finally in the imaginary quadratic case, we have

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

□

**Corollary 13.4** (Slight Refinement of the Quadratic  $L$ -Function Special Value). *If  $F$  is real quadratic then*

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

*If  $F$  is imaginary quadratic then*

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

*Sketch of proof.* It suffices to establish that the Gauss sum of the quadratic character is

$$\tau(\chi_F) = \begin{cases} \sqrt{|D_F|} & \text{if } F \text{ is real quadratic,} \\ i\sqrt{|D_F|} & \text{if } F \text{ is imaginary quadratic.} \end{cases}$$

We already have a similar result for quadratic Gauss sums of prime conductor. And by a writeup on Gauss sums we have under the Sun-Ze isomorphism

$$\chi_F \equiv \chi_2 \times \prod_{\substack{p|D_F \\ \text{odd}}} \chi_p,$$

Here each  $\chi_p = (\cdot/p)$ , but (recalling that  $F = \mathbf{Q}(\sqrt{n})$ )

$$\chi_2(m) = \begin{cases} 1 & \text{if } n \equiv 1 \pmod{4}, \\ (-1)^{(m-1)/2} & \text{if } n \equiv 3 \pmod{4}, \\ (m/2)(-1)^{(n'-1)/2 \cdot (m-1)/2} & \text{if } n = 2n' \equiv 2 \pmod{4}. \end{cases}$$

For uniform notation, let  $n' = n$  if  $n \not\equiv 2 \pmod{4}$ , so that  $n'$  is the odd part of  $D_F$  in all cases. The Gauss sum of the quadratic character factors correspondingly as

$$\tau(\chi_F) = \chi_2(|n'|)\tau(\chi_2) \cdot \prod_{\text{odd } p|n'} \left( \frac{|D_F|/p}{p} \right) \tau\left(\frac{\cdot}{p}\right).$$

Let  $S = \{\text{odd } p \mid |D_F| : p \equiv 3 \pmod{4}\}$ . In all cases the product works out to include the factor  $(-1)^{|S|(|S|-1)/2}i^{|S|}\sqrt{|n'|}$ , which equals  $\sqrt{|n'|}$  or  $i\sqrt{|n'|}$ , but the presence of  $i$  depends on the nature of  $n'$  in a different way for each value of  $n \pmod{4}$ . When  $n \equiv 2 \pmod{4}$  the product also include the factor  $(2/|n'|)$ . The remaining term  $\chi_2(|n'|)\tau(\chi_2)$  of  $\tau(\chi_F)$  works out exactly as necessary for the result, with  $(|n'|/2)$  and  $(2/|n'|)$  cancelling in the  $n \equiv 2 \pmod{4}$  case. The  $n \equiv 2 \pmod{4}$  calculation involves four subcases depending on  $n' \pmod{4}$  and on the sign of  $n'$ .  $\square$

#### 14. FULL PROOF OF THE GAUSS SUM FORMULA (OPTIONAL)

**Lemma 14.1.** *Let  $k$  be a positive, odd, squarefree integer. Then*

$$\prod_{p|k} \left( \frac{k/p}{p} \right) \tau\left(\frac{\cdot}{p}\right) = \begin{cases} \sqrt{k} & \text{if } k \equiv 1 \pmod{4}, \\ i\sqrt{k} & \text{if } k \equiv 3 \pmod{4}. \end{cases}$$

*Proof.* Let  $S = \{p \mid k : p \equiv 3 \pmod{4}\}$ . Compute that

$$\begin{aligned} \prod_{p|k} \left( \frac{k/p}{p} \right) \tau\left(\frac{\cdot}{p}\right) &= \prod_{\substack{p,q|k \\ p \neq q}} \left( \frac{q}{p} \right) \prod_{\substack{p|k \\ p \equiv 1(4)}} \sqrt{p} \prod_{\substack{p|k \\ p \equiv 3(4)}} i\sqrt{p} \\ &= (-1)^{|S|(|S|-1)/2}i^{|S|}\sqrt{k} \end{aligned}$$

If  $|S| = 2s$  then we get  $(-1)^{s(2s-1)+s}\sqrt{k} = \sqrt{k}$ . If  $|S| = 2s + 1$  then we get  $(-1)^{(2s+1)s+s}i\sqrt{k} = i\sqrt{k}$ .  $\square$

Now, if  $n \equiv 1 \pmod{4}$ , so that  $D_F = n$ , we have  $\chi(m) = (m/|n|)$ , and so (using the lemma for the second equality) the Gauss sum is

$$\begin{aligned} \tau(\chi) &= \prod_{p|n} \left( \frac{|n|/p}{p} \right) \tau\left(\frac{\cdot}{p}\right) = \begin{cases} \sqrt{|n|} & \text{if } |n| \equiv 1 \pmod{4}, \\ i\sqrt{|n|} & \text{if } |n| \equiv 3 \pmod{4} \end{cases} \\ &= \begin{cases} \sqrt{|D_F|} & \text{if } n > 0, \\ i\sqrt{|D_F|} & \text{if } n < 0. \end{cases} \end{aligned}$$

Next, if  $n \equiv 3 \pmod{4}$ , so that  $D_F = 4n$ , we have  $\chi(m) = (-1)^{(m-1)/2}(m/|n|)$ , and so, since the quadratic character modulo 4 has Gauss sum  $\tau(\chi_2) = 2i$ , the full Gauss sum is again

$$\begin{aligned} \tau(\chi) &= (-1)^{(|n|-1)/2}2i \prod_{p|n} \left( \frac{|n|/p}{p} \right) \tau\left(\frac{\cdot}{p}\right) = \begin{cases} -2i \cdot i\sqrt{|n|} & \text{if } |n| \equiv 3 \pmod{4}, \\ 2i\sqrt{|n|} & \text{if } |n| \equiv 1 \pmod{4} \end{cases} \\ &= \begin{cases} \sqrt{|D_F|} & \text{if } n > 0, \\ i\sqrt{|D_F|} & \text{if } n < 0. \end{cases} \end{aligned}$$

Third, let  $n = 2 \pmod{8}$ . Here  $D_F = 4n = 8n'$  where  $n' = n/2$  equals  $1 \pmod{4}$ . The quadratic character is

$$\chi(m) = \left(\frac{m}{2}\right) \left(\frac{m}{|n'}\right),$$

so that its mod-8 component is

$$\chi_2(m) = \left(\frac{m}{2}\right) = \begin{cases} 1 & \text{if } m = 1, 7 \pmod{8}, \\ -1 & \text{if } m = 3, 5 \pmod{8}. \end{cases}$$

The corresponding Gauss sum is therefore

$$\tau(\chi_2) = \zeta_8 - \zeta_8^3 - \zeta_8^5 + \zeta_8^7 = \sqrt{8}.$$

Thus the 2-component of the overall Gauss sum is

$$\chi_2(|n'|)\tau(\chi_2) = \left(\frac{|n'|}{2}\right) \sqrt{8}.$$

The rest of the Gauss sum is, by the lemma,

$$\prod_{p|n'} \left(\frac{8|n'|/p}{p}\right) \tau\left(\left(\frac{\cdot}{p}\right)\right) = \left(\frac{2}{|n'}\right) \cdot \begin{cases} \sqrt{|n'|} & \text{if } |n'| = 1 \pmod{4}, \\ i\sqrt{|n'|} & \text{if } |n'| = 3 \pmod{4}. \end{cases}$$

Note that  $|n'| = 1 \pmod{4}$  if and only if  $n' > 0$ . Thus since  $D_F = 8n'$ , the overall Gauss sum works out a third time to

$$\tau(\chi_F) = \begin{cases} \sqrt{|D_F|} & \text{if } n' > 0, \\ i\sqrt{|D_F|} & \text{if } n' < 0. \end{cases}$$

Fourth, let  $n = 6 \pmod{8}$ . Again  $D_F = 4n = 8n'$ , but now  $n' = n/2$  equals  $3 \pmod{4}$ . The quadratic character is

$$\chi(m) = (-1)^{(m-1)/2} \left(\frac{m}{2}\right) \left(\frac{m}{|n'}\right),$$

so that its mod-8 component is

$$\chi_2(m) = (-1)^{(m-1)/2} \left(\frac{m}{2}\right) = \begin{cases} 1 & \text{if } m = 1, 3 \pmod{8}, \\ -1 & \text{if } m = 5, 7 \pmod{8}. \end{cases}$$

The corresponding Gauss sum is therefore

$$\tau(\chi_2) = \zeta_8 + \zeta_8^3 - \zeta_8^5 - \zeta_8^7 = i\sqrt{8}.$$

Thus the 2-component of the overall Gauss sum is

$$\begin{aligned} \chi_2(|n'|)\tau(\chi_2) &= \left(\frac{|n'|}{2}\right) (-1)^{(|n'|-1)/2} i\sqrt{8} \\ &= \left(\frac{|n'|}{2}\right) \cdot \begin{cases} -i\sqrt{8} & \text{if } |n'| = 3 \pmod{4}, \\ i\sqrt{8} & \text{if } |n'| = 1 \pmod{4}. \end{cases} \end{aligned}$$

The rest of the Gauss sum is, by the lemma,

$$\prod_{p|n'} \left(\frac{8|n'|/p}{p}\right) \tau\left(\left(\frac{\cdot}{p}\right)\right) = \left(\frac{2}{|n'}\right) \cdot \begin{cases} i\sqrt{|n'|} & \text{if } |n'| = 3 \pmod{4}, \\ \sqrt{|n'|} & \text{if } |n'| = 1 \pmod{4}. \end{cases}$$

Note that  $|n'| = 3 \pmod{4}$  if and only if  $n' > 0$ . Thus since  $D_F = 8n'$ , the overall Gauss sum works out one last time to

$$\tau(\chi_F) = \begin{cases} \sqrt{|D_F|} & \text{if } n' > 0, \\ i\sqrt{|D_F|} & \text{if } n' < 0. \end{cases}$$

### 15. THE DEDEKIND ZETA FUNCTION OF A QUADRATIC FIELD

**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  $\mathcal{O}_F$ )*

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

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

The Dedekind zeta function rearranges as a Dirichlet series,

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

Thus to analyze  $\zeta_F(s)$  we need to define

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

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

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

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  $\Lambda$  be a complex lattice, and let  $\alpha$  denote the area of any of its fundamental parallelograms,*

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

(As shown just after Proposition 9.2,  $\alpha$  is well defined.) For any  $r > 0$  let  $B_r$  denote the closed complex ball of radius  $r$ . Then for some positive constant  $C$ ,

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

*Proof.* Fix a fundamental parallelogram  $P$ , and for any  $\lambda \in \mathbf{C}$  let  $P_\lambda$  denote the  $\lambda$ -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  $\alpha$  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  $r$  since  $r \geq 1$ . The result follows.  $\square$

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

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

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

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

**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*

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

Note the presence of the ideal class number in Proposition 15.3.

*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

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

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

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

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

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

As in the discussion leading into Lemma 15.2, define

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

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

$$(2) \quad A_n(\mathcal{C}) = \frac{\#\left((\mathfrak{a}_o - 0) \cap B_{\sqrt{nN(\mathfrak{a}_o)}}\right)}{w}.$$

Now specifically take  $\mathfrak{a}_o = (c, -d + \sqrt{m})$  (where briefly  $F = \mathbf{Q}(\sqrt{m})$  since the symbol  $n$  is elsewhere in use here) as in Proposition 10.3, and let  $\alpha_o$  denote the area of the parallelogram spanned by  $c$  and  $-d + \sqrt{m}$ . By (2) and Proposition 10.3 (which says that  $2/\sqrt{|D_F|} = N(\mathfrak{a}_o)/\alpha_o$ ), and then by Lemma 15.2,

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

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

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

sum over ideal classes and use the triangle inequality to get

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

where now the constant  $C$  is independent of ideal classes.  $\square$

**Proposition 15.4** (Properties of the Dedekind Zeta Function). *Let  $F$  be in imaginary quadratic field. The Dedekind zeta function  $\zeta_F(s)$  is analytic on  $\{\text{Re}(s) > 1\}$ , 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  $F$ .*

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

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,

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

where  $\psi$  is analytic. Thus

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

*Proof.* Compute that by Proposition 15.3,

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

so that  $|A_n| \leq Cn$ . The analyticity of  $\zeta_F(s)$  on  $\{\text{Re}(s) > 1\}$  follows from Proposition 11.1.

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

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

By the last statement of Proposition 11.1, the Dirichlet series converges absolutely on  $\{\operatorname{Re}(s) > 1\}$ . Hence so does its rearrangement  $\sum_{\mathfrak{a}} N(\mathfrak{a})^{-s}$ , and now an argument similar to the argument for the Euler–Riemann zeta function shows the equality of this last sum and the product  $\prod_{\mathfrak{p}} (1 - N(\mathfrak{p})^{-s})^{-1}$  on  $\{\operatorname{Re}(s) > 1\}$ .

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

$$\left\{ \begin{array}{l} \zeta_F(s) = \prod_p \prod_{\mathfrak{p}|p\mathcal{O}_F} (1 - N(\mathfrak{p})^{-s})^{-1} \\ \zeta(s) L(\chi, s) = \prod_p (1 - p^{-s})^{-1} (1 - \chi(p)p^{-s})^{-1} \end{array} \right\}, \quad \operatorname{Re}(s) > 1,$$

it suffices to show that for each rational prime  $p$ ,

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

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

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

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  $\operatorname{Re}(s) > 1$ .  $\square$

Thus the equality  $\zeta_K(s) = \zeta(s)L(\chi, s)$  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

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

then

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

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

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

Thus the estimate is  $|\tilde{A}_n| \leq C\sqrt{n}$  for  $n \geq 1$ , and so Proposition 11.1 says that the Dirichlet series

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

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

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

and since

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

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  $F$  is manifested 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 13.3 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*

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

As an example, let  $F = \mathbf{Q}(\sqrt{-5})$ , so that  $D_F = -20$ . The corresponding quadratic character is

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

and by Corollary 13.4,

$$L(\chi_F, 1) = -\frac{\pi}{|20|^{3/2}} (1 + 3 + 7 + 9 - 11 - 13 - 17 - 19).$$

Consequently the ideal class number is

$$h = \frac{w\sqrt{|D_F|}}{2\pi} L(\chi_F, 1) = -\frac{2\sqrt{20}}{2\pi} \cdot \frac{\pi}{20^{3/2}} (-40),$$

which is to say,

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

As another example, let  $F = \mathbf{Q}(\sqrt{-163})$ . Since 163 is prime, the class number formula gives

$$\frac{2\pi h}{2\sqrt{163}} = L(\chi_F, 1) = -\frac{\pi}{163^{3/2}} \sum_{r=1}^{162} \chi_F(r)r,$$

and thus

$$h = -\frac{1}{163} \sum_{r=1}^{162} \chi_F(r)r.$$

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 to compute that  $2^{81} = -1 \pmod{163}$ . Thus the squares modulo 163 are the even powers of 2 reduced modulo 163, and similarly for the nonsquares. From here one can verify by hand or by machine that the sum in the previous display is  $-163$ . Thus:

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