DIRICHLET'S CLASS NUMBER FORMULA

VIVIAN KUPERBERG

Most of this exposition follows Davenport [2], with many helpful realizations had with the help of [1], [3], and [4].

1. Defining the Problem

Consider the field extension $K = \mathbb{Q}(\sqrt{D})/\mathbb{Q}$, for D a squarefree integer. We will stick to the case where D is a *negative* integer. We consider as is standard the ring of integers $\mathcal{O}$, given by

$$\mathcal{O} = \begin{cases} \mathbb{Z}\left[\frac{1+\sqrt{D}}{2}\right] \text{ if } D \equiv 1 \pmod 4 \\ \mathbb{Z}[\sqrt{D}] \text{ if } D \equiv 2, 3 \pmod 4 \end{cases}.$$

Our first question is, what do we mean by the *class number*? The tagline that I at least heard for a long time was that "the class number measures failure of unique factorization in $\mathcal{O}$," and that for example number rings with unique factorization had class number 1, whereas $\mathbb{Z}[\sqrt{-5}]$ does not have class number 1 because $2 \cdot 3 = (1+\sqrt{-5})(1-\sqrt{-5})$. Looking at this example, let's get into a bit more detail.

First of all, as is often the case, we want to be considering ideals rather than elements. One way of describing the problem here is that the ideal $(2, 1+\sqrt{-5})$ is a prime ideal, but it is not principal. So we want to focus on ideals; in fact, the structure that is most convenient is *fractional ideals*.

Definition 1.1. A *fractional ideal* of $\mathcal{O}$ is an $\mathcal{O}$-submodule I of K such that for some $x \in \mathcal{O}$, $xI \subseteq \mathcal{O}$.

Intuitively these are ideals, where we're allowed to divide out by finite denominators. They can also be defined as finitely-generated $\mathcal{O}$-submodules of K.

Fact 1.2. Any fractional ideal of a quadratic number field is generated by two elements of K.

The benefit of fractional ideals is that you can multiply them! You can do this with plain old ideals, too, but since fractional ideals allow fractions, they actually form a group. This is great news, because if we've learned anything from algebraic topology, it's that groups are great tools for measuring the failure of properties. However, there's lots of ideals, so the group of fractional ideals is decidedly not finite, so we have to do something a little bit more. What is that little bit more? Well, our problem case up there is not principal, so the strategy that we'll go with is to quotient the group of fractional ideals by the subgroup of principal fractional ideals. In other words, we'll say that two fractional ideals I, J are *equivalent* if there exists $a \in K$ such that $I = aJ$, and we'll look at the group (but, for our purposes it might as well be a set) of equivalence classes.

Definition 1.3. The *class group of a field* K, denoted H_D, is the group of fractional ideals quotiented by the group of principal ideals. The *class number* h_D is the size of H_D.

Example 1.4. For $K = \mathbb{Q}(\sqrt{-5})$, there are in fact two equivalence classes of fractional ideals; the one containing $\left[1, \frac{1+\sqrt{-5}}{2}\right]$, and the one containing $[1]$.

Example 1.5. If K has trivial class group, then every fractional ideal is principal, and in particular every ideal is principal. For an element $z \in K$, we can always factor the ideal (z) uniquely into prime ideals; since every ideal is principal, this factorization translates directly into a factorization of elements.

This leads to a burning question.

Question 1.6. What is h_D?

Remark 1.7. From here on out, we will refer frequently to a quadratic field via its *discriminant*. The discriminant of a quadratic field is "more or less" the D of $K = \mathbb{Q}(\sqrt{D})$ fame, but not quite. In particular,

$$\text{disc}(K) = \begin{cases} D \text{ if } D \equiv 1 \pmod 4 \\ 4D \text{ otherwise.} \end{cases}$$

If this is confusing, we won't really need it, but if you're working out the details of a certain proof mentioning "minimal polynomials" it is good to keep in mind. The exposition above carries through the same way, so from now on we will always use D to be the actual discriminant, i.e. D is either squarefree and $1 \pmod 4$ or of the form $4D'$ with D' squarefree and not $1 \pmod 4$.

We will refer to numbers that appear as discriminants of quadratic fields as *fundamental* discriminants.

2. From Fields to Forms

Let's now introduce another problem, about counting equivalence classes of quadratic forms, before showing why they are equivalent. The quadratic forms that we are considering are functions of the form

$$f(x, y) = ax^2 + bxy + cy^2,$$

with $a, b, c \in \mathbb{Z}$. The *discriminant* D of a form is the quantity $b^2 - 4ac$, which we will assume to be negative. We will assume always that f is *primitive*, i.e. that $(a, b, c) = 1$. We will also assume that $a > 0$, so that f is *positive definite*. The set of forms of discriminant D admits an $\text{SL}_2(\mathbb{Z})$ action, where if $\gamma = \begin{pmatrix} p & q \\ r & s \end{pmatrix}$, then $\gamma \cdot f$ is defined as

$$\gamma \cdot f(x, y) = f(px + qy, rx + sy).$$

Note that we are making a claim here, that the result has the same discriminant as f. To check this, note that it suffices to check for a set of generators of $\text{SL}_2(\mathbb{Z})$, such as $\left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix} \right\}$, and checking for these two matrices is not prohibitively painful. This $\text{SL}_2(\mathbb{Z})$ action then defines an equivalence relation on forms, so that we can ask about counting equivalence classes:

Question 2.1. Let $h(D)$ be the number of equivalence classes of integer quadratic forms with discriminant $D < 0$. What is $h(D)$?

Remark 2.2. It is known that $h(D)$ is finite, because any binary quadratic form is equivalent to a unique *reduced* form, i.e. one satisfying $-|a| < b \leq |a| < |c|$ or $0 \leq b \leq |a| = |c|$. There are finitely many triples satisfying these inequalities with bounded discriminant, so there must be finitely many equivalence classes.

The nice thing about reduced forms is that they let us pick a canonical representative of each equivalence class of forms; in the future if ever "summing over forms" is mentioned, it'll be summing over representatives, for example the reduced forms.

Before we go about answering this question, let's talk about how it relates to our first question, about quadratic fields. Let $C(D)$ be the set of equivalence classes of integer quadratic forms with discriminant $D < 0$, and again we have H_D be the class group of $\mathbb{Q}(\sqrt{D})$, and h_D the field class number. Then we have the following theorem:

Theorem 2.3. *Let $D < 0$ be a discriminant of a quadratic field. Then the map $\phi : C(D) \to H_D$ defined by*

$$\phi(ax^2 + bxy + cy^2) = \left[a, \frac{-b + \sqrt{b^2 - 4ac}}{2}\right]$$

is a set (and group, although we're not worrying about the group structure here) isomorphism. In particular, $h(D) = h_D$.

Proof. We're going to provide here a sketch of a proof, skipping some details; for full detail, see Cox, Theorem 7.7 [1].

For well-definedness, assume that $f(x,y) = a_f x^2 + b_f xy + c_f y^2$ and $g(x,y) = a_g x^2 + b_g xy + c_g y^2$ are equivalent; let $\begin{pmatrix} p & q \\ r & s \end{pmatrix}$ be the matrix taking f to g. Let τ_f be the element of the upper half plane such that $f(\tau_f, 1) = 0$. In this case $\tau_f = \frac{-b_f + \sqrt{D}}{2a_f}$. Then

$$0 = f(\tau_f, 1) = g(p\tau_f + q, r\tau_f + s) = (r\tau_f + t)^2 g\left(\frac{p\tau_f + q}{r\tau_f + s}, 1\right),$$

so $g\left(\frac{p\tau_f+q}{r\tau_f+s}, 1\right) = 0$, and this first element is also in the upper half-plane; let's call it τ_g. Thus we know two things about τ_g:

(1) By what we've just done, $\tau_g = \frac{p\tau_f+q}{r\tau_f+s}$, and
(2) by the quadratic formula, $\tau_g = \frac{-b_g+\sqrt{D}}{2a_g}$.

So, we want to show that, as fractional ideals,

$$a_f[1, \tau_f] \sim a_g[1, \tau_g].$$

But this follows, because

$$\begin{aligned} a_g[1,\tau_g] &\sim [1,\tau_g] \\ &\sim (r\tau_f+s)\left[1,\frac{p\tau_f+q}{r\tau_f+s}\right] \\ &\sim [r\tau_f+s,p\tau_f+q] \\ &\sim [1,\tau_f] \text{ since the matrix has determinant 1} \\ &\sim a_f[1,\tau_f]. \end{aligned}$$

This argument backwards (with some adjustments) shows injectivity.

To show surjectivity, if we have a fractional ideal I we can pick an integral basis $\{\alpha,\beta\}$ of I. We can assume (by swapping α,β if necessary) that $\tau=\beta/\alpha$ lies in the upper half-plane. We can then pick ax^2+bx+c to be the minimal polynomial of τ, assuming that $(a,b,c)=1$ and $a>0$, so that $f(x,y)=ax^2+bxy+cy^2$ is positive definite of discriminant D, and $f(x,y)$ maps to $a[1,\tau]$ under the map that we've taken. □

3. Counting Forms

Fixing a (negative, fundamental) discriminant D, we will now go about determining $h(D)$, the number of equivalence classes of quadratic forms.

How would we do this? One idea is to consider the quantity

$$R(n):=\#\left\{(f,x,y)\mid f(x,y)=n,\operatorname{disc}(f)=D\right\},$$

as well as the corresponding quantity for a fixed principal quadratic form f with discriminant D, with

$$R(n,f):=\#\left\{(x,y)\mid f(x,y)=n\right\}.$$

Then certainly we have that

$$R(n)=\sum_f R(n,f).$$

Since we would like to count the number of forms f, we could try hoping that $R(n,f)$ is independent of f, and then $h(D)$ would be $\frac{R(n)}{R(n,f)}$ for any f. This has a clear downside, that $R(n,f)$ is emphatically *not* independent of f. However, instead of choosing a specific n, we could try averaging over all n below a cap N, and then taking the limit as $x\to\infty$:

$$\lim_{N\to\infty}\frac{1}{N}\sum_{n\le N}R(n)=\sum_f\lim_{N\to\infty}\frac{1}{N}\sum_{n\le N}R(n,f).$$

Now the summand on the right really does become independent of f, so we'll be able to happily divide out. This will be our plan of action, but we still need to understand every part of the above equation.

Let's start by the $R(n)$ side. The first thing that we'll need to understand is the stabilizer under the $\mathrm{SL}_2(\mathbb{Z})$ action, with elements known as *automorphs*. There are always two trivial automorphs, specifically the identity $f(x,y)=f(x,y)$ and the negative identity, $f(x,y)=f(-x,-y)$. How many more in general?

Theorem 3.1 (Zagier, [4], Section 8)**.** *For $f(x,y) = ax^2 + bxy + cy^2$ a quadratic form with discriminant D, the number of automorphs for f is*

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

Note that this looks suspicially like the number of units; that's because there is a correspondence! In one direction, this correspondence works as follows. If we recall from the correspondence between classes of forms and classes of ideals, we get from a fractional ideal to a form by taking an integral basis $[\alpha, \beta]$, and considering the minimal polynomial of β/α (or α/β). Now, multiplying the basis by a unit u will not change either β/α or α/β, so certainly it cannot change the minimal polynomial! The other direction is harder, and we won't go into it here.

Lemma 3.2. *If $n > 0$ and $(n, D) = 1$, then*

$$R(n) = w \sum_{m|n} \left(\frac{D}{m}\right),$$

with w as above and $\left(\frac{D}{m}\right)$ the Jacobi symbol.

The *Jacobi symbol* is defined as follows. If m is factored as $p_1^{\alpha_1} \cdots p_k^{\alpha_k}$, then

$$\left(\frac{a}{m}\right) = \left(\frac{a}{p_1}\right)^{\alpha_1} \cdots \left(\frac{a}{p_k}\right)^{\alpha_k},$$

where for each prime p,

$$\left(\frac{a}{p}\right) = \begin{cases} 0 \text{ if } a \equiv 0 \pmod{p} \\ 1 \text{ if } a \not\equiv 0 \pmod{p}, a \equiv x^2 \pmod{p} \\ -1 \text{ if } a \not\equiv 0 \pmod{p} \text{ and } a \text{ is not a quadratic residue.} \end{cases}$$

Remark 3.3. The important thing for our purposes is that the Jacobi symbol considered as a function with input m, i.e. $\left(\frac{D}{\cdot}\right) : \mathbb{Z} \to \mathbb{C}$ given by $\left(\frac{D}{\cdot}\right)(m) = \left(\frac{D}{m}\right)$ determines a *Dirichlet character to the modulus D*, i.e. a multiplicative homomorphism from $(\mathbb{Z}/D)^\times \to \mathbb{C}^\times$. Moreover, this character is *nonprincipal*, meaning that it doesn't send everything to 1.

Since it doesn't send everything to 1, it must actually send as many values to -1 as to $+1$, i.e. its average value is 0; this is important and we will use it!

Proof sketch. We will give a sketch of this proof, which can be found in Zagier [4], Satz 3 on page 65.

First, let $R^*(n)$ be the number of triples (f, x, y) as before, where we now require that $(x, y) = 1$. Then

$$R(n) = \sum_{\substack{g \geq 1 \\ g^2 | n}} R^*\left(n/(g^2)\right).$$

The next step is to prove the following formula:

Lemma 3.4.

$$R^*(n) = w\#\{b \pmod{2n} \mid b^2 \equiv D \pmod{4n}\}.$$

Proof. This formula is actually a reflection of a more general purely group theoretic result. Say you have a group G which acts on two sets X, Y, and preserves a subset $S \subseteq X \times Y$ via the diagonal action. Then the fact is that you can count the number of equivalence classes $|S/G|$ in the following two ways:

$$\sum_{x \in X/G} |Y_x/G_x| = |S/G| = \sum_{y \in Y/G} |X_y/G_y|,$$

where $Y_x = \{y \in Y \mid (x,y) \in S\}$, G_x is the stabilizer of x, and similarly for y's.

We apply this to the situation by taking $G = \mathrm{SL}_2(\mathbb{Z})$, X is the set of quadratic forms of discriminant D, Y is the set of pairs $(x,y) \in \mathbb{Z}^2$ that are relatively prime, and S is the set of triples $f(x,y)$, with $(x,y) \in Y$ and $f \in X$, such that $f(x,y) = n$. Then one of the interpretations gives $\sum_{f \text{ reduced}} R^*(n,f)$ and the other interpretation gives exactly this count that we want. □

This formula we have for $R^*(n)$ is wonderful because we can apply the Chinese Remainder theorem and factor into primes; and it turns out that by extension we can do the same thing for $R(n)$. In the prime case, this becomes something we can actually compute based on if p is a quadratic residue modulo D and divisibility, and this gives that

$$R(p^k) = \sum_{0 \le r \le k} \left(\frac{D}{p^r}\right),$$

which then expanding by multiplicativity gives the theorem. □

Using this, we'll determine the average value of $R(n)$ as n varies. Since our expression above is limited to cases when $(n,D) = 1$, we will limit ourselves in the average to cases when $(n,D) = 1$, and we won't lose anything this way. Now, we compute:

$$\begin{aligned} R(n) &= w \sum_{m \mid n} \left(\frac{D}{m}\right) \\ \Rightarrow w^{-1} \sum_{\substack{n=1 \\ (n,D)=1}}^{N} R(n) &= \sum_{\substack{m_1 m_2 \le N \\ (m_1 m_2, D)=1}} \left(\frac{D}{m_1}\right) \\ &= \sum_{m_1 \le \sqrt{N}} \left(\frac{D}{m_1}\right) \sum_{\substack{m_2 \le N/m_1 \\ (m_2,D)=1}} 1 + \sum_{\substack{m_2 < \sqrt{N} \\ (m_2,D)=1}} \sum_{\sqrt{N} < m_1 \le N/m_2} \left(\frac{D}{m_1}\right), \end{aligned}$$

where in the last step we aren't worrying about $(m_1, D) \neq 1$ because in that case $\left(\frac{D}{m_1}\right)$ is 0 regardless.

The first inner sum we can just evaluate up to a small error term; it is

$$\frac{N}{m_1} \frac{\phi(|D|)}{|D|} + O(\phi(|D|)).$$

Meanwhile, since $\left(\frac{D}{m_1}\right)$ is a nonprincipal character and thus has average 0, its sum over *any* range is bounded (say, by $|D|/2$, although there are better bounds). Thus the inside of

the second double sum contributes at most $O(|D|/2) = O(1)$, so the second double sum contributes at most $O(\sqrt{N})$. Putting this all together, we get

$$w^{-1} \sum_{\substack{n=1 \\ (n,D)=1}}^{N} R(n) = N\frac{\phi(|D|)}{|D|} \sum_{m \leq \sqrt{N}} \frac{1}{m}\left(\frac{D}{m}\right) + O(\sqrt{N}),$$

where the $O(\sqrt{N})$ captures the error term from both the first sum and the second sum.

Now we'll use the following fact, which can be proven using partial summation:

Fact 3.5.

$$\sum_{m > \sqrt{N}} \frac{1}{m}\left(\frac{D}{m}\right) = O(N^{-1/2}).$$

Thus $N\frac{\phi(|D|)}{|D|}\sum_{m>\sqrt{N}} \frac{1}{m}\left(\frac{D}{m}\right) = O(\sqrt{N})$, so we can extend the sum above to infinity without increasing the error term to get

$$w^{-1} \sum_{\substack{n=1 \\ (n,D)=1}}^{N} R(n) = N\frac{\phi(|D|)}{|D|} \sum_{m=1}^{\infty} \frac{1}{m}\left(\frac{D}{m}\right) + O(\sqrt{N}),$$

and then divide by N and take the limit as $N \to \infty$ to get

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ (n,D)=1}}^{N} R(n) = w\frac{\phi(|D|)}{|D|} \sum_{m=1}^{\infty} \frac{1}{m}\left(\frac{D}{m}\right).$$

The sum simplifies further more or less by definition into an L-function. We won't talk much about L-functions in general in this talk, but suffice to say that they are extremely useful objects in number theory that are well-studied and (in this context) well-understood, so that connecting this to the value of an L-function is a legitimately useful step. In this case the *Dirichlet L-function* corresponding to a Dirichlet character $\chi : (\mathbb{Z}/D)^\times \to \mathbb{C}^\times$ is the complex function

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

where $\chi(n) = 0$ if $(n, D) \neq 1$. In this case, this means that our expression just *is*

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ (n,D)=1}}^{N} R(n) = w\frac{\phi(|D|)}{|D|} L\left(1, \left(\frac{D}{\cdot}\right)\right).$$

Now let's consider the sum $\sum_{\substack{n\leq N \\ (n,D)=1}} R(n,f)$, for a specific form f. This is the same thing as counting the total number of inputs (x, y) that will have any output which is relatively prime to D and at most N, i.e. we want

$$\#\{(x,y) \mid 0 < ax^2 + bxy + cy^2 \leq N, (ax^2 + bxy + cy^2, D) = 1\}.$$

Let's start with the relatively prime condition. This is just a condition that $ax^2 + bxy + cy^2$ lands in one of the correct $\phi(|D|)$ congruence classes mod D, which rules out some of the congruence classes for x and y mod D. Luckily, the following holds.

Fact 3.6. For $ax^2 + bxy + cy^2$ of discriminant D, there are exactly $|D|\phi(|D|)$ pairs $(x_0, y_0) \pmod{D}$ such that if $x \equiv x_0 \pmod{D}$ and $y \equiv y_0 \pmod{D}$, then $(ax^2 + bxy + cy^2, D) = 1$.

So it suffices to consider, for fixed x_0, y_0, the number of pairs of integers (x, y) such that

$$ax^2 + bxy + cy^2 \leq N, \qquad x \equiv x_0, \qquad y \equiv y_0 \pmod{D}.$$

This inequality is just saying that (x, y) is contained in an ellipse that is centered at the origin; as $N \to \infty$ this ellipse expands uniformly. The area of the ellipse is $\frac{2\pi}{\sqrt{4ac-b^2}}N = \frac{2\pi}{\sqrt{|D|}}N$.

We can then divide the plane into squares of size $|D|$ and zoom out to see that the number of points (x, y) is asymptotic to $\frac{1}{|D|^2}\frac{2\pi}{|D|^{1/2}}N$ as $N \to \infty$. Putting this all together gives

$$\lim_{N\to\infty} \frac{1}{N} \sum_{\substack{n=1 \\ (n,D)=1}}^{N} R(n, f) = \frac{\phi(|D|)}{|D|}\frac{2\pi}{|D|^{1/2}}.$$

Combining this with our nice expression for the limit of average values of $R(n)$ gives

$$w\frac{\phi(|D|)}{|D|}L\left(1, \left(\frac{D}{\cdot}\right)\right) = h(D)\frac{\phi(|D|)}{|D|}\frac{2\pi}{|D|^{1/2}},$$

which simplifies to

$$h(D) = \frac{w|D|^{1/2}}{2\pi}L\left(1, \left(\frac{D}{\cdot}\right)\right)$$

for $D < 0$, so in particular

$$h_D = \frac{w|D|^{1/2}}{2\pi}L\left(1, \left(\frac{D}{\cdot}\right)\right)$$

for $D < 0$, and that's the class number formula!

REFERENCES

[1] Cox, D.A. Primes of the form $x^2 + ny^2$. *John Wiley and Sons, Inc.*, 2013.
[2] Davenport, H. Multiplicative Number Theory. *Springer-Verlag*, 1967.
[3] Smith, K. The Collision of Quadratic Fields, Binary Quadratic Forms, and Modular Forms. `http://math.oregonstate.edu/~swisherh/KarenSmith.pdf`. 2011.
[4] Zagier, D.B. Zetafunktionen und quadratische Körper. *Springer-Verlag*, 1981.