SPECIAL CASES OF THE CLASS NUMBER FORMULA

What we know from last time regarding general theory:

Each quadratic extension K of $\mathbb{Q}$ has an associated discriminant D_K (which uniquely determines K), and an associated primitive quadratic character χ_K of conductor $|D_K|$ (which again uniquely determines K, since the sign of D_K is determined by the value $\chi_K(-1)$).

1. The case of $\mathbb{Q}(i)$

What we know from last time about this case:

We have proved that the units of $\mathbb{Z}[i]$ are $\pm 1, \pm i$. We have proved that $\mathbb{Z}[i]$ is a Euclidean domain, and hence that irreducibles and primes coincide, and that every non-zero element has a unique factorization (up to modification by units) into a product of primes.

Stated last time:

$2 = (-i)(1+i)^2$ (an obvious calculation), while if p is an odd prime (in $\mathbb{Z}$), then p remains prime in $\mathbb{Z}[i]$ if $p \equiv -1 \bmod 4$, while p factors into a product of two primes $p = \pi\overline{\pi}$ if $p \equiv 1 \bmod 4$, where π and $\overline{pi}$ are genuinly different primes (i.e. not related by multiplication by a unit).

We now prove this.

Proof. Using that $(\mathbb{Z}/p)^\times$ is a cyclic group of order $p-1$ (i.e. the existence of primitive roots), we see that there is a square root of -1 (that is, a non-trivial fourth root of 1) in $(\mathbb{Z}/p)^\times$ if and only if $p \equiv 1 \bmod 4$.

Suppose now that $p \equiv -1 \bmod 4$, and suppose that α and β are two elements of $\mathbb{Z}[i]$ such that $p|\alpha\beta$. Then $p^2 = N(p)|N(\alpha)N(\beta)$, and so (after relabelling if necessary) we may assume that $p|N(\alpha)$. Writing $\alpha = x+iy$, we have $x^2+y^2 \equiv 0 \bmod p$. If either x or y is not 0 mod p, we obtain a square root of -1, a contradication. Thus $p|x, y$, and so $p|\alpha$. This proves that p is prime.

Suppose instead that $p \equiv 1 \bmod 4$. Then we can solve $x^2 + 1 \equiv 0 \bmod p$, and hence $p|(x+i)(x-i)$. Since obviously $p \nmid x \pm i$, we see that p is not prime, thus not irreducible, and so p has a proper factor in $\mathbb{Z}[i]$, call it π. Since $N(p) = p^2$, we see that $N(\pi) = p$. One easily sees that an element of prime norm is irreducible (hence prime), and so $p = N(\pi) = \pi\overline{\pi}$ is the prime factorization of p. □ □

Examples: $5 = (2+i)(2-i), 13 = (3+2i)(3-2i), 17 = (4+i)(4-i), \ldots$.

Now any prime of $\mathbb{Z}[i]$ divides a prime of $\mathbb{Z}$ (since if π is such a prime, it divides its norm $N(\pi)$, and hence divides at least one of the prime factors of that integer), and so the primes of $\mathbb{Z}[i]$ are precisely (up to unit) $(1+i)$, p for $p \equiv -1 \bmod 4$, and $\pi, \overline{\pi}$, the prime factors of $p \equiv 1 \bmod 4$.

Now lets count the number of elements of $\mathbb{Z}[i]$ of norm $\leq N$ (for some big integer N). On the one hand, this is roughly the area of the circle of radius $\sqrt{N}$, so $\sim \pi N$ (lattice points roughly correspond to area), with the approximation becoming better and better as $N \to \infty$.

On the other hand, we can count exactly how many elements there are of any norm n. Of course if $n = 0$ there is one element, namely 0.

1.1. **Lemma.** *If $n > 0$, then the number of elements of norm n in $\mathbb{Z}[i]$ equals $4\sum_{d|n}\chi(d)$, where χ is the quadratic character of conductor 4, i.e. $\chi := \chi_{\mathbb{Q}(i)}$.*

Proof. If we factor n into a product of prime powers $n = p_1^{e_1}\cdots p_r^{e_r}$, then $\sum_{d|n}\chi(d)$ factors as the product of the terms

$$\sum_{d|p_i^{e_i}}\chi(d) = \begin{cases} 1 \text{ if } p_i = 2 \\ 1 \text{ if } p_i \equiv -1 \bmod 4 \text{ and } e_i \text{ is even} \\ 0 \text{ if } p_i \equiv -1 \bmod 4 \text{ and } e_i \text{ is odd} \\ 1 + e_i \text{ if } p_i \equiv 1 \bmod 4. \end{cases}$$

From the explicit description of the primes in $\mathbb{Z}[i]$, and the existence and uniqueness of prime factorization, the lemma follows. (The factor of 4 comes from multiplication by units.) □

Thus we compute that the number of elements of $\mathbb{Z}[i]$ of norm $\leq N$ are

$$1 + \sum_{1\leq n\leq N} 4\sum_{d|n}\chi(d)$$

(here the first "1" is just counting the number 0)

$$= 1 + 4\sum_{1\leq d\leq N}\chi(d)\big[\frac{N}{d}\big].$$

Dividing by N and letting $N \to \infty$, we obtain

$$\pi = \lim_{N\to\infty}\frac{1}{N} + 4\sum_{1\leq d\leq N}\chi(d)\big[\frac{N}{d}\big]\frac{1}{N} = 4L(1,\chi).$$

Thus we have given a(nother) proof that $L(1,\chi) = \pi/4$.

2. The case of $\mathbb{Q}(\sqrt{2})$

Again in this case we have a Euclidean algorithm. Even though the elements of $\mathbb{Q}(\sqrt{2})$ are real numbers, we still plot them in the plane, plotting $x + \sqrt{2}y$ as the point (x, y) in the plane.

Then if $a, b \in \mathbb{Z}[\sqrt{2}]$, with $b \neq 0$, then $a/b \in \mathbb{Q}[\sqrt{2}]$. Let q be the nearest point with integer coordinates. Then $a/b - q = u + v\sqrt{2}$, with $|u|, |v| \leq 1/2$. One easily checks that $-1/2 \leq N(a/b - q) \leq 1/4$. Thus, if we set $r = a - bq$, then $N(r) < N(b)$. Consequently we have $a = qb + r$ with $N(r) < N(b)$, and $\mathbb{Z}[\sqrt{2}]$ is a Euclidean domain.

Hence once again primes and irreducibles coincide, and we have unique factorization into primes, up to units.

On the other hand, there are many more units!

E.g. $1 + \sqrt{2}$ is a unit, and it is > 1, hence so are all its powers, and so it is a unit of infinite order!

[Brief aside:] There is another phenomenon which can cause a little bit of pain, namely norms can be negative as well as positive. (E.g. $N(1+\sqrt{2}) = 1 - 2 = -1 < 0$.) A key point though is that a non-zero element always has non-zero norm. Also, if $\alpha \in \mathbb{Z}[\sqrt{2}]$ has negative norm, then $(1 + \sqrt{2})\alpha$ has positive norm. Thus, after

multiplying by a unit, we can always make the norm of an element positive. [End of aside.]

Let us pin down the structure of the units. For this, recall that we think of $\mathbb{Z}[\sqrt{2}]$ as sitting as a lattice in the (x, y)-plane, by mapping an element $x + \sqrt{2}y$ to (x, y).

Now make the linear change of coordinates in the plane, from (x, y) to (w, z), where $w = x + \sqrt{2}y$, $z = x - \sqrt{2}y$. (The inverse map is $x = (w + z)/2$, $y = (w - z)/2\sqrt{2}$. In the new coordinates, $\mathbb{Z}[\sqrt{2}]$ is still a discrete set, although it is no longer a square lattice. A point $x + \sqrt{2}y$ now maps to the point $(x + \sqrt{2}y, x - \sqrt{2}y)$ (which is more natural in a way, if slightly harder to visualize).

Now consider the first quadrant in the (w, z)-coordinates, i.e. the points where $w, z > 0$. Then we can define yet another set of coordiantes, $u = \log w$, $v = \log z$. This is non-linear change of coordinates, with inverse $w = e^u$, $z = e^v$. It takes the first quadrant in the (w, z)-plane to the entire (u, v)-plane. The points of $\mathbb{Z}[\sqrt{2}$ which lie in the first quadrant are a discrete set in that quadrant, and so give rise to a discrete set in the (u, v)-plane.

2.1. **Lemma.** *The group of positive units of norm* 1 *is an infinite cyclic group.*

Proof. If $x + \sqrt{2}y$ is positive and of norm 1, then $x - \sqrt{2}y$ must also be positive (its product with the positive number $x + \sqrt{2}y$ gives 1), and so $x + \sqrt{2}y$ corresponds to a point (w, z) in the first quadrant. Indeed, the positive units of norm 1 are precisely the units in the first (w, z)-quadrant.

Now $(w, z) \mapsto (u, v)$ takes multiplication in $\mathbb{Z}[\sqrt{2}]$ to addition in the (u, v) plane. Thus the group of positive units of norm 1 gets identified with an additive subgroup of the (u, v)-plane. It is a discrete subgroup of the (u, v)-plane (because we saw that the entire set of points of $\mathbb{Z}[\sqrt{2}]$ lying in the first (w, z)-quadrant give a discrete subset of the (u, v)-plane).

Finally, it lies on the line $u + v = 0$, because $u + v = \log(x^2 - 2y^2)$, and we are looking at units of norm 1.

Thus we have a discrete subgroup of the line $u + v = 0$. Such a thing is either trivial, or else infinite cyclic. Trivial is impossible, because e.g. $(1 + \sqrt{2})^2$ is a non-trivial member. (We take a square here just to ensure norm 1 rather than -1.) Thus it must be cyclic of infinite order. □ □

We let ε denote a generator of the infinite cyclic group of positive units of norm 1; actually there are two such choices, but we pin down ours by asking that $\varepsilon > 1$. (In fact $\varepsilon = (1 + \sqrt{2})^2 = 3 + 2\sqrt{2}$, but we won't use that fact for the moment.)

Now we pin down the structure of the primes. As in the preceding case, to determine the primes, it is enough to determine how primes in $\mathbb{Z}$ factor in $\mathbb{Z}[\sqrt{2}]$. Now let $\chi := \chi_{\mathbb{Q}(\sqrt{2})}$; it is the character given by $\chi(1) = 1, \chi(3) = \chi(5) = -1, \chi(7) = 1$.

We have $2 = \sqrt{2}^2$, and $\sqrt{2}$ is prime (since it has prime norm).

2.2. **Lemma.** *If p is an odd prime number, then p is prime in $\mathbb{Z}[\sqrt{2}]$ iff $\chi(p) = -1$, while if $\chi(p) = 1$, then $p = \pi\overline{\pi}$ factors as a product of two primes, a prime π and its conjugate $\overline{\pi}$, which are distinct (even after multiplying by arbitrary units).*

Proof. Have to show that $(\mathbb{Z}/p)^\times$ contains a square-root of 2 if and only if $\chi(p) = 1$; then the proof proceeds as in the previous case.

You can choose your favourite proof of this fact (or just give it to them; probably some have seen it in a number theory class, since it is one of the supplementary laws of quadratic reciprocity). □

Now we would like to compute $L(1,\chi)$ via computing a volume and counting lattice points, as before. The fact that there are infinite many units causes a complication, because it means that there are infinitely many elements of a given norm.

So from the very beginning we are forced to count elements mod units. An argument as in the previous case, using the classification of primes we just worked out, shows that the number of elements, up to multiplication by a unit, of norm $n > 0$ is equal to

$$\sum_{d|n} \chi(d).$$

Thus, the number of elements of norm between 1 and N is equal to

$$\sum_{1\le n\le N} \sum_{d|n} \chi(d) = \sum_{1\le d\le N} \chi(d)\big[\frac{N}{d}\big],$$

and so the number of such elements, divided by N, equals

$$\sum_{1\le d\le N} \chi(d)\big[\frac{N}{d}\big]\frac{1}{N},$$

which approaches $L(1,\chi)$ as $N \to \infty$.

We now want to count this number differently, as an area. Since multiplying by -1 and/or $1+\sqrt{2}$ allows us to make any element both positive and of positive norm, and hence lying in the first (w,z)-quadrant, we restrict our attention to elements in this quadrant, up to multiplication by units which preserve this quadrant, i.e. which are positive and of norm 1.

By multiplying by powers of ε (which after taking logs comes to adding multiplies of $\log\varepsilon$), we may assume that the coordinate w, that is $x+\sqrt{2}y$ itself, lies between 1 and ε. Thus we are counting lattice points in the region

$$1 \le x^2 - 2y^2 \le N, \quad 1 \le x+\sqrt{2}y \le \varepsilon.$$

This region is not quite convex, but is close enough, and so the lattice points are roughly approximated by the area (computed using (x,y)-coordinates, since these are the coordinates in which $\mathbb{Z}[\sqrt{2}]$ is the usual integer lattice), with the approximation getting better and better as $N \to \infty$. [It probably helps to draw a picture at this point.]

This area is not hard to work out. One way is to check (by computing the relevant Jacobian) that it is equal to the integral

$$\frac{1}{2\sqrt{2}} \int_{1\le u\le \log\varepsilon, 0\le u+v\le \log N} e^{u+v} du dv$$
$$= \frac{1}{2\sqrt{2}} \int_{1\le u\le \log\varepsilon, 0\le u+v\le \log N} e^{u+v} du d(u+v) = (N-1)\frac{\log\varepsilon}{2\sqrt{2}}.$$

Dividing by N and letting $N \to \infty$, and comparing with our above computation, we find that $L(1,\chi) = \dfrac{\log\varepsilon}{2\sqrt{2}}$.

At this point we might want to pin down ε. Here is one way: We know that $(1+\sqrt{2})^2 = (3+2\sqrt{2}) = \varepsilon^n$ for some integer n. Thus $nL(1,\chi) = \dfrac{\log(1+\sqrt{2})}{\sqrt{2}}$ for some integer n. Computing the roughest approximation of either side shows that in fact $n = 1$, hence $\varepsilon = (1+\sqrt{2})^2$, and we recover our previous formula

$$L(1,\chi) = \frac{\log(1+\sqrt{2})}{\sqrt{2}}.$$