Mauro Cutz Braunstein

Math 129

Final Paper

Finding the Class Number for a Quadratic Field

The class number h_K of a quadratic field $K = \mathbf{Q}(\sqrt{d})$ ($\mathbf{Q}$ is the field of rationals) is the order of C_K, the class group, defined as the group of fractional ideals (with respect to ideal multiplication) modulo the group of principal ideals of O_K, the ring of integers of *K*. By the discussion in Chapter 8 of this class we know that h_K is finite. In this paper, I will show how one may compute it for an arbitrary quadratic field (an arbitrary squarefree *d*, positive or negative). The information comes mostly from Gerald J. Janusz's clear *Algebraic Number Fields* (Second Edition, 1996, American Mathematical Society).

We will compute h_K by evaluating a certain limit in two different ways and equating the two ways, one of which involves an h_K for which we can solve. We'll start off with a formula that takes us too far afield to prove: $\lim_{s\to 1}(s-1)\zeta_K(s) = \frac{2^{r+s}\pi^s reg(K)}{\omega_K |\Delta_K|^{1/2}} h_K$. Here, $\zeta_K(s)$ is the zeta function on *K*, which we will discuss; *r* and *s* are the number of real

embeddings and the number of pairs of complex embeddings, respectively; ω_K is the number of roots of unity in K; $reg(K)$ is the regulator of K (that is, the volume of the lattice of units); Δ_K is the discriminant of the field. Right away we can make some simplifications: for $d > 0$, $r = 2$, $s = 0$, and $\omega_K = 2$, the only roots being 1 and –1; for $d < 0$, $r = 0$, $s = 1$; since by the Dirichlet Unit Theorem the rank of the free abelian group part of U_K, the group of units, is $r + s - 1$, when $d < 0$ the regulator is 1. The discriminant is d for $d \equiv 1 \bmod 4$ and $4d$ for $d \equiv 2,3 \bmod 4$ (never 0, of course, because then it would not be squarefree); let $D = |\Delta_K|$. From our class work in section 9.1, if u generates the free part of U_K and $u > 1$, the regulator is $\ln u$. Therefore, we can solve for the class number: $h_K = \frac{\sqrt{D}}{2 \ln u} \lim_{s \to 1} (s-1)\zeta_K(s)$ for $d > 0$ and $h_K = \frac{\omega_K \sqrt{D}}{2\pi} \lim_{s \to 1} (s-1)\zeta_K(s)$ for $d < 0$. What remains is now to evaluate the limit.

The zeta function on K is defined in a similar way as the Riemann zeta function, though over all integral ideals rather than all positive integers, and using the norms of those ideals: $\zeta_K(s) = \sum_{U} \frac{1}{N(\boldsymbol{U})^s}$. Since the norm is multiplicative, we can use that wonderful factorization trick in Dirichlet series and express this infinite sum over all ideals as an infinite product over prime ideals: $\zeta_K(s) = \prod_{\boldsymbol{p}} \left(1 - \frac{1}{N(\boldsymbol{p})^s}\right)^{-1}$. The norm of each prime ideal $\boldsymbol{p}$ is either a prime p or the square of a prime in a quadratic field; there is also the problem with ramification. A given prime p, may remain prime (in which case the prime ideal corresponding to it has norm p^2), split, or ramify (in which two cases the

prime ideals corresponding to it have norm p); if it splits, p presents a contribution to two $\boldsymbol{p}$'s in the product, and if it ramifies, only one.

We may summarize this by saying that the contribution to the product for a given prime p is $(1-p^{-2s})^{-1}$ if p remains prime, $(1-p^{-s})^{-2}$ if p splits, and $(1-p^{-s})^{-1}$ if p ramifies. We'd like to write these in a more unified manner; if we factor out $(1-p^{-s})^{-1}$, we have remaining factors of $(1+p^{-s})^{-1}$, $(1-p^{-s})^{-1}$, and 1 respectively. We can define a function $\chi(p)$ on the set of integral primes such that it equals –1 when p remains prime, 1 when p splits, and 0 when p ramifies, and rewrite the contributions as $(1-p^{-s})^{-1}(1-\chi(p)p^{-s})^{-1}$.

We can extend $\chi(p)$ to the positive integers by declaring it multiplicative (such that $\chi(m)\chi(n)=\chi(mn)$ for all integer m, n) and to the negative integers with $\chi(-1)=1$ if $d>0$ and –1 if $d<0$. We will not prove that $\chi(p)$ is periodic with period D, but using this fact, as well as the obvious $\chi(1)=1$, we know that $\chi(p)$ is an abelian character on $\mathbf{Z}/(D)$, and since it is not the trivial character, the sum of $\chi(p)$ over the group must be 0 by Schur's Lemma. We call $\chi(p)$ the quadratic character on K.

We review the conditions for whether a prime remains prime, ramifies, or splits. A prime p ramifies if it divides the discriminant. If the polynomial x^2-d or $x^2-x+\frac{1}{4}(1-d)$, depending on whether d is congruent to 2,3 or 1 mod 4, respectively, is irreducible in $\mathbf{F}_p$, p remains prime; else, it splits. We can rewrite those two polynomials as $x^2-\frac{\Delta}{4}$ and $(x-\frac{1}{2})^2-\frac{\Delta}{4}$, so either way, the question is whether Δ is a square mod p (except when p is 2, in which case the fractions make no sense and the original forms

have to be employed). For primes that do not divide the discriminant, then, $\chi(p) = \left(\frac{\Delta}{p}\right)$.

To use quadratic reciprocity we must have primes on both sides; we can factor the discriminant into ramified primes and use quadratic reciprocity on each one. However, since the quadratic character is periodic, we know that this computation is finite and only necessary for the units of **Z**/(*D*).

Returning now to the task at hand, we can separate the product into products of each contribution separately, and doing this we obtain two functions,

$\zeta(s) = \prod_p \left(1 - \frac{1}{p^s}\right)^{-1}$ and $L(s,\chi) = \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1}$, such that $\zeta_K(s) = \zeta(s)L(s,\chi)$.

Both products are over integer primes, and the first of the two functions is the Riemann zeta function. We will not prove that $\lim_{s\to 1}(s-1)\zeta(s) = 1$ or that $L(s,\chi)$ is continuous at 1, but given these facts, the limit evaluates to $L(1,\chi)$. It remains to evaluate $L(1,\chi)$.

Expanding the product back into a sum for *L*, we get

$L(s,\chi) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$, which we can separate into one term for each congruence class mod *D* into $L(s,\chi) = \sum_{m=0}^{D-1} \chi(m) \sum_{n=1}^{\infty} \frac{c_m(n)}{n^s}$, where $c_m(n) = 1$ when *n* is congruent to *m* mod *D*, 0 otherwise. We can rewrite *c*, by means of being clever, as $c_m(n) = \frac{1}{D}\sum_{j=0}^{D-1} \gamma^{(m-n)j}$, γ being a primitive *D*th root of unity; this works because when the exponent is not zero, the sum adds all the way around the circle, canceling out to 0, but when the exponent is 0, each term contributes 1 to the sum. Substituting, we find that

$$L(s,\chi)=\frac{1}{D}\sum_{j=0}^{D-1}\left(\sum_{m=0}^{D-1}\chi(m)\gamma^{mj}\right)\sum_{n=1}^{\infty}\frac{\gamma^{-nj}}{n^{s}}.$$

Call the inner sum $g(\chi,\gamma^{j})$; we will not prove that $g(\chi,\gamma^{j})=\chi(j)g(\chi,\gamma)$ or that $|g(\chi,\gamma)|=\sqrt{D}$, but these are true.

We will employ the complex logarithm function; the principal value of which will lie in $(-\pi,\pi]$. For this principal value,

$\log(1-z)=-\left(z+\frac{z^{2}}{2}+\ldots+\frac{z^{n}}{n}+\ldots\right)$ is the Taylor series around $z=0$. Look familiar?

We can therefore rewrite the sum to the right of the parentheses as $-\log(1-\gamma^{-j})$, and rewrite $L(s,\chi)=-\frac{1}{D}g(\chi,\gamma)\sum_{j=0}^{D-1}\chi(j)\log(1-\gamma^{-j})$. Call that sum *S*, because that's what we'll evaluate now.

Let $\gamma=e^{2\pi i/D}$. For $0<j<D$, we have

$$1-\gamma^{-j}=\gamma^{-j/2}(\gamma^{j/2}-\gamma^{-j/2})=2i\gamma^{-j/2}\sin\frac{\pi j}{D}=2\sin\frac{\pi j}{D}e^{\left(\frac{\pi}{2}-\frac{\pi j}{D}\right)i},$$

so

$$\log(1-\gamma^{-j})=\ln\left|1-\gamma^{-j}\right|+\left(\frac{\pi}{2}-\frac{\pi j}{D}\right)i.$$

Consider first positive *d*, for which $\chi(-1)=1$. We can replace *j* by $D-j$ in *S* because the sum would sum over the same numbers with the exception of the overlap of 0 and *D*, and every instance of *j* here is periodic with period *D* so that doesn't matter. Hence,

$$S=\sum_{j=0}^{D-1}\chi(j)\log(1-\gamma^{-j})=\sum_{j=0}^{D-1}\chi(-j)\log(1-\gamma^{j})=\chi(-1)\sum_{j=0}^{D-1}\chi(j)\log(1-\gamma^{j})$$

$= \sum_{j=0}^{D-1} \chi(j) \log(1-\gamma^j)$. Adding the first and last of these expressions gives us

$2S = \sum_{j=0}^{D-1} \chi(j)\left(\log(1-\gamma^j) + \log(1-\gamma^{-j})\right)$. The two log arguments are complex conjugates of one another, so their principal value amplitudes cancel out and we are left with $S = \sum_{j=1}^{D-1} \chi(j) \ln\left(2\sin\frac{\pi j}{D}\right)$. The 2 goes away because the sum of a nontrivial character is 0 as has already been mentioned. By pairing together j and $D - j$ terms that are equal, we can cut the number of terms in half, finally getting

$L(1,\chi) = -\frac{2}{D} g(\chi,\gamma) \sum_{j=1}^{D/2} \chi(j) \ln\left(\sin\frac{\pi j}{D}\right)$, where the sum only runs through j relatively prime to D, since otherwise it will have a ramifying factor and the character will evaluate to 0. Since we know we are only dealing with positive real numbers, the actual value of g is unimportant; we need only the absolute value, which, as we shall not prove, is $\sqrt{D}$. Solving for the class number we find that, for $d > 0$,

$h_K = \frac{1}{\ln u}\left|\sum_{j=1}^{D/2} \chi(j) \ln\left(\sin\frac{\pi j}{D}\right)\right|$, the sum going over j relatively prime to D for convenience in computation.

Consider now negative d, for which $\chi(-1) = -1$. Similarly, we get

$S = \sum_{j=0}^{D-1} \chi(j) \log(1-\gamma^{-j}) = \sum_{j=0}^{D-1} \chi(-j) \log(1-\gamma^j) = \chi(-1) \sum_{j=0}^{D-1} \chi(j) \log(1-\gamma^j)$
$= -\sum_{j=0}^{D-1} \chi(j) \log(1-\gamma^j)$; again adding the first and last give us

$$2S = \sum_{j=0}^{D-1} \chi(j)\left(\log(1-\gamma^j) - \log(1-\gamma^{-j})\right).$$

This time, since the log arguments are complex conjugates, the real parts cancel out,

leaving $S = \sum_{j=1}^{D-1} \chi(j)\left(\frac{\pi}{2} - \frac{\pi j}{D}\right)i = -\frac{\pi i}{D}\sum_{j=1}^{D-1}\chi(j)j$ ($\frac{\pi}{2}$ cancels because the character is orthogonal to the trivial character, again). We have $L(1,\chi) = \frac{\pi i g(\chi,\gamma)}{D^2}\sum_{j=1}^{D-1}\chi(j)j$, and we become happy with $h_K = \frac{\omega_K}{2D}\left|\sum_{j=1}^{D-1}\chi(j)j\right|$, again with j only coprime with D.

The most difficult part of this formula is determining the fundamental unit for positive d; we have discovered a way to find the class number for a quadratic extension of the rationals. Let us then compute the class number for a few simple cases to see how this works, starting with $d = 2$.

$D = 8$; the numbers relatively prime to it are 1, 3, 5, and 7. 1 and 7 have character 1 ($7 = -1 \bmod 8$), so 3 and 5 must have character -1 since the sum of the four has to be 0. We must then compute $\ln\sin\frac{\pi}{8} - \ln\sin\frac{3\pi}{8}$, since we only need the first half for the formula. The fundamental root is $1+\sqrt{2}$, from the zeroth convergent of the partial fraction for $\sqrt{2}$. Because $\pi/8$ and $3\pi/8$ are complements, the ln expression is $\ln\tan\frac{\pi}{8} = \ln\frac{\sin\frac{\pi}{4}}{1+\cos\frac{\pi}{4}} = \ln\frac{\sqrt{2}}{2+\sqrt{2}} = \ln\frac{1}{1+\sqrt{2}}$. Then we have $\ln\frac{1}{1+\sqrt{2}} \Big/ \ln\left(1+\sqrt{2}\right) = -1$, and the class number is the absolute value, 1.

Let's now try an imaginary field, $d = -6$. This is not in Gauss's list of imaginary quadratic fields with class number 1, so we should not expect that to be our answer. $D = 24$, so the numbers relatively prime to it are 1, 5, 7, 11, –11, –7, –5, –1. The characters, by checking whether –24 is a square modulo 5, 7, and 11, are 1, 1,

1, 1, –1, –1, –1, –1, respectively, for the eight. The sum, therefore, is 1 + 5 + 7 + 11 – 13 – 17 – 19 – 23 = –48. Since there are only two roots of unity, namely 1 and –1, the formula gives us $\frac{2}{2 \cdot 24}|-48| = 2$ for the class number. Of course, both these examples are confirmed by PARI, which is good to know.

Quadratic number fields are one of the most interesting parts of number theory partly for their simplicity, but the class number problem is a difficult one. Gauss found that fields with $-d = 1, 2, 3, 7, 11, 19, 43, 67$, and 163 have class number 1, but not until much later, in the 1960's, was it proved that there are no other imaginary fields with class number 1. Finding which real fields have class number 1 is still an open problem.