November 2:

Math 431 Class Lecture Notes

- Remarks on class group computations
- Pythagoras, via elementary means
- Pythagoras, via Gaussian integers
- Pythagoras, via algebraic geometry
- Splitting of primes

0.1 Remarks on class group computations

The last phase of computing a class group involves verifying that various ideals are nonprincipal. In the case of imaginary quadratic fields this is usually quite easy, since one has to show that a positive definite quadratic form doesn't have a given value; usually the value is so small that the verification is trivial and in any case it is a finite problem.

Things can be a little harder for real quadratic fields, since the corresponding norm forms are indefinite. For instance, in the case of the field $\mathbf{Q}(\sqrt{70})$ we had to show that the equation

$$x^2 - 70y^2 = 2$$

was impossible. Fortunately, this particular case could be handled by congruence considerations (e.g., looking at the equation modulo 5). Sometimes more is needed, and we will return to this after we understand the structure of units a little better.

In the case of quadratic fields, it is sometimes handy to know the following lower bound on the power of 2 that divides the class number. Suppose that s distinct primes divide the discriminant of a quadratic field F. Then the class number is divisible at least by 2^{r-1} if F is imaginary and 2^{r-2} if F is real.

0.2 Pythagoras, via elementary means

We now begin a discussion of Diophantine equations, with the primary goal being to see how algebraic number theory can be of use.

Let's start with the famous Pythagorean equation $x^2 + y^2 = z^2$. Here are three possible approaches.

First, one can find all solutions by elementary number theory. We can divide out by a common factor if necessary to assume that x, y, and z are pairwise relatively prime. It is impossible for all three to be odd, and impossible for x and y to be odd (the square of an odd number $(2k+1)^2$ is congruent to 1 modulo 4, and the perfect square z^2 can not be congruent to 2 modulo 4). Thus one of x or y is even, and we can assume, to fix the ideas, that y is even. Then the equation can be written

$$y^2 = z^2 - x^2 = (z-x)(z+x).$$

Dividing by 4 gives

$$\left(\frac{y}{2}\right) = \left(\frac{z-x}{2}\right)\left(\frac{z+x}{2}\right).$$

We claim that the factors on the RHS are relatively prime. Indeed, if p divides both of them then it divides their sum, z, and their difference, x, which is impossible.

By unique factorization (in the rational integers!) if the product of two relatively prime integers is a perfect square then each factor is a perfect square. If $(z+x)/2 = m^2$ and $(z-x)/2 = n^2$ then we find that

$$z = m^2 + n^2, \quad x = m^2 - n^2, \quad y = 2mn.$$

In order to meet our congruence conditions, m and n must have opposite parity.

The conclusion is that if $x^2 + y^2 = z^2$ where x, y, and z are pairwise relatively prime integers, and y is even, then there are relatively prime integers m and n, of opposite parity, such that x, y, and z are described as above.

0.3 Pythagoras, via Gaussian integers

Perhaps a more natural, but more advanced, approach to $x^2 + y^2 = z^2$ is to observe that the LHS factors in the number ring $\mathbf{Z}[i]$. Assuming that x, y, and z are relatively prime, with y even, as above, we write

$$x^2 + y^2 = (x + iy)(x - iy) = z^2.$$

Any divisor of the two factors on the LHS divides their sum, $2x$, and their difference $2y$, and hence divides 2. Since x and y have opposite parity, neither factor is divisible by the prime $1 + i$ that divides 2, and the two factors are relatively prime. It follows from unique factorization of ideals that $(x + iy)$ is a perfect square, i.e., that

$$x + iy = u(m + ni)^2$$

where u is a unit. It follows by taking the conjugate that

$$x - iy = \overline{u}(m - ni)^2.$$

Since the square of $m + ni$ has even imaginary part it follows that $u = \pm 1$ (rather than $u = \pm i$) and by switching m and n if necessary we can take $u = 1$. Thus

$$x = m^2 - n^2, \quad y = 2mn$$

as above.

The idea of this proof can be used to solve the equation in $\mathbf{Z}[i]$.

0.4 Pythagoras, via algebraic geometry

It is interesting to thing of the solutions as an algebraic curve, a simple geometric idea shows how to find all such solutions.

Go to Ben's talk to find out about this!

0.5 Splitting of primes

The factorization of most (all but finitely many) rational primes in $\mathbf{Z}_F$ can be determined by factoring the minimal polynomial of a generator modulo the corresponding primes.

Theorem 1. Let $F = \mathbf{Q}(\alpha)$, where α is an algebraic integer with minimal polynomial $f(x)$, and let p be a rational prime. If

$$f(x) \equiv \prod_i f_i(x)^{e_i} \bmod p$$

where the f_i are distinct irreducible polynomials mod p, then

$$(p) := p\mathbf{Z}_F = \prod_i P_i^{e_i}$$

where the P_i are distinct prime ideals defined by

$$P_i = (p, f_i(\alpha)).$$

Example 2. If $f(x) = x^3 + x + 1$ then

$$f(x) \equiv (x - 14)^2(x - 3) \bmod 31$$

so $(31) = P^2Q$ in $\mathbf{Z}_F$, where $P = (31, \alpha - 14)$, and $Q = (31, \alpha - 3)$.

Example 3. If $f(x) = x^3 - x^2 - 2x - 8$ then we have seen then there are three distinct homomorphisms from $\mathbf{Z}_F$ to $\mathbf{F}_2$. Thus there are three prime ideals of degree one over 2 (the kernels of those three maps) and 2 splits completely $(2) = PP'P''$ in the field. This means that there is no α such that $\mathbf{Z}_F = \mathbf{Z}[\alpha]$! I.e., no power bases exists for this field. The reason is simple: if such an α did exist then its minimal polynomial would have to factor modulo 2 into the product of three distinct linear polynomials modulo 2; the only irreducible linear polynomials modulo 2 are x and $x + 1$.

The following theorem provides useful information on how primes split. A prime p is said to **ramify** in $\mathbf{Z}_F$ if and only if its factorization into primes in $\mathbf{Z}_F$ involves repeated factors, i.e., if and only if some e_i is bigger than 1.

Theorem 4. A prime p ramifies if and only if it divides the discriminant D_F.

The fact that ramify primes divide the discriminant isn't too hard, but the reverse implication (that a prime dividing the discriminant does in fact ramify) is harder.