November 7:

Math 431 Class Lecture Notes

- Fermat's Last Theorem
- Fermat's Last Theorem for $n = 3$
- Quadratic Forms

0.1 Fermat's Last Theorem

Many interesting (i.e., most of the partially or fully solvable) Diophantine equations are of the form $f(x, y) = 0$, $f \in \mathbf{Z}[x, y]$. The complex solutions to this equation form (at least when augmented with a finite number of points) a "Riemann surface." A Riemann surface is a compact surface that also has the structure of a one-dimensional complex manifold — any point has a neighborhood that comes equipped with an isomorphism to open subset of the complex plane, and any two such isomorphisms correspond to analytic mappings on the complex plane on their overlap.

Because of the complex structure, a Riemann surface is orientable and is therefore isomorphic (as a surface) to a sphere with some number g of handles; the number g is called the *genus* of the surface. It turns out, by an amazing instance of the unity of mathematics, that the behavior of a Diophantine equation is governed by the genus of the corresponding Riemann surface.

If the genus is 0 (i.e., the Riemann surface is isomorphic to the sphere) then either the corresponding curve has 0 solution or it has at least 1, and in the latter case the solutions can be parametrized in a natural way by rational numbers.

If the genus is 1 (i.e., the Riemann surface is isomorphic to the torus) then the curve is said to be an elliptic curve, and the theory is very interesting. The set of solutions has the structure of a finitely generated abelian group; and much is known about this group, but there are also some famous open questions about these groups.

If the genus is 2 or more then there are only finitely many solutions, by a famous theorem of Faltings from the 1980's.

The Fermat equation provides a good example. Let p be a prime, and consider the equation

$$x^p + y^p = z^p.$$

The $p = 2$ this equation has genus 0. Since it certainly has a rational point we can parametrize all solutions, and we've already seen several ways to do this.

If $p = 3$ then the equation has genus 1; it is a famous theorem (stated by Fermat, most likely first proved by Euler) that there are no nontrivial solutions.

If $p > 3$ then the equation has genus 2 or bigger and, for a given p, Faltings' theorem implies that there are only finitely many solutions. In fact, as we all know, work of Wiles and Taylor shows that there are no nontrivial solutions for any p. Curiously, their proof was indirect, and made extensive use of the elaborate theory of curves of genus 1, i.e., elliptic curves.

0.2 Fermat's Last Theorem for $n = 3$

We will now look at the elliptic curve $x^3 + y^3 = z^3$. The main tool will be the arithmetic (algebraic number theory) of the field $F = \mathbf{Q}(\omega)$ where $\omega = e^{2\pi i/3} = (-1 + \sqrt{-}3)/2$, and $\mathbf{Z}_F = \mathbf{Z}[\omega]$. Of course, this field arises because the Fermat equation $x^3 + y^3 = z^3$ factors over F as

$$(x + y)(x + \omega y)(x + \overline{\omega} y) = z^3.$$

We recall some basic facts about the arithmetic of F. There are six units in the ring of integers

$$(\mathbf{Z}_F)^* = \{\pm 1, \pm\omega, \pm\overline{\omega}\}.$$

The class group is trivial, so $\mathbf{Z}_F$ is a PID and a UFD. The prime 3 is ramified, and

$$(3) = P^2, \text{ where } P = (\pi), \pi = 1 - \omega.$$

To see the latter, note that

$$\begin{aligned} \pi^2 &= 1 - 2\omega + \omega^2 \\ &= -3\omega \end{aligned}$$

so that π^2 is an associate of 3.

There is one more special, somewhat surprising, fact that we need. This asserts that cubes of elements x of $\mathbf{Z}_F$ that are prime to π are congruent to 1 modulo a higher-than-expected power of π. This is somewhat analogous to the fact that squares of odd integers $x \in \mathbf{Z}$ are congruent to 1 modulo 8.

Lemma 1. If $x \in \mathbf{Z}_F$, $\gcd(x, \pi) = 1$ then

$$x^3 \equiv \pm 1 \bmod \pi^4.$$

Proof. Since $\mathbf{Z}_F/P = \mathbf{Z}/3\mathbf{Z} = \{-1, 0, 1\}$ we can assume, by multiplying x by -1 if necessary, that $x = 1 + \pi y$. Then

$$\begin{aligned} x^3 &= 1 + 3\pi y + 3\pi^2 y^2 + \pi^3 y^3 \\ &\equiv 1 + \pi y(3 + \pi^2 y^2) \bmod \pi^4. \end{aligned}$$

Substituting $\pi^2 = -3\omega$ gives

$$x^3 \equiv 1 + 3\pi y(1 - \omega y^2) \bmod \pi^4.$$

If $y \equiv 0 \bmod 3$ then the second term on the RHS is divisible by π^4 and the lemma follows. If $y \equiv \pm 1 \bmod 3$ then $y^2 \equiv 1 \bmod 3$ and

$$1 - \omega y^2 \equiv 1 - \omega = \pi\pi \bmod 3.$$

Thus in either case we find that $x^3 \equiv 1 \bmod \pi^4$ as claimed. □

Now we consider the Fermat equation $x^3 + y^3 = z^3$. WLOG x, y, z are pairwise relatively prime. Using the Lemma and looking at the equation modulo π^4 we see that there is no way for the equation to hold if all of the variables are prime to π, and that in fact exactly one of them is divisible by π.. By permuting variables (and negating) as necessary we assume, to fix the ideas, that z is divisible by π, and x and y are relatively prime to π.

To clarify the terminology, for any nonzero a in $\mathbf{Z}_F$ we let $v(a)$ be the exponent on the exact power of π that divides a. We note that $v(ab) = v(a) + v(b)$, and $v(a + b) \geq \min(v(a), v(b))$.

We prove that no solutions exist by induction on $v(z)$. As often happens with induction assertions it is easier to generalize the assertion and prove a harder statement, since this makes the induction hypothesis stronger.

Theorem 2. There do not exist x, y, z in $\mathbf{Z}_F$ and a unit $u \in \mathbf{Z}_F^*$, with x and y relatively prime, $v(x) = v(y) = 0, v(z) > 0$, such that

$$x^3 + y^3 = uz^3.$$

Proof. The proof is by induction on $v(z)$. If $v(z) = 1$ then $z = \pi w$ where w has $v(w) = 0$, i.e., w is relatively prime to π. Then

$$x^3 + y^3 = u\pi^3 w^3.$$

Looking modulo π^4 and using the Lemma we see that the requirement that the LHS be divisible by π forces x^3 and y^3 have opposite sign, so that

$$1 - 1 \equiv x^3 + y^3 \equiv u\pi^3 w^3 \bmod \pi^4.$$

This equation is manifestly impossible since the LHS is 0, and the RHS is nonzero modulo π^4.

Now suppose that the assertion is true for z with $v(z) = n$. Suppose that $v(z) = n + 1$, i.e., that $z = \pi^{n+1} w$ where $v(w) = 0$. Write the equation as

$$(x + y)(x + \omega y)(x + \overline{\omega} y) = u\pi^{3n+3} w^3.$$

The gcd between any two factors on the LHS is equal to π. For instance,

$$(x + y) - (x + \omega y) = \pi y, \quad \omega(x + y) - (x + \omega y) = -\pi y$$

and since x and y are relatively prime the gcd is equal to π. Thus one of the factors is divisible by π^{3n+1} and the other two are divisible by π but no higher power of π. Fix the notation (by multiplying y by ω as needed) so that

$$v(x + y) = 3n + 1, \quad v(x + \omega y) = 1, \quad v(x + \overline{\omega} y) = 1,$$

i.e.,

$$x + y = \pi^{3n+1} w_0, \quad x + \omega y = \pi w_1, \quad x + \overline{\omega} y = \pi w_2$$

where $v(w_i) = 0$, and the w_i are pairwise relatively prime. Substituting these into our equation and canceling powers of π gives

$$w_0 w_1 w_2 = uw^3.$$

Using unique factorization, we conclude that each of the w_i is a unit times a cube, say $w_i = u_i x_i^3$. From the curious identity

$$(x + y) + \overline{\omega}(x + \omega y) + \omega(x + \overline{\omega} y) = (x + y)(1 + \omega + \overline{\omega}) = 0$$

we get

$$\pi^{3n+1}u_0x_0^3 + \pi u_1x_1^3 + \pi u_2x_2^3 = 0$$

or, by dividing by πu_0,

$$x_1^3 + u'x_2^3 = u''(x_0\pi^n)^3$$

where u and u'' are units. A brief calculation using the Lemma shows that this equation is impossible modulo π^4 unless $u' = \pm 1$ and, multiplying x_2 by -1 if necessary, we see that we have found a solution to our original equation with $v(z) = n$. This is impossible by the induction hypothesis, finishing the proof. □

The idea of reducing a known solution to a smaller one can be used to give a (much shorter) proof of the impossibility of a solution for Fermat's equation with exponent 4, and this "method of descent" is a mainstay of the techniques of finding rational points on elliptic curves.

0.3 Quadratic forms

The quadratic form $f(x,y) = ax^2 + bxy + cy^2$ has discriminant $D = b^2 - 4ac$. In the case $D = -20$ it turns out that, up to a linear change of variables, there are only two quadratic forms:

$$f_1(x,y) = x^2 + 5y^2, \qquad f_2(x,y) = 2x^2 + 2xy + 3y^2.$$

More precisely, if $f(x,y)$ is a binary quadratic form as above and it has discriminant -20 then there is an invertible change of variables such that

$$f(rx + sy, tx + uy)$$

is one of the above forms, where $ru - st = \pm 1$.

It turns out that this is intimately connected with the fact that the field $\mathbf{Q}(\sqrt{-5})$, of discriminant -20, has class number two.

The two forms can be expressed as

$$x^2 + 5y^2 = N(x + y\sqrt{-5}), \qquad 2x^2 + 2xy + 3y^2 = N(2x + (1 + \sqrt{-5})y)/2.$$

Thus in order to find n as a value of the first form we must find an element of $\mathbf{Z}_F$ whose norm is n, and in order to find n as a value of the second form we must find an element of

$$P := (2, 1 + \sqrt{-5}) = \langle 2, 1 + \sqrt{-5} \rangle$$

whose norm is $2n$. The former is accomplished by finding a principal ideal of norm n, and this can be done by understanding how the prime divisors of n factor into primes in $\mathbf{Q}(\sqrt{-5})$, and whether or not those primes are principal ideals. The latter can be accomplished by finding principal ideals of the form PI, where I has norm n, and is again predicated on an understanding of the class group (P is a nonprincipal ideal and therefore generates the class group).