Chapter 13 Lecture Notes

Greg Knapp

May 25, 2022

0.1 Intro

- Recall that a Diophantine equation is a polynomial equation where the only coefficients are integers
- We learned last term that for linear Diophantine equations: $ax + by = c$ has a solution in integers x and y if and only if $(a, b) \mid c$
- We also learned how to solve them when there are solutions (the Euclidean algorithm)
- What about other Diophantine equations?
  - Can we classify when there are solutions?
  - Can we solve them?
- The answer to the second question (and hence the first) is: no
- Hilbert's 10th problem asks the following: "Given a Diophantine equation with any number of unknown quantities and with rational integral numerical coefficients: To devise a process according to which it can be determined by a finite number of operations whether the equation is solvable in rational integers"
- See `https://logic.pdmi.ras.ru/~yumat/Julia/`
- This of course means that it's a substantial and difficult problem.
- It took about 70 years to give a complete proof that no such algorithm exists.
- Proof passes through mathematical logic and essentially shows that every set which is recursively enumerable is Diophantine.
- Since some recursively enumerable sets are noncomputable, some Diophantine sets are noncomputable
- So the best we can hope to do is solve or classify solutions to some Diophantine equations

1 Pythagorean Triples

1.1 Intro

- Turns out that we're pretty familiar with a nonlinear Diophantine equation: $a^2 + b^2 = c^2$
- We even know some solutions: $(3, 4, 5), (5, 12, 13), (6, 8, 10)$
- How many solutions are there?
- Can we classify all of the solutions?
- **Def:** A <u>Pythagorean triple</u> is a triple (a, b, c) of positive integers so that $a^2 + b^2 = c^2$
- Note: here we use (a, b, c) for the triple, not for the gcd...context should make it clear which we mean.

1.2 A Reduction

- We first claim that there are infinitely many Pythagorean triples: Since $3^2+4^2=5^2$, note that for any integer k, $(3k)^2+(4k)^2=(5k)^2$.
- Hence, $a=3k$, $b=4k$, and $c=5k$ gives a solution
- Note that $k=2$ was how we got $(6,8,10)$
- But also note that $(5,12,13)$ doesn't come from one of these values of k
- So okay, now $a=5k$, $b=12k$, and $c=13k$ gives an infinite family of solutions
- Are there any that we didn't get yet?
- It would be nice to associate a word to "minimal" Pythagorean triple
- **Def:** A Pythagorean triple is primitive if x, y and z are relatively prime
- We have already seen that any primitive Pythagorean triple can be multiplied by an integer to yield a nonprimitive Pythagorean triple
- On the other hand, we claim that a nonprimitive Pythagorean triple is a multiple of a primitive Pythagorean triple.
- Proof:
  - Suppose that (a,b,c) are integers satisfying $\gcd(a,b,c)=d$ and $a^2+b^2=c^2$
  - Then there exist integers a', b', c' so that $a=a'd$, $b=b'd$, $c=c'd$
  - As a consequence $\gcd(a',b',c')=1$
  - Moreover, $a^2+b^2=c^2$ implies $\left(\frac{a}{d}\right)^2+\left(\frac{b}{d}\right)^2=\left(\frac{c}{d}\right)^2$, i.e. $a'^2+b'^2=c'^2$
  - So (a,b,c) is a multiple of the primitive Pythagorean triple (a',b',c')
- So we can now revise our questions from before: how many primitive Pythagorean triples are there?

1.3 Infinitely Many!

- **Thm:** If m, n are relatively prime positive integers with $m>n$ and $m \not\equiv n \mod 2$, then $x=m^2-n^2$, $y=2mn$, and $z=m^2+n^2$ is a primitive Pythagorean triple
- Corollary: there are infinitely many Pythagorean triples
- Proof:
  - Need to check two things: $x^2+y^2=z^2$ and $\gcd(x,y,z)=1$
  - For the first:

$$\begin{aligned} x^2+y^2 &= (m^2-n^2)^2+(2mn)^2 \\ &= m^4-2m^2n^2+n^4+4m^2n^2 \\ &= (m^2+n^2)^2 \\ &= z^2 \end{aligned}$$

  - Great, so we have a Pythagorean triple.
  - If (x,y,z) is not primitive, there exists a prime p so that $p \mid x, y, z$
  - Since $m \not\equiv n \mod 2$ and $x=m^2-n^2$, $x \equiv 1 \mod 2$, so $p \neq 2$
  - Since $p \mid x$ and $p \mid z$, $p \mid x+z=2m^2$ and $p \mid z-x=2n^2$ so $p \mid m, n$.

  - But this contradicts the fact that $(m,n)=1$.
  - Hence, (x,y,z) is primitive.

- Moreover, the converse is true: every primitive Pythagorean triple has this form.
- Given (x,y,z), take $r=(z+x)/2$ and $s=(z-x)/2$.
- Prove that r and s are squares and let $m=\sqrt{r}$ and $n=\sqrt{s}$.
- Then prove that m and n have the desired quantities.

1.4 Geometric Perspective

- Of course, Pythagorean triples have something to do with geometry
- So shouldn't we be able to talk to Pythagorean triples by talking about triangles or something?
- Answer: kinda sorta
- Picking a Pythagorean triple (a,b,c) is the same as picking a point in the xy-plane (a,b) so that its distance from the origin is an integer
- Draw picture
- But it's easier if we look at where that line intersects the unit circle
- Where does that line intersect the unit circle?
- We make a vector (a,b) into a unit vector by dividing by its distance, $\sqrt{a^2+b^2}$
- But because we picked a Pythagorean triple point, that distance is an integer c
- So our point on the unit circle is $\left(\frac{a}{c},\frac{b}{c}\right)$
- On the other hand, if we start with a rational point on the unit circle $\left(\frac{p}{q},\frac{r}{s}\right)$, we can get a Pythagorean triple by multiplying both sides of $\left(\frac{p}{q}\right)^2+\left(\frac{r}{s}\right)^2=1$ by q^2s^2 to get $(ps)^2+(rq)^2=(qs)^2$
- So what we find is that we have a bijection between

$$\{\text{rational points on unit circle in quadrant 1}\} \leftrightarrow \{\text{Pythagorean triples}\}$$

- Now that we've made this connection, we want to ask if it's any easier to describe rational points on the circle than it is to describe Pythagorean triples
- Let's start with a rational point on the circle: $(-1,0)$
- This may seem like an odd choice because this definitely isn't going to yield anything close to a Pythagorean triple, but it works because it's far away from such points
- Note that if we start with any rational point (x,y) on the unit circle, then the slope of the line between $(-1,0)$ and (x,y) is $\frac{y}{x+1}$ which is rational
- So rational points on the circle yield rational slope lines
- We claim that rational slope lines also yield rational points on the circle
- Check on your own: the line with slope t passing through the point $(-1,0)$ also intersects the circle at $\left(\frac{1-t^2}{1+t^2},\frac{2t}{1+t^2}\right)$
- If t is rational, this yields a rational point.

- What we've shown is that all rational points on the circle have the form $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$ where t is a rational number
- What if we write $t = \frac{n}{m}$ for positive integers n and m?
- Then some arithmetic yields the point $\left(\frac{m^2-n^2}{m^2+n^2}, \frac{2mn}{m^2+n^2}\right)$
- And the corresponding Pythagorean triple is $(m^2 - n^2, 2mn, m^2 + n^2)$

1.5 An Application to Teaching Calculus

- How is this kind of thing useful to non-number-theorists?
- Recall the arc length formula: the arc length of the curve given by $y = f(x)$ between $x = a$ and $x = b$ is
$$\int_a^b \sqrt{1 + f'(x)^2}\, dx$$
- Let's say that you're teaching MATH 252 and you need to come up with a good example to illustrate this formula for your students
- But you haven't taught them trig sub yet because the book doesn't cover things in that order
- So you would really really like it if you could have $\sqrt{1 + f'(x)^2} = g(x)$ for some rational function $g(x)$ that you can actually integrate
- Well that's the same thing as saying that $1 + f'(x)^2 = g(x)^2$
- But you know how to rationally parametrize the circle because you took number theory: Rearranging the formula
$$\left(\frac{1-x^2}{1+x^2}\right)^2 + \left(\frac{2x}{1+x^2}\right)^2 = 1$$
into
$$(1 - x^2)^2 + (2x)^2 = (1 + x^2)^2$$
and then
$$\left(\frac{1-x^2}{2x}\right)^2 + 1 = \left(\frac{1+x^2}{2x}\right)^2$$
means that if you take $f'(x) = \frac{x^2-1}{2x}$, then you get $g(x) = \frac{x^2+1}{2x}$
- Then $f'(x) = \frac{x}{2} - \frac{1}{2x}$ implies that you should start with $f(x) = \frac{x^2}{4} - \frac{1}{2}\log|x|$
- So you ask your students to compute the arc length of $\frac{x^2}{4} - \frac{1}{2}\log|x|$ on the interval "whatever" and then, ta-da!, the integral works out magically.

2 Fermat's Last Theorem

3 Sums of Squares

3.1 Intro

- We previously looked at $x^2 + y^2 = z^2$, i.e. "which squares are the sum of two other squares?"
- But why not generalize and just ask "which integers are the sum of two other squares?"
- I.e. for which n do there exist $x, y \in \mathbb{Z}$ so that $x^2 + y^2 = n$?

- Note: prima facie, this is a question about additive number theory
- We're asking about adding up squares to get a given number
- However, we can quickly turn it into a question about multiplicative number theory:
- **Thm:** If m and n are the sum of two squares, then mn is the sum of two squares.
- Pf:
  - Suppose that $m = a^2 + b^2$ and $n = c^2 + d^2$
  - Verify yourself that $mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2$
- This converts our problem from an additive problem into (partially) a multiplicative problem
- Now that we know that "being a sum of squares" is a multiplicative problem, we can start by asking "which primes are the sum of squares?"
- At least then, we'll have a partial answer to "which integers are sums of squares" because we'll be able to take products of primes which are sums of squares
- E.g. we can easily check that $5 = 2^2 + 1^2$ and $13 = 2^2 + 3^2$ are sums of two squares. So all numbers of the form $5^n \cdot 13^m$ are sums of two squares

3.2 Primes as the Sum of Two Squares

- **Thm:** If $p \equiv 3 \mod 4$ is prime, then p is not the sum of two squares
- Pf
  - Sums of squares are always $0, 1, 2$ mod 4, never 3
- The surprising thing is that the converse is also true
- **Thm:** If $p \equiv 1, 2 \mod 4$ is prime, then p is the sum of two squares
- There are plenty of elementary proofs of this fact, but there are very few easy proofs.
- Due to lack of time, we'll skip this proof.

3.3 The Classification of Integers as the Sum of Two Squares

- So now we know that products of primes $\equiv 1 \mod 4$ can be written as the sum of two squares
- Is this all of the integers which can be written as the sum of two squares?
- No!
- Warm-up: find an integer which is not the product of primes $\equiv 1 \mod 4$ and which is the sum of two squares
- 9 works for a silly example and $18 = 3^2 + 3^2$ works for a less silly example
- So what's the classification?
- **Thm:** The positive integer n is the sum of two squares if and only if each prime factor $\equiv 3 \mod 4$ occurs to an even power in the prime factorization of n
- Proof:
  - First suppose that each prime factor $\equiv 3 \mod 4$ appears to an even power in the prime factorization

- Then we can write $n = t^2 u$ where every prime $p \mid n$ with $p \equiv 3 \mod 4$ has $p \mid t$
- Since u is a product of primes $\equiv 1 \mod 4$, we can write u as the sum of two squares $u = x^2 + y^2$
- But then $n = t^2 u = (tx)^2 + (ty)^2$
- Where's the lie?
- Okay, what if $u = 1$? Then $u = 0^2 + 1^2$ and everything works fine
- For the converse, suppose that n is the sum of two squares, $n = x^2 + y^2$ and that $n = p^{2j+1} r$ for $p \nmid r$
- Let $(x, y) = d$, $a = x/d$, $b = y/d$, and $m = n/d^2$ so that $(a, b) = 1$ and $a^2 + b^2 = m$
- If p^k is the largest power of p dividing d, then m is divisible by $p^{2j-2k+1}$ and in particular, $p \mid m$
- $p \nmid a, b$ because if it divided a, then it would divide $m - a^2 = b^2$ and vice versa
- Hence, there exists z so that $az \equiv b \mod p$ (note the change of modulus)
- But now we have
$$0 \equiv m = a^2 + b^2 \equiv a^2 + (az^2) \equiv a^2(1 + z^2) \mod p$$
- Since a^2 is not divisible by p, we must have $1 + z^2 \equiv 0 \mod p$, i.e. $z^2 \equiv -1 \mod p$
- Hence, -1 is a quadratic residue mod p
- Hence, $p \equiv 1, 2 \mod 4$...contradiction
- Therefore, n is only divisible by even powers of primes $\equiv 3 \mod 4$

3.4 More Squares

- Okay, sure now we know which integers can be written as the sum of two squares
- We can definitely write more numbers as a sum of three squares: e.g. $3 = 1^2 + 1^2 + 1^2$
- Is it all of them?
- Nope: 7 can't be written as a sum of three squares
- But 7 can be written as the sum of four squares: $7 = 2^2 + 1^2 + 1^2 + 1^2$
- And if you keep searching, you'll find that every positive integer you pick can be written as the sum of four squares
- **Thm:** (Lagrange) Every positive integer can be written as the sum of four squares.
- This theorem begins similarly to the discussion on sums of two squares
- **Thm:** If m and n are each the sum of four squares, then mn is the sum of four squares
- This again follows from a weird algebraic identity.