Lecture 23
Pythagorean Triples, Fermat Descent

Diophantine Equations - We start with **Pythagorean Triples** (x, y, z) where $x^2 + y^2 = z^2$. Problem is to find all Pythagorean triples. Reductions - can scale triples, so can assume $\gcd(x, y, z) = 1$. We are looking for primitive solutions. Enough to classify solutions. Suppose (x, y, z) is such a triple. Then $(x, y) = (y, z) = (x, z) = 1$, for if $a|x$ and $a|y$ then $a^2x'^2 + a^2y'^2 = z^2 \Rightarrow a|z$, contradicts primitivity.

So, $x, y, z \in \mathbb{N}$, coprime in pairs. x, y can't both be even, and can't both be odd (else $x^2 + y^2 \equiv 2 \mod 4$, which can't be a square), so are opposite parity. wlog assume x odd and y even.

$$\begin{aligned} x^2 + y^2 = z^2 &\Rightarrow y^2 = z^2 - x^2 = (z - x)(z + x) \\ &\Rightarrow \frac{y^2}{4} = \left(\frac{y}{2}\right)^2 = \left(\frac{z - x}{2}\right)\left(\frac{z + x}{2}\right) \end{aligned}$$

Still all integers. $\left(\frac{z-x}{2}\right)$ and $\left(\frac{z+x}{2}\right)$ are coprime, since if $a|$both, then $a|$sum $\Rightarrow a|z$, and $a|$difference $\Rightarrow a|x$.

So we have two coprime integers, whose product is a square $\Rightarrow$ both are squares.

$$\begin{aligned} &\frac{z + x}{2} = r^2,\ \frac{z - x}{2} = s^2 \text{ for some } r, s \in \mathbb{N} \\ &\Rightarrow z = r^2 + s^2, x = r^2 - s^2 \\ &\Rightarrow \left(\frac{y}{z}\right)^2 = r^2s^2 \Rightarrow y = 2rs \\ &\Rightarrow (x, y, z) = (r^2 - s^2, 2rs, r^2 + s^2) \\ &\text{eg., } r = 1, s = 2 \Rightarrow (3, 4, 5) \end{aligned}$$

Since $x > 0$, $r > s$ and r and s must have opposite parity (since $r^2 \pm s^2$ odd), and $\gcd(r, s) = 1$ (else if $a|rs$, then $a|x = r^2 - s^2$ and $a|z = r^2 + s^2$).

A more geometrical way of seeing the result, if $x^2 + y^2 = z^2 \Rightarrow \frac{x}{z}^2 + \frac{y}{z}^2 = 1$. Set $\alpha = \frac{x}{z}, \beta = \frac{y}{z} \Rightarrow \alpha^2 + \beta^2 = 1$. In other words, finding solutions to $x^2 + y^2 = z^2$ in integers and solutions to $\alpha^2 + \beta^2 = 1$ in rationals is equivalent.

Find all rational points on curve $x^2 + y^2 = 1$ (unit circle) - obvious solution $(1, 0)$.

Suppose (u, v) is some other rational solution. Consider the line joining $(1, 0)$

and (u, v). Slope $m = \frac{v}{u-1}$ is rational since u, v are rational. Line is $y = m(x-1)$.

$$\begin{aligned} m = \frac{v}{u-1} &\Rightarrow v = m(u-1) \\ &\Rightarrow u^2 + v^2 = 1 \\ &\Rightarrow u^2 + m^2(u-1)^2 = 1 \\ m^2(u-1)^2 &= 1 - u^2 \\ &= (1-u)(1+u) \\ &\Rightarrow m^2 = \frac{1+u}{1-u} \text{ (can divide since } 1-u \neq 0\text{)} \end{aligned}$$

If we solve for u we get $u = \frac{m^2-1}{m^2+1}$, which means that $v = m(u-1) = \frac{-2m}{m^2+1}$.

$$(u, v) = \left(\frac{m^2-1}{m^2+1}, \frac{-2m}{m^2+1}\right), m \in \mathbb{Q}$$

to get integer solution, set $m = -\frac{r}{s}$, then you get

$$\left(\underbrace{\frac{r^2-s^2}{r^2+s^2}}_{u}, \underbrace{\frac{2rs}{r^2+s^2}}_{v}\right) \Rightarrow (\underbrace{r^2-s^2}_{x}, \underbrace{2rs}_{y}, \underbrace{r^2+s^2}_{z})$$

We can apply this general method to any (nice) conic curve (plane curve cut out by equation of total degree in x, y of 2 - circles, parabola, hyperbolas, ellipses). Given a conic curve, and we know at least one rational point on it, then this slope method will give us all the rational points on the curve. (NOTE - not always true that conic curves have rational points - eg., $x^2 + y^2 + 1 = 0$ has no real (or rational) points)

Remember Fermat's Last Theorem - $x^n + y^n = z^n$ has no non-trivial (ie., $xyz \neq 0$) solutions if $n \geq 3$. We'll show this for $n = 4$. Proof uses method called Fermat's infinite descent: Given any integer solution, can produce a smaller integer solution. Since only finitely many positive integers smaller than initial solution, there cannot be any solutions. We'll actually show that there does not exist $x, y, z \in \mathbb{N}$ such that $x^4 + y^4 = z^2$, which is stronger.

Theorem 82. *$x^4 + y^4 = z^2$ has no solutions in $\mathbb{Z}_{>0}$*

Proof. Suppose there is a solution. Let z be the size of the solution. Then there's a possibly smaller solution with x, y coprime, for if $a|xy$ then $a^4|z^2 \Rightarrow a^2|z \Rightarrow \left(\frac{x}{a}\right)^4 + \left(\frac{y}{a}\right)^4 = \left(\frac{z}{a^2}\right)^2$. So we may as well assume x, y coprime. Then x, y, z are coprime in pairs. $x^4 + y^4 = z^2$ can be rewritten as $(x^2)^2 + (y^2)^2 = z^2$, with

x^2, y^2, z coprime in pairs. wlog, we can assume x odd and y even, and by what we know of Pythagorean triplets,

$$(x^2, y^2, z) = (r^2 - s^2, 2rs, r^2 + s^2)$$
$$r > s > 0$$
$$(r, s) = 1 \text{ and are opposite parity}$$

First equations gives that $x^2 + s^2 = r^2$. We have x odd and $r + s$ odd, which forces s to be even, r odd, and so

$$(x, s, r) = (t^2 - u^2, 2tu, t^2 + u^2)$$
$$t > u > 0$$
$$(t, u) = 1 \text{ and are opposite parity}$$

Now $y^2 = 2rs$, y even, s even.

$$\left(\frac{y}{2}\right)^2 = r\left(\frac{s}{2}\right)$$

and r and $\frac{s}{2}$ are coprime since r, s are coprime, which means that r and $\frac{s}{2}$ must both be squares. Define $\frac{s}{2} = m^2$ and $r = n^2$, and so $\frac{s}{2} = tu = m^2$, and with t, u coprime, t and u are squares and we can write $t = k^2, u = l^2$. Plug into $r = t^2 + u^2 \Rightarrow n^2 = k^4 + l^4$, which gives another solution (k, l, n) to equation, with $k, l, n > 0$.

$$n \le n^2 = r \le r^2 < r^2 + s^2 = z$$

and so this is a smaller solution. ■

Techniques for Diophantine Equations and interesting examples

Say we need to show some diophantine equation (some polynomial equation with integer coefficients) has no solutions. If you can show that there are no solutions mod m, then there are no solutions (known as checking for local solutions)

Eg. $x^2 = 3 + 4y^3$ has no solutions because mod 4 this says $x^2 \equiv 3 \mod 4$

Eg. $x^3 + y^3 - 7z^3 = 3$ has no solutions because this says $x^3 + y^3 \equiv 3 \mod 7$, and a cube mod 7 can only be $0, \pm 1$ (± 1 since $x^6 = (x^3)^2 \equiv 1 \mod 7$ by FlT)

Eg. Only solution to $x^3 + 2y^3 + 4z^3 = 0$ is $(0, 0, 0)$.

Proof. By infinite descent. Assume non-trivial, produce smaller. Assume $\gcd(x, y, z) = 1$ (otherwise can get smaller solution). $\mod 2 \Rightarrow x^3 \equiv 0 \mod 2 \Rightarrow x \equiv 0 \mod 2$. Set $x = 2x'$

$$\begin{aligned} 8x'^3 + 2y^3 + 4z^3 &= 0 \\ 4x'^3 + y^3 + 2z^3 &= 0 \\ &\Rightarrow y = 2y' \\ &\Rightarrow z = 2z' \\ &\Rightarrow 2|x, y, z \end{aligned}$$

and so (x', y', z') is smaller solution ■

Eg. $y^2 = x^3 + D$ is a classical equation

Theorem 83. *$y^2 = x^3 + 7$ has no integer solutions.*

Proof. $y^2 \geq 0$ so $x \geq -1$, so RHS is nonzero. Now if x were even, we'd have $y^2 \equiv 7 \equiv 3 \mod 4$, which is impossible, so x is odd, which means that $x^3 + 7$ is even, so y is even. Rewrite as

$$y^2 + 1 = x^3 + 8 = (x + 2)(x^2 - 2x + 4)$$

So if some prime p divides $y^2 + 1$, then p has to be odd and $y^2 \equiv -1 \mod p$, which means that $p \equiv 1 \mod 4$.

But also, $x^3 \equiv y^2 - 7 \equiv 0 - 7 \mod 4 \equiv 1 \mod 4$, and so $x \equiv 1 \mod 4$, which means that $x + 2 \equiv 3 \mod 4 \geq 1$. So there exists a prime dividing $x + 2$ which is $3 \mod 4$, and so $p|y^2 + 1$, which is a contradiction. ■

18.781 Theory of Numbers
Spring 2012