MATH 115, SUMMER 2012
LECTURE 24

JAMES MCIVOR

Today we study Pythagorean triples: integers x, y, z satisfying the equation

$$x^2 + y^2 = z^2.$$

This is our first non-linear diophantine equation. We'll give two proofs that all Pythagorean triples have a certain form; later (i.e., next week) we will try to adapt both our arguments to other types of equations.

1. Preliminary Observations

- You probably know a few Pythagorean triples: 3,4,5 or 5,12,13 or 7,24,25 or 8,15,17.

- if we have a triple x, y, z, then any multiple of this triple gives another triple.

- the triples represent side lengths of a right triangle. the multiples of triangles give similar triangles.

- we only care about distinct triangles, so we seek all the triples where the gcd of x, y, z is 1. These triples are called **primitive**.

- actually it's enough to require only that the gcd of x, y is 1 (see the beginning of the second proof)

- thus our task is to find all positive primitive Pythagorean triples.

2. Geometric Solution

- for this argument, we describe not the primitive triples, but *all* triples. You can go back and figure out which ones are primitive, but we won't do so, since our second argument makes the primitive ones more explicit.

- we are working over integers, but here we can actually work over rationals numbers instead:

- if we have a pythagorean triple x, y, z, then neither x nor y nor z is zero, so we get an expression

$$\left(\frac{x}{z}\right)^2 + \left(\frac{y}{z}\right)^2 = 1$$

in rational numbers.

Conversely, suppose we have two rational numbers $\frac{a}{b}$ and $\frac{c}{d}$, which we may take to be reduced, i.e., $(a, b) = (c, d) = 1$ satisfying the equation

$$X^2 + Y^2 = 1$$

Then we get

$$(ad)^2 + (cb)^2 = (bd)^2,$$

a pythagorean triple.

So we have a bijection between pythagorean triples and rational numbers satsifying $X^2 + Y^2 = 1$.

- since this is the equation of a circle, we call rational solutions to this equation **rational points** on the circle.

- here's how to find them all:

- draw cicle. Fix point $P = (-1, 0)$ on the circle. If (x, y) is a rational point different from P on the circle, then the line from it to P has rational slope, so we get a rational number.

- conversely, given any rational number m, the line through P with slope m passes through the circle. We check that it has rational coordinates, as follows.

- the given line through P is

$$y = m(x + 1)$$

plug into equation of circle:

$$x^2 + m^2(x + 1)^2 = 1$$

rearranging:

$$(m^2 + 1)x^2 + 2m^2x + m^2 - 1 = 0$$

Use quadratic formula:

$$\begin{aligned} x &= \frac{-2m^2 \pm \sqrt{4m^4 - 4(m^2 + 1)(m^2 - 1)}}{2(m^2 + 1)} \\ &= \frac{-2m^2 \pm 2}{2(m^2 + 1)} \\ &= \frac{-m^2 \pm 1}{m^2 + 1} \end{aligned}$$

if we use the negative sign, we get $x = -1$, which corresponds to the point P.

If we use the plus sign, we get the x-coordinate of the other point on the circle, namely $x = \frac{1-m^2}{1+m^2}$.

- plug this into the equation of the line to get $y = \frac{2m}{1+m^2}$.

- so for each rational number m we get a rational point

$$\left(\frac{1 - m^2}{1 + m^2}, \frac{2m}{1 + m^2} \right)$$

Thus all the rational points on the circle (except for P, which corresponds to slope $m = \infty$) have this form.

- don't forget that we were originally interested in pythagorean triples. what triples do the above rational points give us?

- write $m = \frac{a}{b}$ (we can take $\gcd(a, b) = 1$ if we like), and plug in to the above, giving

$$\left(\frac{1 - \frac{a}{b}^2}{1 + \frac{a}{b}^2}, \frac{2\frac{a}{b}}{1 + \frac{a}{b}^2} \right) = \left(\frac{b^2 - a^2}{a^2 + b^2}, \frac{2ab}{a^2 + b^2} \right)$$

these are our rational solutions to $X^2 + Y^2 = 1$. By clearing the denominators, the corresponding solutions to $x^2 + y^2 = z^2$ have the form

$$(b^2 - a^2)^2 + (2ab)^2 = (a^2 + b^2)^2$$

It's not clear which values of a and b make this a primitive triple, but we'll deal with that in the next proof anyway.

3. Solution by Factoring

Here we show that the Pythagorean triples have the form

$$(b^2 - a^2)^2 + (2ab)^2 = (a^2 + b^2)^2$$

by a different argument.

- so from now on, let x, y, z be a primitive triple

- we may also assume that x, y, z are all positive, since they are all squared in the equation.

- first we show that even if the gcd of just two of x, y, and z is one, then still x, y, z is a primitive triple.

- the idea is that if a divides two of x, y and z, then it divides the third, so all three have the same common divisors, hence the same gcd.

- for example, if $a|x$ and $a|z$, then $a^2|z^2 - x^2 = y^2$, so $a|y$

- now assume x, y, z is primitive and positive. x and y can't both be even, since by the above this would mean 2 divides all three, and they wouldn't be primitive.

- x and y can't both be odd, since going mod 4 would give $1 + 1 \equiv 1$ or 0 mod 4, since 0,1 are the only squares mod 4.

- so assume x is odd, y is even. This means z is odd

- we show that x, y, z have the form stated above.

- **Key Step - Clever Factoring Trick:** rewrite the equation as

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

which is possible since x, z both odd implies $z + x$, $z - x$ both even.

- if an integer n divides both $\frac{z-x}{2}$ and $\frac{z+x}{2}$, then it divides z and x

- but x and z are coprime, thus $\frac{z-x}{2}$ and $\frac{z+x}{2}$ must be coprime, too

- now we use the following:

Lemma 1. *If m, n are coprime and mn is a perfect square, then m and n are both perfect squares.*

Proof. Write $m = \prod p_i^{a_i}$, $n = \prod q_j^{b_j}$, where the p_is are distinct from the q_is by coprimality. $mn = \prod p_i^{a_i} \prod q_j^{b_j}$ is a perfect square, so all exponents are even, hence m and n are squares.

□

Applying the lemma to $m = \frac{z-x}{2}$, $n = \frac{z+x}{2}$ gives that they are both squares, say

$$\frac{z-x}{2} = a^2, \quad \frac{z+x}{2} = b^2$$

hence $\frac{y}{2} = ab$.

Solving these equations for x, y, z gives

$$\begin{aligned} z &= \frac{z-x}{2} + \frac{z+x}{2} = a^2 + b^2 \\ x &= \frac{z+x}{2} - \frac{z-x}{2} = b^2 - a^2 \\ y &= 2ab \end{aligned}$$

Note also that:

1) z is odd, so $a^2 + b^2$ is odd, which means one of a, b is odd and the other even.

2) z, x both positive implies $\frac{z+x}{2} > \frac{z-x}{2}$, i.e., $b > a$

3) $\frac{z+x}{2}, \frac{z-x}{2}$ coprime implies $1 = (a^2, b^2) = (a, b)^2$ (by a problem on HW1!), so a, b are coprime

Conclusion The *primitive* positive Pythagorean triples all have the form

$$(b^2 - a^2)^2 + (2ab)^2 = (a^2 + b^2)^2$$

where $b > a$ are coprime, one of them even and the other odd.

In cocnlusion, this second approach, of clever factoring of our equation, leads naturally into the study of algebraic number theory, which we will hopefully touch on in the final week of the course.