Lecture 1

Monday, January 3, 2022 12:54 PM

Office hrs:

Pollack: Thursdays 11am - 1pm (on Zoom)

McGlade: Fridays 2pm - 4pm (excluding this Friday)

Number theory: is about integers $(0, 1, 2, 3, 4, 5, \ldots, -1, -2, -3, \ldots)$

and/or the rational numbers: $\frac{p}{q}$ where p, q are integers, $q \neq 0$.

A broad class of problems:

Finding and understanding solutions to polynomial equations w/ rational coefficients

E.g.

(1) $2^x + 3 = y^2$: is not a polynomial eq$^{\underline{n}}$

Are there integers x, y that satisfy this eq$^{\underline{n}}$?

(2) $y^2 - x^3 = 1$: is a polynomial eq$^{\underline{n}}$

What are all the integers (x, y) that satisfy this eq$^{\underline{n}}$?

E.x. $y = 3$, $x = 2 \Rightarrow y^2 - x^3 = 9 - 8 = 1$.

(3) $y^2 - \pi x^3 = 1$: <u>is</u> a polynomial eq$^{\underline{n}}$, but not w/ rational coefficients.

$$\boxed{2^x + 3 = y^2}$$

<u>Real # sol$^{\underline{n}}$s</u>: x = anything

$y = \sqrt{2^x + 3}$

<u>Integer sol$^{\underline{n}}$s</u>: • $x = 0$, $y = 2$ or $y = -2$

• <u>$x=1$</u> $2^1 + 3 = 5 \neq y^2$

• <u>$x=2$</u> $2^2 + 3 = 7 \neq y^2$

• <u>$x=3$</u> $2^3 + 3 = 11 \neq y^2$

<u>Claim</u>: $x=0$, $y = \pm 2$ are the only integer sol$^{\underline{n}}$s

<u>Pf</u>: Suppose $x \geq 2$. Then I claim: $2^x + 3$ is not a $\square$.

If $x \geq 2$, then 4 divides 2^x

$\Longrightarrow$ $2^x + 3$ has remainder 3 when I divide by 4

<u>Claim</u>: y^2 is either divisible by 4, or has remainder 1 when dividing by 4.

when dividing by 4.

<u>Pf of Claim:</u>

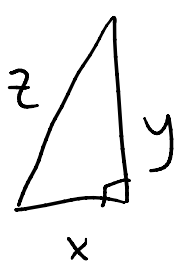
<u>y even:</u> $y = 2n \Rightarrow y^2 = 4n^2$ is div. by 4

<u>y odd:</u> $y = 2n+1 \Rightarrow y^2 = (2n+1)^2 = \underbrace{4n^2 + 4n}_{} + 1$

has remainder 1 when dividing by 4.

$2^x + 3 = y^2$ has no sol'ns w/ $x \geq 2$ and y integers

<u>Another example</u>: $x^2 + y^2 = z^2$, w/ x, y, z integers



w/ integer side-lengths

<u>e.g.</u> $(x,y,z) = (3,4,5)$

$(5,12,13)$: $5^2 + 12^2 = 25 + 144 = 169 = 13^2$

$(7,24,25)$:

$(9,40,41)$:

* <u>Q</u>: ① Are there infinitely many solutions? ☆

Q: ② Can we parametrize all the solutions?

Based on the examples above, let's try

$$(x, y, z) = (x, y, y+1)$$

$$x^2 + \cancel{y^2} = (y+1)^2 = \cancel{y^2} + 2y + 1$$

$$\Longrightarrow \quad x^2 = 2y + 1$$

$$\Longrightarrow \quad y = \frac{x^2 - 1}{2}$$

e.g. $x = 2$ Does not work

$x = 3$ does work

If x is odd, x^2 is odd $\Rightarrow$ $x^2 - 1$ is even

$\Longrightarrow$ $\frac{x^2-1}{2}$ is an integer

x odd: $\left(x, \boxed{\frac{x^2-1}{2}}, \boxed{\frac{x^2+1}{2}}\right)$ is a sol$^{\underline{n}}$ to our eqn.

<u>Should check!</u> $x^2 + \left(\frac{x^2-1}{2}\right)^2 = \left(\frac{x^2+1}{2}\right)^2$

<u>How about!</u> $x^3 + y^3 = z^3$

$x^4 + y^4 = z^4$ w/ (x, y, z) integers ≥ 1.

$x^5 + y^5 = z^5$

$\vdots$

$$x^n + y^n = z^n, \quad n > 2 \text{ an integer}$$

NO SOLUTIONS

One last example: $x^2 - 1141y^2 = 1$.

Any sol$^{\underline{n}}$s to this eq$^{\underline{n}}$ with (x,y) integers, $y > 0$.

NO SOLNS w/ $y < 10^{24}$!

But there is a sol$^{\underline{n}}$ w/ y having 26 digits,
and in fact ∞'ly many sol$^{\underline{n}}$s

We'll discuss the eq$^{\underline{n}}$s $x^2 - dy^2 = 1$, d a positive integer

---

Some other number theory questions

Recall: A positive integer > 1 is prime if its only divisors are 1 and itself

E.g. 2, 3, 5, 7, 11, 13, 17 are prime

(0, 15, 12, 4, ...) are not prime

<u>Thm</u>: There are infinitely many prime numbers

<u>Warm-up</u>: Every positive integer N has a prime divisor.

<u>Pf of warm-up</u>:
- If N is prime, done.
- O.w., $N = ab$ w/ $1 < a < N$, $1 < b < N$.
- By induction, $\exists$ prime # p s.t. p divides a, $a = pa'$.

$\Rightarrow N = ab = pa'b \Rightarrow p$ divides N.

<u>Note</u>: We don't include 1 as a prime