Office hrs:
Pollack: Thursdays 11am-1pm (on Zoom)
McClade: Fridays 2pm-4pm (excluding this Friday)

Number theory: is about integers (0, 1, 2, 3, 4, 5, ..., -1, -2, -3, ...) 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 with rational coefficients

E.g.
1. \( 2^x + 3 = y^2 \): is not a polynomial eq.
   Are there integers \( x, y \) that satisfy this eq.?
2. \( y^2 - x^3 = 1 \): is a polynomial eq.
   What are all the integers \( (x, y) \) that satisfy this eq.?
   E.x. \( y = 3, x = 2 \Rightarrow y^2 - x^3 = 9 - 8 = 1 \).
\[ y^2 - \pi x^3 = 1 \] is a polynomial eqn, but not w/ rational coefficients.

\[ 2^x + 3 = y^2 \]

**Real solns:**
\[
\begin{align*}
\text{Real solns:} \quad x &= \text{anything} \\
y &= \sqrt{2^x + 3}
\end{align*}
\]

**Integer solns:**
\[
\begin{align*}
\text{Integer solns:} \quad x &= 0, \ y = 2 \text{ or } y = -2 \\
x &= 1, \quad 2^1 + 3 = 5 \neq y^2 \\
x &= 2, \quad 2^2 + 3 = 7 \neq y^2 \\
x &= 3, \quad 2^3 + 3 = 11 \neq y^2
\end{align*}
\]

**Claim:** \( x = 0, \ y = \pm 2 \) are the only integer solns.

**Pf:** Suppose \( x > 2 \). Then I claim: \( 2^x + 3 \) is not a D.

If \( x > 2 \), then 4 divides \( 2^x \)

\[ \Rightarrow \quad 2^x + 3 \] has remainder 3 when I divide by 4

**Claim:** \( y^2 \) is either divisible by 4, or has remainder 1 when dividing by 4.
when dividing by 4.

**Pf of Claim:**

- **Given:** $y = 2n \Rightarrow y^2 = 4n^2$ is div. by 4
- **Odd:** $y = 2n+1 \Rightarrow y^2 = (2n+1)^2 = 4n^2 + 4n + 1$ has remainder 1 when dividing by 4.

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

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

\[ \begin{array}{c}
\text{z} \\
\text{y} \\
\text{x}
\end{array} \]

w/ integer side-lengths

E.g. $(x, y, z) = (3, 4, 5)$

- $(5, 12, 13): \ 5^2 + 12^2 = 25 + 144 = 169 = 13^2$
- $(7, 24, 25)$:
- $(9, 40, 41)$:

\* Q (1): Are there infinitely many solutions?

Q (2): Can we parametrize all the solutions?
Based on the examples above, let's try

\[(x, y, z) = (x, y, y+1)\]

\[x^2 + y^2 = (y+1)^2 = y^2 + 2y + 1\]

\[\implies x^2 = 2y + 1\]

\[\implies y = \frac{x^2 - 1}{2}\]

E.g., \(x = 2\) does not work
\(x = 3\) does work

If \(x\) is odd, \(x^2\) is odd \(\implies x^2 - 1\) is even

\[\implies \frac{x^2 - 1}{2}\] is an integer

\(x\) odd:
\[(x, \frac{x^2 - 1}{2}, \frac{x^2 + 1}{2})\]

is a solution to our equation

Should check:

\[x^2 + \left(\frac{x^2 - 1}{2}\right)^2 = \left(\frac{x^2 + 1}{2}\right)^2\]

How about:

\[x^3 + y^3 = z^3\]
\[x^4 + y^4 = z^4\]
\[x^5 + y^5 = z^5\]
\[\vdots\]

w/ \((x, y, z)\) integers \(\geq 1\).
\[ x^n + y^n = z^n, \quad n > 2 \text{ an integer} \]

**No Solutions**

One last example: \[ x^2 - 1141y^2 = 1. \]

Any solns to this eqn with \((x,y)\) integers, \(y > 0\).

**No Solns w/ \(y < 10^{24}\)**!

But there is a soln w/ \(y\) having 26 digits, and in fact only many solns.

We'll discuss the eqns \( x^2 - dy^2 = 1, \quad d \) 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.

\((0, 15, 12, 4, \ldots)\) are not prime.
Thm: There are infinitely many prime numbers

Warm-up: Every positive integer $N$ has a prime divisor.

Pf of warm-up: If $N$ is prime, done.

O.w., $N = ab$ w/ $1 < a < N$, $1 < b < N$.

By induction, $\exists$ prime $\neq p$ s.t. $p$ divides $a$, $a = pa'$.

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

Note: We don't include 1 as a prime.