Math 4400 – Introduction to number theory
Spring 2022

Week 1:
... Wait, what's number theory?

(Video lecture for Thursday, 1/13).

Step 1: What are numbers?

$\mathbb{N}$ - natural/counting numbers. 1, 2, 3, 4, 5

0 - zero! 0

$\mathbb{Z}$ - integers – add in negative numbers $3 - 5 \cdot 1 = -2$

$\mathbb{Q}$ - allow ratios of integers. $\frac{3}{2}$

circumference of a circle

$\mathbb{R}$ — Ontological — geometric quantities $\pi = \frac{\quad}{\text{diameter}}$

— Constructive — approximation by rationals.

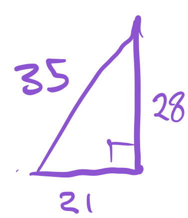
$\mathbb{C}$ - solving all polynomial equations. i ($i^2 = -1$ solution to x^2+1)

Number Theory: The study of relations between different ways to express numbers.

Example: $35 = 1+1+1+1+1+1+1+1+1+1+1+1+1+1$
$+1+1+1+1+1+1+1+1+1+1+1$
$+1+1+1+1+1+1+1+1+1+1$

or $35 = 7 \cdot 5$

or $35 = \sqrt{21^2 + 28^2}$



$\times$ 35 is <u>not</u> the area of a right triangle with rational side lengths.

Some important questions in number theory:

- How many prime numbers are there less than 100? 1000? 1,000,000? N?
  Answer $\sim \underline{N}$ primes less than N — learn in a graduate complex analysis

$\log N$ (Prime # Theorem) class.

Control the error and win \$1,000,000! (Riemann Hypothesis)

- How many ~~prime~~ squarefree numbers are there less than 100? 1000? 1,000,000? N?

  E.g. $7 \cdot 5 = 35$ squarefree $20 = 2^2 \cdot 5$ is not square-

  $\sim \frac{4}{\pi^2} N$ square free #s less than N. (calculus).

- Is π a rational number? Is e?

  $e = \lim_{n\to\infty} (1+\frac{1}{n})^n$

  $= 1 + \frac{1}{2!} + \frac{1}{3!} + \frac{1}{4!} + \dots$

  Lindemann-Weierstrass:

  π transcendental

  e transcendental. (difficult application of calculus)

- Which positive integers can be written as sums of two squares? Four squares? Eight squares? In how many ways?

  $5 = 2^2 + 1^2$

  $5 = (-2)^2 + 1^2$

  7 can't be written as sum of 2 squares.

  $7 = 2^2 + 1^2 + 1^2 + 1^2$

- Is $\sqrt{2}$ rational? If not, how well can I approximate it by rational numbers?

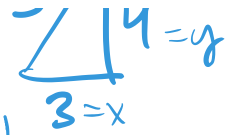
  Does $x^2 - 2 = 0$ have a solution in $\mathbb{Q}$?

  $\sqrt{2} = \frac{a}{b}$ a, b integers?

- Are there right triangles all of whose sides have integer lengths?

  $x^2 + y^2 = z^2$ $z = 5$

x, y, z integers



Pythagorean triples - can find all of these.

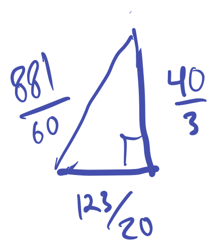
- Integer solutions to $x^n + y^n = z^n$, $n > 2$?

  No solutions - Fermat's Last Theorem

  Proved by Wiles + Wiles-Taylor in the 90s

  BIG DEAL!

- Which integers are the areas of right triangles with rational sides?



Area = 41.

Congruent number problem.

Number theory: simple questions, ~~hard~~ ~~answers~~. Simple answers, hard justifications.

True theoretically <u>and</u> computationally.

Theorem (Unique Factorization):

If $n \in \mathbb{N}$, then there is exactly one way to write

$$n = p_1^{a_1} p_2^{a_2} \cdots p_k^{a_k}$$

where $p_1 < p_2 < p_3 < \dots < p_k$ are prime numbers and $a_1, \dots, a_k \in \mathbb{N}$.

Example: • $91 = 7 \cdot 13$ $\quad p_1 = 7 \quad a_1 = 1$
$\quad p_2 = 13 \quad a_2 = 1$

• $199008 = 2^5 \cdot 3^2 \cdot 691$ $\quad p_1 = 2 \quad a_1 = 5$
$\quad p_2 = 3 \quad a_2 = 2$
$\quad p_3 = 691 \quad a_3 = 1.$

Given n, it's hard to find the factorization $n = p_1^{a_1} \cdots p_k^{a_k}$

It's hard to even check if n is prime!

This is a feature, not a bug!

Number theory supplies problems like this for cryptography

(Need hard problems to establish a safe shared secret.).