# MATH 3070 Theory of Numbers

Shane Chern Department of Mathematics and Statistics Dalhousie University

Sep 06, 2022



We are expected to learn the properties of

- integers  $(0, \pm 1, \pm 2, ...)$ 
  - especially primes (2,3,5,7,11,...)
- as well as mathematical objects made out of integers, e.g., rationals
- ▶ and generalizations of the integers, e.g., *algebraic integers*

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

Let's start with

$$9 + 16 = 25;$$

this is just simple arithmetic, not part of number theory.

Let's start with

$$9 + 16 = 25;$$

this is just simple arithmetic, not part of number theory.

Something trickier

$$3^2 + 4^2 = 5^2$$
.

An instance of the Pythagorean theorem.





◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

More generally,

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

◆□> <圖> < E> < E> E のQ@

More generally,

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

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 のへぐ

• A. Can we determine all its integer solutions?

More generally,

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

- A. Can we determine all its integer solutions?
- B. What integers can be written as x<sup>2</sup> + y<sup>2</sup> with x and y integers? And how many such representations?

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

More generally,

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

- A. Can we determine all its integer solutions?
- ► B. What integers can be written as x<sup>2</sup> + y<sup>2</sup> with x and y integers? And how many such representations?
- ► C. What happens if we replace the square with an *n*-th power with n ≥ 3

$$x^n + y^n = z^n?$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

Do we still have integer solutions?

A. All integer solutions of

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

◆□> <圖> < E> < E> E のQ@

A. All integer solutions of

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

Theorem All integer solutions of

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

can be parameterized as

$$x = k \cdot (r^2 - s^2), \quad y = k \cdot 2rs, \quad z = k \cdot (r^2 + s^2).$$

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?

B. Representation of

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

<□ > < @ > < E > < E > E のQ @

B. Representation of

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

### Theorem (Pierre de Fermat)

A square-free integers m is representable as  $x^2 + y^2$  with x and y integers if and only if n has no prime factors of the form 4k + 3.



C. Any integer solutions of

$$x^n + y^n = z^n?$$

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへぐ

C. Any integer solutions of

$$x^n + y^n = z^n?$$

Theorem (Fermat's last theorem, proved by Andrew Wiles) There is no integer solution with  $x, y, z \neq 0$  to

$$x^n + y^n = z^n$$

for  $n \geq 3$ .





- A. Multiplicative problems
  - Divisors
  - Primes, composites
  - Arithmetic functions

▲□▶ ▲圖▶ ▲≣▶ ▲≣▶ = 差 = のへで

- A. Multiplicative problems
  - Divisors
  - Primes, composites
  - Arithmetic functions

## E.g.,

- *Prime number theorem*: The number of primes  $\leq x$ .
- Gauss circle problem: The number of integer lattice points there are in a circle centered at the origin and with radius r.

- B. Additive problems
  - Representation of integers

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?

- B. Additive problems
  - Representation of integers

# E.g.,

- Sum of two squares: Representation of  $n = x^2 + y^2$ .
- Integer partitions: Representation of n as a sum of nonincreasing positive integers.

$$5 = 4 + 1 = 3 + 2 = 3 + 1 + 1 = 2 + 2 + 1 = 2 + 1 + 1 + 1 = 1 + 1 + 1 + 1 + 1$$





- C. Diophantine equations
  - Integer solutions to polynomial equations

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?

- C. Diophantine equations
  - Integer solutions to polynomial equations

E.g.,

- Fermat's last theorem:  $x^n + y^n = z^n$ .
- ▶ Pell's equation: x<sup>2</sup> dy<sup>2</sup> = 1 with d a non-square positive integer.
- Sum of three cubes:  $x^3 + y^3 + z^3 = 33$ .

 $8866128975287528^3 + (-8778405442862239)^3 + (-2736111468807040)^3 = 33.$ 

This is the first known solution to the above Diophantine equation, discoved by Andrew Booker in 2019.

- D. Diophantine approximations
  - Approximation of real numbers by rational numbers

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?

- D. Diophantine approximations
  - Approximation of real numbers by rational numbers

E.g.,

 The best Diophantine approximation: Given a real number α, find the rational number p/q such that

$$\left| \alpha - \frac{p}{q} \right| \le \left| \alpha - \frac{p'}{q'} \right|$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

for every rational number p'/q' with  $0 < q' \leq q$ .

For Natural Sciences, especially Experimental Sciences, nobody can prove that a phenomenon or a rule is real in general.

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

For Natural Sciences, especially Experimental Sciences, nobody can prove that a phenomenon or a rule is real in general.

QUESTION. Will *Newtonian mechanics* expire in the scale of the UNIVERSE or ATOMS?

< □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > < □ > <

# Proofs: Why do we need PROOFS? Lord Kelvin's two CLOUDS in physics

#### **Clouds on the Horizon**

"Beauty and clearness of theory... Overshadowed by two clouds..."



Lord Kelvin

**Baltimore Lectures** 

Johns Hopkins University

1900

The two clouds:

Failure of the Michelson – Morley experiment → Einstein's Relativity

# Failure of classical electrodynamics to describe thermal radiation $\rightarrow$ Quantum Mechanics

19 January 2011

Modern Physics III Lecture 2

▲ロト ▲帰 ト ▲ヨト ▲ヨト - ヨ - の々ぐ

However, in Mathematics, with a few axioms, MOST statements can be claimed *True* or *False*.

▲□▶ ▲圖▶ ▲≣▶ ▲≣▶ = 差 = のへで

However, in Mathematics, with a few axioms, MOST statements can be claimed *True* or *False*.

Theorem (Gödel's incompleteness theorem) There are statements which can neither be proved nor disproved in an axiomatic system.

However, in Mathematics, with a few axioms, MOST statements can be claimed *True* or *False*.

Theorem (Gödel's incompleteness theorem) There are statements which can neither be proved nor disproved in an axiomatic system.

But what can be proved or disproved is already very vast!

The existence of *large counterexamples*!

The GCD (greatest common divisor) of n<sup>17</sup> + 9 and (n+1)<sup>17</sup> + 9:

$$gcd(1^{17} + 9, 2^{17} + 9) = gcd(10, 131081) = 1;$$
  
 $gcd(2^{17} + 9, 3^{17} + 9) = gcd(131081, 129140172) = 1;$   
 $gcd(3^{17} + 9, 4^{17} + 9) = gcd(129140172, 17179869193) = 1.$ 

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 臣 の�?

The existence of *large counterexamples*!

The GCD (greatest common divisor) of n<sup>17</sup> + 9 and (n+1)<sup>17</sup> + 9:

$$\begin{aligned} & \gcd(1^{17}+9,2^{17}+9) = \gcd(10,131081) = 1; \\ & \gcd(2^{17}+9,3^{17}+9) = \gcd(131081,129140172) = 1; \\ & \gcd(3^{17}+9,4^{17}+9) = \gcd(129140172,17179869193) = 1. \end{aligned}$$

Is it true for all positive integers n that

$$gcd(n^{17} + 9, (n+1)^{17} + 9) = 1?$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

The existence of *large counterexamples*!

The GCD (greatest common divisor) of n<sup>17</sup> + 9 and (n+1)<sup>17</sup> + 9:

$$\begin{aligned} & \gcd(1^{17}+9,2^{17}+9) = \gcd(10,131081) = 1; \\ & \gcd(2^{17}+9,3^{17}+9) = \gcd(131081,129140172) = 1; \\ & \gcd(3^{17}+9,4^{17}+9) = \gcd(129140172,17179869193) = 1. \end{aligned}$$

Is it true for all positive integers n that

$$gcd(n^{17} + 9, (n+1)^{17} + 9) = 1?$$

NO! But the *first* counterexample appears when

n = 8424432925592889329288197322308900672459420460792433.

▲□▶ ▲圖▶ ▲≣▶ ▲≣▶ = 差 = のへで

The existence of large counterexamples!

Skewes's number.

The existence of large counterexamples!

Skewes's number.

$$\pi(x) := \text{the number of primes} \le x,$$
$$\text{li}(x) := \int_0^x \frac{dt}{\log t}.$$

Prime number theorem.  $\pi(x) \sim li(x)$ . I.e.,

$$\lim_{x\to\infty}\frac{\pi(x)}{\mathsf{li}(x)}=1.$$

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

The existence of large counterexamples!

Skewes's number.

What can we say about the difference  $\pi(x) - \text{li}(x)$ ? — It is negative for all small x.

The existence of large counterexamples!

Skewes's number.

What can we say about the difference  $\pi(x) - \text{li}(x)$ ? — It is negative for all small x.

John Littlewood (1914).  $\pi(x) - li(x)$  changes sign infinitely often.

The existence of *large counterexamples*!

Skewes's number.

What can we say about the difference  $\pi(x) - \text{li}(x)$ ? — It is negative for all small x.

John Littlewood (1914).  $\pi(x) - li(x)$  changes sign infinitely often.

But for which x, the first sign change appears? — We don't know!

The existence of *large counterexamples*!

Skewes's number.

What can we say about the difference  $\pi(x) - \text{li}(x)$ ? — It is negative for all small x.

John Littlewood (1914).  $\pi(x) - li(x)$  changes sign infinitely often.

But for which x, the first sign change appears? — We don't know!

Skewes proved that such x is smaller than

$$e^{e^{e^{e^{7.705}}}}$$
.

• It is believed that such x is around  $10^{316}$ .

# A BELIEF IS NEVER A PROOF.

▲□▶ ▲圖▶ ▲臣▶ ▲臣▶ ―臣 … のへで

Direct deduction

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへぐ

Direct deduction

E.g.

$$1+2+\cdots+n=\frac{n(n+1)}{2}.$$

E.g.

Direct deduction

$$1+2+\cdots+n=\frac{n(n+1)}{2}.$$

Proof.

$$S_n = 1 + 2 + \cdots + n - 1 + n$$
  
 $S_n = n + n - 1 + \cdots + 2 + 1$ 

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへぐ

E.g.

Direct deduction

$$1+2+\cdots+n=\frac{n(n+1)}{2}.$$

Proof.

$$S_n = 1 + 2 + \cdots + n - 1 + n$$
  
 $S_n = n + n - 1 + \cdots + 2 + 1$ 

$$2S_n = (1 + n) + (2 + (n - 1)) + \dots + (n + 1)$$
  
= (n + 1) + (n + 1) + \dots (n + 1) [n copies of (n + 1)]  
= n(n + 1).

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへぐ

E.g.

Direct deduction

$$1+2+\cdots+n=\frac{n(n+1)}{2}.$$

Proof.

$$S_n = 1 + 2 + \cdots + n - 1 + n$$
  
 $S_n = n + n - 1 + \cdots + 2 + 1$ 

$$2S_n = (1+n) + (2+(n-1)) + \dots + (n+1)$$
  
= (n+1) + (n+1) + \dots (n+1) [n copies of (n+1)]  
= n(n+1).

$$1+2+\cdots+n=S_n=\frac{n(n+1)}{2}.$$

▲□ ▶ ▲圖 ▶ ▲ 圖 ▶ ▲ 圖 ▶ ● ● ● ● ● ●

Induction



Induction

E.g. 
$$1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

◆□> <圖> < E> < E> E のQ@

Induction

E.g. 
$$1^2 + 2^2 + \dots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

Proof.

• Is the statement TRUE for n = 1?

$$1^2 = 1 = \frac{1(1+1)(2 \times 1 + 1)}{6}.$$

◆□> <圖> < E> < E> E のQ@

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$$

### Proof.

• Assume that the statement is true for some  $n = k \ge 1$ :

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}.$$

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへぐ

Prove that it is also true for n = k + 1.

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

### Proof.

• Assume that the statement is true for some  $n = k \ge 1$ :

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$$

Prove that it is also true for n = k + 1.

$$1^{2} + 2^{2} + \dots + k^{2} + (k+1)^{2} = \frac{k(k+1)(2k+1)}{6} + (k+1)^{2}$$
$$= \frac{(k+1)(k+2)(2(k+1)+1)}{6}.$$

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへぐ

$$1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}.$$

#### Proof.

• Assume that the statement is true for some  $n = k \ge 1$ :

$$1^2 + 2^2 + \cdots + k^2 = \frac{k(k+1)(2k+1)}{6}$$

Prove that it is also true for n = k + 1.

$$1^{2} + 2^{2} + \dots + k^{2} + (k+1)^{2} = \frac{k(k+1)(2k+1)}{6} + (k+1)^{2}$$
$$= \frac{(k+1)(k+2)(2(k+1)+1)}{6}.$$

▲□▶ ▲圖▶ ▲≣▶ ▲≣▶ = 差 = のへで

• Conclude that the statement is true for all positive integers *n*.

#### Contradiction

◆□▶ ◆□▶ ◆臣▶ ◆臣▶ 三臣 - のへぐ

### Contradiction

E.g.

Pigeonhole principle.

If N + 1 balls are placed in N boxes, then there must be some box with at least 2 balls.

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

### Contradiction

E.g.

Pigeonhole principle.

If N + 1 balls are placed in N boxes, then there must be some box with at least 2 balls.

◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

Proof.

Assume that no boxes contain at least 2 balls.

### Contradiction

E.g.

Pigeonhole principle.

If N + 1 balls are placed in N boxes, then there must be some box with at least 2 balls.

Proof.

- Assume that no boxes contain at least 2 balls.
- Then the total number of balls is  $\leq N \times 1 = N$ .

### Contradiction

E.g.

Pigeonhole principle.

If N + 1 balls are placed in N boxes, then there must be some box with at least 2 balls.

### Proof.

- Assume that no boxes contain at least 2 balls.
- Then the total number of balls is  $\leq N \times 1 = N$ .
- But there are N + 1 balls, thereby leading to a contradiction.

### Contradiction

E.g.

Pigeonhole principle.

If N + 1 balls are placed in N boxes, then there must be some box with at least 2 balls.

### Proof.

- Assume that no boxes contain at least 2 balls.
- Then the total number of balls is  $\leq N \times 1 = N$ .
- But there are N + 1 balls, thereby leading to a contradiction.
- So our assumption is false There must be some box with at least 2 balls.

# Unsolved Problems in Number Theory

Richard K. Guy, *Unsolved Problems in Number Theory, Third edition*, Springer-Verlag, New York, 2004.





◆□▶ ◆□▶ ◆三▶ ◆三▶ 三三 のへぐ

MATH 3070 – Theory of Numbers

We will switch back to the traditional "chalk-and-blackboard" style in the rest of this semester.

