Introduction to Number Theory

Xu Gao

UC Santa Cruz (Fall 2022)

Instructor: Xu Gao (xgao26@ucsc.edu)

Lecture: MWF 2:40 - 3:45 PM @ Soc Sci 2 071 (in-person)

Sep. 23 - Dec. 2.

Office Hours: MW 4:30-5:30 PM or by appointment.

@McH 1292.

Discussion Sections:

Tu 9:20 ~ 10:25AM @ Cowell 216

F 9:20-10:25AM @ Mc H 1270

TA: Yuk Shing Lam (ylam14@ucsc.edu)

TA's office hours: Tu/F 11AM-12PM @McH 1261.

check Canvas for detailed syllabus.

- **Numbers**

"natural"

$\mathbb{N} = \{0, 1, 2, \dots\}$ "natural number" $+$ & $\times$

"Zahlen" → $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$ "integers"

"quotient" → $\mathbb{Q} = \left\{ \frac{p}{q} : p, q \in \mathbb{Z} \text{ and } q \neq 0 \right\}$ "rational numbers"

$\sqrt{2} \neq \frac{p}{q}$.

$\mathbb{Q}_p$ "p-adic numbers"

$\mathbb{R}$ "real numbers"

$\mathbb{C} = \{a + b\sqrt{-1} : a, b \in \mathbb{R}\}$ "complex numbers"

• Topics in Number Theory.

- Solve polynomial equations in certain number set:

Eg. 1. Does $2x - 1 = 0$ have an integer solution?

$\frac{1}{2}$ is NOT an integer !!!

Eg. 2. Does $x^2 + y^2 = 1$ have an rational solution?
What are all of them?

Yes! Pythagoth theorem, rational points on unit circle.

Eg. 3. Solutions of $y^2 = x^3 + ax + b$ elliptic Curve

– Prime numbers

Count prime number 1. There are infinitely many!

2. $\pi(n) := \#\{\text{prime } p : p \le n\}$.

⇝ Prime Number Theorem

$$\pi(n) \sim \frac{n}{\ln(n)}$$

(related to Riemmann's zeta function)

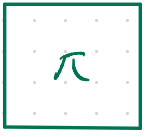
– Transcendentality

e.g. "Can there be a square with area π ?"

Start with the unit length 1.

Use only straight ruler & compass, (no measures)

can you draw a SQUARE of area π ?



π is not a solution of a polynomial.

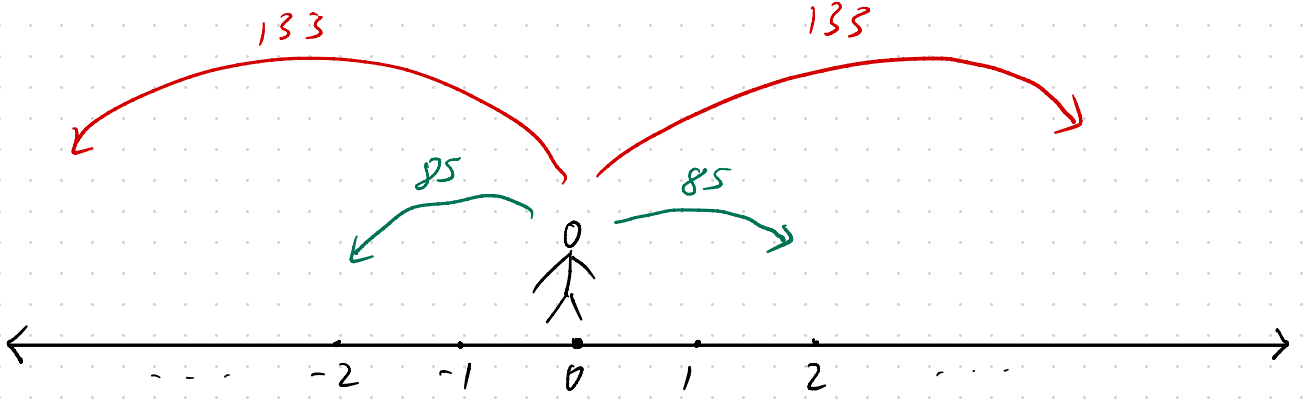
NO!

(Linear Diophantine Equation)

Our first topic: Find integer solutions to

$$Ax + By = C$$

Example



Suppose we can only

(A) hop 133 unit to left or right

(B) Skip 85 unit to left or right

E.g. hop once to R & skip twice to L.

$$133 \cdot 1 + 85 \cdot (-2) = -37$$

Q: Using hop & skip only, can we move from 0 to 1?

Purpose: Check if $Ax + By = C$ has an integer solution & find all of them.

Euclidean Algorithm.

Euclidean Algorithm.

Initial: two positive integers a & b (we may assume $a \geq b$)

Action: divide a by b:

$$a = q \cdot b + r$$

Test if $r = 0$ $\rightsquigarrow$ halt!

otherwise, repeat the previous steps with (a, b) replaced by (b, r).

* this process will terminate in finite steps.

  Since after each action, we either get $r = 0$ or a replaced by b

  But $b < a$ and there are only finitely many positive integers $< a$.

Back to our example:

$a = 133$, $b = 85$.

$133 = 1 \cdot 85 + 48$

$85 = 1 \cdot 48 + 37$

$48 = 1 \cdot 37 + 11$

$37 = 3 \cdot 11 + 4$

$11 = 2 \cdot 4 + 3$

$4 = 1 \cdot 3 + 1$

$3 = 3 \cdot 1 + 0$ → halt;

$1 = 4 - 1 \cdot 3$

$3 = 11 - 2 \cdot 4$

$4 = 37 - 3 \cdot 11$

$11 = 48 - 1 \cdot 37$

$37 = 85 - 1 \cdot 48$

$48 = 133 - 1 \cdot 85$

$37 = 85 - 1 \cdot (133 - 1 \cdot 85)$

$= -1 \cdot 133 + 2 \cdot 85$

$11 = (133 - 1 \cdot 85) - 1 \cdot (-1 \cdot 133 + 2 \cdot 85)$

$= 2 \cdot 133 - 3 \cdot 85$

$4 = -1 \cdot 133 + 2 \cdot 85 - 3 \cdot (2 \cdot 133 - 3 \cdot 85)$

$= -7 \cdot 133 + 11 \cdot 85.$

$3 = 2 \cdot 133 - 3 \cdot 85 - 2 \cdot (-7 \cdot 133 + 11 \cdot 85)$

$= 16 \cdot 133 - 25 \cdot 85$

$$1 = -7 \cdot 133 + 11 \cdot 85 - (16 \cdot 133 - 25 \cdot 85)$$

$$= \underbrace{-23}_{x} \cdot 133 + \underbrace{36}_{y} \cdot 85$$

Another Way:

$$1 = 4 - 1 \cdot 3 = 4 - 1 \cdot (11 - 2 \cdot 4) = -1 \cdot 11 + 3 \cdot 4 = -1 \cdot 11 + 3 \cdot (37 - 3 \cdot 11)$$

$$= 3 \cdot 37 - 10 \cdot 11 = 3 \cdot 37 - 10 \cdot (48 - 1 \cdot 37) = -10 \cdot 48 + 13 \cdot 37$$

$$= -10 \cdot 48 + 13 \cdot (85 - 1 \cdot 48) = 13 \cdot 85 - 23 \cdot 48$$

$$= 13 \cdot 85 - 23 \cdot (133 - 1 \cdot 85) = -23 \cdot 133 + 36 \cdot 85$$

Some after-school reading suggestions:

- Chapter 0 of the textbook provides a wonderful introduction to this course.
  - One central concept is the **division with remainder** (see Prop. 0.18 for one proof).
  - Another related central concept is **divisibility**. $x \mid y$ means that there is an integer m such that $y = mx$. Try to show that the relation $\mid$ has the following analogous relations with $\leqslant$: **reflexive**, **antisymmetric**, and **transitive**. See Prop. 0.26, 0.27, and 0.28 for the proofs. I encourage you to think before reading the proofs. The **2-out-of-3** (see Coro. 0.31) is also an important property.
- Today's topic is the Euclidean algorithm. You can refer to 1.1–1.6 for today's contents. I encourage you to read the rest of Chapter 1 preparing for our next meeting.