M 328K: Lecture 1

Katherine Ho

August 27, 2024

1 Open Problems

- Twin Primes Conjecture: Do there exist infinitely many pairs of primes that are 2 apart?
- Collatz Conjecture, 3n+1 Problem - Does this process eventually stop for all n?
- Fermat's Last Theorem: The equation $x^n + y^n = z^n$ has no (non-trivial) integer solution when $n \geq 3$.
  Note: When $n = 2$, there are infinite solutions (Pythagorean triples)

2 Notation

- Natural numbers: $\mathbb{N} = \{1, 2, 3, 4, \dots\}$
- Integers: $\mathbb{Z} = \{\dots, -2, -1, 0, 1, 2, \dots\}$
- Rational Numbers: $\mathbb{Q} = \{\frac{a}{b} | a, b \in \mathbb{Z}, b \neq 0\}$

3 Divisibility

Definition 3.1. *Let $n, m \in \mathbb{Z}$. We say that n divides m and write $n|m$ if there exists an integer k such that $m = nk$.*

Ex: $2|4, 5|-5, 3|0, 0|0$

If n does not divide m: $n \nmid m$

Ex: $2 \nmid 3, 0 \nmid 5$

Theorem 3.1. *For $a, b, c \in \mathbb{Z}$, the following hold:*

1. $a|0$, $1|a$, $a|a$
2. $a|1$ *iff* $a = \pm b$
3. *If* $a|b$ *and* $c|d$ *then* $ac|bd$
4. *If* $a|b$ *and* $b|c$ *then* $a|c$
5. $a|b$ *and* $b|a$ *iff* $a = \pm b$
6. *If* $a|b$ *and* $b \neq 0$*, then* $|a| \leq |b|$
7. *If* $a|b$ *and* $a|c$*, then* $a|(bx + cy)$ *for* $x, y \in \mathbb{Z}$
   Ex. If b, c are even, then (any multiple of b) + (any multiple of c) is even.

Proof (2). First, assume $a|1$. By definition, there exists an integer k such that $1 = ak$.
Note: $k \neq 0$ and $a \neq 0$, so

$$|ak| = |a||k| \geq |a| \text{ since } |k| \geq 1$$

Thus, $1 = |ak| \geq |a|$.
Also, $|a| \geq 1$ since $a \neq 0$ and $a \in \mathbb{Z}$. Thus, $|a| = 1$ which is equivalent to $a = \pm 1$.

Next, assume $a = \pm 1$.

- If $a = 1$: $a|1$ since $1 = a \cdot 1$
- If $a = -1$: $1 = a \cdot -1$

In both cases, $a|1$ as desired. □

Proof (4). Assume $a|b$ and $b|c$.
By definition, there exist integers i and j such that $b = a \cdot i$ and $c = b \cdot j$.
Then, $c = (a \cdot i) \cdot j = a(ij)$.
So, $a|c$ by definition. □

4 The Division Algorithm

Theorem 4.1. *Given integers a and b with $b \neq 0$, there exist unique integers q and r such that*

$$a = bq + r, \ 0 \leq r \leq |b|$$