# Intro to Number Theory

Robert Y. Lewis

CS 0220 2025

February 26, 2025

# Overview

# Definition of divides

Unless otherwise indicated, all numbers in this section of the course should be assumed to be integers.

$a$ divides $b$ if there is a $k$ such that $ak = b$.

Other names:

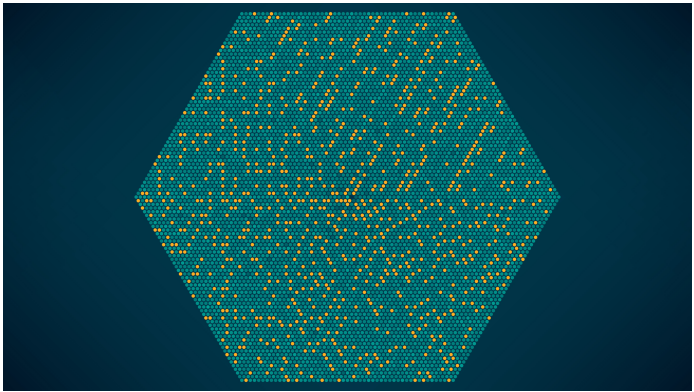
- $a|b$
- $a$ divides $b$
- $a$ is a divisor of $b$
- $a$ is a factor of $b$
- $a$ goes evenly into $b$
- $b$ is divisible by $a$
- $b$ is a multiple of $a$

By this definition: $n|0$ ($k = 0$), $n|n$ ($k = 1$), and $1|n$ ($k = n$).

# Prime numbers

Definition: A *prime* is a number greater than 1 that is divisible only by itself and 1. (Otherwise, it is *composite*.)

Note: There are infinitely many primes.



# Divisibility properties

1. If $a|b$ and $b|c$, then $a|c$. (Transitivity.)
2. If $a|b$ and $a|c$, then $a|sb + tc$ for all $s$ and $t$. (Integer linear combination.)
3. For all $c \neq 0$, $a|b$ if and only if $ca|cb$.

**Proof**: All follow from the definition of divisibility we gave. We've even proven some in Lean! Here's the linear combination theorem:

Suppose $a \mid b$ and $a \mid c$. We have $k_1$ and $k_2$ such that $ak_1 = b$ and $ak_2 = c$. We want $k_3$ such that $sb + tc = ak_3$. We can calculate: $sb + tc = s(ak_1) + t(ak_2) = a(sk_1 + tk_2)$. So let $k_3 = sk_1 + tk_2$; this calculation shows our goal.

Definition: A number $n$ is a *linear combination* of numbers $b_0, \ldots, b_n$ iff $n = s_0b_0 + s_1b_1 + \cdots + s_nb_n$ for some $s_0, \ldots, s_n$.

# Infinitely many primes

**Theorem**: There are infinitely many prime numbers.

(Definition: a set $S$ is *finite* if you can enumerate its elements with a sequence $(s_0, \ldots, s_n)$. $S$ is *infinite* if it is not finite. This is not the only way to define "infinite"!)

**Proof**. Suppose for the sake of contradiction that there were only finitely many prime numbers $p_0, \ldots, p_n$. Let $P = p_0 \cdot p_1 \cdot \ldots \cdot p_n + 1$. By a theorem we proved last class, there is some prime $q$ such that $q \mid P$.

Since we listed all the primes, then $q = p_k$ for some $k$. So $q \mid P$ and $q \mid p_0 \cdot p_1 \cdot \ldots \cdot p_n$. By the linear combination property, $q \mid (P - p_0 \cdot p_1 \cdot \ldots \cdot p_n)$. But this means $q \mid 1$ which implies $q = 1$, a contradiction since 1 is not prime.

# Famous conjectures

- Goldbach Conjecture: Every even integer greater than two is equal to the sum of two primes. Status: Every even number is the sum of at most 6 primes.
- Twin Prime Conjecture: There are infinitely many primes $p$ such that $p + 2$ is also a prime. Status: There is some $k \leq 246$ such that there are infinitely many primes $p$ such that $p + k$ is also prime.
- Primality Testing: There is an efficient way to determine whether a number is prime. Status: Yes, solved in 2002 (AKS).
- Factoring: Given the product of two large primes $n = pq$, there is an efficient way to recover the primes $p$ and $q$. Status: Believed to be false.
- Fermat's Last Theorem: There are no positive integers $x$, $y$, and $z$ such that $x^n + y^n = z^n$ for some integer $n > 2$. Status: Yes, solved in 1994 (Andrew Wiles).

# Water pitcher problem

Given a source of water and two perfectly calibrated pitchers of size 3 gallons and 5 gallons, can you measure out exactly 4 gallons?

Breadth-first search:

- $(0, 0)$
- $(5, 0)$, $(0, 3)$
- $(2, 3)$, $(5, 3)$, $(3, 0)$
- $(2, 0)$, $(3, 3)$
- $(0, 2)$, $(5, 1)$
- $(5, 2)$, $(0, 1)$
- $(4, 3)$, $(1, 0)$
- $(4, 0)$, $(1, 3)$

Yes! Indeed: 1, 2, 3, 4 and 5.

# Water pitcher theorem

**Lemma**: With pitchers of sizes $a$ and $b$, the amount of water in each pitcher is always an integer linear combination of $a$ and $b$.

**Proof**: We proceed by induction. The induction hypothesis $P(n)$ is the proposition that, after $n$ moves, the amount of water in each pitcher is a linear combination of $a$ and $b$.

**Base case**: In the initial state $(0, 0)$, both pitchers are empty, and $0$ is a linear combination of $a$ and $b$. Specifically, $0 = 0 \cdot a + 0 \cdot b$.

# Inductive step

**Inductive step**: Suppose the state is $(x, y)$ after $n$ moves. By our induction hypothesis, both $x$ and $y$ are linear combinations of $a$ and $b$. We proceed by cases:

- Empty a pitcher so that it contains zero gallons. That's a linear combination of $a$ and $b$.
- Fill a pitcher from the water source. It contains either $a$ gallons or $b$ gallons, either of which are linear combinations of $a$ and $b$.
- Pour water from one pitcher to the other until the first pitcher is empty. The other contains $x + y$ gallons, which is a linear combination of $a$ and $b$ since both $x$ and $y$ were.
- Pour water from one pitcher to the other until the second pitcher is full. The full pitcher contains $a$ or $b$. The other pitcher contains $x + y - a$ or $x + y - b$, both of which are linear combinations of $a$ and $b$.

Since linear combinations are maintained, the lemma is true.

# 3 and 5 cent coins

We proved that we can make all values greater than or equal to 8. That was with *positive* linear combinations. By “owing” (or giving change) we can create general linear combinations.

Prove we can make all values.

- We can make $1 = 2 \times 3 - 5$.
- Any $k$ is then $k = 2k \times 3 - 5k$.

Some sets of coins let you make any value with only positives. Some let you make any value if you are allowed to give back change. Are there other sets where even *that* isn’t enough to make all values?