Intro to Number Theory

Robert Y. Lewis

CS 0220 2022

February 28, 2022

Overview

1 Divisibility (8.1)

2 Facts about Divisibility (8.1.1)

3 When Divisibility Goes Bad (8.1.2)

4 Die Hard (8.1.3)

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.

Definition: A *Mersenne prime* is a prime number that can be written as $2^p - 1$ where p is prime.

- $2^2 - 1 = 3$? Yes, 2 and 3 are prime.
- $2^3 - 1 = 7$? Yes, 3 and 7 are prime.
- $2^9 - 1 = 511 = 7 \times 73$? No, neither 9 nor 511 are prime.
- $2^{11} - 1 = 2047 = 23 \times 89$? No, 2047 is not prime.

Note: $2^m - 1$ is composite if m is. (Can prove by induction!)

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.

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. Best algorithm peters out after 300 digits.
- 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.

Division theorem

Theorem: Let n and $d > 0$ be integers. There exists a unique pair of integers q and r, such that $n = q \cdot d + r$ and $0 \leq r < d$.

$q = \text{qcnt}(n, d)$ is the quotient, $r = \text{rem}(n, d)$ is the remainder. I'd call them "integer division" and "mod".

Examples:

- $\text{qcnt}(2716, 10) = 271$. Since $2716 = 271 \cdot 10 + 6$
- $\text{rem}(2716, 10) = 6$. Same reason.
- $\text{rem}(-11, 7) = 3$. Since $-11 = -2 \cdot 7 + 3$

Water jug problem

As seen in *Die Hard 3*: Given a source of water and two perfectly calibrated jugs 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 jug theorem

Lemma: With jugs of sizes a and b, the amount of water in each jug is always an integer linear combination of a and b.

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

Base case: In the initial state $(0, 0)$, both jugs 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 inductive hypothesis, both x and y are linear combinations of a and b. We proceed by cases:

- Empty a jug so that it contains zero gallons. That's a linear combination of a and b.
- Fill a jug 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 jug to the other until the first jug 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 jug to the other until the second jug is full. The full jug contains a or b. The other jug 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?