Intro to Number Theory

Michael L. Littman

CS 22 2020

February 12, 2020

Overview

Definition of divides

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

$a|b ::= [ak = b \text{ for some } k]$.

Other names:

- $a|b$
- a divides b
- a is a divisor of b
- a is a factor of 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.

Note: There are infinitely many primes.

Definition: A *Mersenne prime* is a number that can be written $n = 2^p - 1$ where p and n are both 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!)

Perfect numbers

Definition: A number is *perfect* if it equals the sum of its positive divisors, excluding itself.

$6 = 1 + 2 + 3$ and $28 = 1 + 2 + 4 + 7 + 14$ are perfect numbers.

$10 \neq 1+2+5 = 8$ and $12 \neq 1+2+3+4+6 = 16$ are not perfect.

- $q(q+1)/2$ is an even perfect number whenever q is a Mersenne prime (Euclid, 300 BC).
- All even perfect numbers have this form (Euler, 1700s).
- Are there infinitely many? Unknown!
- Is any odd number perfect? Unknown!

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. For example:

$a|b$ means $\exists k, ak = b$. Multiplying by c, we have $\exists k, cak = cb$. So, $ca|cb$. Also, if $ca|cb$, we have $\exists k, cak = cb$. If $c \neq 0$, that implies $\exists k, ak = b$, in other words, $a|b$. QED.

Definition: A number n is a *linear combination* of numbers $b_0, \ldots, b_n$ iff $n = s_0 b_0 + s_1 b_1 + \cdots + s_n b_n$ for some $s_0, \ldots, s_n$.

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: Infinitely many primes p such that $p + 2$ is the product of at most two primes.
- Primality Testing: There is an efficient way to determine whether a number is prime. Status: Yes, solved in 2002.
- 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". Languages?

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 $-11 = -2 \cdot 7 + 3$

Range notation:

- $(k, n) ::= \{i | k < i < n\}$
- $[k, n) ::= (k, n) \cup \{k\}$
- $(k, n\,] ::= (k, n) \cup \{n\}$
- $[k, n\,] ::= (k, n) \cup \{k, n\}$

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 a 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.