Number Theory I

Expanded

02/17/2020

Core definitions

Mod and div: (also called floor or integer division in CS) In the equality from the division theorem: $a = dq + r$, d is the divisor, a is the dividend, q is the quotient and r is the remainder

$q = a \text{ div } d$ $\quad r = a \bmod d$

$q = \left\lfloor \frac{a}{d} \right\rfloor$ $\quad a = \left\lfloor \frac{a}{d} \right\rfloor d + a \bmod d$

$r = 4 \bmod 3 = 1$

$r = -2 \bmod 5 = 3$

$q = 6 \text{ div } 12 = 0$

$q = 18 \text{ div } 12 = 1$

$q = -2 \bmod 5 = -1$

$-2 = \left\lfloor \frac{-2}{5} \right\rfloor \cdot 5 + 3$

Divisibility: if a and b are integers with $a \neq 0$, we say that a divides b if there is some integer c s.t. $ac = b$ or equivalently $b \bmod a = 0$. We denote this $a \mid b$ when the proposition $b \bmod a = 0$ is true and $a \nmid b$ if $b \bmod a = 0$ is false. We say that a (evenly) divides b, that a is a factor of b, and that b is a multiple of a.

$a \mid 0$ for any $a \in \mathbb{Z}^{\neq 0}$

$1 \mid a$ for any $a \in \mathbb{Z}$

$2 \mid 4$

$3 \mid 6$

$4 \nmid 6$

Congruence: Two integers, a and b are congruent mod k, written $a \equiv_k b$ or $a \equiv b \pmod{k}$ if $a \bmod k = b \bmod k$

$3 \equiv_3 6$

$5 \equiv_3 2$

$-2 \equiv_5 0$

Prime: An integer $p \geq 2$ is prime if the only positive factors of p are 1 and p. An integer $p \geq 2$ that is not prime is composite.

13 is prime

7 is prime

6 is not prime

GCD: The greatest common divisor of two positive integers, n and m, written $\gcd(n, m)$ is the largest $d \in \mathbb{Z}^{>0}$ s.t. $d \mid n$ and $d \mid m$

$\gcd(6, 27) = 3$

$\gcd(1, 9) = 1$

$\gcd(12, 6) = 6$

$\gcd(2, 4) = 2$

Relative Primality: Two positive integers n, m are relatively prime if $\gcd(n, m) = 1$.

$\gcd(21, 50) = 1$

21 and 50 are relatively prime (note 21 and 50 are not prime)

Field: $\mathbb{Z}_p$, the set of integers $\{0, 1, \ldots, p-1\}$ is called a field, a finite field, or a Galois field.

Core Theorems

The Division Theorem:

Let $a \in \mathbb{Z}$ and $d \in \mathbb{Z}^{>0}$, then there exists unique integers q and r with $0 \leq r < d$ such that $a = dq + r$

$d = 7 \quad a = 3 \mid q = 2 \quad r = 1$

$d = 202 \quad n = -404 \mid q = -2 \quad r = 0$

$d = 10 \quad n = -21 \mid q = -3 \quad r = 9$

r is always positive

Bezout's Identity:

Let n, m be any positive integers and let $r = \gcd(n, m)$, then there exists $x, y \in \mathbb{Z}$ s.t. $xn + ym = r$

$\gcd(2, 9) = 1$

$1 = x \cdot 2 + y \cdot 9$

$= 5 \cdot 2 + (-1) \cdot 9$

5 is the inverse of 2 mod 9

On the Existence of Integer Multiplicative Inverses:

Let $n \geq 2$ and $a \in \mathbb{Z}_n$. Then a^{-1} exists in $\mathbb{Z}_n$ if and only if n and a are relatively prime.

Given two positive integers n, m $m \geq n$ if $\gcd(n, m) = 1$ then $in^{-1} \in \mathbb{Z}_m$ is $x \bmod m$.

Corollary to Existence of Inverses:

if p is prime then every nonzero $a \in \mathbb{Z}_p$ has a multiplicative inverse

Corollary to Existence of Inverses:

Shamir's Secret Sharing is defined over $\mathbb{Z}_p$ when p is a prime.

Core Algorithms

Euclid(n, m):

Input: n, m are positive integers and $m \geq n$

output: gcd(n, m)

1. if m mod n = 0 then
2. return n
3. else
4. return Euclid(m mod n, n)

$1024 \bmod 48 \neq 0$

$Euclid(48, 1024) = Euclid(\underbrace{1024 \bmod 48}_{16}, 48)$

$48 \bmod 16 = 0$

return 16

$= 16$

$42 \bmod 17 \neq 0$

$Euclid(17, 42) = Euclid(\underbrace{42 \bmod 17}_{8}, 17)$

$17 \bmod 8 \neq 0$

$= Euclid(\underbrace{17 \bmod 8}_{1}, 8)$

$8 \bmod 1 = 0$

return 1

$= 1$

Extend Euclidean Algorithm (n, m)

aka EEA(n, m)

Input: n, m are positive integers and $m \geq n$

output: x, y, r where $r = gcd(n, m) = xn + ym$

1. if m mod n = 0 then
2. return 1, 0, n

Note, n is a multiple of n then we have found the gcd, namely n. And moreover $1 \cdot n + 0 \cdot m = n$ so we return $x = 1$ and $y = 0$

3. else
4. $x, y, r = EEA(m \bmod n, n)$
5. return $y - \lfloor \frac{m}{n} \rfloor \cdot x, x, r$

$EEA(12, 18)$ because $18 \bmod 12 \neq 0$ we recurse

$EEA(\underbrace{18 \bmod 12}_{6}, 12)$ because $12 \bmod 6 = 0$ we hit base case

$= 1, 0, 6$

$= y - \lfloor \frac{m}{n} \rfloor \cdot x, x, r$ we recurse up and in this case $n = 12$ $m = 18$

$= 0 - \lfloor \frac{18}{12} \rfloor \cdot 1, 1, 6$

$= 0 - 1 \cdot 1, 1, 6$

$= -1, 1, 6$

$6 = \underset{x}{-1} \cdot 12 + \underset{y}{1} \cdot 18$

$EEA(12, 18)$

$EEA(\underbrace{30 \bmod 18}_{12}, 18)$

$EEA(\underbrace{18 \bmod 12}_{6}, 12)$

$= 1, 0, 6$

$= -1, 1, 6$ from above

$= y - \lfloor \frac{m}{n} \rfloor x, x, r$

$= 1 - \lfloor \frac{30}{18} \rfloor \cdot (-1), -1, 6$

$= 1 - (1)(-1), -1, 6$

$= 2, -1, 6$

$6 = 2 \cdot 18 + -1 \cdot 30$:)