

Chapter 1 Summary and Study Guide

1.1 Divisors

Division Algorithm: Given integers $a \geq 1$ and b , there exist unique integers q and r such that (i) $b = qa + r$ and (ii) $0 \leq r < a$.

Three proofs of the Division Alg: (1) well-ordering; (2) induction; (3) floor function

Divisor: $a|b$ means there exists an integer q such that $b = qa$, or equivalently, the remainder using the Division Algorithm is 0. (a is not allowed to be 0.) We also say b is a multiple of a .

Common Divisors: d is a common divisor of a and b means $d|a$ and $d|b$.

Greatest Common Divisor: $g = GCD(a, b)$ means d is the largest common divisor of a and b . $GCD(a, b)$ is often written (a, b) .

Proposition: If d is a common divisor of a and b , then d divides (a, b) .

POW Problem: Bring back 1 quart of water with a - and b -quart pails.

Euclidean Algorithm: Idea: if $b = aq + r$, then $(b, a) = (a, r)$. Yields integers m and n such that $ma + nb = g$, where $g = (a, b)$.

Matrix Version.

1.2 Primes

Primes: 2, 3, 5, 7, 11, ...

Composites: 4, 6, 9, 10, 12, ...

Unit: 1

Sieve of Eratosthenes: Cross out multiples of 2, 3, 5, 7, 11, up to \sqrt{n} .

Relatively Prime: a and b are relatively prime means $(a, b) = 1$.

Basic Fact: If a and b are relatively prime, then there exist integers m and n such that $ma + nb = 1$.

Basic Lemma: If $a|bc$ and $(a, b) = 1$, then $a|c$.

Consequence for Primes: If p is a prime and $p|ab$, then $p|a$ or $p|b$.

Unique Factorization into Primes: Every integer $n \geq 2$ can be written uniquely as a product of primes, up to the order of the factors.

Strange Examples where unique factorization fails

Katie's Theorem: n and $n + 1$ are relatively prime.

Prime Desert Theorem: There exist prime deserts, i.e., given an integer k no matter how large, there exist k consecutive composite integers. For example, 62, 63, 64, 65, 66 are 5 consecutive composites.

Infinitude of Primes Theorem: There exist infinitely many primes.

Common Multiple: m is a common multiple of a and b means $a|m$ and $b|m$.

Least Common Multiple. $L = LCM[a, b]$ means L is the smallest positive integer which is a common multiple of a and b . $LCM[a, b]$ is often written $[a, b]$.

Proposition: If m is a common multiple of a and b , then $[a, b]$ divides m .

Theorem: $(a, b) [a, b] = ab$

Representations of GCD and LCM using prime representation:

If $a = p_1^{e_1} p_2^{e_2} \cdots p_r^{e_r}$ and $b = p_1^{f_1} p_2^{f_2} \cdots p_r^{f_r}$, $e_i \geq 0$ and $f_i \geq 0$, then
 $GCD(a, b) = \prod_{i=1}^r p_i^{\min(e_i, f_i)}$ and $LCM[a, b] = \prod_{i=1}^r p_i^{\max(e_i, f_i)}$.

1.3 Congruences

Definition: $a \equiv b \pmod{n}$ means $n|a - b$

Equivalently, $a \equiv b \pmod{n}$ if and only if a and b have the same remainder when divided by n .

Algebra of Congruences: You can add, subtract, and multiply congruences.

Solving Polynomial Congruences by trial and error: Working mod n , if n is small, try all values $x = 0, 1, 2, \dots, n - 1$.

In-class worksheet: If p is a prime, then the congruence $x^2 \equiv -1 \pmod{p}$ has a solution if and only if $p = 2$ or $p = 4n + 1$.

Solving linear congruences $ax \equiv b \pmod{n}$.

Let $d = (a, n)$.

If $d = 1$, unique solution mod n

If $d > 1$, then

$d \nmid b$ implies no solution

$d|b$ implies d solutions, obtained by solving

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}.$$

Chinese Remainder Theorem: For solving systems of congruences, when each pair of moduli is relatively prime.

two congruences: see book

three congruences: see CRT Handout giving

(1) one-at-a-time method

(2) $i - j - k$ method.

1.4 Congruences Classes

$$[a]_n \stackrel{\text{def}}{=} \{x : x \equiv a \pmod{n}\}$$

$$[a]_n = [b]_n \text{ if and only if } a \equiv b \pmod{n}.$$

$$\text{The integers mod } n: \mathbb{Z}_n \stackrel{\text{def}}{=} \{[0]_n, [1]_n, [2]_n, \dots, [n-1]_n\}.$$

Plus and times tables mod n .

Multiplication mod p , a prime, rearranges the elements $1, 2, 3, \dots, p-1$.

Fermat's Little Theorem: If p is a prime and $(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$.

First Proof: Rearrangement

Second Proof: Uses the fact that for a prime p , the binomial coefficient $\binom{p}{k} \equiv 0 \pmod{p}$, if $1 \leq k \leq p-1$.

$$\text{The invertible integers mod } n: \mathbb{Z}_n^\times \stackrel{\text{def}}{=} \{[k]_n : (k, n) = 1\}.$$

Note: $(k, n) = 1$

\iff there exist integers i and j such that $ik + jn = 1$

\iff the congruence $kx \equiv 1 \pmod{n}$ has a solution $x = i$

\iff there exists a congruence class $[i]_n$ such that $[i]_n[k]_n = [1]_n$.

The Phi Function: $\phi(n) \stackrel{\text{def}}{=} \text{the number of integers } k, 1 \leq k \leq n, \text{ which are relatively prime to } n$.

Formula for finding phi:

$$\phi(n) = \left(\prod_{p|n} \frac{p-1}{p} \right) \cdot n$$

where the product is taken over all prime divisors of n .

$$\text{Example: } \phi(60) = \frac{4}{5} \frac{2}{3} \frac{1}{2} 60 = \frac{4}{5} \frac{2}{3} 30 = \frac{4}{5} 20 = 16.$$

Example: For a prime p : $\phi(p) = p-1$.