[Number Theory] Exam #3 Study Guide

Past Material

[1] Bezout's Identity

Theorem: For any $a, b \in \mathbb{Z}$, there exists $x, y \in \mathbb{Z}$ such that

$$ax + by = \gcd(a, b) \tag{28}$$

[2] Euclidean Algorithm

Theorem: $\gcd(a, b, c) = \gcd(a, \gcd(b, c)) = \gcd(\gcd(a, b), c)$

Example: Find the $\gcd(1071, 462)$.

$$\begin{aligned} 1071 &= 2(462) + 147 \\ 462 &= 3(147) + 21 \\ 147 &= 7(21) + 0 \end{aligned}$$

This means that $\gcd(1071, 462) = 21$.

[3] Fundamental Theorem of Arithmetic

Fundamental Theorem of Arithmetic: Every integer $n > 1$ can be UNIQUELY factored as the product of primes.

Corollary: Any positive integer $n > 1$ can be written uniquely in a canonical form:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_t^{k_t} \tag{29}$$

where for all i:

- p_i is prime
- $p_1 < p_2 < \cdots < p_t$
- k_i are positive integers

Theorem (Euclid): There are infinitely many primes.

Definition: The integers a, b are congruent mod n if $n \mid (a - b)$. We write this $a \equiv b \bmod n$.

[4] Greatest Common Divisor

Definition: The greatest common divisor of integers a, b, also known as $\gcd(a, b)$ is defined as follows.

$$\gcd(a, b) = \max\{d \in \mathbb{Z} : d \mid a \cap d \mid b\} \tag{30}$$

[5] Solvability Theorem

Definition (Solvability): The equation $ax \equiv b \bmod n$ has a solution $\iff \gcd(a, n) \mid b$.

Lemma: If $\gcd(a, n) = 1$, then $ax \equiv b \bmod n$ has a unique solution $\bmod n$.

[6] Chinese Remainder Theorem

Lemma: When $\gcd(a, n) \mid b$, the number of solutions to $ax \equiv b \bmod n$ is $\gcd(a, n)$.

Chinese Remainder Theorem: Let $n_1, n_2, \ldots, n_t$ be positive integers such that $\gcd(n_i, n_j) = 1$ for all $i \neq j$. Then

$$\begin{aligned} x &\equiv a_1 \bmod n_1 \\ x &\equiv a_2 \bmod n_2 \\ &\vdots \\ x &\equiv a_t \bmod n_t \end{aligned}$$

has a simultaneous solution which is unique $\bmod n_1 n_2 \cdots n_t$.

[7] Fermat's Little Theorem

Theorem (Fermat): Suppose p is prime and $p \nmid a$. Then,

$$a^{p-1} \equiv 1 \bmod p \tag{31}$$

Corollary: If p is prime, then for every a,

$$a^p = a \bmod p \tag{32}$$

[8] Wilson's Theorem

Theorem (Wilson): If p is prime, then $(p-1)! \equiv -1 \bmod p$.

Converse of Wilson's Theorem: If $(n-1)! \equiv -1 \bmod n$, then n is prime.

New Material

[16 Lecture]

Definition (Tau): Let n be any integer.

$$\tau(n) := \#\text{ of positive divisors of } n = \sum_{d|n} 1 \tag{33}$$

Claim: $\tau(n) = (k_1+1)(k_2+1)(k_3+1)\cdots(k_r+1)$ if $n = p_1^{k_1}p_2^{k_2}\cdots p_r^{k_r}$.

[17 Lecture]

Theorem:

$$n^{\frac{\tau(n)}{2}} = \prod_{d|n} d \tag{34}$$

Definition: A number theoretic function f is multiplicative if $f(mn) = f(m)f(n)$ whenever $\gcd(m,n) = 1$.

Definition:

$$\varphi(n) = \#\{m : 1 \leq m \leq n \text{ and } \gcd(m,n) = 1\} \tag{35}$$

Lemma: $\varphi(n) = n-1 \iff n$ is prime.

Theorem: If p is prime and $k > 0$, then $\varphi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right)$.

Theorem:

$$\varphi(n) = n \cdot \prod_{i=1}^{s}\left(1 - \frac{1}{p_i}\right) \tag{36}$$

[20 Lecture]

Theorem: For all $n > 2$, we have that $\varphi(n)$ is always even.

Euler's Theorem: If $\gcd(a,n) = 1$, then $a^{\varphi(n)} \equiv 1 \pmod{n}$.

[21 Lecture]

Definition: A group $(G, *)$ is a set G equipped with a binary operation (denoted $*$) such that:

- **Identity:** there is an identity element e_G such that $e_G * g = g * e_G = g$ for all $g \in G$.
- **Associativity:** $g_1 * (g_2 * g_3) = (g_1 * g_2) * g_3$
- **Inverse:** Every element has an inverse, that is, $\forall a \in G, \exists\, b \in G$ such that

$$a * b = b * a = e \tag{37}$$

Definition:

$$(\mathbb{Z}/n\mathbb{Z})^* = \{x : x \in \mathbb{Z}/n\mathbb{Z} \text{ and } \gcd(x, n) = 1\} \tag{38}$$

is a group and the group operation is multiplication!

Definition: Given a group $(G, *)$, the order of g is the smallest m such that $g * g * \cdots * g = e_g$. When, $G = (\mathbb{Z}/n\mathbb{Z})^*$, the order of g is the smallest m such that $g^m \equiv 1 \pmod{n}$.

Theorem: Suppose $a \in (\mathbb{Z}/n\mathbb{Z})^*$ and $\text{ord}(a) = k$. Then,

$$a^h \equiv 1 \pmod{n} \iff k \mid h \tag{39}$$

Corollary: For any $a \in (\mathbb{Z}/n\mathbb{Z})^*$, $\text{ord}(a) \mid \varphi(n)$.

Definition: If $\gcd(a, n) = 1$ and $\text{ord}(a) = \varphi(n)$, then a is called a primitive root of n.

[22 Lecture]

Theorem: If p is prime, and $d \mid p - 1$, then there are exactly $\varphi(d)$ integers of order d.

Corollary: $(\mathbb{Z}/p\mathbb{Z})^*$ has $\varphi(p - 1)$ many primitive roots.

Theorem: $(\mathbb{Z}/n\mathbb{Z})^*$ has a primitive root $\iff n = 2, 4, p^k, 2p^k$.

[23 Lecture]

Definition: Let p be an odd prime and suppose $\gcd(a, p) = 1$. If the congruence $x^2 \equiv a \pmod{p}$ has a solution, then we say that a is a quadratic residue of p. If a cannot be realized this way, then a is a quadratic non-residue of p.

Euler's Criterion: Let p be an odd prime and suppose $\gcd(a, p) = 1$. Then, a is a quadratic residue of $p \iff a^{\frac{p-1}{2}} \equiv 1 \bmod p$.

Corollary: If p is an odd prime and $\gcd(a, p) = 1$, then

$$a^{\frac{p-1}{2}} \equiv \begin{cases} 1 & a \text{ is a quadratic residue} \\ -1 & a \text{ is a quadratic nonresidue} \end{cases} \tag{40}$$

[24 Lecture]

Theorem: Suppose p is an odd prime. Then, 2 is a quadratic residue $\pmod{p}$ iff $p \equiv 1 \pmod{8}$ or $p \equiv 7 \pmod{8}$.

Theorem: If p and $2p+1$ are both odd primes, then the integer $(-1)^{\frac{p-1}{2}} \cdot 2$ is a primitive root of $2p+1$.

[25 Lecture]

Verman Encryption: Choose an arbitrary sequence of 1's and 0's with the same length as the numerical plaintext. This will be the KEY, which you add to the binary value of the thing.

Diffie Hellman Encryption: Secure for key-exchange.

- Bob and Alice both agree on a primitive root x and a modulus p
- Bob and Alice each pick a secret key A, B
- They do $x^A \pmod{p}$ and $x^B \pmod{p}$ respectively to get the public keys, which they then exchange
- They each then take the other's and do $\beta^A \pmod{p}$ and $\alpha^B \pmod{p}$ to get the shared secret (which they can use to encrypt messages)

[26 Lecture]

RSA: Hard to break because it requires the hacker to know how to factor N which is a pain the ass!

- Alice picks two large primes p, q and calculates $N = pq$
- Alice then picks some e such that $\gcd(e, \varphi(N)) = 1$
- Alice puts e, N in some public directory
- Bob wants to send a message $m = 66$ to Alice $(B \mapsto 66)$
- Bob calculates the ciphertext, $C = B^e \pmod{N}$
- Alice decrypts it by computing her private key $d \equiv e^{-1} \pmod{\varphi(N)}$
- The original message $m = c^d \pmod{N}$