FinalPrep of Math 312

Tom Wang

Spring, 2024

1 Induction

Induction/ Strong Induction is basically another way of Well well-ordering principle.

Theorem 1. *Every non-empty subset of* $\mathbb{N}$ *has a smallest element.*

1.1 Division algorithm

Theorem 2. *For any integers* a *and* b *with* $b > 0$*, there exist unique integers* q *and* r *such that* $a = bq + r$ *and* $0 \leq r < b$*. Moreover,* q *is called the quotient and* r *is called the remainder and they are unique.*

2 Primes

Definition 1. *A natural number* p *is called a prime if* $p > 1$ *and the only positive divisors of* p *are 1 and* p*.*

2.1 Euclid's Lemma

Lemma. *There are infinitely many primes.*

2.2 Sieve of Eratosthenes

Theorem 3. $\exists$ *a prime* p *s.t.* $p \leq n, \forall n \in \mathbb{N}, n > 1.$

2.3 The prime number theorem

Theorem 4. *Let $\pi(x)$ be the number of primes less than or equal to x. Then $\lim_{x\to\infty} \frac{\pi(x)}{x/\ln(x)} = 1$.*

In other words, the number of primes less than x is approximately less than or equal to $x/\ln(x)$.

3 Division

3.1 GCD

Definition 2. *Let a and b be integers, not both zero. The greatest common divisor of a and b, denoted $\gcd(a, b)$, is the largest integer that divides both a and b.*

Corollary. *e is a divisor of a and b if and only if e is a divisor of $\gcd(a, b)$.*

Corollary. *$ax + by = c$ has an integer solution if and only if $\gcd(a, b)$ divides c.*

3.2 Bezout's Identity

Theorem 5. *$\gcd(a, b)$ is the **smallest** positive integer that can be written in the form $ax + by$. (linear combination of a and b)*

3.3 Euclidean Algorithm

Lemma. *If $a = bq + r$, for $a, b, q, r \in \mathbb{Z}$, then $\gcd(a, b) = \gcd(b, r)$.*

While loop version:

Input: $a, b \in \mathbb{Z}$
Output: $\gcd(a, b)$
Procedure:
while $b \neq 0$ **do**
  $r = a \mod b$
  $a = b$
  $b = r$
end while
return a

Recursive version:

Input: $a, b \in \mathbb{Z}$
Output: $\gcd(a, b)$
Procedure:
if $b = 0$ **then**
  return a
else
  return $\gcd(b, a \mod b)$
end if

3.4 Linear equations

Solve linear equations in the form of $ax + by = c$.

1. Use the Euclidean Algorithm to find $\gcd(a, b)$.
2. Check if $\gcd(a, b)$ divides c.
3. If it does, find x_0, y_0 such that $ax_0 + by_0 = \gcd(a, b)$.
4. Multiply the equation by $c/\gcd(a, b)$ to get the solution.
5. The general solution is $x = x_0 + c \cdot k, y = y_0 - c \cdot k$ for $k \in \mathbb{Z}$.
6. If $\gcd(a, b)$ does not divide c, there is no solution.

3.4.1 Describe all solutions

Theorem 6. *Let $d = \gcd(a, b)$. The equation $ax + by = c$ has a solution if and only if d divides c. The set of solutions is given by*

$$\{(x_0 + \frac{b}{d}t, y_0 - \frac{a}{d}t) | t \in \mathbb{Z}\}$$

Here x_0, y_0 is a particular solution.

x_0, y_0 can be found by solving $ax + by = d$ using the Euclidean Algorithm as described above.

3.4.2 Key lemma

Lemma. *Let $a, b \in \mathbb{Z}$ and $d = \gcd(a, b)$. $d = 1 \iff (a|bc \implies a|c)$.*

Note how it is not true for $d > 1$.

3.5 Fundemental Theorem of Arithmetic

Theorem 7. *$\forall n \in \mathbb{N}$, $n > 1$, n can be written as a product of primes. Moreover, this factorization is unique.*

Usually, we write $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Note that e_i can be 0 and p_i are distinct primes.

Corollary. *Let p be a prime. $p|a_1 a_2 \cdots a_n \implies p|a_i$ for some i.*

Proposition. *Suppose $m = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$ and $n = p_1^{f_1} p_2^{f_2} \cdots p_k^{f_k}$, then $\gcd(m, n) = p_1^{\min(e_1,f_1)} p_2^{\min(e_2,f_2)} \cdots p_k^{\min(e_k,f_k)}$ and lcm$(m, n) = p_1^{\max(e_1,f_1)} p_2^{\max(e_2,f_2)} \cdots p_k^{\max(e_k,f_k)}$.*

Corollary. *$\gcd(m, n) \cdot$ lcm$(m, n) = mn$.*

4 Congruences

Definition 3. *Let $a, b, n \in \mathbb{Z}$ with $n > 0$. We say a is congruent to b modulo n if $n|(a - b)$. We write $a \equiv b \pmod{n}$.*

Note that it is reflective, symmetric and transitive. It is also closed under addition, exponentiation and multiplication.

4.1 Congruence Class

Definition 4. *Let $n \in \mathbb{Z}$ with $n > 0$. The congruence class of a modulo n is the set of all integers that are congruent to a modulo n. We denote this by $[a]_n$.*

$$[a]_n = \{x \in \mathbb{Z} | x \equiv a \pmod{n}\}$$

4.2 Modular exponentiation

Theorem 8. *Let $a, b, n \in \mathbb{Z}$ with $n > 0$. Then $a \equiv b \pmod{n} \implies a^k \equiv b^k \pmod{n}$.*

Thus, we can calculate large powers by repetitively squaring the number and multiply the result.

4.2.1 Representations of integer

Theorem 9. *Let $b \in \mathbb{Z}$ with $b > 1$. Then every integer n can be written in the form*

$$n = a_k b^k + a_{k-1} b^{k-1} + \cdots + a_1 b + a_0$$

where $0 \leq a_i < b, a_k \neq 0, k \in \mathbb{N}$.

Moreover this representation is unique.

This is how binary representation works and it can extend to any base.

4.3 Linear Congruences

$ax \equiv b \pmod{n}$ is a linear congruence. It has a solution if and only if $\gcd(a, n) | b$. Basically expressing it as $ax + ny = b$ and solving it.

Theorem 10. *If $d = \gcd(a, n)$ and $d|b$, then the linear congruence $ax \equiv b \pmod{n}$ has exactly d solutions modulo n.*

Solutions are considered the same if they differ by a multiple of n/d.

4.4 Multiplicative Inverse

Definition 5. *Let $a, n \in \mathbb{Z}$ with $n > 0$. The multiplicative inverse of a modulo n is an integer x such that $ax \equiv 1 \pmod{n}$. We denote this by a^{-1}.*

Corollary. *Let p be a prime, then every $a \neq 0 \pmod{p}$ has a multiplicative inverse.*

Corollary. *Let p be a prime, $a \equiv a^{-1} \pmod{p} \iff a \equiv \pm 1 \pmod{p}$.*

4.5 Chinese Remainder Theorem

Theorem 11. *Let $n_1, n_2, \cdots, n_k$ be positive integers that are pairwise relatively prime. Then the system of congruences*

$$\begin{cases} x \equiv a_1 \pmod{n_1} \\ x \equiv a_2 \pmod{n_2} \\ \vdots \\ x \equiv a_k \pmod{n_k} \end{cases}$$

has a unique solution modulo $n_1 n_2 \cdots n_k$.

Theorem 12. *The system of linear congruences*

$$\begin{aligned} x &\equiv a_1 \pmod{n_1} \\ x &\equiv a_2 \pmod{n_2} \\ &\vdots \\ x &\equiv a_r \pmod{n_r} \end{aligned}$$

has a solution if and only if $a_i \equiv a_j \pmod{\gcd(n_i, n_j)}$ *for all* i, j*. Moreover, the solution is unique modulo* $N =$ *lcm*$(n_1, n_2, \ldots, n_r)$.

4.5.1 Algorithm

Let $N = n_1 n_2 \cdots n_k$. Then $N_i = N/n_i$. Let y_i be the multiplicative inverse of N_i modulo n_i. Then the solution is

$$x = a_1 y_1 N_1 + a_2 y_2 N_2 + \cdots + a_k y_k N_k$$

To see that $x \equiv a_i \pmod{n_i}$, note that $N_i \equiv 0 \pmod{n_j}$ for $j \neq i$ and $N_i \equiv 1 \pmod{n_i}$. Thus $x \equiv a_i y_i \pmod{n_i}$ and $a_i y_i \equiv 1 \pmod{n_i}$.

4.6 Divisibility criteria

To be added if needed.

5 Fermat's Little Theorem

5.1 Wilson's Theorem

Theorem 13. *let* p *be a prime. Then* $(p-1)! \equiv -1 \pmod{p}$.

5.2 Fermat's Little Theorem

Theorem 14. *Let* p *be a prime and* $a \in \mathbb{Z}$ *with* $p \nmid a$*. Then* $a^{p-1} \equiv 1 \pmod{p}$.

Corollary. *Let* p *be a prime and* $a \in \mathbb{Z}$*. Then if* $d \equiv e \pmod{p-1}$*, then* $a^d \equiv a^e \pmod{p}$.

Proof. Let $d = e + k(p-1)$. Then $a^d \equiv a^{e+k(p-1)} \equiv a^e a^{k(p-1)} \equiv a^e (a^{p-1})^k \equiv a^e \pmod{p}$. $\square$

5.3 Euler's Theorem

Theorem 15. *Let $n \in \mathbb{Z}$ with $n > 0$ and $a \in \mathbb{Z}$ with $\gcd(a, n) = 1$. Then $a^{\phi(n)} \equiv 1 \pmod{n}$.*

Lemma. $\gcd(a, n) = 1 \wedge \gcd(b, n) = 1 \implies \gcd(ab, n) = 1$.

Lemma. *Suppose $n = p^r$ for some prime p and $r \in \mathbb{N}$. Then $\phi(n) = p^r - p^{r-1}$.*

Lemma. *If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$.*

5.3.1 Euler's phi function

Definition 6. *Let $n \in \mathbb{Z}$ with $n > 0$. The Euler's phi function $\phi(n)$ is the number of positive integers less than n that are relatively prime to n.*

Theorem 16. *Let $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$. Then $\phi(n) = n(1 - \frac{1}{p_1})(1 - \frac{1}{p_2}) \cdots (1 - \frac{1}{p_k})$.*

Note that it is because of the two lemmas above. ϕ is morphism and is multiplicative.

Theorem 17. $\sum_{d|n} \phi(d) = n$

This is because $\phi(d)$ is the number of elements in the set $\{x \in \mathbb{Z} | 1 \leq x \leq n, \gcd(x, n) = d\}$.

5.3.2 Multiplicative group

Note that the Euler ϕ function is multiplicative only if $\gcd(m, n) = 1$.

Lemma. *If $n = p_1^{e_1} p_2^{e_2} \cdots p_k^{e_k}$, where p_i are distinct primes and $e_i \geq 1$, then*

$$f(n) = \prod_{i=1}^{k} f(p_i^{e_i}) = \prod_{i=1}^{k} p_i^{e_i - 1}(p_i - 1)$$

Theorem 18. *If $f(n)$ is multiplicative, so is $F(n) = \sum_{d|n} f(d)$.*

Definition 7. *Define two more multiplicative functions:*

- *$\sigma(n)$ is the sum of all positive divisors of n.*
- *$\tau(n)$ is the number of positive divisors of n.*

5.4 Perfect numbers

Theorem 19. *Let n be a positive integer, then n is a perfect number if and only if $\sigma(n) = 2n$.*

Or equivalently, n is the sum of its proper divisors.

Theorem 20. *Suppose $m \leq 2$ is a prime and $p = 2^m - 1$ is also a prime. Then $n = 2^{m-1}p$ is a perfect number.*

Lemma. *If $2^m - 1$ is prime, then m is prime.*

Definition 8. *Mersenne prime is a prime of the form $2^m - 1$.*

Theorem 21. *Even numbers of the form $n = 2^{m-1}(2^m - 1)$ are perfect if $2^m - 1$ is prime.*

5.4.1 Euler's Perfect Number Theorem

Theorem 22. *Let n be an even perfect number. There exists a prime m such that $n = 2^{m-1}(2^m - 1)$ and $2^m - 1$ is prime.*

5.5 Mobius Inversion Formula

Definition 9. *The Mobius function $\mu(n)$ is defined as*

$$\mu(n) = \begin{cases} 1 & \text{if } n = 1 \\ 0 & \text{if } p^2 | n \text{ for some prime } p \\ (-1)^k & \text{if } n = p_1 p_2 \cdots p_k \text{ for distinct primes } p_i \end{cases}$$

If $f(n)$ is a multiplicative function, and $F(n) = \sum_{d|n} f(d)$ is also multiplicative. We want to recover $f(n)$ from $F(n)$.

Definition 10. *The Mobius inversion formula is*

$$f(n) = \sum_{d|n} \mu(d) F(n/d)$$

Note that $\mu(n)$ is multiplicative.

Corollary.

$$f(n) = \sum_{d|n} F(d)\mu(n/d) = \sum_{d|n} F(n/d)\mu(d)$$

Note $F(n/d) = \sum_{e|\frac{n}{d}} f(e)$.
Then

$$f(n) = \sum_{d|n} F(\frac{n}{d})\mu(d) = \sum_{d|n}\sum_{e|\frac{n}{d}} f(e)\mu(d) = \sum_{e|n}\sum_{d|\frac{n}{e}} f(e)\mu(d) = \sum_{e|n} f(e)\sum_{d|\frac{n}{e}}\mu(d)$$

5.6 Primality Testing

5.6.1 Fermat's Primality Test

If there exists an a such that $a^{n-1} \not\equiv 1 \pmod n$, then n is composite. Otherwise, n is probably prime. (Fermat's Little Theorem)

5.6.2 Carmichael Numbers

Definition 11. *A composite number n is a Carmichael number if $a^{n-1} \equiv 1 \pmod n$ for all a such that $\gcd(a, n) = 1$.*

Suppose $n = p_1 p_2 \cdots p_r$ where $p_1, p_2, \ldots, p_r$ are distinct primes. If $p_i - 1 \mid n - 1$ for all i, then n is a Carmichael number.

So each prime of Carmichael number would satisfy Fermat's Primality Theorem to get $b^{p_i - 1} \equiv b^{n-1} \equiv 1 \pmod n$. Then by CRT, we can get $b^{n-1} \equiv 1 \pmod n$.

5.6.3 Miller-Rabin Primality Test

To deal with Carmichael numbers, we use the Miller-Rabin Primality Test. It is a probabilistic algorithm.

1. Start out the same way as Fermat's Primality Test. Choose a random integer b in $[2, n-2]$. Then compute $b^{n-1} \pmod n$.

2. If $b^{n-1} \not\equiv 1 \pmod n$, then n is not prime.

3. If $b^{n-1} \equiv 1 \pmod n$, then we probe a bit deeper by computing $x \equiv b^{(n-1)/2} \pmod n$. (Here we are assuming that $n-1$ is even. If $n-1$ is odd, then n is not prime since $b \geq 2$)

4. Note that $x^2 = b^{n-1} \equiv 1 \pmod{n}$. If n is a prime, then $x \equiv \pm 1 \pmod{n}$.

5. If $x \equiv 1 \pmod{n}$, and $\frac{n-1}{2}$ is odd, We cannot say anything here, pick another b and repeat the test.

6. If $x \equiv -1 \pmod{n}$, then n is **probably** prime. We cannot say anything here, pick another b and repeat the test.

7. However, if $x \equiv 1 \pmod{n}$, and $\frac{n-1}{2}$ is even, then we can dig deeper by computing $y \equiv b^{(n-1)/4} \pmod{n}$.

8. Same idea: If $y \equiv -1 \pmod{n}$, or $y \equiv 1 \pmod{n}$ and $\frac{n-1}{4}$ is odd, then pick another b and repeat the test.

9. If $y \equiv 1 \pmod{n}$, and $\frac{n-1}{4}$ is even, then repeat checking.

10. The only stop criterion is when we conclude that n is composite.

11. We never conclude with 100% certainty that n is prime. We can only say that n is **probably** prime. It is a probabilistic test!

5.6.4 Rabin's Theorem

Theorem 23. *Fix a composite number n. Pick $a \in [2, n-2]$ at random. Then the probability that $a^{n-1} \equiv 1 \pmod{n}$ is at most $\frac{1}{4}$.*

In other words, the Miller-Rabin Primality Test can detect a composite number with probability at least $\frac{1}{4}$.

Thus if we run m iterations of the test, the probability that n is composite is at most $(\frac{3}{4})^m$.

5.7 Pollard's Factorization Algorithm

Goal: factor a given composite number n.

1. Choose $r_0 \equiv 2^{0!} \pmod{n}$.

2. Compute the next one using the formula $r_k \equiv r_{k-1}^k \pmod{n}$.

3. For each k compute $\gcd(r_k - 1, n) = g_k$. Note that $1 \leq g_k \leq r_{k-1} \leq n-2$ and g_k divides n.

4. For each k So if $g_k > 1$, then we have found a factor of n which is greater than 1.

5. Repeat the process till we find a factor of n.

The idea is that if n is prime, $2^{k!} \equiv 1 \pmod{n}$. If n is composite, then $2^{k!} \not\equiv 1 \pmod{n}$.

6 Cryptography

6.1 Classical Cryptography

No public key.

6.1.1 Affine Cipher

Basically solving two linear congruences. $\begin{cases} ax_1 + b \equiv c_1 \pmod{26} \\ ax_2 + b \equiv c_1 \pmod{26} \end{cases}$ where c_1, c_2 are the ciphertext and x_1, x_2 are the plaintext. Then we can recover a, b by solving the system of congruences.

Start by eliminating one variable by subtracting the two equations. Then solve for the other variable.

6.1.2 Exponentiation Cipher

Use the lemma:

Lemma. $de \equiv 1 \pmod{\phi(n)} \implies m^{de} \equiv m \pmod{n}$.

Then we can encrypt by $c \equiv m^e \pmod{n}$ and decrypt by $m \equiv c^d \pmod{n}$.

6.2 RSA

Theorem 24. *Let $n = pq$ where p, q are distinct primes. Let e be an integer such that $\gcd(e, \phi(n)) = 1$. Then the encryption function is $c \equiv m^e \pmod{n}$ and the decryption function is $m \equiv c^d \pmod{n}$ where d is the multiplicative inverse of e modulo $\phi(n)$.*

A variation of the Exponentiation Cipher.

6.2.1 Fermat's Factorization Method

Theorem 25. *Let n be a composite number. Then n can be factored as $n = a^2 - b^2 = (a+b)(a-b)$.*

One of a, b is larger than $\sqrt{n}$ and the other is smaller. We can find a by computing $\lceil \sqrt{n} \rceil$ and keep incrementing until we find a square. Then we can find b by computing $a^2 - n$ and keep incrementing until we find a square.