CSI 2101 Lecture Notes

Last updated:

April 13, 2023

Contents

Definitions, Theorems, Lemmas, and Corollaries

Definition 4.1.1. *Let a and b be two integers such that $a \neq 0$. We say that a divides b if there exists c such that $b = ac$. If a divides be we say a is a factor or divisor of b. We also can say b is a multiple of a.*

Theorem 4.1.1. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$.*

1. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$*
2. *If $a \mid b$, then $a \mid bc$ for every integer*
3. *If $a \mid b$ and $b \mid c$, then $a \mid c$*

Corollary 4.1.1. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a \mid b$ and $a \mid c$, $a \mid (mb + nc)$ for all integers m and n*

Theorem 4.1.2 (The Division Algorithm)**.** *Let $a, d \in \mathbb{Z}$ with $d > 0$. There exists a unique q and r such that*

$$0 \leq r \leq d$$

and

$$a = dq + r$$

We write

$$q = a \ div \ d$$

$$r = a \ mod \ a$$

Definition 4.1.2. *Let $a, b, m \in \mathbb{Z}$ with $m \geq 2$. We say a is congruent to b modulo m if $m \mid (a - b)$. We write $a \equiv b \ (mod \ m)$*

Theorem 4.1.3. *Let $a, b, c, d, m \in \mathbb{Z}$ with $m \geq 2$. If $a \equiv b \ (mod \ m)$ and $c \equiv d \ (mod \ m)$, then*

1. *$a + c \equiv b + d \ (mod \ m)$*
2. *$ac \equiv bd \ (mod \ m)$*

Definition 5.1.1. *A positive integer p is prime if it admits exactly two divisors.*

Theorem 5.1.1 (Fundamental Theorem of Arithmetic)**.** *All integers greater than 1 can be written as a product of prime numbers. This representation is unique if we write the prime numbers in non-decreasing order.*

Theorem 5.1.2. *Let $n > 1$ be an integer. If n is not prime, then n has a prime divisor p such that $p \leq \sqrt{n}$.*

Corollary 6.0.1. *Let*

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$

$$a = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_k^{b_k}$$

Where p_i is prime, $a_i \geq 0$ and $b_i \geq 0$, $1 \leq i \leq k$. Then

$$gcd(a, b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \ldots \cdot p_k^{\min(a_k,b_k)}$$

$$lcm(a, b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ldots \cdot p_k^{\max(a_k,b_k)}$$

$$gcd(a, b) \cdot lcm(a, b) = ab$$

Lemma 6.0.1. *Let a, b, q, r be integers such that*

$$a = b \cdot q + r$$

Then

$$gcd(a, b) = gcd(b, r)$$

Definition 6.0.1 (Euclidean Algorithm)**.**

$$x = a$$

$$y = b$$

while $y \neq 0$

$$r = x \mod y$$

$$x = y$$

$$y = r$$

return x

Theorem 6.0.1 (Bézout)**.** *Let $a, b \in \mathbb{Z}$ be positive integers. There exists $s, t \in \mathbb{Z}$ such that*

$$s \cdot a + t \cdot b = gcd(a, b)$$

Lemma 6.0.1. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $gcd(a, b) = 1$ and $a \mid (bc)$, then $a \mid c$.*

Lemma 8.0.1. *Let $a, b, c \in \mathbb{Z}$, with $a \neq 0$. If $gcd(a, b) = 1$, and $a \mid (bc)$, then $a|c$.*

Theorem 8.0.1. *Let $a, b, c, m \in \mathbb{Z}$, with $m \geq 2$. Assume $ac \equiv bc \pmod{m}$ and $gcd(c, m) = 1$. Then $a \equiv b \pmod{m}$.*

Lemma 8.0.2. *Let p be a prime number and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid (a_1 \cdot a_2 \cdot \cdots \cdot a_n)$, then there exists $1 \leq i \leq n$ such that $p \mid a_i$.*

Theorem 8.0.2. *Let $m \in \mathbb{Z}$ with $m \geq 2$ and let $a \in \mathbb{Z}_m$. The multiplicative inverse of $a \pmod{n}$ exists if and only if $gcd(a, m) = 1$. When it exists, the inverse of $a \pmod{n}$ is unique.*

Lecture 1

Logic and Proof Techniques

TBC.

Lecture 2

Proof Examples

TBC.

Lecture 3

Proof by Induction and More Examples

Lecture 4

Intro to Number Theory

4.1 Divisibility

Definition 4.1.1. *Let a and b be two integers such that $a \neq 0$. We say that a divides b if there exists c such that $b = ac$. If a divides be we say a is a factor or divisor of b. We also can say b is a multiple of a.*

Theorem 4.1.1. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$.*

1. *If $a \mid b$ and $a \mid c$, then $a \mid (b + c)$*
2. *If $a \mid b$, then $a \mid bc$ for every integer*
3. *If $a \mid b$ and $b \mid c$, then $a \mid c$*

Proof.

1. We have to prove if $a \mid b$ and $a \mid c$, then $a \mid (b + c)$ Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. Assume that $a \mid b$ and $a \mid c$, then for some $k, l \in \mathbb{Z}$

$$b = k \cdot a$$

$$c = l \cdot a$$

Thus, we have

$$b + c = k \cdot a + l \cdot a = a(k + l)$$

So $a \mid (b + c)$

2. We have to prove if $a \mid b$, $a \mid bc$ for every c. Let $a, b \in \mathbb{Z}$ with $a \neq 0$. Assume that $a \mid b$. Then for some $k \in \mathbb{Z}$,

$$b = k \cdot a$$

Let $c \in \mathbb{Z}$, so

$$bc = k \cdot a \cdot c = a \cdot (kc)$$

Therefore, $a \mid bc$

3. We have to prove if $a \mid b$ and $b \mid c$, then $a \mid c$. Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. Assume $a \mid b$ and $b \mid c$. Then we have for some $k, l \in \mathbb{Z}$

$$b = k \cdot a$$

$$c = l \cdot b$$

So,

$$c = l \cdot b = l \cdot (k \cdot a) = (lk)a$$

Therefore $a \mid c$

□

Corollary 4.1.1. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $a \mid b$ and $a \mid c$, $a \mid (mb + nc)$ for all integers m and n*

Proof. Let $a, bc \in \mathbb{Z}$ with $a \neq 0$. Assume $a \mid b$ $a \mid c$. By the previous theorem (part 2), we have $a \mid mb$ and $a \mid nc$. Therefore, by the previous theorem (part 1), $a \mid (mb + nc)$ □

Theorem 4.1.2 (The Division Algorithm)**.** *Let $a, d \in \mathbb{Z}$ with $d > 0$. There exists a unique q and r such that*

$$0 \leq r \leq d$$

and

$$a = dq + r$$

We write

$$q = a \ div \ d$$

$$r = a \ mod \ a$$

Definition 4.1.2. *Let $a, b, m \in \mathbb{Z}$ with $m \geq 2$. We say a is congruent to b modulo m if $m \mid (a - b)$. We write $a \equiv b \ (mod \ m)$*

Example: Prove or disprove. We have $a \equiv b \ (mod \ m)$ if and only if $b \equiv a \ (mod \ m)$

$$\begin{aligned}
& a \equiv b \ (mod \ m) \\
\iff & m \mid (a - b) && \text{(by definition)} \\
\iff & a - b = km && (k \in \mathbb{Z}) \\
\iff & b - a = -km \\
\iff & m \mid (b - a) \\
\iff & b \equiv a \ (mod \ b) && \text{(by definition)}
\end{aligned}$$

Theorem 4.1.3. *Let $a, b, c, d, m \in \mathbb{Z}$ with $m \geq 2$. If $a \equiv b \ (mod \ m)$ and $c \equiv d \ (mod \ m)$, then*

1. $a + c \equiv b + d \ (mod \ m)$

2. $ac \equiv bd \ (mod\ m)$

Proof. 1. We have to prove $a + c \equiv b + d \ (mod\ m)$. Since $a \equiv b$ and $c \equiv d$, we have

$$m \mid (a - b)$$

$$m \mid (c - c)$$

By theorem 4.1.1 (part 1),we have

$$m \mid ((a - b) + (c - d)$$

$$m \mid ((a + c) - (b + d))$$

Therefore,

$$a + c \equiv b + d \ (mod\ m)$$

2. We have to prove $ac \equiv cd \ (mod\ m)$

Since $a \equiv b$ and $c \equiv d$, we have $m \mid (a - b)$ and $m \mid (c - d)$. By Corollary 4.1.1, we have

$$m \mid (c(a - b) + b(c - d)$$

$$m \mid (ac - bc + bc - bd)$$

$$m \mid (ac - bd)$$

Therefore $ac \equiv bd$.

□

4.2 Arithmetic Modulo m

Let $m \geq 2$ be an integer and

$$\mathbb{Z}_m = \{0, 1, 2, \ldots, m - 1\}$$

We define

$$a +_m b = (a + b) \ (mod\ m)$$

$$a \cdot_m b = (a \cdot b) \ (mod\ m)$$

in $\mathbb{Z}_m$, this is arithmetic modulo m. TBC

Lecture 5

Prime Numbers and GCD

5.1 Prime Numbers

Definition 5.1.1. *A positive integer p is prime if it admits exactly two divisors.*

Theorem 5.1.1 (Fundamental Theorem of Arithmetic)**.** *All integers greater than 1 can be written as a product of prime numbers. This representation is unique if we write the prime numbers in non-decreasing order.*

Proof. **(Existence)** By induction,

- **Base Case:** Take $n = 2$. We have $2 = 2$, the product of 1 prime number.
- **Induction Hypothesis:** Let $k \geq 2$ be an integer. Suppose that all numbers $2, 3, 4, \ldots, k-1, k$ can be written as a product of primes.
- **Induction Step:** Consider $k + 1$. If $k + 1$ is prime, then we're done. If not, then $K + 1 = d \cdot e$ for integers $1 < d < k + 1$ and $1 < e < k + 1$ By the induction hypothesis, d and e can be written as products of prime. So $k + 1 = d \cdot e$ can be written as a product of primes.

(Uniqueness) to be seen later. $\square$

Theorem 5.1.2. *Let $n > 1$ be an integer. If n is not prime, then n has a prime divisor p such that $p \leq \sqrt{n}$.*

Proof. Let $n > 1$, if n is not prime, then $n = a \cdot b$ for two integers $1 < a < n$ and $1 < b < n$. We will show that $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$ by contradiction. Assume $a > \sqrt{n}$ and $b > \sqrt{n}$. Then $n = a \cdot b > \sqrt{n} \cdot \sqrt{n} = n$. This is a contradiction so $a \leq \sqrt{n}$.

Assume without loss of generality that $a \leq \sqrt{n}$. If a is prime, we're done. If not, then by the fundamental theorem of arithmetic, a is divisible by a prime number p $\square$

Theorem 5.1.3. *There exists an infinite number of prime numbers.*

Proof. By contradiction, suppose there exists a finite number of prime numbers, say k prime numbers, and we order them

$$p_1 < p_2 < p_3 < \cdots < p_k$$

Consider the number

$$Q = p_1 \cdot p_2 \cdot \ldots \cdot p_k + 1 \in \mathbb{Z}$$

Since $Q > p_k$, then Q is not prime by our assumption. By Theorem 5.1.2, Q is divisible by a prime number. So $p_i \mid Q$ for some $1 \leq i \leq k$. We also have that

$$p_i \mid (p_1 \cdot p_2 \cdot \ldots \cdot p_i \cdot \ldots \cdot p_k)$$

By Corollary 4.1.1, we get

$$p_i \mid (Q - p_1 \cdot p_2 \cdot \ldots \cdot p_k)$$

$p_i \mid 1$ Therefore $p_i = 1$, this is a contradiction since we assumed p_k is the largest prime but $Q > p_k$ is prime. $\square$

Lecture 6

Euclidean Algoirthm and Bézout's Theorem

Corollary 6.0.1. *Let*

$$a = p_1^{a_1} \cdot p_2^{a_2} \cdot \ldots \cdot p_k^{a_k}$$
$$a = p_1^{b_1} \cdot p_2^{b_2} \cdot \ldots \cdot p_k^{b_k}$$

Where p_i is prime, $a_i \geq 0$ and $b_i \geq 0$, $1 \leq i \leq k$. Then

$$gcd(a,b) = p_1^{\min(a_1,b_1)} \cdot p_2^{\min(a_2,b_2)} \cdot \ldots \cdot p_k^{\min(a_k,b_k)}$$
$$lcm(a,b) = p_1^{\max(a_1,b_1)} \cdot p_2^{\max(a_2,b_2)} \cdot \ldots \cdot p_k^{\max(a_k,b_k)}$$
$$gcd(a,b) \cdot lcm(a,b) = ab$$

Example:

$$24 = 2^3 \cdot 3$$
$$36 = 2^2 \cdot 3^2$$
$$gcd(24,36) = 2^2 \cdot 3^1 = 12$$
$$lcm(24,36) = 2^3 \cdot 3^2 = 72$$
$$12 \cdot 72 = 864 = 24 \cdot 36$$

Lemma 6.0.1. *Let a, b, q, r be integers such that*

$$a = b \cdot q + r$$

Then

$$gcd(a,b) = gcd(b,r)$$

Proof. Let a, b, q, r be integers such that

$$a = bq + r$$

Let $d \in \mathbb{Z}$. We will prove that

$$d \mid a \wedge d \mid b \iff d \mid b \wedge d \mid r$$

($\Longrightarrow$) Let $d \in \mathbb{Z}$. Assume $d \mid a$ and $d \mid b$. Then $d \mid (1 \cdot a + (-q) \cdot b)$, by Corollary 4.1.1. Then $a = bq + r \implies r = a - bq$, so $d \mid (1 \cdot a + (-q) \cdot b) \implies d \mid r$.

($\Longleftarrow$) Let $d \in \mathbb{Z}$. Assume $d \mid b$ and $d \mid r$. Then $d \mid (q \cdot b + 1 \cdot r)$ by Corollary 4.1.1. Then $d \mid a$, therefore $d \mid a$ and $d \mid b$ ☐

Example: $gcd(414, 662)$, $662 = 1 \cdot 414 + 248$

$$\begin{aligned} 662 &= 1 \cdot 414 + 248 \\ 414 &= 1 \cdot 248 + 166 \\ 248 &= 1 \cdot 166 + 82 \\ 166 &= 2 \cdot 82 + 2 \\ 82 &= 41 \cdot 2 + 0 \end{aligned}$$

The last none-zero remainder of this sequence is the gcd of 414 and 662 by the previous lemma. (can someone find which lemma this is!)

Definition 6.0.1 (Euclidean Algorithm)**.**

$$x = a$$

$$y = b$$

while $y \neq 0$

$$r = x \mod y$$

$$x = y$$

$$y = r$$

return x

This algorithm returns the gcd of a and b.

Example:$gcd(465, 144)$

$$\begin{aligned} 465 &= 3 \cdot 144 + 33 \\ 144 &= 4 \cdot 33 + 12 \\ 33 &= 2 \cdot 12 + 9 \\ 12 &= 1 \cdot 9 + 3 \\ 9 &= 3 \cdot 3 + 0 \end{aligned}$$

Therefore $gcd(465, 144) = 3$.

Note: When you show the trace of Euclid's algorithm, you must include the last line with a remainder of 0.

Theorem 6.0.1 (Bézout)**.** *Let $a, b \in \mathbb{Z}$ be positive integers. There exists $s, t \in \mathbb{Z}$ such that*

$$s \cdot a + t \cdot b = gcd(a, b)$$

Proof. Let $a, b \in \mathbb{N} \setminus \{0\}$. Run Euclidian algorithm, and assume without loss of generality $b \leq a$.

$$\begin{aligned}
a &= q \cdot b + r \\
r_0 &= q_1 \cdot r_1 + r_2 \\
r_1 &= q_2 \cdot r^2 + r_3 \\
r_2 &= q_3 \cdot r_3 + r_4 \\
&\vdots \\
r_{n-3} &= q_{n-2} \cdot r_{n-2} + r_{n-1} \\
r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n \\
r_{n-1} &= q_n \cdot r_n + 0
\end{aligned}$$

Then, we have

$$\begin{aligned}
gcd(a, b) &= r_n \\
&= r_{n-2} - q_{n-1} \cdot r_{n-1} \\
&= r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2}r_{n-2}) \\
&= r_{n-2} - q_{n-1}(r_{n-3} - q_{n-2}r_{n-2}) \\
&= -q_{n-1} \cdot +(1 + q_{n-2}q_{n-1}) \cdot r_{n-2} \\
&\vdots \\
&= s \cdot r_0 + t \cdot r_1 \\
&= s \cdot a + t \cdot tb
\end{aligned}$$

So we read the trace of Euclid's algorithm backward while keeping $gcd(a, b)$ on the same side of the equality. ☐

TBC.

Lemma 6.0.2. *Let $a, b, c \in \mathbb{Z}$ with $a \neq 0$. If $gcd(a, b) = 1$ and $a \mid (bc)$, then $a \mid c$.*

Proof. Assume $gcd(a, b) = 1$ and $a \mid (bc)$. By Bézout, there exist $s, t \in \mathbb{Z}$ such that

$$s \cdot a + t \cdot b = gcd(a, b) = 1$$

$$s \cdot a \cdot c + t \cdot b \cdot c = c \tag{*}$$

Since $a \mid a$ and $a \mid (bc)$, we have

$$a \mid (s \cdot c \cdot a + t \cdot b \cdot c$$

By Corollary 4.1.1. Then from (*), this means

$$a \mid c$$

$\square$

Lecture 7

Applications of Bézout's Theorem

TBC.

Lecture 8

GCD and Modulo n, Multiplicative Inverses in Modulo n

Lemma 8.0.1. *Let $a, b, c \in \mathbb{Z}$, with $a \neq 0$. If $gcd(a, b) = 1$, and $a \mid (bc)$, then $a|c$.*

Proof. Seen last week. □

Theorem 8.0.1. *Let $a, b, c, m \in \mathbb{Z}$, with $m \geq 2$. Assume $ac \equiv bc \ (mod\ m)$ and $gcd(c, m) = 1$. Then $a \equiv b \ (mod\ m)$.*

Proof. Let $a, b, c, m \in \mathbb{Z}$ with $m \geq 2$. Assume $ac \equiv bc \ (mod\ m)$ and $gcd(c, m) = 1$.

$$\begin{aligned} m &\mid (ac - bc) && \text{(def of mod)} \\ m &\mid (c(a - b)) && \\ m &\mid (a - b) && \text{(by previous lemma)} \\ a &\equiv b \ (mod\ m) && \text{(def of mod)} \end{aligned}$$

□

Lemma 8.0.2. *Let p be a prime number and $a_1, a_2, \ldots, a_n \in \mathbb{Z}$. If $p \mid (a_1 \cdot a_2 \cdot \cdots \cdot a_n)$, then there exists $1 \leq i \leq n$ such that $p \mid a_i$.*

Proof. By induction on n.

- **Base Case:** $n = 1$. Let p be a prime number, if $p \mid a_1$, then $p \mid a_1$
- **Induction Hypothesis:** Let $k \geq 1$ be an integer. Suppose that for all integers $a_1, a_2, \ldots, a_k$

$$p \mid (a_1 \cdot a_2 \cdot \ldots \cdot a_k) \implies \exists 1 \leq i \leq k \ s.t \ p \mid a_i$$

If $p \mid a_{k+1}$, then we're done. If not, then

$$gcd(p, a_{k+1}) = 1$$

So $p \mid (a_1 \cdot a_2 \cdot \ldots \cdot a_k)$ by the previous lemma. By the induction hypthesis, ther exists $1 \leq i \leq k$ such that $p \mid a_i$.

Induction Step: Suppose

$$p \mid (a_1 \cdot a_2 \cdot \ldots \cdot a_k \cdot a_{k+1})$$

$\square$

Theorem 8.0.2. *Let $m \in \mathbb{Z}$ with $m \geq 2$ and let $a \in \mathbb{Z}_m$. The multiplicative inverse of a $(mod\ n)$ exists if and only if $gcd(a, m) = 1$. When it exists, the inverse of a $(mod\ n)$ is unique.*

Proof. Let $m \in \mathbb{Z}$ with $m \geq 2$ and $a \in \mathbb{Z}_m$

($\Longrightarrow$): Assume the multiplicative inverse of a $(mod\ n)$ exists. Let $\bar{a}$ be this inverse. By definition,

$$\begin{aligned} a \cdot \bar{a} &\equiv 1\ (mod\ m) \\ m &\mid (a \cdot \bar{a} - 1) && \text{(def. of modulo)} \end{aligned}$$

Then, $a \cdot \bar{a} - 1 = k \cdot m$ for some $m \in \mathbb{Z}$. Let $d = gcd(a, m)$ Then $d|a$ and $d|m$. By a result seen in class,

$$\begin{aligned} &d \mid (\bar{a} \cdot a + (-k)m) \\ &d \mid 1 \end{aligned}$$

So, $d = 1$

($\Longleftarrow$): Assume $gcd(a, m) = 1$. By Bézout, there exists $s, t \in \mathbb{Z}$ such that

$$s \cdot a + t \cdot m = gcd(a, m) = 1$$

$$\begin{aligned} s \cdot a + t \cdot m &\equiv 1\ (mod\ m) \\ s \cdot a + t \cdot 0 &\equiv 1\ (mod\ m) \\ s \cdot a &\equiv 1\ (mod\ m) \end{aligned}$$

So, we can take $\bar{a} \equiv s$ $(mod\ m)$

(Uniqueness): Consider two arbitrary multiplicative inverses of a $(mod\ m)$. Denote them by, $s, s' \in \mathbb{Z}_m$. So by definition

$$sa \equiv 1\ (mod\ m) \text{ and } s'a \equiv 1\ (mod\ m)$$

Then $gcd(a, m) = 1$ by the previous proof, also we have

$$\begin{aligned}
sa &\equiv s'a \ (mod\ m) && \\
m &\mid (sa - s'a) && \text{(def. of modulo)} \\
m &\mid (a(s - s')) && \\
m &\mid (s - s') && \text{(since } gcd(a, m) = 1\text{)} \\
s &\equiv s' \ (mod\ m) && \text{(def. of modulo)}
\end{aligned}$$

Therefore, s and s' are the same in $\mathbb{Z}_m$. $\square$

Example: Find the multiplicative inverse of 101 (mod 4620).

Euclid:

$$\begin{aligned}
4620 &= 45 \cdot 101 + 75 \\
101 &= 1 \cdot 75 + 26 \\
75 &= 2 \cdot 26 + 23 \\
26 &= 1 \cdot 23 + 3 \\
23 &= 7 \cdot 3 + 2 \\
3 &= 1 \cdot 2 + 1 \\
2 &= 2 \cdot 1 + 0
\end{aligned}$$

Bézout:

$$\begin{aligned}
1 &= 3 - 1 \cdot 2 \\
1 &= 3 - 1 \cdot (23 - 7 \cdot 3) \\
1 &= 3 - 1 \cdot 23 + 7 \cdot 3 \\
1 &= 8 \cdot 3 - 1 \cdot 23 \\
1 &= -1 \cdot 23 + 8 \cdot 3 \\
1 &= -1 \cdot 23 + 8 \cdot (26 - 1 \cdot 23) \\
1 &= -1 \cdot 23 + 8 \cdot 26 - 8 \cdot 23 \\
1 &= -9 \cdot 23 + 8 \cdot 26 \\
1 &= 8 \cdot 26 - 9 \cdot 23 \\
1 &= 8 \cdot 26 - 9 \cdot (75 - 2 \cdot 26) \\
1 &= 8 \cdot 26 - 9 \cdot 75 + 18 \cdot 26 \\
1 &= -9 \cdot 75 + 26 \cdot 26 \\
1 &= -9 \cdot 75 + 26 \cdot (101 - 1 \cdot 75) \\
1 &= -9 \cdot 75 + 26 \cdot 101 - 26 \cdot 75 \\
1 &= 26 \cdot 101 - 35 \cdot 75 \\
1 &= 26 \cdot 101 - 35 \cdot (4620 - 45 \cdot 101) \\
1 &= 26 \cdot 101 - 35 \cdot 4620 + 1575 \cdot 21 \\
1 &= -35 \cdot 4620 + 1601 \cdot 101
\end{aligned}$$

So,

$$\begin{aligned} -35 \cdot 4620 + 1601 \cdot 101 &\equiv 1 \ (mod\ 4620) \\ -35 \cdot 0 + 1601 \cdot 101 &\equiv 1 \ (mod\ 4620) \\ 1601 \cdot 101 &\equiv 1 \ (mod\ 4620) \\ 101 &\equiv 1601 \ (mod\ 4620) \end{aligned}$$

Therefore, the inverse of 101 in $\mathbb{Z}_{4620}$ is 1601.

Example: Find the multiplicative inverses in $\mathbb{Z}_{10}$.

- $\bar{0}$ does not exist since $gcd(0, 10) = 10 \neq 1$
- $\bar{1} \equiv 1 \ (mod\ 10)$
- $\bar{2}$ does not exist since $gcd(2, 10) = 2 \neq 1$
- $\bar{3} \equiv 7 \ (mod\ 10)$
- $\bar{4}$ does not exist since $gcd(4, 10) = 2 \neq 1$
- $\bar{5}$ does not exist since $gcd(5, 10) = 5 \neq 1$
- $\bar{6}$ does not exist since $gcd(6, 10) = 2 \neq 1$
- $\bar{7} \equiv 3 \ (mod\ 10)$
- $\bar{8}$ does not exist since $gcd(8, 10) = 2 \neq 1$
- $\bar{9} \equiv 9 \ (mod\ 10)$

This concludes the material for midterm 1.

Lecture 9

Solving Congruences

Definition 9.0.1 (Linear Congruence)**.** $ax \equiv b$ *(mod m)*

Example:

$$3x \equiv 5 \ (mod\ 7)$$

$$x \equiv 0 \ (mod\ 7)$$

$$x - 0 = 7k$$

Question: What is the multiplicative inverse of 3 (mod 7) So we have $3x \equiv 5$ (mod 7).

$$15x \equiv 25 \ (mod\ 7)$$

$$x \equiv 4 \ (mod\ 7)$$

$$3 \cdot 4 = 12 \equiv 5 \ (mod\ 7)$$

9.1 Linear Congruence System

Find x such that

$$x \equiv a_1 \ (mod\ m_1)$$

$$x \equiv a_2 \ (mod\ m_n)$$

$$\vdots$$

$$x \equiv a_n \ (mod\ m_n)$$

Example:

$$x \equiv 2 \ (mod\ 3)$$

$$x \equiv 3 \ (mod\ 5)$$

$$x \equiv 5 \ (mod\ 7)$$

Try $x = 68$

$$68 \equiv 2 \ (mod\ 3)$$

$$68 \equiv 3 \ (mod\ 5)$$
$$68 \equiv 5 \ (mod\ 7)$$

So, $x = 68$ is a solution to the system.

9.1.1 Substitution Method

$$x \equiv 2 \ (mod\ 3)$$
$$x = 3 \cdot t + 2$$

For some $t \in \mathbb{Z}$

$$x \equiv \ (mod\ 5)$$
$$3t + 2 \equiv 3 \ (mod\ 5)$$
$$3t \equiv 1 \ (mod\ 5)$$

Multiply $3x$ by the multiplicative inverse of 3 in $\mathbb{Z}_5$.

$$2 \cdot 3t \equiv 2 \cdot 1 \ (mod\ 5)$$
$$t \equiv 2 \ (mod\ 5)$$
$$t = 5u + 2 \ (mod\ 5)$$

For an $u \in \mathbb{Z}$

$$\left.\begin{aligned} x &= 3t + 2 \\ t &= 5u + 2 \end{aligned}\right\}$$
$$\implies x = ?$$
$$x = 3(5u + 2) + 2 = 15u + 8$$

$$\begin{aligned} 15u + 8 &\equiv 5 \ (mod\ 7) \\ 15u &\equiv -3 \ (mod\ 7) \\ 15u &\equiv 4 \ (mod\ 7) \\ 15u - 14u &\equiv 4 \ (mod\ 7) \\ u &\equiv 4 \ (mod\ 7) \end{aligned}$$

So $u = 7v + 4$ for some $v \in \mathbb{Z}$. Thus,

$$\begin{aligned} x &= 15u + 8 \\ &= 15(7v + 4) + 8 \\ &= 105v + 68 \end{aligned}$$

So,

$$105v + 68 \equiv 2 \ (mod\ 3)$$
$$105v + 68 \equiv 3 \ (mod\ 5)$$
$$105v + 68 \equiv 5 \ (mod\ 7)$$

Example:

$$x \equiv 1 \ (mod\ 4)$$
$$x \equiv 3 \ (mod\ 5)$$

Then $x = 4t + 1$ for some $t \in \mathbb{Z}$. Then from the second equation, we get

$$4t + 1 \equiv 3 \ (mod\ 5)$$
$$4t + 1 - 1 \equiv 3 - 1 \ (mod\ 5)$$
$$4t \equiv 2 \ (mod\ 5)$$
$$4 \cdot 4t \equiv 4 \cdot 2 \ (mod\ 5)$$
$$16t \equiv 8 \ (mod\ 5)$$
$$16t \equiv 8 \ (mod\ 5)$$
$$16t - 15t \equiv 8 - 5 \ (mod\ 5)$$
$$t \equiv 3 \ (mod\ 5)$$

Thus, $t = 5u + 3$ for some $u \in \mathbb{Z}$. So $x = 20u + 13$ is a solution to the system.

$$20u + 13 \equiv 1 \ (mod\ 4)$$
$$20u + 13 \equiv 3 \ (mod\ 5)$$

Question: Are there systems that admit no solution? Consider

$$x \equiv 2 \ (mod\ 4)$$

$$x \equiv 3 \ (mod\ 6)$$

So $x = 4t + 2$ for some $t \in \mathbb{Z}$

$$4t + 2 \equiv 3 \ (mod\ 6)$$

$$4t \equiv 1 \ (mod\ 6)$$

But, 4 does not have a multiplicative inverse in $\mathbb{Z}_6$ since $gcd(4, 6) \neq 1$.

Theorem 9.1.1 (Chinese Remainder Theorem)**.** *Let $m_1, m_2, \ldots, m_r \in \mathbb{Z}$ be pairwise co-prime integers such that $m_i \geq 2$ for $1 \leq i \leq r$*

Definition 9.1.1 (Pairwise Co-prime)**.** $gcd(m_i, m_j) = 1$

Let $a_1, a_2, \ldots, a_r \in \mathbb{Z}$, then the system

$$\begin{aligned} x &\equiv a_1 \ (mod\ m_1) \\ x &\equiv a_2 \ (mod\ m_2) \\ &\vdots \\ x &\equiv a_r \ (mod\ m_r) \end{aligned}$$

admits a unique solution $(mod\ m_1 \cdot m_2 \cdots m_r)$.In other words, the solution exists and is unique in $\mathbb{Z}_{m_1 \cdot m_2 \cdots m_r}$

Consider the system

$$\begin{aligned} x &\equiv 2 \ (mod\ 3) \\ x &\equiv 3 \ (mod\ 5) \\ x &\equiv 5 \ (mod\ 7) \end{aligned}$$

So we have $\mathbb{Z}_{3 \cdot 5 \cdot 7} = \mathbb{Z}_{105}$, $68 \in \mathbb{Z}_{105}$ and $x = 105u + 68$.

Lecture 10

Fermat's Theorem

Theorem 10.0.1 (Fermat's Theorem)**.** *Let $p, a \in \mathbb{Z}$ such that p is prime, then*

1. $$a^p \equiv a \ (mod \ p)$$

2. *If $gcd(a,p) = 1$, then $a^{p-1} \equiv 1 \ (mod \ p)$*

Example:

$$1534^{2016} \pmod{2017}$$

2017 is prime and $1534 < 2017$, so $gcd(1534, 2017) = 1$ and $1534^{2016} \equiv 1 \pmod{2017}$

Proof. For (2), we need to usthe following property

$$1 \cdot a, 2 \cdot a, 3 \cdot a, \ldots, (p-1) \cdot a$$

are all different $\pmod{p}$.Consider $s, e \in \{1, 2, \ldots, p-1\}$ such that

$$ra \equiv sa \pmod{p}$$

Since $\gcd(a, p) = 1$, we can divide both sides by a to get

$$r \equiv s \pmod{p}$$

Then since $r, s < p$, then $r = s$‘’

$\square$

Lecture 12

Intro to Cryptography

Lecture 13

Asympotic Notation

13.1 Big-O Notation

The *O-notation* describes an asympotic upper bound.

Definition 13.1.1. *Let*

$$f : \mathbb{N} \to \mathbb{R}^+$$
$$g : \mathbb{N} \to \mathbb{R}^+$$

be two functions. We say that f is O(g) *if there exists a real number $c > 0$ and $k \in \mathbb{N}$ such that for all $n \geq k$,*

$$f(n) \leq c \cdot g(n)$$

Notation:

$$f(n) \leq c \cdot g(n)$$
$$f = O(g)$$
$$\exists c \exists k \forall n (n \geq k \implies f(n) \leq c \cdot g(n))$$

Domain: $k, n \in \mathbb{N}$, $c \in \mathbb{R}^+ \setminus \{0\}$

Example: $13x^3 + 12x^2 + 5 = O(x^3)$. We have

$$13x^3 + 12x^2 + 5 \leq 13x^3 + 12x^3 + 5x^2 = 30x^3$$

Take $c = 30$ and $k = 1$. So

$$13x^3 + 12x^2 + 5 \leq 30 \cdot x^3$$

for all $x \geq 1$. Therefore $13x^3 + 12x^2 + 5 = O(x^3)$.

Example: $x^2 = O\left(\frac{1}{2}x^2 - 10x\right)$. We have

$$x^2 \leq 2\left(\frac{1}{2}x^2 - 10x\right)$$

Now we want

$$x^2 \geq 40x$$

so that that $x^2 - 40x$ is positive. So

$$x > 40$$

Then,

$$\begin{aligned} x^2 &= 2x^2 - x^2 \\ &\leq 2x^2 - 40x \\ &= 4\left(\frac{1}{2}x^2 - 10x\right) \end{aligned}$$

So take $c = 4$ and $k = 40$. Then $x^2 = O\left(\frac{1}{2}x^2 - 10x\right)$ for all $x \geq 40$.

Proposition 13.1.1. *Let $a > 0$ and $b > 0$. be two rael numbers. We have*

$$log^a(x) = O(x^b)$$

Proof. Let $a > 0$ and $b > 0$ be two real numbers. We'll use that fact that $\forall x \geq 0$, we have $x \leq e^x$. From which, we have $log(x) \leq x$. Let x be an integer. We have, by the previous property,

$$\begin{aligned} \log(x^{\frac{b}{a}}) &\leq x^{\frac{b}{a}} \\ \frac{b}{a}\log(x) &\leq x^{\frac{b}{a}} \\ \left(\frac{b}{a}\right)^a \log^a(x) &\leq x^b \\ \log^a(x) &\leq \left(\frac{a}{b}\right)^a x^b \end{aligned}$$

So we take $c = \left(\frac{a}{b}\right)^a$ and $k = 1$. $\square$

13.2 Big-Omega Notation

The Ω-*notation* describes an asympotic lower bound.

Definition 13.2.1. *Let*

$$f : \mathbb{N} \to \mathbb{R}^+$$

$$g : \mathbb{N} \to \mathbb{R}^+$$

be two functions. We say that f is $\Omega(g)$ if there exists a real number $c > 0$ and $k \in \mathbb{N}$ such that for all $n \geq k$,

$$f(n) \geq c \cdot g(n)$$

Notation:

$$f(n) = \Omega(g(n))$$
$$f = \Omega(g)$$
$$\exists c \exists k \forall n (n \geq k \implies f(n) \geq c \cdot g(n))$$

Domain: $k, n \in \mathbb{N}$, $c \in \mathbb{R}^+ \setminus \{0\}$

Example: $13x^3 + 12x^2 + 5 = \Omega(x^3)$.

$$13x^3 + 12x^2 + 5 \geq 13x^3$$

Take $c = 13$ and $k = 0$. So $13x^3 + 12x^2 + 5 = \Omega(x^3)$.

Example: $x^2 = \Omega\left(\frac{1}{2}x^2 - 10x\right)$.

$$\begin{aligned} x^2 &\geq \frac{1}{2}x^2 \\ &\geq \frac{1}{2}x^2 - 10x \\ &= 1 \cdot \left(\frac{1}{2}x^2 - 10x\right) \end{aligned}$$

Take $c = 1$ and $k = 0$. So $x^2 = \Omega\left(\frac{1}{2}x^2 - 10x\right)$ $\forall x \geq k$.

Proposition 13.2.1. *Let $f(n)$ and $g(n)$ be two functions.*

$$f(n) = O(g(n)) \iff g(n) - \Omega(f(n))$$

Proof. ($\implies$) Let $f(n)$ and $g(n)$ be two functions. Assume $f(n) = O(g(n))$. Then there exists $c > 0$ and $k \in \mathbb{N}$ such that for all $n \geq k$, we have $f(n) \leq c \cdot g(n)$. So,

$$f(n) \leq c \cdot g(n)$$

given that $n \geq g(n)$, then

$$g(n) \geq \frac{1}{c} f(n)$$

($\impliedby$) The proof follows the same. □

13.3 Big-Theta Notation

The Θ-*notation* describes an asympotic upper and lower bound.

Definition 13.3.1. *Let*

$$f : \mathbb{N} \to \mathbb{R}^+$$
$$g : \mathbb{N} \to \mathbb{R}^+$$

be two functions. We say that f is $\Theta(g)$ if there exists a real number $c_1 > 0$, $c_2 > 0$ and $k \in \mathbb{N}$ such that for all $n \geq k$. In otherwords,

$$f(n) = O(g(n)) \text{ and } f(n) = \Omega(g(n))$$

Notation:

$$f(n) = \Theta(g(n))$$

$$f = \Theta(g)$$

Proposition 13.3.1. *Let $f(n)$ and $g(n)$ be two functions. $f(n) = \Theta(g(n))$ if and only if $f(n) = O(g(n))$ and $g(n) = \Omega(f(n))$.*

Proof.

$$f(n) = \Theta(g(n)) \iff f(n) = O(g(n)) \text{ and } f(n) = \Omega(g(n))$$

By the definition of theta, so

$$g(n) = \Omega(f(n)) \text{ and } g(n) = O(f(n))$$

From the previous proposition, then

$$g(n) = \Theta(f(n))$$

$\square$

Lecture 14

Recursivity

Lemma 14.0.1. *Let $F_n = F_{n-1} + F_{n-2}$ denote the nth term of the Fibonacci sequence with $F_0 = 0$ and $F_1 = 1$. And let $\alpha = \frac{\sqrt{5}+1}{2}$ (golden ratio). Then $\forall n \geq 3$,*

$$F_n > \alpha^{n-2}$$

Proof. By induction,

$$\textbf{\textit{Note:}}\ \alpha^2 = \left(\tfrac{\sqrt{5}+1}{2}\right)^2 = \tfrac{5+2\sqrt{5}+1}{4} = \tfrac{\sqrt{5}+3}{2} = \tfrac{\sqrt{5}+1}{2} + 1 = \alpha + 1$$

- **Base case:** $n = 3$. Then $F_3 = F_2 + F_1 = 1 + 1 = 2$. We have

$$\begin{aligned} 3 &> \sqrt{5} \\ 4 &> \sqrt{5} + 1 \\ 2 &> \frac{\sqrt{5}+1}{2} \\ F_3 &> \frac{\sqrt{5}+1}{2}^2 = \alpha^{3-2} \end{aligned}$$

  For $n = 4$, $F_4 = F_3 + F_2 = 2 + 1 = 3$. We have

$$\begin{aligned} 2 &> \alpha \\ 2 + 1 &> \alpha + 1 && \text{(From Note)} \\ 3 &> \alpha^2 \\ F_4 &> \alpha^2 = \alpha^{4-2} \end{aligned}$$

- **Induction Hypothesis:** Let $k \geq 4$ be an integer. Assume $F_i > \alpha^{i-2}$ for all $3 \leq i \leq k$.

- **Induction Step:**

$$\begin{aligned}
F_{k+1} &= F_k + F_{k-1} && \text{(By def.)} \\
&> \alpha^{k-2} + \alpha^{(k-1)-2} && \text{(By IH)} \\
&= \alpha^{k-2} + \alpha^{k-3} \\
&= \alpha^{k-3}(\alpha^1 + 1) \\
&= \alpha^{k-3}(\alpha^2) && \text{(From Note)} \\
&= \alpha^{k-1} \\
&= \alpha^{(k+1)-2}
\end{aligned}$$

□

Theorem 14.0.1 (Lamé). *Let $a, b \in \mathbb{Z}$ such that $a \geq b > 0$. Euclid's algorithm takes $O(\log(b))$ steps.*

Proof. Let $a, b \in \mathbb{Z}$ such that $a \geq b > 0$. Euclid's algorithm performs the following devisions:

$$\begin{aligned}
a &= q \cdot b + r & 0 \leq & r < b \\
r_0 &= q_1 \cdot r_1 + r_2 & 0 \leq & r_2 < r_1 \\
r_1 &= q_2 \cdot r_2 + r_3 & 0 \leq & r_3 < r_2 \\
&\vdots & &\vdots \\
r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n & 0 \leq & r_n < r_{n-1} \\
r_{n-1} &= q_n \cdot r_n + r_{n+1} & 0 \leq & r_{n+1} < r_n
\end{aligned}$$

We have

- $r_n = \gcd(a, b)$
- $q_i \geq 1 \; 1 \leq i \leq n-1$
- $q_n \geq 2$
- n is the number of divisons performed by Euclid's algorithm

Therefore, $r_n = \gcd(a, b) \geq 1 = F_2$

$$\begin{aligned}
r_{n-1} &= q_n \cdot r_n \geq 2 \cdot 1 = 2 = F_3 \\
r_{n-2} &= q_{n-1} \cdot r_{n-1} + r_n \geq 1 \cdot F_3 + F_2 = F_4 \\
r_{n-3} &= q_{n-2} \cdot r_{n-2} + r_{n-1} \geq 1 \cdot F_4 + F_3 = F_5 \\
&\vdots \\
r_2 &= q_3 \cdot r_3 + r_4 \geq 1 \cdot F_{n-1} + F_{n-2} = F_n \\
b = r_1 &= q_2 \cdot r_2 + r_3 \geq 1 \cdot F_n + F_{n-1} = F_{n+1}
\end{aligned}$$

Sp $b \geq F_{n+1} > \alpha^{(n+1)-2}$ by the previous lemma.

$$\begin{aligned}
b &> \alpha^{n-1} \\
\log(b) &> \log(\alpha^{n-1}) \\
\log(b) &> n - 1 \log(\alpha) \\
\log(b) &> (n-1) \log\left(\frac{\sqrt{5}+1}{2}\right) \\
\log(b) &> (n-1)\frac{2}{5} \\
\frac{5\log(b)}{2} + 1 &> n
\end{aligned}$$

Therefore the number of steps $n < 1 + \frac{5}{2}\log(b) < \log(b) + \frac{5}{2}\log(b) = \frac{7}{2}\log(b)$ $\forall b > 3$. So $n = O(\log(b))$. $\square$

The Fibonnaci recurrence is an example of a linear homogenous recurrence of order k.

$$a_n = c_1 \cdot a_n n - 1 + c_2 \cdot a_{n-2} + \ldots + c_k \cdot a_{n-k}$$

In general, a solution of the form

$$a_n = r^n$$

will work for some $r \in \mathbb{R}$

$$r^n = c_1 \cdot r^{n-1} + c_2 \cdot r^{n-2} + \ldots + c_k \cdot r^{n-k}$$

Divide by r^{n-k},

$$r^k = c_1 \cdot r^{k-1} + c_2 \cdot r^{n-2} + \ldots + c_k$$

$$r^k - c_1 \cdot r^{k-1} + c_2 \cdot r^{n-2} + \ldots + c_k = 0$$

This is known as the characteristic equation. The solutions to this equation are called the *characteristic roots*.

Example: $a_n = 1 \cdot a_{n-1} + 2 \cdot a_{n-2}$. Characteristic Equation:

$$r^2 - 1 \cdot r - 2 = 0 \implies (r+1)(r-1) = 0$$

So we have the roots $r_1 = -1$ and $r_2 = 1$. So,

$$(-1)^n = 1 \cdot (-1)^{n-1} + 2(-1)^{n-2}$$

$$2^n = 1 \cdot 2^{n-1} + 2 \cdot 2^{n-2}$$

Moreover, for all $\alpha, \beta \in \mathbb{R}$, we have

$$(\alpha(-1)^n + \beta \cdot 2^n) = 1 \cdot \left(\alpha \cdot (-1)^{n-1} + \beta \cdot 2^{n-1}\right) + 2 \cdot \left(\alpha(-1)^{n-2} + \beta \cdot 2^{n-2}\right)$$

Any linear combintion works.

Example: $F_0 = 0$, $F_1 = 1$, $F_n = F_{n-1} + F_{n-2}$. Charactereristic Equation:

$$r^2 - r - 1 = 0$$

$$r = \frac{1 \pm \sqrt{5}}{2}$$

So,

$$F_n = \alpha \left(\frac{1+\sqrt{5}}{2}\right)^n + \beta \left(\frac{1-\sqrt{5}}{2}\right)^n$$

is a solution for any $\alpha, \beta \in \mathbb{R}$. Now we can find α, β to match the base cases.

$$F_0 = \alpha \left(\frac{1+\sqrt{5}}{2}\right)^0 + \beta \left(\frac{1-\sqrt{5}}{2}\right)^0 = 0 \implies \alpha + \beta = 0$$

$$F_1 = \alpha \left(\frac{1+\sqrt{5}}{2}\right)^1 + \beta \left(\frac{1-\sqrt{5}}{2}\right)^1 = 1$$

So, $\beta = -\alpha$. Then,

$$\alpha \left(\frac{1+\sqrt{5}}{2}\right) - \alpha \left(\frac{1-\sqrt{5}}{2}\right) = 0$$

$$\alpha \left(\left(\frac{1+\sqrt{5}}{2}\right) - \left(\frac{1-\sqrt{5}}{2}\right)\right) = 1$$

$$\alpha\sqrt{5} = 1$$

$$\alpha = \frac{1}{\sqrt{5}}$$

Sos $\beta = -\alpha = -\frac{1}{\sqrt{5}}$. Therefore,

$$F_n = \frac{1}{\sqrt{5}} \left(\frac{1+\sqrt{5}}{2}\right)^n - \frac{1}{\sqrt{5}} \left(\frac{1-\sqrt{5}}{2}\right)^n$$

Lecture 15

Recursivity Continued

Let us consider the special case where some characteristic roots are repeated. We only focus on the case of order $k = 2$.

$$a_n = c_1 \cdot a_{n-1} + c_2 \cdot a_{n-2}$$

Charactereristic Equation:

$$1 \cdot r^2 - c_1 \cdot r - c_2 = 0$$

Since the roots are repeated, we have

$$(r-t)^2 = 0 \to r^2 - 2rt + t^2 = 0$$

For some $t \in \mathbb{R}$. So $c_1 = 2t$, $c_2 = -t^2 = \frac{-c_1^2}{4}$. And the repeated root is $t = \frac{c}{2}$.

For any $\alpha, \beta \in \mathbb{R}$, the general solution is

$$a_n = \alpha \left(\frac{c_1}{2}\right)^n + \left(\beta \cdot n \cdot \frac{c_1}{2}\right)^n$$

Indeed we have

$$\left(\alpha \left(\frac{c_1}{2}\right)^n + \beta \cdot n \cdot \left(\frac{c_1}{2}\right)^n\right) = c_1 \cdot \left(\alpha \left(\frac{c_1}{2}\right)^{n-1} + \left(\beta \cdot (n-1) \cdot \frac{c_1}{2}\right)^{n-1}\right) + c_2 \cdot \left(\alpha \left(\frac{c_1}{2}\right)^{n-1} + \left(\beta \cdot (n-1) \cdot \frac{c_1}{2}\right)^{n-2}\right.$$

Example: $a_0 = 1$, $a_1 = 6$, $a_n = 6a_{n-1} - 9a_{n-2}$ for $n \geq 2$. Charactereristic Equation

$$r^2 - 6r + 9 = 0 \to (r-3)^2 = 0$$

So

$$a_n = \alpha \cdot 3^n + \beta \cdot n \cdot 3^n$$

For some $\alpha, \beta \in \mathbb{R}$. We have

$$a_n = \alpha \cdot 3^0 + \beta \cdot 0 \cdot 3^0 = 1$$

$$a_n = \alpha \cdot 3^1 + \beta \cdot 1 \cdot 3^1 = 6$$

$$\alpha = 1$$

$$3\alpha + 3\beta = 6$$

So $\alpha = 1$, and $\beta = 1$, so

$$a_n = 1 \cdot 3^n + 1 \cdot n \cdot 3^n = (n+1) \cdot 3^n$$

Example: $a_0 = 1$, $a_1 = 1$, $a_n = 4a_{n-1} - 4 \cdot a_{n-2}$ for $n \geq 2$. Charactereristic Equation:

$$r^2 - 4r + 4 = 0$$

$$(r-2)^2 = 0$$

So

$$a_n = \alpha \cdot 2^n \beta \cdot n \cdot 2^n$$

for some $\alpha, \beta \in \mathbb{R}$. We have

$$a_0 = \alpha \cdot 2^0 + \beta \cdot 0 \cdot 2^0 = 0$$

$$a_1 = \alpha \cdot 2^1 + \beta \cdot 1 \cdot 2^1 = 1$$

Then $\alpha = 0$, $2\alpha + 2\beta = 1$. So $alpha = 0$, $\beta = \frac{1}{2}$. So

$$a_n = 0c\dot{2}^n + \frac{1}{2} \cdot n \cdot 2^n = n \cdot 2^{n-1}$$

Example: Let S be the set defined recursively by

- $3 \in S$
- If $x, y \in S$, then $x + y \in S$

So we can take $x = 3$, $y = 3$, then $3 + 3 \in S$ and so on.

Conjecture: Let $E = \{3, 6, 9, \ldots\}$ and $S = E$.

Proof. We will prove $S \subseteq E$ and $E \subseteq S$.

$S \subseteq E$ By induction,

- **Base Case:** $3 \in S$ and $3 \in E$
- **Inductive Hypothesis:** Let $x, y \in S$. Assume $x \in E$, and $y \in E$.
- **Induction Step:** We have $x + y \in S$ by definition. We want to show $x + y \in E$. Since $x, y \in E$ (from the induction hypthesis), then $x = 3k$, $y = 3l$ For some $k, l \in \mathbb{Z}$ with $k, l \geq 1$. So $x + y = 3k + 3l = 3(k + l) \in E$.

$E \subseteq S$ By induction,

- **Base Case:** $3 \in E$ and $3 \in S$

- **Inductive Hypothesis:** Let $m \in E$. Assume that $m \in S$
- **Induction Step:** We want to prove that $m + 3 \in S$. By definition, $3 \in S$. By the induction hypthesis, $m \in S$. From the definition of S, $m + 3 \in S$.

$\square$

Example: Find a rexursvie definition for the set

$$E = \{0, \frac{1}{2}, \frac{2}{3}, \frac{3}{4}, \frac{4}{5}, \dots\}$$

How do we get $\frac{k+1}{k+2}$ from $\frac{k}{k+1}$?

If $x = \frac{k}{k+1}$, then we have

$$kx + x = k \implies x = k(1-x)$$

$$\frac{x}{1-x} = k$$

$$\frac{k+1}{k+2} = \frac{\frac{x}{1-x} + 1}{\frac{x}{1-x} + 2} = \frac{\frac{x}{1-x} + \frac{1-x}{1-x}}{\frac{x}{1-x} + \frac{2-2x}{1-x}}$$

$$= \frac{\frac{1}{1-x}}{\frac{2-x}{1-x}}$$

$$= \frac{1}{2-x}$$

Conjecture:

- $0 \in S$
- If $x \in S$, then $x + \frac{1}{2-x} \in S$

Proof. We want to prove $E = S$, so we will prove $E \subseteq S$ and $S \subseteq E$.

$E \subseteq S$ By induction,

- **Base Case:** $0 \in E$, and $0 \in S$.
- **Inductive Hypothesis:** Let $x \in E$. Assume $x \in S$.
- **Induction Step:** Since $x \in E$, $x = \frac{k}{k+1}$, for an integer $k \geq 0$. We want to show

  $$\frac{k+1}{k+2} \in S$$

  We know $x \in S$ by the induction hypothesis. By the definition of S,

  $$\frac{1}{2-x} \in S$$

  So,

  $$\frac{1}{2-x} = \frac{1}{2 - \frac{k}{k+1}} = \frac{k+1}{2(k+1) - k} = \frac{k+1}{k+2} \in S$$

$S \subseteq E$ By induction,

- **Base Case:** $0 \in S$, and $0 \in E$.
- **Inductive Hypothesis:** Let $x \in S$. That is, assume

  $$x = \frac{k}{k+1}$$

  for some integer $k \geq 0$
- **Induction Step:** We want to prove that

  $$\frac{1}{2-x} \in E$$

  We have

  $$\begin{aligned} \frac{1}{2-x} &= \frac{1}{2-\frac{k}{k+1}} && \text{(By the IH.)} \\ &= \frac{k+1}{2(k+1)-k} \\ &= \frac{k+1}{(k+1)+1} \in E \end{aligned}$$

□

15.1 K-ary Trees

Definition 15.1.1. *A complete k-ary tree with height h and root r is defined recursively by*

- *An isolated node r is a complete k-ary tree with height 0 and root r*
- *Let $h \geq 0$. Let T_i be a complete k-ary tree with height h and root r_i with $1 \leq i \leq k$, and let r be an isolated node. The graph obtained by adding the edges $\{r, r_i\}$ is a complete tree with heigh $h+1$ and root r.*

Lecture 16

K-Ary Trees

The size of a K-ary tree T (number of nodes) denoted by $n(T)$ is

$$n(T) = \begin{cases} 1 & \text{if } T \text{ is a single node} \\ 1 + \sum_{i=1}^{k} n(T_i) & \text{if } T \text{ is a complete } k\text{-ary tree with height } h \text{ and root } r \end{cases}$$

T_i is a subtree of T, since the tree is complete, we have

$$\begin{aligned} 1 + \sum_{i=1}^{k} n(T_i) &= 1 + k \cdot n(T_1) \\ &= 1 + k \cdot n(T_1) \end{aligned}$$

If we write $n(T)$ in terms of the height of T, we get

$$n(h) = \begin{cases} 1 & \text{if } h = 0 \\ 1 + k \cdot n(h-1) & \text{otherwise} \end{cases}$$

So

$$\begin{aligned} n(0) &= 1 \\ n(1) &= 1 + k \cdot n(0) && = 1 + k \\ n(2) &= 1 + k \cdot n(1) && = 1 + k + k^2 \\ n(3) &= 1 + k \cdot n(2) && = 1 + k + k^2 + k^3 \\ &\vdots n(h) && = 1 + k + k^2 + k^3 + \ldots + k^h \end{aligned}$$

This can be proven by induction, then we get

$$k \cdot n(h) = k + k^2 + k^3 + \ldots + k^{h+1}$$
$$k \cdot n(h) - n(h) = k^{h+1} - 1$$
$$(k-1)n(h) = k^{h+1} - 1$$
$$n(h) = \frac{k^{h+1} - 1}{k - 1}$$

16.1 Recursive Algorithms

We usually refer to recursive algorithms when designing algorithm with the so-called Divide-and-Conquer approach. TO solve a problem of size n, the approach is to

- **Divide:** Dive the problem into smaller problems of size $< n$
- **Conquer:** Solve the smaller problems recursively
- **Combine/Merge:** Combine the solutions to each of the smaller problems to obtain a solution to the original problem

Example: Count the number of positive numbers in an array.

Algorithm 1 Count the number of positive numbers in an array

```
procedure NB(A[1, ... n])
    if thenn = 1
        if A[1] > 0 then return 1
        elsereturn 0
        end if
    else
        m ← ⌊n/2⌋
        a1 ← NB(A[1, ... m])
        a2 ← NB(A[m + 1, ... n])
        a ← a1 + a2
        return a
    end if
end procedure
```

- We split the problem into 2 smaller problems each of size $n/2$.
- We make 2 recursive calls to call the same function on the 2 smaller problems.
- Then we combine the outputs from the two recursive calls

Let $T(n)$ be the number of steps executed by $NB(A[1,\ldots,n])$.

$$T(1) = 3 \quad (n = 3)$$

$$T(n) = 2 \cdot T\left(\frac{n}{2}\right) + 4 \quad (n > 1)$$

We can prove that $T(n) = O(n)$ later in this chapter. Lets prove this algorithm is correct by induction.

- **Base Case:** $n = 1$. If A contains only one element, then NB returns 1 if $A[1] > 0$, and returns 0 otherwise. So it is correct for $n = 1$.

- **Induction Hypothesis:** Let $k \geq 1$ be an integer. Assume that NB returns the number of strictly positive numbers in $A[1,\ldots,l]$ for all arrays $A[1,\ldots,l]$ with $1 \leq l \leq k$.

- **Induction Step:** Consider an array $A[1,\ldots,(k+1)]$ of numbers. NB does

  $$m = \lfloor \frac{k+1}{2} \rfloor \leq k$$

  Then it does

  $$a_1 = NB(A[1,\ldots m])$$

  $$a_2 = NB(A[m+1,\ldots k+1])$$

  By the induction hypothesis, a_1 is the number of positive numbers in $A[1,\ldots m]$, and a_2 is the number of positive numbers in $A[m+1,\ldots k+1]$. So $a = a_1 + a_2$ is the number of positive numbers in $A[1,\ldots k+1]$.

Example: To Merge the sublists, we compare the left most numbers in both

Algorithm 2 Sort an array of n numbers.

```
procedure MergeSort(A[1, ..., n])
    if n = 1 then return A[1, ... n]
    else
        m ← ⌊n/2⌋
        L ← MergeSort(A[1, ... m])
        R ← MergeSort(A[m + 1, ... n])
        Merge L and R into one array B[1, ... n] return B
    end if
end procedure
```

arrays, take out the smallest one, and write it as the next number in B. We create 2 smaller problems of size $\frac{n}{2}$, and we make 2 recursive calls.

Lecture 17

Recursive Algorithms

Continuing the Merge Sort example, let $T(n)$ be the number of steps taken by MergeSort($A[1, \dots, n]$).

$$T(1) = 2$$
$$T(n) = 2 \cdot T\left(\frac{n}{2}\right) + n + 3 \quad (n \geq 2)$$

We can show that $T(n) = O(n \log n)$. (Later on)

Example: At the beginning, we call BIN($A[1, \dots, n]$), 1, n, x. We create 2

Algorithm 3 Binary Search

```
procedure BIN(A[1,...,n]), i, j, x
    if i = j then
        if A[i] = x then return i
        elsereturn nil
        end if
    else
        m ← ⌊(i+j−1)/2⌋
        if x ≤ A[m] then
            index ← BIN(A[1,...,n], i, m, x)
        else
            index ← BIN(A[1,...,n], m+1, j, x)
        end ifreturn index
    end if
end procedure
```

smaller problems of size $\frac{n}{2}$, and we make 1 recursive call with *no merge step.* Let $T(n)$ be the number of steps taken my the algorithm,

$$T(1) = 3$$
$$T(n) = T\left(\frac{n}{2}\right) + 4 \ (n \geq 2)$$

We can show that $T(n) = O(\log n)$. (Later on)

17.1 Solving Recurrences

How do we solve these recurrences?

$$T(n) = 2T\left(\frac{n}{2}\right) + 4$$
$$T(n) = 2T\left(\frac{n}{4}\right) + (n + 3)$$
$$T(n) = T\left(\frac{n}{4}\right) + 4$$

By unfolding,

Example:

$$T(n) = \begin{cases} 3 & n = 1 \\ 2T\left(\frac{n}{2}\right) + 4 & n \geq 2 \end{cases}$$

Assume $n = 2^k$ for some $k \in \mathbb{N}$.

$$
\begin{aligned}
T(n) &= 2T\left(\frac{n}{2}\right) + 4 \\
&= 2\left(2 \cdot T\left(\frac{n/2}{2}\right) + 4\right) + 4 \\
&= 2^2 T\left(\frac{n}{2^2}\right) + 2 \cdot 4 + 4 \\
&= 2^2\left(2 \cdot T\left(\frac{n/2^2}{2}\right) + 4\right) + 2 \cdot 4 + 4 \\
&= 2^3 T\left(\frac{n}{2^3}\right) + 2^2 \cdot 4 + 2^1 \cdot 4 + 2^0 \cdot 4 \\
&\vdots \\
&= 2^k T\left(\frac{n}{2^k}\right) + 2^{k-1} \cdot 4 + 2^{k-2} \cdot 4 + \ldots + 2^1 \cdot 4 + 2^0 \cdot 4 \\
&= 2^k T\left(\frac{n}{2^k}\right) + \sum_{i=0}^{k-1} 2^i \cdot 4 \\
&= n \cdot T(1) + \sum_{i=0}^{k-1} 2^i \cdot 4 && (n = 2k) \\
&= n \cdot 3 + (2^k - 1) \cdot 4 \\
&= n \cdot 3 + (n - 1) \cdot 4 \\
&= 7n - 4 \\
&= O(n)
\end{aligned}
$$

Example:

$$
T(n) = \begin{cases} 2 & n = 1 \\ 2T\left(\frac{n}{2}\right) + (n+3) & n \geq 2 \end{cases}
$$

By unfolding. Assume that $n = 2^k$.

$$
\begin{aligned}
T(n) &= 2T\left(\frac{n}{2}\right) + (n+3) \\
&= 2\left(2 \cdot T\left(\frac{n/2}{2}\right) + \left(\frac{n}{2} + 3\right)\right) + (n+3) \\
&= 2^2 + \frac{n}{2^2} + 2n + 2 \cdot 3 + 3 \\
&= 2^2 \cdot \left(2 \cdot T\left(\frac{n/2}{2}\right) + \left(\frac{n}{2^2} + 3\right)\right) + 2n + 2 \cdot 3 + 3 \\
&= 2^3 \cdot T\left(\frac{n}{2^3}\right) + 3n + 2^2 \cdot 3 + 2^1 \cdot 3 + 2^0 \cdot 3 \\
&\vdots \\
&= 2^k T\left(\frac{n}{2^k}\right) + kn + \sum_{i=0}^{k-1} 2^i \cdot 3 \\
&= n + T(1) + \log_2(n) \cdot n + \sum_{i=0}^{k-1} 2^i \cdot 3 && (n = 2^k) \\
&= 2 \cdot n + n \log_2(n) + (2^k - 1) \cdot 3 \\
&= n \log_2(n) + 5n - 3 \\
&= O(n \log n)
\end{aligned}
$$

Lecture 18

Graphs

Definition 18.0.1. *A* graph *G is made of a non-empty set V of* vertices *(nodes) together with a set E of* edges*. Each edge in E is an unordered pair $u, v \subseteq V$ with $u \neq v$. We write $G = (V, E)$. Graphs without loops and parallel edges are said to be* simple*.*

Important Note: All graphs this semester are simple.

We say that u is *adjacent* to v (u and v are neighbors) if $\{u, v\}$ is an edge. An edge e is said to be *incident* to u if one of the two endpoints of e is u. The *degree* of a vertex $u \in V$ is the number of edges incident u.

Theorem 18.0.1 (Handshaking Lemma)**.** *Let $G = (V, E)$ be a graph.*

$$\sum_{u \in V} \deg(u) = 2|E|$$

Proof. Look at an abritrary edge $u, v \in E$. Each edge is counted twice. $\square$

Theorem 18.0.2. *Let $G = (V, E)$ be a graph. Then G has an even number of vertices with an odd degree.*

Proof. By contradiction. Let V_{even} denote the set of vertices of G with an even degree, and V_{odd} denote the set of vertices of G with an odd degree. So

$$V_{even} \cap V_{odd} = \emptyset$$

$$V_{even} \cup V_{odd} = V$$

For a contradiction, assume $|V_{odd}|$ is odd. Then

$$\begin{aligned}
2|E| &= \sum_{u \in V} \deg(u) && \text{(Handshaking Lemma)} \\
&= \sum_{u \in V_{even}} \deg(u) + \sum_{u \in V_{odd}} \deg(u) \\
&= 2k + 2l + 1 \\
&= 2(k + l) + 1
\end{aligned}$$

But $2|E|$ is even, so this is a contradiction.

$\square$

Example: Can you find a graph with 5 verices with degrees 1,2,3,3,3? Yes, since by the previous theorem, we have an even number of vertices with an odd degree.

Example: Can you find a graph with 5 vertices with degrees 1,2,2,3,3? No, since by the previous theorem, we have an odd number of vertices with odd degree.

Definition 18.0.2 (Length)**.** *A* path *in a graph $G = (V, E)$ is a sequence of vertices $v_0, v_1, \ldots, v_l$ such that $\{v_i, v_{i+1}\} \in E$ for all $0 \leq i \leq l - 1$. A path can also be described as a sequence of the l edges. The vertices v_0 and v_l are the* endpoints *of the path and l is its* length*.*

Definition 18.0.3. *If there is a path with endpoints $u, w \in V$, we say that v and w are* connected*. If any two vertices of a graph are connected, then we say that the graph is* connected*.*

Lecture 20

More on Graphs

Definition 20.0.1 (Cycles)**.** *A* cycle *is a sequence of vertices $v_0, v_1, v_2, \ldots, v_{l-1}, v_0$ such that $v_0, v_1, v_2, \ldots, v_{l-1}$ is a path and $\{v_0, v_1\}, \{v_1, v_2\}, \ldots, \{v_{l-2}, v_{l-1}\}, \{v_{l-1}, v_0\}$ are distinct edges. The* length *of this cycle is l*

> **Note:** Cycles of length 0,1,2 are now allowed by this definition.

Definition 20.0.2 (Walks)**.** *A* walk *is a path where we allow vertices to be repeated. A* closed walk *is a cycle where we allow vertices to be repeated.*

Definition 20.0.3 (Subgraph)**.** *Let $G = (V, E)$ be a graph. A* subgraph *H of G, denoted by $H \subseteq G$, is a graph $H = (V', E')$, where $V' \subseteq V$ and $E' \subseteq E$.*

Definition 20.0.4 (Connectedness)**.** *A* connected component *of G is a subgraph of G consisting of*

- *All vertices that are connected to a given vertex.*
- *Together with all edges incident to them.*

Definition 20.0.5 (Forests)**.** *A* forest *is a graph that has no cycle. A* tree *is a connect forest. A* leaf *in a forest is a vertex of degree 1.*

Theorem 20.0.1. *Let $G = (V, E)$ be a graph. Let $n = |V|$ and $m = |E|$. If G is a forest, then $n > m$ and G has $n - m$ connected componenets (trees).*

Proof. By induction on m.

- **Base Case:** $m = 0$. If a forest has no edges, then $n > 0 = m$. Moreover, each vertex is its own connected component, so there are exactly $n = n - 0 = n - m$ connected components.
- **Induction Hypothesis:** Let $k \geq 0$ be an integer. Assume that for all graphs G with n vetices and k edges, if G is a forest, then $n > k$ and G has $n - k$ connected componenets.

- **Induction Step:** Let G be a forest with n vertices and $k+1$ edges. Remove an arbitrary edge $e = \{a, b\}$ from G without modifying the vertices. Removing e from G does not create a cycle, so the resulting graph G' is a forest with n vertices and k edges. By the induction hypothesis, $n > k$ and G' has $n - k$ connected components.

Observe that a and b cannot both belong to the same connected component of G'. Otherwise, the path from a to b would create a cycle in G and so G would not be a forest. So, a and b are in two different connected components of G'. So,

$$n - k \geq 2 \implies n \geq 2 + k = 1 + (1 + k) > k + 1$$

If we put e back in G, this connects the two connected components for a and b together. So G has

$$(n - k) - 1 = n - (k + 1)$$

connected components, as required. $\square$

Corollary 20.0.1. *Let $G = (V, E)$ be a tree. Then*

$$n = |V| = |E| + 1 = m + 1$$

Proof. A tree is a forest with 1 connected component. By the previous theorem, $n - m = 1$, so $n = m + 1$. $\square$

Definition 20.0.6 (Spanning Tree)**.** *A* spanning tree *of a connected graph G is a subgraph of G that includes all vertcies of G and that is a tree.*

Lecture 21

Spanning Trees Bipartite Graphs

Theorem 21.0.1. *Every connected graph graph $G = (V, E)$ has a spanning tree.*

Proof. Let $G = (V, E)$ be a connected graph. By induction on the $m = |E|$.

- **Base Case:** $m = 0$. For G to be connected graph, it must contain a single vertext v. Then v itself is a spanning tree.
- **Induction Hypothesis:** Let $k \geq 0$ be an integer. Assume that all connected graphs with k edges have a spanning tree.
- **Induction Step:** Let G be a connected graph with $k + 1$ edges. We consider two cases.
  - **Case 1:** G is a tree, then it is its own spanning tree.
  - **Case 2:** If G is not a tree, since G is connected, then G has a cycle. Remove an edge $e = \{a, b\}$ from this cycle. We get a graph G' that is connected. Indeed, if a path uses e, we can reroute it along the other edges of the cycle. So G' is connected and it has k edges. By the induction hypothesis, G' has a spanning tree T. T covers all vertice of G', so it covers all vertices of G, so T is a spanning tree of G.

□

This gives us a way to build a spanning tree; If G is a tree, then it is its own spanning tree. Otherwise, find a cycle, remove an edge from this cycle, and recursively find a spanning tree.

Corollary 21.0.1. *Every graph with n vertices and m edges has at least $n - m$ connected components.*

Proof. Let G be a graph with n vertices and m edges. By the previous theorem, every connected component of G has a spanning tree. Let F be the union of these spanning trees. Then F is a forest with n vertices, and $m' \leq m$. Moreover, the number of connected components in F is the same as in G. So G has $n - m' \geq n - m$ connected components. $\square$

We say that two sets S and T *partition* a set E if

- $S \neq \emptyset$
- $T \neq \emptyset$
- $S \cup T = E$
- $S \cap T =$

We say that a graph $G = (V, E)$ is *bipartite* if V can be partitioned into two sets A and B such that each edge has one endpoint in A and one endpoint in B.

Lecture 22

Bipartite Graphs

Note: Final Exam Topics

- All lectures and all exercises
- 2 hour Exam
- 6 long answer questions and **nothing** Examples
- Study notes and exercises!

Lemma 22.0.1. *let $G = (V, E)$ be a bipartite graph with partition (A, B). Then*

$$\sum_{v \in A} \deg(v) = \sum_{v \in B} \deg(V)$$

Proof. In the proof of the handshaking lemma, we saw that each edge in

$$\sum_{v \in V} \deg(v)$$

is counted twice. Since each edge has one endpoint in A and one endpoint in B, the equality follows. $\square$

Lemma 22.0.2. *Let $G = (V, E)$ be a graph. If G has a closed walk of odd length, then G has a cycle of odd length.*

Proof. By induction on the length l of the closed walk.

- **Base Case:** $l = 1$. Closed walks of length 1 do not exist. So the base case holds trivially.
- **Induction Hypothesis:** Let $K \in \mathbb{Z}$ be an odd integer. Assume that if a graph has a closed walk of odd length at most K, then it has a cycle of odd length.

- **Induction Step:** Let $G = (V, E)$ be a graph having a closed walk of length $k + 2$ (which is odd). Let

$$v_0, v_1, v_2, \dots v_{k+1}, v_0$$

be this closed walk. If all v_i's are different then this is a cycle with odd length. Otherwise, two vertices must be repeated, say v_i and v_j

$$v_0, v_1, v_2, \dots, v_{i-1}, v_i, \dots v_{j-1}, v_j, \dots, v_k, v_{k+1}$$

Consider the closed walks

$$v_i, v_{i+1}, \dots, v_{j-1}, v_j = v_i$$

$$v_j, v_{j+1}, \dots, v_{k+1}, v_0, v_1, \dots, v_{i-1}, v_i = v_j$$

Since the length of the walk is $k + 2$, we have the length of the first walk is less than $k + 2$ and the second walk as well. Since $k + 2$ is odd, then either the first walk or the second walk has odd length. By the induction hypothesis, one of these walks is a cycle. Therefore G has a cycle of odd length.

$\square$

Theorem 22.0.1. *A graph is bipartite if and only if it has no odd cycles.*

Proof. ($\implies$) Assume G is bipartite with partition $V = A \cup B$. If G has no cycle, then it is bipartite. Otherwise, let

$$v_0, v_1, v_2, \dots, v_{l-1}, v_0$$

be a cycle of length $l \geq 3$. We will show that l is even. Without loss of generality, assume $v_0 \in A$. Since $v_0 \in A$, we must have $v_1 \in B$, then $v_2 \in A$, and so on. So $v_{l-1} \in A$ if $l - 1$ is even and $v_{l-1} \in B$ if $l - 1$ is odd. Since $\{v_{l-1}, v_0\}$ is an edge of the cycle, v_{l-1} must be in B. So $l - 1$ is odd, and l is even.

($\impliedby$) Assume G has no cycle of odd length. We want to prove that G is bipartite. Consider two cases where G is connected and where G is not connected.

- **Case 1: G is connected.** We need to build A and B. Let v_0 be an arbitrary vertext. Let

$$A = \{w \in V : \text{ there is a path of even length between } v_0 \text{ and w}\}$$

$$B = \{w \in V : \text{ there is a path of odd length between } v_0 \text{ and } w\}$$

We will show that A and B are disjoint and that $A \cup B = V$, so A and B partition V. Since G is connected, every vertex is connected to v_0, so every vertex belongs to either A or B. We want to show that A and B

are disjoint. For a contradiction, suppose $u \in A \cap B$. Since $v \in A$, there is a path of even length

$$v_0, v_1, \ldots, v_s = u$$

where s is even. Since $v \in B$, there is a path of odd length between v_0 and v. The reverse path also has odd length.

$$u = v_s, v_{s+1}, v_{s+2} \ldots, v_{s+t} = v_0$$

where t is odd. Now

$$v_0, v_1, \ldots, v_s, v_{s+1}, \ldots, v_{s+t} = v_0$$

is a closed walk of length $s + t$ where $s + t$ is odd. By the previous lemma, there is a cycle of odd length. This is a contradiction. So $A \cap B = \emptyset$. So A, B is a partition of V. It remains to show that all edges have one endpoint in A and one endpoint in B. For a contradiction, suppose there is an edge $\{u, w\}$ with both endpoints in A. Then there is a path of even length from u to v_0 and a path of even length from v_0 to w. If u and w are different, then this is a cycle of even length then take the edge $\{u, w\}$ we get an odd length. by the previous lemma, there is a cycle of odd length. Thus, a contradiction.

- **Case 2: G is not connected.** Then we can apply case (1) to each connected component C of G. For each C, we get a partition (A_c, B_c). It remains to take

  $$A = \bigcup_{C \in G} A_C \text{ and } B = \bigcup_{C \in G} B_C$$

  So G is bipartite.

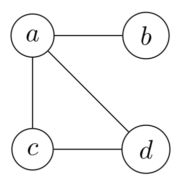
$\square$

Lecture 23

Matchings

Definition 23.0.1 (Matching)**.** *A* matching *in a graph $G = (V, E)$ is a subset of $M \subseteq E$ where no pair of edges share a vertex.*

Example:

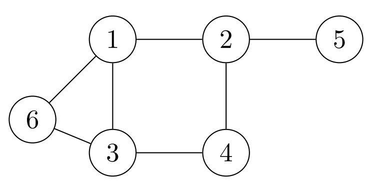


$$M = \{\{a, b\}, \{c, d\}\}$$

$M = \emptyset$ is a matching.

Definition 23.0.2 (Maximum Matching)**.** *A* maximum matching *if it contains the greatest number of edges possible.*

Example:



$$M = \{\{6, 3\}, \{6, 1\}\}$$

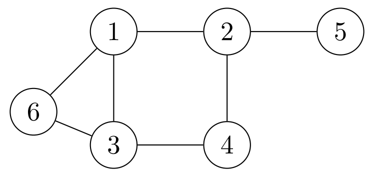
This is not a maximum matching because we could add the edge $\{1, 2\}$ to get a matching with 3 edges. So

$$M = \{\{6, 3\}, \{6, 1\}, \{2, 1\}\}$$

This matching is maximum.

Definition 23.0.3 (Perfect Matchings)**.** *A matching is* perfect *if it matches* all *vertices.*

Example:



$$M = \{\{6,3\},\{6,1\},\{2,1\}\}$$

is a perfect matching. In general, if a graph has an odd number of vertices, it cannot have a perfect matching.

Theorem 23.0.1. *Let $G = (V, E)$ be a graph whose set of edges is the union of two matchings. Then G is bipartite.*

Proof. Let M_1 and M_2 be the two matchings such that $E = M_1 \cup M_2$. We have to prove that G does not have a cycle of odd length. By the previous theorem, this implies that G is bipartite. For a contradiction, let

$$v_0, v_1, v_2, \ldots, v_{l-1}, v_0$$

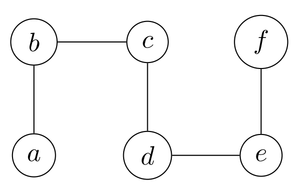
be a cycle of odd length. The edge $\{v_0, v_1\}$ is in M_1 or M_2. Without loss of generality, assume that $\{v_0, v_1\} \in M_1$. Then $\{v_1, v_2\} \in M_2$ otherwise M_1 would not be a matching. Then $\{v_2, v_3\} \in M_1$ and so on. So we have

$$\{v_i, v_{i+1}\} \in M_1 \text{ if } i \text{ is even}$$

$$\{v_i, v_{i+1}\} \in M_2 \text{ if } i \text{ is odd}$$

Then, $\{v_{l-2}, v_{l-1} \in M_2\}$ since $l-2$ is odd, and $\{v_{l-1}, v_0\} \in M_1$ since $l-1$ is even. But, the edge $\{v_0, v_1\}$ in M_1 shares an edge with $\{v_{l-1}, v_0\}$ in M_1. This is a contradiction since M_1 is a matching. □

Example:



$$M_1 = \{\{a,b\},\{c,d\},\{e,f\}\}$$

$$M_2 = \{\{b,c\},\{d,e\}\}$$

$M_1 \cup M_2$ is equal to the set of edges. So this graph is bipartite.

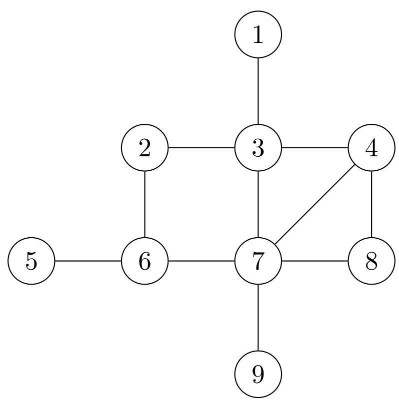
Lecture 24

Neighbour Sets

Definition 24.0.1 (Neighbour Set)**.** *Let $G = (V, E)$ be a graph. Let $S \subseteq V$. The* neighbour set *of S, denoted $N(S)$ is the set of vertices having at least one neighbour in S.*

$$N(S) = \{v \in V | \{v, s\} \text{ is an edge for some } s \in S\}$$

Example:



$$N(\{3, 4\}) = \{1, 2, 3, 4, 7, 8\}$$
$$N(\{1\}) = \{3\}$$
$$N(\{2, 3, 4\}) = \{1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

Theorem 24.0.1 (Hall's Theorem)**.** *Let $G = (V, E)$ be a bipartite graph with partition (A, B). There exists a matching that matches all vertices in A if and only for every $S \subseteq A$. We have $|N(S)| \geq |S|$.*

Proof. ($\Longrightarrow$) Suppose all vertices in A can be matched. Let $S \subseteq A$ be a subset. We need to show that $|N(S)| \geq |S|$. For every $s \in S$, let v be its partner in the matching. All these v's are different. So there are $|S|$ of them. They are all neighbours of vertices in S. So they are in $N(S)$. Therefore, $|N(S)| \geq |S|$.

($\Longleftarrow$) Assume that for every subset $S \subseteq A$, we have $|N(S)| \geq |S|$. We want to prove that all vertices in A can be matched. By indunction,

- **Base Case:** $n = |A| = 1$. Then $|N(A)| \geq |A| = 1$. So the unique vertex in A has a neighbour in B and it can be matched.
- **Induction Hypothesis:** Let $K \geq 1$ be an integer. Assume that for all bipartite graphs G with partition (A, B) where $|A| \leq K$, if $|N(S)| \geq |S|$ for all $S \subseteq A$, then all vertices in A can be matched.
- **Induction Step:** Let G be a bipartite graph with partition (A, B) where $|A| = k+1$. Consider two cases where for every $X \subset A$, we have $|N(X)| \geq |X| + 1$, and there exists a subset $X \subset A$ such that

$$|N(X) < |X| + 1 \implies |N(X)| = |X|$$

  - **Case 1:** Let $a \in A$ and match it with an arbitrary neighbour $b \in B$. Remove a and b from G. Now for every proper subset $X \subset A$, we have $|N(X)| \geq |X|$. By the induction hypothesis, all vertices in $A \setminus \{a\}$ can be matched. So all vertices in A can be matched.
  - **Case 2:** Let $X \subset A$ be a proper subset such that $|N(X)| = |X|$. Observe that all subsets $X' \subseteq X$ are subsets of A, and $|N(X')| \geq |X'|$. So by the induction hypothesis, all vertices in X can be matched. Remove all vertices in X and $N(X)$ from G. Suppose we can show that for all subsets $Y \subseteq A \setminus X$, Y has at least $|Y|$ neighbours in $B \setminus N(X)$, then we apply the induction hypothesis to match all vertices in $A \setminus X$. Combining the two matchings will give us a matching that matches all vertices in A. To prove our supposition, suppose for a contradiction that there exists a subset $Y \subseteq A \setminus X$ that has less than $|Y|$ neighbours in $B \setminus N(X)$. Then the vertices in $X \cup Y$ have less than $|N(X)| + |Y|$ neighbours in G. Then

$$\begin{aligned} |N(X \cup Y)| &< |N(X)| + |Y| \\ &= |X| + |Y| \\ &= |X \cup Y| \\ &\leq |N(X \cup Y)| \end{aligned}$$

    Which is a contradiction.

$\square$