

## 4.1 Divisibility

$a \mid b \leftrightarrow \exists c$  such that  $b = ac$

### + Theorems

Let  $a, b, c \in \mathbb{Z}$  with  $a \neq 0$ :

- If  $a \mid b$  and  $a \mid c$ , then  $a \mid (b + c)$ 
  - We also have  $a \mid (mb + nc) \forall m, n \in \mathbb{Z}$
- If  $a \mid b$ , then  $a \mid bc \forall c \in \mathbb{Z}$
- If  $a \mid b$  and  $b \mid c$ , then  $a \mid c$

## 4.2 Division Algorithm

Let  $a, d \in \mathbb{Z}$  with  $d > 0$

$\exists! q, r \in \mathbb{Z}$  such that  $a = dq + r$  for  $0 \leq r < d$

Notation: If  $a = dq + r$  for  $0 \leq r < d$ , we write:

- $q = a \text{ div } d$
- $r = a \text{ mod } d$

## 4.3 Modulo

Let  $a, b, m \in \mathbb{Z}$  with  $m \geq 2$ .  $a$  is congruent to  $b$  modulo  $m$  if  $m \mid (a - b)$ , and we denote it as  $a \equiv b \pmod{m}$

Note:  $a \equiv b \pmod{m} \leftrightarrow b \equiv a \pmod{m}$

### + Theorems

- ▶ Let  $a, b, c, d, m \in \mathbb{Z}$  with  $m \geq 2$ . If  $a \equiv b \pmod{m}$  and  $c \equiv d \pmod{m}$ , then:
  - $a + c \equiv b + d \pmod{m}$
  - $ac \equiv bd \pmod{m}$
- ▶  $a + c \equiv b + c \pmod{m} \rightarrow a \equiv b \pmod{m}$
- ▶  $c \not\equiv 0 \pmod{m}, ac \equiv bc \pmod{m} \rightarrow a \equiv b \pmod{m}$

## 4.4 Arithmetic Modulo

For  $m \geq 2$ , define  $\mathbb{Z}_m = \{0, 1, 2, \dots, m - 1\}$

$a +_m b = (a + b) \pmod{m}$

$a \cdot_m b = (a \cdot b) \pmod{m}$

## 5.1 Prime Numbers

$p \in \mathbb{Z}$  is prime if it has exactly two divisors, 1 and itself

## 5.2 Fundamental Theorem of Arithmetic

All integers greater than 1 can be written as a unique product of prime numbers

### + Theorems

- ▶ For  $n \in \mathbb{Z}$  such that  $n > 1$ . If  $n$  is not prime, then  $n$  has a prime divisor  $p$  such that  $p \leq \sqrt{n}$
- ▶ There exists an infinite number of prime numbers

## 5.3 Greatest Common Divisor

For  $a, b \in \mathbb{Z}$  such that  $a \neq 0$  or  $b \neq 0$

The greatest integer  $d$  such that  $d \mid a$  and  $d \mid b$  is the GCD of  $a$  and  $b$

$a, b$  are coprime if  $\text{GCD}(a, b) = 1$

## 5.4 Least Common Divisor

For  $a, b \in \mathbb{Z}$  such that  $a \neq 0$  and  $b \neq 0$

The least integer  $m$  such that  $a \mid m$  and  $b \mid m$  is the LCM of  $a$  and  $b$

### + Theorems

- ▶ For  $n = p_1^{a_1} p_2^{a_2} \dots p_k^{a_k}$  where  $p_i$  are prime numbers and  $a_i > 0$  are integers and for  $d \in \mathbb{Z}$   
Then  $d \mid n \leftrightarrow d = p_1^{b_1} p_2^{b_2} \dots p_k^{b_k}$  where  $0 \leq b_i \leq a_i$
- ▶ For  $\begin{cases} a = p_1^{a_1} \dots p_k^{a_k} \\ b = p_1^{b_1} \dots p_k^{b_k} \end{cases}$  with  $p_i$  primes and  $a_i, b_i \geq 0$ :
  - $\text{GCD}(a, b) = p_1^{\min(a_1, b_1)} \dots p_k^{\min(a_k, b_k)}$
  - $\text{LCM}(a, b) = p_1^{\max(a_1, b_1)} \dots p_k^{\max(a_k, b_k)}$
- ▶  $\text{GCD}(a, b) \times \text{LCM}(a, b) = a \times b$
- ▶ For  $a, b, q, r \in \mathbb{Z}$  such that  $a = bq + r$ , then  $\text{GCD}(a, b) = \text{GCD}(b, r)$

## 6.1 Euclid's Algorithm

$a = q_1 \times b + r_1$

$b = q_2 \times r_1 + r_2$

$r_1 = q_3 \times r_2 + r_3$

$\vdots$

$r_{n-2} = q_n r_{n-1} + r_n$

$r_{n-1} = q_{n+1} r_n + r_{n+1}$

And  $\text{GCD}(a, b) = r_n$  when  $r_{n+1} = 0$

## 6.2 Bezout's Algorithm

For  $a, b \in \mathbb{Z}$  and  $a, b > 0$ , then there exists  $s, t \in \mathbb{Z}$  such that  $sa + tb = \text{GCD}(a, b)$

We run Euclid's algorithm backwards:

$\text{GCD}(a, b) = r_n = r_{n-2} - q_{n-1} \times r_{n-2} = \dots = sa + tb$

## + Example of Euclid and Bezout

Run Euclid first for  $\text{GCD}(662, 414)$

$$a: 662 = 1 \times 414 + 248$$

$$b: 414 = 1 \times 248 + 166$$

$$c: 248 = 1 \times 166 + 82$$

$$d: 166 = 2 \times 82 + 2$$

$$e: 82 = 41 \times 2 + 0$$

$$\text{So } \text{GCD}(662, 414) = 2$$

Run Bezout now:

$$2 = 166 - 2 \times 82 \text{ from } d$$

$$= 166 - 2(248 - 1 \times 166) \text{ from } c$$

$$= -2 \times 248 + 3 \times 166 \text{ simple rearranging}$$

$$= -2 \times 248 + 3(414 - 1 \times 248) \text{ from } b$$

$$= 3 \times 414 - 5 \times 248 \text{ simple rearranging}$$

$$= 3 \times 414 - 5(662 - 1 \times 414) \text{ from } a$$

$$= 8 \times 414 - 5 \times 662 \text{ simple rearranging}$$

$$= -5 \times 662 + 8 \times 414$$

$$\text{So } -5 \times 662 + 8 \times 414 = 2 = \text{GCD}(662, 414)$$

## + Theorems

- ▶ If  $\text{GCD}(a, b) = 1$  and  $a \mid (bc)$ , then  $a \mid c$
- ▶  $\exists s, t \in \mathbb{Z}$  such that  $sa + tb = m \leftrightarrow \text{GCD}(a, b) \mid m$
- ▶ For  $m \geq 2$ : If  $ac \equiv bc \pmod{m}$ ,  $\text{GCD}(c, m) = 1$ , then  $a \equiv b \pmod{m}$
- ▶ For  $p$ , a prime number and  $a_1, \dots, a_n \in \mathbb{Z}$   
If  $p \mid (a_1 \times \dots \times a_n)$ , then  $\exists 1 \leq i \leq n$  s.t  $p \mid a_i$
- ▶ For  $m \geq 2$  and  $a \in \mathbb{Z}_m$   
The unique multiplicative inverse of  $a \pmod{m}$  exists if and only if  $\text{GCD}(a, m) = 1$

## 9 Chinese Remainder Theorem

Let  $m_1, m_2, \dots, m_r \in \mathbb{Z}$  be pairwise co-prime integers such that  $m_i \geq 2$  ( $1 \leq i \leq r$ )

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

$$x \equiv a_1 \pmod{m_1}$$

$\vdots$

$$x \equiv a_r \pmod{m_r}$$

admits a unique solution

## 10 Fermat's Little Theorem

Let  $p, a \in \mathbb{Z}$  such that  $p$  is prime. Then:

- $a^p \equiv a \pmod{p}$
- If  $\text{gcd}(a, p) = 1$ , then  $a^{p-1} \equiv 1 \pmod{p}$

## + Theorems

Let  $p, q, M \in \mathbb{Z}$  such that  $p, q$  are two different primes, and  $\text{gcd}(M, pq) = 1$ , then:  $M^{(p-1)(q-1)} \equiv 1 \pmod{pq}$

## 13 Asymptomatic Notation

Let  $f, g$  be functions  $N \rightarrow \mathbb{R}^+$  and let  $c \in \mathbb{R}^+$  and  $k \in \mathbb{N}$ :

- ▶ Big  $O$ -Notation: Asymptotic Upper Bound  
 $f = O(g)$  if  $\exists c, k$  such that  $f(n) \leq c \cdot g(n) \forall n \geq k$
- ▶ Big  $\Omega$ -Notation: Asymptotic Lower Bound  
 $f = \Omega(g)$  if  $\exists c, k$  such that  $f(n) \geq c \cdot g(n) \forall n \geq k$
- ▶ Big  $\Theta$ -Notation: Asymptotic Tight Bound  
 $f = \Theta(g)$  if  $f = O(g)$  and  $f = \Omega(g)$

## + Theorems

- ▶ For  $a, b \in \mathbb{R}$  s.t  $a, b > 0$ . We have  $\log^a(x) = O(x^b)$
- ▶  $f(n) = O(g(n)) \leftrightarrow g(n) = \Omega(f(n))$
- ▶  $f(n) = \Theta(g(n)) \leftrightarrow g(n) = \Theta(f(n))$

## 14.1 Recursivity

Example: *Fibonacci Sequence*

$$F_0 = 0$$

$$F_1 = 1$$

$$F_n = F_{n-1} + F_{n-2} \quad (n \geq 2)$$

## 14.2 Characteristic Equation and Roots

Characteristic equation for a recursive function:

$$r^k - c_1 r^{k-1} - c_2 r^{k-2} - \dots - c_k = 0$$

The solutions are called the *characteristic roots*.

Example: *Fibonacci Sequence*

Characteristic Equation:  $r^2 - 1r^1 - 1 = 0$

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

Using the quadratic formula, we get

$$r = 1 \pm \frac{\sqrt{(-1)^2 - 4(1)(-1)}}{2(1)} = \frac{1 \pm \sqrt{5}}{2}$$

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

is a solution for any  $\alpha, \beta \in \mathbb{R}$

Now we must find  $\alpha, \beta$  such that the formula matches the base cases

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

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

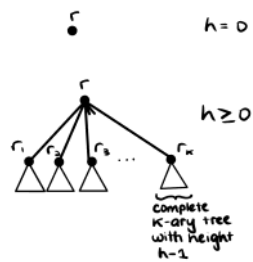
After solving, we get  $\alpha = \frac{1}{\sqrt{5}}$  and  $\beta = -\frac{1}{\sqrt{5}}$

## + Theorems

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

## 15 K-ary Trees

A complete k-ary tree with *height*  $h$  and *root*  $r$  is defined recursively as follows:



Recursive Definition for size:

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

Function Definition:

$$n(h) = \frac{k^{h+1} - 1}{k - 1}$$

## 16 Recursive Algorithms

Example: Number of strictly positives  $NB(A[1, \dots, n])$

If  $n = 1$ : Base Case for size  $n = 1$

If  $A[1] > 0$ : Return 1

Else: Return 0

Else:

$$m = \left\lfloor \frac{n}{2} \right\rfloor$$

Split into 2 subproblems

$a_1 = NB(A[1, \dots, m])$  Recursive Call

$a_2 = NB(A[m+1, \dots, n])$  Recursive Call

Return  $a = a_1 + a_2$  Combining Step

$$\text{Number of step in } NB \begin{cases} T(1) = 3, & (n = 1) \\ T(n) = 2 \times T\left(\frac{n}{2}\right) + 4, & (n > 1) \end{cases}$$

- 2 is the number of recursive calls
- $T\left(\frac{n}{2}\right)$  is the size of the recursive step
- 4 is the merge step + extra work

## 17 Unfolding

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

Assume  $n = 2^k$  for some  $k \in \mathbb{N}$ , since  $n$  has to be divisible by 2

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

## 18.1 Graphs

A graph  $G$  is made of a non-empty set  $V$  of vertices (nodes) together with a set  $E$  of edges

Each edge in  $S$  is an unordered pair  $\{u, v\} \subseteq V$  with  $u \neq v$

We write  $G = (V, E)$

- Loops aren't allowed so  $\{u, u\} = \{u\}$  is not a pair
- Parallel edges  $\{\{u, v\}, \{u, v\}\} = \{\{u, v\}\}$  aren't allowed
- Graphs with no loops and parallel edges are simple

### + Terminology

- **Adjacent:**  $u$  is adjacent to  $v$  if  $\{u, v\}$  is an edge
- **Incident:** An edge  $e$  is incident to  $u$  if one of the two endpoints of  $e$  is  $u$
- **Degree:** The degree of a vertex  $v \in V$  is the number of edges incident to  $v$

### + Theorems

- ▶ Handshaking Lemma:  $\sum_{v \in V} \deg(v) = 2|E|$
- ▶  $G$  has even number of vertices with an odd degree

## 18.2 Paths

A path is a sequence of distinct vertices  $v_0, \dots, v_l$  such that  $\{v_i, v_{i+1}\} \in E$  for  $0 \leq i < l$

It can be described as  $l - 1$  edges  $\{v_0, v_1\}, \dots, \{v_{l-1}, v_l\}$   
The vertices  $v_0$  and  $v_l$  are the endpoints of the path and  $l$  its length

If  $\exists$  a path with endpoints  $v, w \in V$ , then  $v$  and  $w$  are connected

If all vertex-pairs are connected, then the graph is connected

## 20.1 Cycles

A cycle is a sequence of vertices  $v_0, v_1, \dots, v_{l-1}, v_0$  s.t.:

- $v_0, v_1, \dots, v_{l-1}$  is a path
- $\{v_0, v_1\}, \{v_1, v_2\}, \dots, \{v_{l-1}, v_0\}$  are distinct edges

The length of this cycle is  $l$

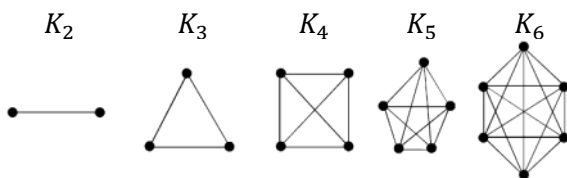
Note: Cycles of length 0, 1 or 2 are not allowed

## 20.2 Walks

- ▶ A walk is a path where we allow repeated vertices
- ▶ A closed walk is a cycle where we allow repeated vertices

## 20.2 Families of Graphs

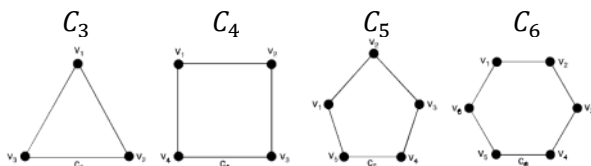
### 20.2.1 Complete Graphs $K_n$ for $n \geq 1$



Every pair of vertices is connected by a unique edge  
Each vertex is connected to  $n - 1$  other vertices

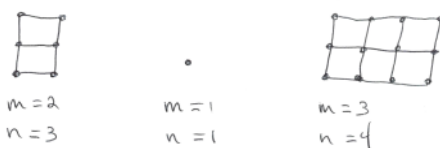
Number of edges:  $|E| = \frac{n(n-1)}{2} = O(n^2)$

### 20.2.2 Cycles $C_n$ for $n \geq 3$



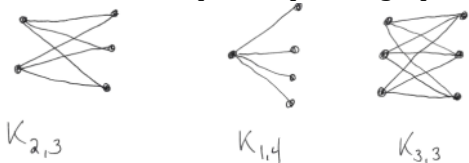
The whole graph is a single cycle with  $n$  vertices, the graph makes a closed chain

### 20.2.3 $(m \times n)$ -grids for $n \geq m \geq 1$



## 22 Usual Family of Bipartite Graphs $K_{m,n}$

For  $n \geq m \geq 1$ , a complete bipartite graphs  $K_{m,n}$



## 20.3 Subgraphs

$H = (V', E')$ , where  $V' \subseteq V$  and  $E' \subseteq E$ , then  $H \subseteq G$

## 20.4 Connected Components

A connected component is a subgraph consisting of:

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

## 20.4 Forests, Trees and Leaves

- **Forest:** A forest is a graph that has no cycle
- **Tree:** A tree is a connected forest
- **Leaf:** A leaf in a forest is a vertex of degree 1

### + Theorems

- For  $n = |V|$ ,  $m = |E|$ . If  $G$  is a forest, then  $n > m$  and  $G$  has  $n - m$  connected components
- For a tree  $G$ ,  $n = |V| = |E| + 1 = m + 1$

## 20.5 Spanning Trees

A spanning tree of a connected graph  $G$  is a subgraph of  $G$  that includes all vertices of  $G$  that is a tree  
Every connected graph has a spanning tree

### 21.1 Partitions

Two sets  $S, T$  partition a set  $E$  if:

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

### 21.2 Bipartite Graphs

A graph is bipartite if  $V$  can be partitioned into  $A$  and  $B$  s.t each edge has one endpoint in  $A$  and one in  $B$

### + Theorems

- For a bipartite graph with partition  $(A, B)$ :

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

- If a graph  $G$  has a closed walk of odd length, then  $G$  has a cycle of odd length
- A graph is bipartite  $\leftrightarrow$  No odd-length cycles

## 23 Matching

- A matching is a graph with a subset  $M \subseteq E$  where no pair of edges share a vertex
- A matching is maximum if it contains the greatest number of edges possible
- A matching is perfect if it matches all vertices

### + Theorems

- If a graph has an odd number of vertices, it cannot have a perfect matching
- If the set of edges is the union of two matchings s.t one isn't empty, then  $G$  is bipartite

## 23 Neighbour Set

Let  $G = (V, E)$  be a graph and let  $S \subseteq V$

The neighbour set of  $S$  (denoted  $N(S)$ ) is the set of vertices having at least one neighbour in  $S$

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

### + Theorems (Hall's Theorem)

- For  $G$ , a bipartite graph with partition  $(A, B)$ :  
 $\exists$  a matching that matches all vertices in  $A$   $\leftrightarrow$  For every subset  $S \subseteq A$  we have  $|N(S)| \geq |S|$

## 12 RSA

### 12.1 Key Generation

- ▶  $p, q$ : Two prime numbers
- ▶  $n = pq$ ,  $n$  is the modulo used. It's part of the public key
- ▶  $\lambda(n) = \text{lcm}(p-1, q-1) = \frac{|(p-1)(q-1)|}{\text{gcd}(p-1, q-1)}$ , is kept a secret
- ▶  $e$ , an integer such that  $2 < e < \lambda(n)$  and  $\text{GCD}(e, \lambda(n)) = 1$ . It's part of the public key
- ▶  $d$ : The private key. It's defined as  $de \equiv 1 \pmod{(p-1)(q-1)}$ , the multiplicative inverse of  $e \pmod{(p-1)(q-1)}$   
Another formula for  $d$ :  $de - k(p-1)(q-1) = 1$

### 12.2 Key Distribution

If Bob wants to send a text to Alice:

- Bob needs to know Alice's public key to encrypt the message
- Alice uses her private key to decrypt it

So Alice sends Bob her public key  $(n, e)$

### 12.3 Encryption

Given the public key  $(n, e)$ , we can encrypt the message  $M$

We first turn the plaintext  $M$  into integers  $m_1, \dots, m_k$  such that  $0 \leq m < n$

Then we compute the ciphertext of each  $m$  using the public key  $(n, e)$ :

$$c \equiv m^e \pmod{n} \text{ for each } m_1, \dots, m_k$$

Then we send the ciphertext values  $c$  to Alice

### 12.1 Decryption

Alice can decrypt the message  $c$  using the private key  $d$ :

$$c^d \equiv m \pmod{n}$$

Alice can then regroup all the integers  $m$  into the original message  $M$