VE203 Final Review

Presenter: Yue & Yinchen

2023/7/30

Outline

- Master Theorem
- Partial order
- Graph theory
  - Connectivity
  - Bipartition
  - Matching
    - Hall's Theorem
    - Kőnig-Egerváry Theorem
  - Tree
  - algorithm
- Number Theory
  - Divisibility
  - Modular Arithmetic
  - RSA
- Group Theory
  - Cyclic Group
  - Symmetric Group
  - Homomorphism

Master Theorem - Notation

	Notation	Formal definition	Limit definition
Asymptotic upper bound	$f(n) = O(g(n))$	exist positive constants c and n_0 such that $0 \leq f(n) \leq cg(n)$ for all $n \geq n_0$	$\lim_{n\to\infty} sup \left(\frac{f(n)}{g(n)}\right) < \infty$
Asymptotic lower bound	$f(n) = \Omega(g(n))$	exist positive constants c and n_0 such that $0 \leq cg(n) \leq f(n)$ for all $n \geq n_0$	$\lim_{n\to\infty} inf \left(\frac{f(n)}{g(n)}\right) > 0$
Asymptotic tight bound	$f(n) = \Theta(g(n))$	exist positive constants c1, c2, and n_0 such that $0 \leq c1g(n) \leq f(n) \leq c2g(n)$ for all $n \geq n_0$	The two above

Stirling approximation: $n! \sim \sqrt{2\pi n}\left(\frac{n}{e}\right)^n$

Given $f(n) = 1 + \cos(\pi n/2)$ and $g(n) = 1 + \sin(\pi n/2)$, then (Summer 2021)

- ☐ f(n) = O(g(n))
- ☐ g(n) = O(f(n))
- ☐ f(n) = Θ(g(n))
- ☐ g(n) = Θ(f(n))

	Notation	**Formal definition**	**Limit definition**
Asymptotic upper bound	$f(n) = O(g(n))$	exist positive constants c and n_0 such that $0 \leq f(n) \leq cg(n)$ for all $n \geq n_0$	$\lim_{n\to\infty} sup \left(\frac{f(n)}{g(n)}\right) < \infty$
Asymptotic lower bound	$f(n) = \Omega(g(n))$	exist positive constants c and n_0 such that $0 \leq cg(n) \leq f(n)$ for all $n \geq n_0$	$\lim_{n\to\infty} inf \left(\frac{f(n)}{g(n)}\right) > 0$
Asymptotic tight bound	$f(n) = \Theta(g(n))$	exist positive constants c1, c2, and n_0 such that $0 \leq c1g(n) \leq f(n) \leq c2g(n)$ for all $n \geq n_0$	The two above

Master Theorem

If $T(n) = aT(n/b) + f(n)$ (for constants $a \geq 1$, $b > 1$), then

1. $T(n) = \Theta(n^{\log_b a})$ if $f(n) = O(n^{\log_b a - \varepsilon})$ for some constant $\varepsilon > 0$.
2. $T(n) = \Theta(n^{\log_b a} \lg n)$ if $f(n) = \Theta(n^{\log_b a})$.
3. $T(n) = \Theta(f(n))$, if $f(n) = \Omega(n^{\log_b a + \varepsilon})$ for some constant $\varepsilon > 0$, and if $af(n/b) \leq cf(n)$ for some constant $c < 1$ and all sufficiently large n (regularity condition).

Exercise 5.2 (2 pts) Let $a \geq 1$ and $b > 1$ be constants, and $T(n)$ satisfies the recurrence

$$T(n) = aT(n/b) + f(n)$$

Show that if $f(n) = \Theta(n^{\log_b a} \lg^k n)$, $k \geq 0$, then the recurrence has solution $T(n) = \Theta(n^{\log_b a} \lg^{k+1} n)$. Assume n is integer power of b for simplicity.

If $T(n) = aT(n/b) + f(n)$ *(for constants* $a \geq 1$, $b > 1$*), then*

1. $T(n) = \Theta(n^{\log_b a})$ *if* $f(n) = O(n^{\log_b a - \varepsilon})$ *for some constant* $\varepsilon > 0$.
2. $T(n) = \Theta(n^{\log_b a} \lg n)$ *if* $f(n) = \Theta(n^{\log_b a})$.
3. $T(n) = \Theta(f(n))$, *if* $f(n) = \Omega(n^{\log_b a + \varepsilon})$ *for some constant* $\varepsilon > 0$, *and if* $af(n/b) \leq cf(n)$ *for some constant* $c < 1$ *and all sufficiently large* n *(regularity condition).*

Exercise:

1. $T(n) = kT\left(\frac{n}{2}\right) + \theta(n^2)$
2. $T(n) = T(\sqrt{n}) + \lg(n)$

Partial Order

Poset $(P, \leq)$

- Reflexive: $\forall x \in P, x \leq x$
- Antisymmetric: $\forall x, y \in P, x \leq y \wedge y \leq x \rightarrow x = y$
- Transitive: $\forall x, y, z \in P, x \leq y \wedge y \leq z \rightarrow x \leq z$

(maybe for some x, y no relation between them)

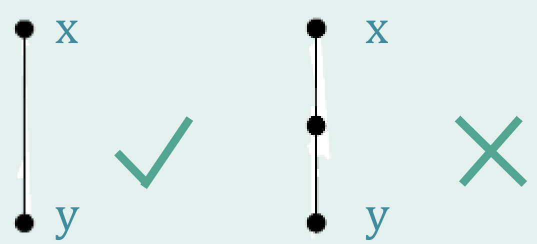
+ dichotomy $\forall x, y \in P$ ($x \leq y$ or $y \leq x$)
  (any two elements are comparable)

$\Rightarrow$ Linear/Total order

+ original order relation kept

$\Rightarrow$ Linear extention

y cover x



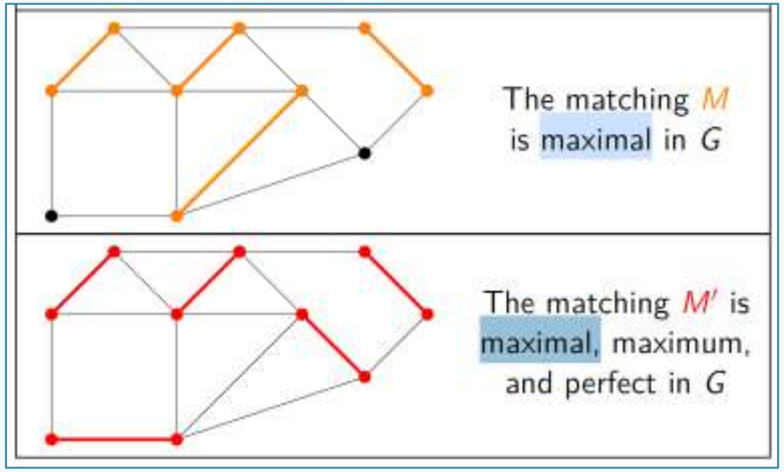
Maximal & maximum ?

Minimal/maximal: (among those who comparable with it)
no larger/smaller (may not unique), can't be extended

Compare with every element

⇩

Minimum/maximum(unique if exist)



- If $z \in P$ but $\nexists x \in P$ such that $z < x$, then z is a ***maximal element***.
- If $x \leq z$ for all $x \in P$, then z is the ***maximum element***.

Definition

A chain C in P is

- ***maximal*** if there exists no chain C' such that $C \subsetneq C'$.
- ***maximum*** if for all chain C', $|C| \nless |C'|$.

Definition

- A matching M is maximal if there is no matching M' such that $M \subsetneq M$
- A matching M is maximum if there is no matching M' such that $|M| < |M'|$.
- A ***perfect matching*** is a matching M such that every vertex of G is incident with an edge in M.

Definition

A maximal connected subgraph of G is a subgraph that is connected and is ***not*** contained in any other connected subgraph of G.

Chain & Antichain

Chain: a subset of comparable elements (a complete graph)

Antichain: a subset of incomparable elements

- **Maximal**: can't be extended
- **Maximum**: max length

Height: maximum size of chain

Width: maximum size of antichain

Exercise

Given a finite set S, then

- ☐ $(2^S, \preceq)$ is a poset, where $A \preceq B$ iff $|A| \le |B|$ for $A, B \subset S$.
- ☐ The width of $(2^S, \subset)$ is at least $|S|$.
- ☐ The height of $(2^S, \supset)$ is at most $|S|$.
- ☐ The height of $(2^S, \supset)$ is at least $|S|$.

Dilworth's Theorem

k: least integer that P is a union of k chains

m: size of largest antichain of P

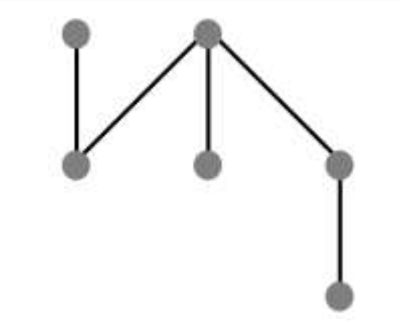
Dilworth Theorem: k=m

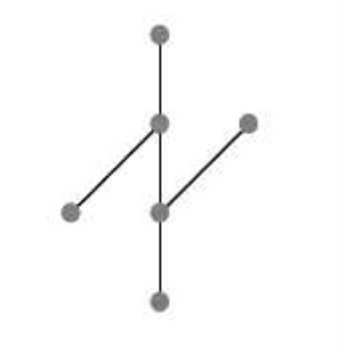
"dual":

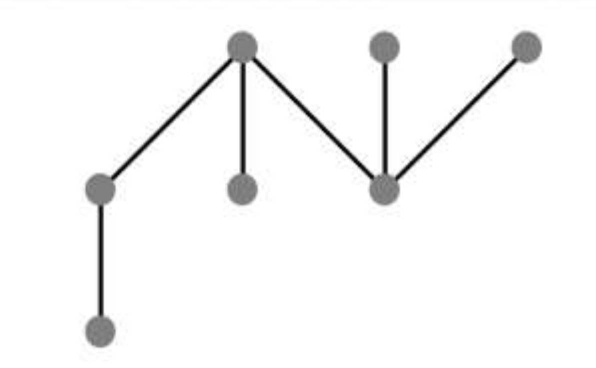
k: least integer that P is a union of k antichains

m: size of largest chain

Mirsky's Theorem: k=m







Example:

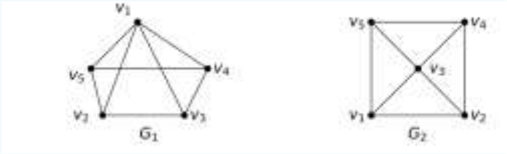
width of the graph on the right?

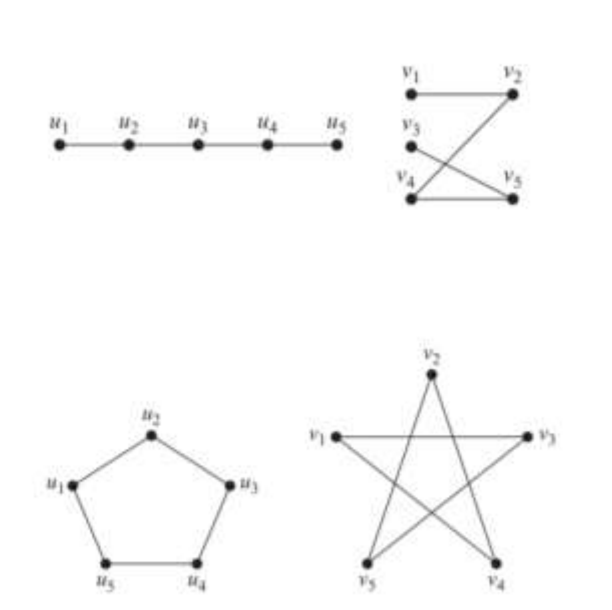
Given a finite poset, would removing a maximal chain decreases the width of the poset?

Basic Graph Definitions

- Loop, parallel, simple graph

- Isomorphism G ≅ H
    - Bijection from V(G) -> V(H) that keep the edges
    - Equivalence relation





- Complement: $uv \in E(\overline{G})$ iff $uv \notin E(G)$.
- Complete graph(K_n)/**Clique**: pairwise adjacent, simple graph
- Path(P_n): no repeat vertices
- Cycle graph(C_n): Path + $e_n = v_n v_1$
- Induced subgraph: every edge: both ends in the subgraph => edge in subgraph
- Bipartition: V(G) => (A, B), no edge has both ends in A or B

Double Counting

- Relation between Degree & Edge
- Handshaking lemma
- Exercise:
  - In any graph with at least two nodes, there are at least two nodes of the same degree
  - Is it true that a finite graph having exactly two vertices of odd degree must contain a path from one to the other? Give a proof or a counterexample.
  - Theorem: Consider a 6-clique where every edge is colored red or blue. The graph contains a red triangle or a blue triangle

For all finite graph $G = (V, E)$,

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

Connectivity

Path: the vertices can be ordered as $v_1, v_2, \ldots, v_k$ and edges can be ordered as $e_1, e_2, \ldots, e_{n-1}$ that $e_i = v_i v_{i+1}$

Walk: a sequence of (not necessarily distinct) vertices $v_1, v_2, \ldots, v_k$ such that $v_i v_{i+1} \in E$ for $i = 1, 2, \ldots, k-1$.

- Distinct Vertices => path
- $v_0 = v_n$ => closed

Length: number of edges

Theorem: If there is a walk from u to v, then there is a path from u to v.

Connected: A graph G is connected if for all u, v ∈ V(G), there is a walk from u to v

(intuitively, one can pick up an entire graph by grabbing just one vertex)

G is **disconnected** iff there is a partition {X,Y } of V(G) such that no edge has an end in X and an end in Y

Each **maximal connected** piece of a graph is called a connected **component**

Which of the following statements about graphs are correct?

- ☐ $C5$ is self-complementary.
- ☐ $P4$ is self-complementary.
- ☐ $K2,2$ is induced in $C4$.
- ☐ $C1$ is induced in $K5$.

Bridge

If the deletion of a edge/vertex v from G causes the number of components to increase, then v is called a **cut edge**/vertex

- *either e is a cut-edge and* $\text{comp}(G - e) = \text{comp}(G) + 1$;
- *or e is NOT a cut-edge and* $\text{comp}(G - e) = \text{comp}(G)$.

an edge e is a bridge of G if and only if e lies on no cycle of G

Bipartition & Matching

Matching:

- A subset of edges
- No common vertices

Or each node has either zero or one edge incident to it.

Perfect matching: every vertex of G is incident with an edge in M.

Theorem

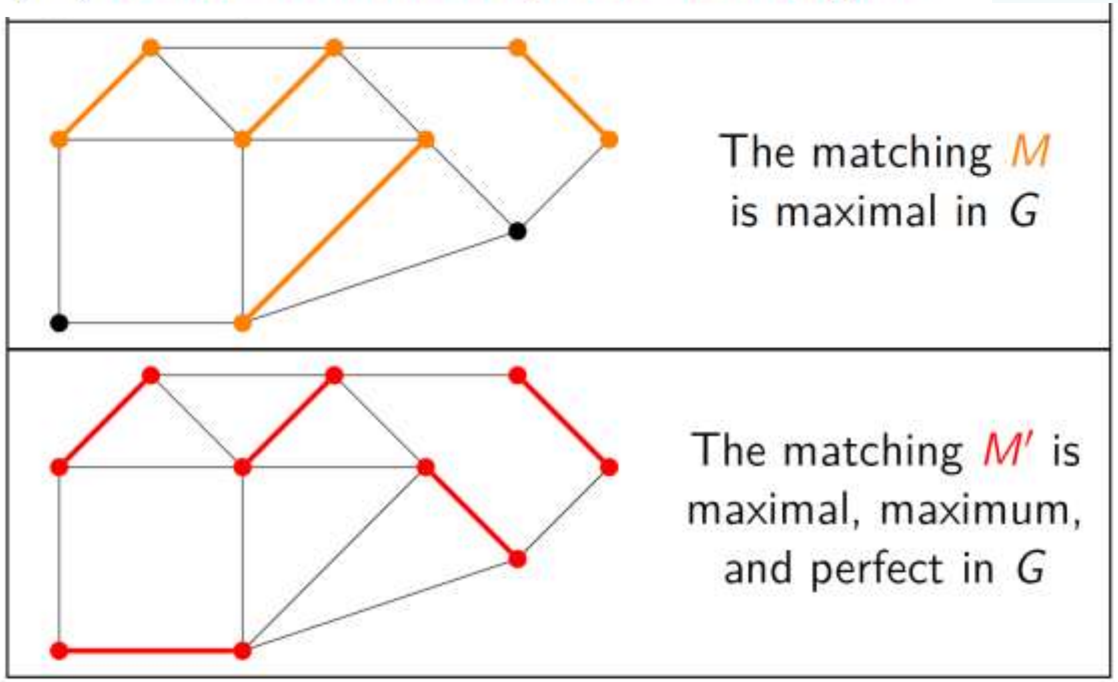
For every graph G, TFAE

(i) *G is bipartite.*

(ii) *G has no cycle of odd length.*

(iii) *G has no closed walk of odd length.*

(iiii) *G has no induced cycle of odd length.*



Matching

Hall's theorem

Let G be a finite bipartite graph with bipartition (A, B).

There exists a matching covering A iff $|N(X)| \geq |X|\ \forall X \subseteq A$ **(Hall's condition)**

- If $X \subset V(G)$, the ***neighbors*** of X is $N(X) := \{v \in V(G) \setminus X \mid v \text{ is adjacent to a vertex in } X\}$
- The edges $S \subset E(G)$ ***covers*** $X \subset V(G)$ if every $x \in X$ is incident to some $e \in S$.

Exercise 7 (10 Marks)

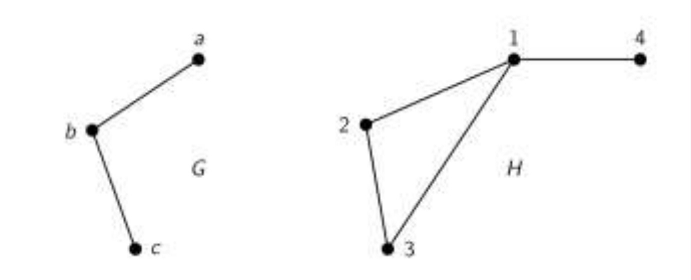
Let G be a bipartite graph with bipartation (A, B), and G has no isolated vertices. If the minimum degree of vertices in A is no less than the maximum degree of vertices in B, show that there exists a matching covering A.

König-Egeváry Theorem

The matching number (i.e., size of a largest matching(edge set)) is equal to
the vertex cover number (i.e., size of a smallest vertex cover) for a bipartite graph.

- Prove that a k-regular bipartite graph has a perfect matching ($k>=1$)
  k-regular: $deg(v) = k$ for all v in $V(G)$

Homomorphism



Definition:

- simple graphs G and H
- a map from V(G) to V(H) which takes edges to edges

=> nonedge can be mapped to anything

=> There is an injective homomorphism from G to H (i.e., one that never maps distir vertices to one vertex) if and only if G is a subgraph of H.

If a homomorphism f : G → H is a bijection whose inverse function is also a graph homomorphism, then f is a graph isomorphism. This is same as the Definition in slides

If there is a homomorphism G → H and another homomorphism H → G. Are the maps surjective or injective?

Tree

forest: no cycles => comp(G) = |V(G)| – |E(G)|.

tree: any two of {connected, no cycles, |V(T)| = |E(T)| + 1}

spanning tree of G = subgraph + tree + contain all vertices

Theorem

Let T be a graph with n vertices. TFAE

(i) *T is a tree;*

(ii) *T contains no cycles, and has $n-1$ edges;*

(iii) *T is connected, and has $n-1$ edges;*

(iv) *T is connected, and each edge is a bridge;*

(v) *any two vertices of T are connected by exactly one path;*

(vi) *T contains no cycles, but the addition of any new edge creates exactly one cycle.*

Theorem:
For connected graph with |V(G)|>2,

- subgraph H is a spanning tree
- Iff H is a minimal connected graph with V(T) =V(G)
- Iff H is a maximal subgraph without cycles

Exercise 5 (10 pts) Given a graph G. Show that an edge $e \in E(G)$ is a cut-edge iff e is contained in every spanning tree of G.

Which of the following graph is a tree?

- ☐ A simple graph with a unique path between any 2 vertices.
- ☐ A connected simple graph in which every edge is a cut edge.
- ☐ A connected simple graph with n vertices and $n - 1$ edges.
- ☐ A connected simple graph with no cycle.

G is a finite graph

(10 pts) Let T be a spanning tree of G, $e \in E(T)$, and $f \in E(G) - E(T)$. Let $P \subset T$ be the unique path connecting the ends of f, and $e \in P$. Show that $T - e + f$ is a spanning tree.

(ii) (10 pts) Given two **distinct** cycles $C, D \subset G$, and an edge $e \in C \cap D$. Show that $C \cup D - e$ contains a cycle.

Algorithm

Kruskal's Algorithm

Aim: Find a minimum-cost tree

Greedy approach

- Maintain a "forest," or a group of trees /disjoint sets
- Iteratively select cheapest edge in graph
    - If adding the edge forms a cycle, don't add it
    - Otherwise, add it to the forest
- Continue until all vertices are part of the same set

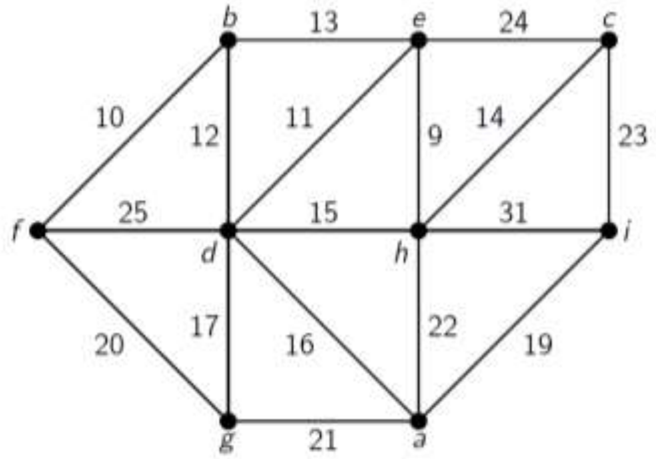
Dijkstra's Algorithm

Aim: shortest path spanning tree for a certain vertex

Greedy Approach

- Separate vertices into two groups:
    - "Innies": vertices that are present in your partial spenning tree at any point in time
    - "Outies" : the other vertices
- Iteratively add **nearest outie**, converting to an innies

Given the following weighted graph G:



- Find a minimum-weight spanning tree using Kruskal’s Algorithm
- Given the root vertex a, find a shortest path spanning tree using Dijkstra’s Algorithm

Outline

- Master Theorem
- Partial order
- Graph theory
  - Connectivity
  - Bipartition
  - Matching
    - Hall's Theorem
    - Kőnig-Egerváry Theorem
  - Tree
  - algorithm
- Number Theory
  - Divisibility
  - Modular Arithmetic
  - RSA
- Group Theory
  - Cyclic Group
  - Symmetric Group
  - Homomorphism

Divisibility

Definition

Let $n, d \in \mathbb{Z}$ with $d \neq 0$, we say that d divides n, denoted by $d \mid n$, if $n = dk$, for some $k \in \mathbb{Z}$, i.e.,

$$d \mid n \Leftrightarrow (\exists k \in \mathbb{Z})(n = dk)$$

By convention, $0 \mid n$ only if $n = 0$.

- $a \mid a$ (**reflexive**)
- $a \mid b \land b \mid c \Rightarrow a \mid c$ (**transitive**)
- $a \mid b \land b \mid a \Rightarrow a = \pm b$ (**?**)

1. $\mid$ on $\mathbb{Z}$: **pre-order**
2. $\mid$ on $\mathbb{N}$: **partial-order**

Prime Numbers

Definition

A natural number $p \in \mathbb{N}$ is a prime number (or simply, a prime) if $p \geq 2$ and if p is divisible only by itself and 1.

Remark

A natural number $p \in \mathbb{N}$ is a prime number if it has exactly two distinct factors. The set of all primes is sometimes denoted by $\mathbb{P}$.

Theorem (Unique Factorization)

*Every positive integer $n \geq 2$ can be **uniquely** expressed in the form*

$$n = \prod_{i=1}^{k} p_i^{\alpha_i}, \; p_i \in \mathbb{P}, \; \alpha_i \in \mathbb{Z}^+$$

Infinitude of Prime

Exercise 7.2 (4 pts) Show that

(i) (2 pts) There exist infinitely many primes of the form $3n+2$, $n \in \mathbb{N}$.

(ii) (2 pts) There exist infinitely many primes of the form $6n+5$, $n \in \mathbb{N}$.

Q1: Prove that there are infinite primes in form of $3n+2$.

A1: Suppose that there are only finite of them, and the largest of them is the m-th prime $p_m = 3k+2$. Consider $N = 3p_1p_2\cdots p_m + 2$, it is not divisible by any primes among $p_1, p_2, \ldots p_m$, so all the prime factor of N is in the form of $3n+1$. But all the $3n+1$ form primes times up would give a number in the form of $3n+2$ like N, contradiction.

Greatest Common Divisor

Definition

Let $a, b \in \mathbb{Z} \setminus \{0\}$, The **greatest common divisor** of a and b, denoted by $\gcd(a, b)$, is the greatest positive integer d such that $d|a \wedge d|b$.

Notice that $(\mathbb{N}, |, \wedge := \gcd, \vee := (a, b) \mapsto \frac{ab}{\gcd(a,b)})$ is a **lattice** where $\top = 0$ and $\bot = 1$.

How to calculate?

① 1. **Euclidean Algorithm**

② 2. Factorization

Exercise: Find solution for

$$111x - 321y = 75$$

Exercise

Let F_n be **Fermat Primes**, $F_n = 2^{2^n} + 1$. Prove that they are pairwise **coprime**, namely $\gcd(F_n, F_m) = 1$.

Motivation: everything starts from division!

$$F_n = k \cdot F_{n-1} + r \Rightarrow F_n = 2^{2^n} - 1 + 2 = F_{n-1} \cdot \left(2^{2^{n-1}} + 1\right) + 2$$

$$\gcd(F_n, F_{n-1}) = (F_{n-1}, 2) = 1$$

But actually:

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

Modular Arithmetic

Definition

Given $a, b \in \mathbb{Z}$, a and b are said to be ***congruent modulo*** n, i.e.,

$$a \equiv b \pmod{n}$$

if $n \mid b - a$, i.e., $b = a + nk$ for some $k \in \mathbb{Z}$.

Remark

This is an equivalence relation. The equivalence classes are called ***congruence***

We can do "arithmetic" in $\mathbb{Z}/n\mathbb{Z}$, e.g.,

$$\overline{a} + \overline{b} = \overline{a + b}$$
$$\overline{a} \cdot \overline{b} = \overline{a \cdot b}$$

which are well-defined.

2.1.44. Theorem. Let $a \in \mathbb{Z}_+$ and $m \in \mathbb{N} \setminus \{0, 1\}$. If $\gcd(a, m) = 1$, the inverse of a modulo m exists. This inverse is unique modulo m.

Arithmetic Functions

A function $f : \mathbb{N} \setminus \{0\} \to \mathbb{N} \setminus \{0\}$ is ***multiplicative*** if $f(1) = 1$ and $f(m_1 m_2) = f(m_1) f(m_2)$ for $\gcd(m_1, m_2) = 1$.

Theorem

The Euler's Totient Function φ is multiplicative.

This is a consequence of the following more general fact.

Euler's Totient Function

The ***Euler's Totient Function***, or the ***Euler phi function***, denoted $\varphi(n)$ or $\phi(n)$ counts the number of positive integers less than n and relatively prime to n, i.e.

$$\varphi(n) = |\{k \in \mathbb{N} \mid \gcd(k, n) = 1, 1 \leq k \leq n\}|$$

Properties of Euler's Function

$$\varphi(p) = p - 1$$

$$\varphi(p^k) = p^k - p^{k-1}\ (k \geq 1)$$

$$\varphi(mn) = \varphi(m) \cdot \varphi(n), \text{if } \gcd(m, n) = 1$$

$$\varphi(a) = \prod_{i=1}^{k} (p_i - 1) p_i^{\alpha_i - 1}$$

$$\varphi(a) = a\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_k}\right)$$

Exercise

- Which of following statements are **correct**?

A. φ is non-decreasing
B. φ is **multiplicative**
C. $\varphi(n)$ is even for all $n \in \mathbb{N} \setminus \{0\}$
D. $\varphi(n)$ is the number of **generators** of the group $(\mathbb{Z}/n\mathbb{Z})^{\times}$

Euler's Theorem

Theorem (Euler)

For $m \in \mathbb{N} \setminus \{0\}$ *and* $a \in \mathbb{Z}$ *such that* $\gcd(a, m) = 1$,

$$a^{\varphi(m)} \equiv 1 \pmod{m}$$

where $\varphi(m)$ *is the number of invertible integers modulo* m.

Theorem (Fermat-I)

Given $a \in \mathbb{Z}$ *and* $p \in \mathbb{P}$, *such that* $(a, p) = 1$, *then*

$$a^{p-1} \equiv 1 \pmod{p}$$

Exercise

4. Given $a, n \in \mathbb{N}$ and $a, n > 1$, show that $n \mid \varphi(a^n - 1)$.

Solution 1:

Let $m = a^n - 1$, consider the multiplicative group $G = (\mathbb{Z}/m\mathbb{Z})^{\times}$.

First we prove the order of a is n. Indeed, $a^n \equiv 1 \pmod{m}$ and $a^x \not\equiv 1 \pmod{m}$ for $1 < x < m$ since $1 < a^x < a^n = m$.

According to Lagrange's theorem, therefore the order of a divides the order of G, that is, $n \mid \varphi(a^n - 1)$.

Solution 2:

$$\left.\begin{aligned} m = a^n - 1 \Rightarrow a^n &\equiv 1 \pmod{m} \\ \text{Euler} \Rightarrow a^{\varphi(m)} &\equiv 1 \pmod{m} \end{aligned}\right\} \Rightarrow n \mid \varphi(m) \text{ (why?)}$$

Fermat Primality Test

Fermat Primality Test

Given $n \in \mathbb{N}$, calculate $2^n \pmod{n}$,

- If $2^n \not\equiv 2 \pmod{n}$, then n is COMPOSITE.
- If $2^n \equiv 2 \pmod{n}$, then n is PROBABLY prime. (Try other numbers next.)

Such test is called ***probabilistic test***.

Fast Modular Exponentiation

Example: Test if 35 is prime.

Note that $35 = (100011)_2 = 2^5 + 2^1 + 2^0$, then

$$2^{35} = 2^{32} \times 2^2 \times 2^1$$

Chinese Remainder Theorem

General Form

Given $x \equiv a_i \pmod{m_i}$, $i = 1, \ldots, r$, $a_1, \ldots, a_r \in \mathbb{Z}$, and $m_1, \ldots, m_r$ are pairwise relatively prime. The unique solution is given by

$$x = a_1 y_1 + a_2 y_2 + \cdots + a_r y_r \pmod{m}$$

where $m = m_1 \cdots m_r$ and $y_i = \delta_{ij} \pmod{m_j}$, e.g., $y_i = (m/m_i)^{\varphi(m_i)}$.

Exercise 6 (10 points)

Solve the following system of linear Diophantine equations,

$$x \equiv 3 \pmod{8}, \qquad x \equiv 1 \pmod{15}, \qquad x \equiv 11 \pmod{20}$$

Chinese Remainder Theorem

Solution: Note that by Chinese remainder's theorem, the original system is equivalent to

$$x \equiv 3 \pmod 8 \tag{12}$$
$$x \equiv 1 \pmod 3 \tag{13}$$
$$x \equiv 1 \pmod 5 \tag{14}$$
$$x \equiv 11 \pmod 4 \tag{15}$$
$$x \equiv 11 \pmod 5 \tag{16}$$

Note that (12) implies (15), and (14) and (16) are the same, hence the original system is equivalent to

$$x \equiv 3 \pmod 8 \tag{17}$$
$$x \equiv 1 \pmod 5 \tag{18}$$
$$x \equiv 1 \pmod 3 \tag{19}$$

RSA Cryptography!

- The **public key** to be published is a pair of positive integers $(n := pq, E)$ where $p, q \in \mathbb{P}$ and $p \neq q$, and $E < \varphi(n)$, $\gcd(E, \varphi(n))$.
- The **encryption function** is

$$y = e(x) := x^E \mod n$$

- The **private key** $D := E^{-1} \mod \varphi(n)$. The **decryption function** is therefore

$$d(y) := y^D = x^{ED} = x \mod n$$

RSA Cryptography!

In an RSA procedure, the **public key** is chosen as (n, E) = (2077, 97), i.e., the encryption function e is given by

$$e(x) = x^{97} (\text{mod } 2077)$$

Note: $2077 = 31 \times 67$

1. Compute **private key** $D = E^{-1} \left(\text{mod } \varphi(n)\right)$ A: -347(1633)
2. Decrypt the message 279:

find $x, y = e(x) \equiv 279 \text{ (mod } 2077) \Leftrightarrow x = 279^D$ A: 1984

Group Theory

Definition

A group is a pair $(G, \cdot)$, where G is a set, and $\cdot : G \times G \to G$, $(g, h) \mapsto g \cdot h = gh$, is a law of composition (aka group law) that has the following properties:

- The law of composition is associative: $(ab)c = a(bc)$ for all $a, b, c \in G$.
- G contains an identity element 1, such that $1a = a1 = a$ for all $a \in G$.
- Every element $a \in G$ has an inverse, an element b such that $ab = ba = 1$.

An abelian group is a group whose law of composition is commutative.

Definition

A subset H of a group G is a subgroup if it has the following properties:

- Closure: If $a, b \in H$, then $ab \in H$.
- Identity: $1 \in H$.
- Inverses: If $a \in H$, then $a^{-1} \in H$.

Exercise

Given a group G, for $a, b \in G$, let $a \sim b$ **if and only if** there exists $g \in G$ such that $b = gag^{-1}$ (**conjugate** of a by g). Show that $\sim$ is an **equivalence relation**.

Solution:

- Reflexivity: For all $x \in G$, $x = exe^{-1}$. Thus $x \sim x$ for all $x \in G$.
- Symmetry: Let $x \sim y$ for $x, y \in G$. So $\exists g \in G$ such that $y = gxg^{-1}$. Therefore $\exists g^{-1}$ such that $x = g^{-1}yg$, i.e., $y \sim x$.
- Transitivity: Let $x \sim y$ and $y \sim z$ for $x, y, z \in G$. So $\exists g, h \in G$ such that $y = gxg^{-1}$ and $z = hyh^{-1}$. Therefore $\exists hg \in G$ such that $z = hgxg^{-1}h^{-1} = (hg)x(hg)^{-1}$, so $x \sim z$.

Cyclic Group

A group is cyclic if it can be generated by a single element.
The cyclic subgroup generated by g is

$$\langle g \rangle = \{g^k \mid k \in \mathbb{Z}\}.$$

Let G be a group, $g \in G$. The order of g is the smallest natural integer n such that $g^n = 1$. If there is no positive integer n such that $g^n = 1$, then g has infinite order.

A group G is cyclic if $G = \langle g \rangle$ for some $g \in G$. g is a generator of $\langle g \rangle$.

Exercise

Given a group G, for $a, b \in G$, $a \sim b$ **if and only if** there exists $g \in G$ such that $b = gag^{-1}$ (**conjugate** of a by g). Given that $\sim$ is an **equivalence relation**, find the **partition** of cyclic group C_4 by $\sim$.

Suppose $C_4 = \langle x \rangle = \{e, x, x^2, x^3\}$, then the partition is given by $\{\{e\}, \{x\}, \{x^2\}, \{x^3\}\}$

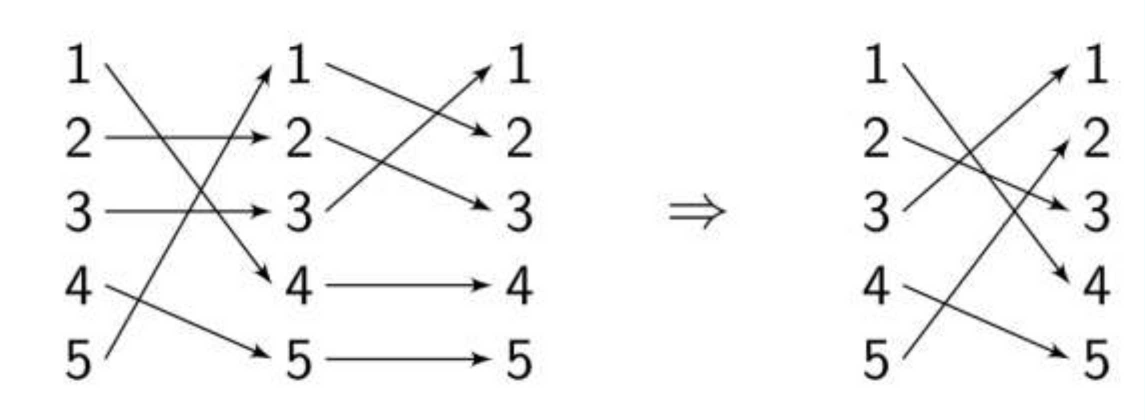
Symmetric Group

Symmetric Group S_n

Given $n \in \mathbb{N} \setminus \{0\}$, we have the following ***symmetric group of degree*** n,

$$\begin{aligned} S_n &= \{\text{All permutations on } n \text{ letters/numbers}\} \\ &= \mathrm{Sym}\{1, 2, 3, \ldots, n\} \\ &= \{f : [n] \to [n] \mid f \text{ bijective}\} \end{aligned}$$

Note that it is a finite group of ***order*** $n!$, i.e., $|S_n| = n!$.



Alternating Group

A permutation of the form (ab) where $a \neq b$ is called a **transposition**.

A permutation that can be expressed as a product of an even/odd number of **transpositions** is called an even/odd permutation.

The set of even permutations in S_n forms a subgroup of S_n, denoted A_n, is called the alternating group of degree n.
$|A_n| = n!/2$ for $n > 1$.

Exercise

Given a group G, for $a, b \in G$, $a \sim b$ **if and only if** there exists $g \in G$ such that $b = gag^{-1}$ (**conjugate** of a by g). Given that $\sim$ is an **equivalence relation**, find the **partition** of A_4 by $\sim$.

Solution: Using cycle notation, the partition is given by

$$\begin{aligned}
\{&\{1\},\\
&\{(12)(34), (13)(24), (14)(23)\},\\
&\{(123), (243), (134), (142)\},\\
&\{(132), (234), (143), (124)\}\}
\end{aligned}$$

Homomorphism

Definition

Given groups G, G', a homomorphism is a map $f : G \to G'$ such that for all $x, y \in G$,

$$f(xy) = f(x)f(y)$$

Theorem

Let $f : G \to G'$ be a group homomorphism, then

- *If $a_1, \ldots, a_k \in G$, then $f(a_1 \cdots a_k) = f(a_1) \cdots f(a_k)$.*
- $f(1_G) = 1_{G'}$.
- $f(a^{-1}) = f(a)^{-1}$ *for $a \in G$.*

isomorphism?

Cosets

Definition

Given a group G, if $H \leq G$ is a subgroup and $a \in G$, the notation aH will stand for the set of all products ah with $h \in H$,

$$aH = \{g \in G \mid g = ah \text{ for some } h \in H\}$$

This set is called a ***left coset*** of H in G

Definition

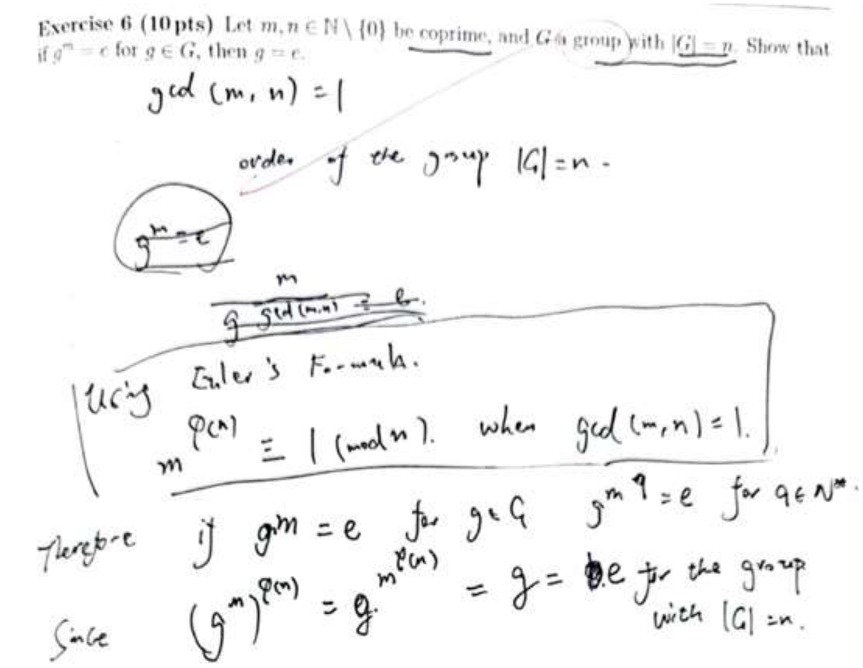
The number of ***left cosets*** of a subgroup is called the ***index*** of H in G. The index is denoted by $[G : H]$ (which could be infinite if $|G| = \infty$).

Counting formula: $|G| = |H| \cdot [G : H]$.

Lagrange's Theorem: Let H be a subgroup of a finite group G. The order of H divides the order of G.

Exercise?

Exercise 6 (10 pts) Let $m, n \in \mathbb{N} \setminus \{0\}$ be coprime, and G a group with $|G| = n$. Show that if $g^m = e$ for $g \in G$, then $g = e$.



Exercise 6 (10 pts) Let $m, n \in \mathbb{N} \setminus \{0\}$ be coprime, and G a group with $|G| = n$. Show that if $g^m = e$ for $g \in G$, then $g = e$.

$\gcd(m, n) = 1$

order of the group $|G| = n$.

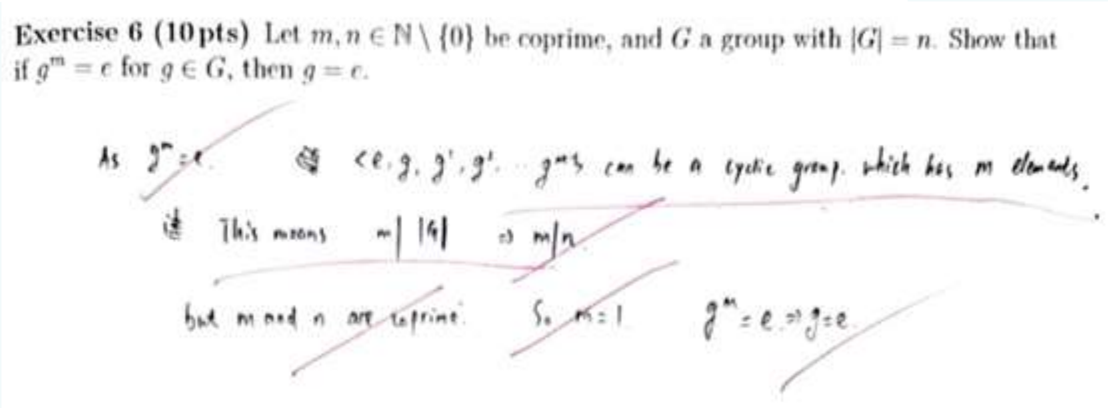
$g^m = e$

~~$g^{\frac{m}{\gcd(m,n)}} = e$.~~

Using Euler's Formula.
$m^{\varphi(n)} \equiv 1 \pmod n$. when $\gcd(m,n) = 1$.

Therefore if $g^m = e$ for $g \in G$ $g^{mq} = e$ for $q \in \mathbb{N}^*$.

Since $(g^m)^{\varphi(n)} = g^{m^{\varphi(n)}} = g = e$ for the group with $|G| = n$.



Exercise 6 (10 pts) Let $m, n \in \mathbb{N} \setminus \{0\}$ be coprime, and G a group with $|G| = n$. Show that if $g^m = e$ for $g \in G$, then $g = e$.

As $g^m = e$. $\langle e, g, g^2, g^3 \cdots g^{m-1} \rangle$ can be a cyclic group, which has m elements.

This means $m \mid |G| \Rightarrow m \mid n$

but m and n are coprime. So $m = 1$ $g^m = e \Rightarrow g = e$

Solution: Let $|g| = d$, then by Lagrange's theorem, $g^m = e$ implies that $d \mid m$. Also by Lagrange's theorem $g \mid n$. Thus $d \mid \gcd(m, n)$, i.e., $d \mid 1$. So $|g| = 1$, that is, $g = e$.

Exercise

- Let G, H be finite groups. Which of following statements are **correct**?

A. If G cyclic and $d \in \mathbb{N} \setminus \{0\}$, the number of elements of order d in G is $\varphi(d)$.

B. If G and H are cyclic groups with $|G| = |H|$, then G and H are isomorphic

C. If $H \leq G$ and $a \in G$ then $|aH| = |Ha|$

D. If $\mathrm{H} \leq G$ and $a, b \in G$, then either $aH = Hb$ or $aH \cap Hb = \emptyset$

End

~~QAQ~~Q&A

Reference

- Summer 2021 final exam
- Fall 2021 midterm 2 exam
- Spring 2023 final exam
- Kőnig-Egerváry theorem (omath.club)
- Prof. Cai, Runze. MATH2030J SU 2023 Lecture Slides
- Zhao, Jiayuan. VE203 FA 2021 Recitation Class Exercises.
- Xue, Runze. VE203 FA 2021 Recitation Class Exercises.