M344 Final Exam

Quick Reference Study Guide

Yolymatics Tutorials

November 5, 2025

Best wishes on your final exam today!
You've prepared well – trust yourself and show what you know!

Exam Time: 2:00 PM ★ **You've got this!** ★

---

1 Number Theory: Ring of Integers Modulo n

The Ring $(\mathbb{Z}/n\mathbb{Z}$

Definition: $\mathbb{Z}/n\mathbb{Z} = \{[0], [1], [2], \ldots, [n-1]\}$ where $[a] = \{x \in \mathbb{Z} : x \equiv a \pmod{n}\}$
Operations: $[a] + [b] = [a + b]$ and $[a] \cdot [b] = [ab]$

Proving $\mathbb{Z}/n\mathbb{Z}$ is a Ring

Must verify:

1. **Addition forms an abelian group:**
   - Closure: $[a] + [b] \in \mathbb{Z}/n\mathbb{Z}$
   - Associativity: $([a] + [b]) + [c] = [a] + ([b] + [c])$
   - Identity: $[0]$ is additive identity
   - Inverses: $-[a] = [n - a]$
   - Commutativity: $[a] + [b] = [b] + [a]$
2. **Multiplication is associative:** $([a] \cdot [b]) \cdot [c] = [a] \cdot ([b] \cdot [c])$
3. **Distributive laws:** $[a] \cdot ([b] + [c]) = [a] \cdot [b] + [a] \cdot [c]$ and $([a] + [b]) \cdot [c] = [a] \cdot [c] + [b] \cdot [c]$

Group of Units $(\mathbb{Z}/n\mathbb{Z})^*$

$(\mathbb{Z}/n\mathbb{Z})^* = \{[a] \in \mathbb{Z}/n\mathbb{Z} : \gcd(a, n) = 1\}$
These are elements with multiplicative inverses. $|(\mathbb{Z}/n\mathbb{Z})^*| = \phi(n)$

2 Relations and Equivalence Relations

Relation

A relation R on set A is a subset of $A \times A$. Write $a \sim b$ if $(a, b) \in R$.

Proving a Relation is an Equivalence Relation

Must verify three properties:

1. **Reflexive:** $a \sim a$ for all $a \in A$
2. **Symmetric:** If $a \sim b$, then $b \sim a$
3. **Transitive:** If $a \sim b$ and $b \sim c$, then $a \sim c$

Example: Congruence mod n

Relation: $a \sim b$ iff $n|(a-b)$

- **Reflexive:** $n|(a-a)=0$
- **Symmetric:** If $n|(a-b)$, then $n|-(a-b)=(b-a)$
- **Transitive:** If $n|(a-b)$ and $n|(b-c)$, then $n|(a-b+b-c)=(a-c)$

3 Solving Linear Congruences: $ax \equiv b \pmod{n}$

Solvability Criteria

Let $d = \gcd(a, n)$.

- **If $d \nmid b$:** NO solutions
- **If $d|b$:** Exactly d solutions modulo n

Case 1: $\gcd(a$

Method: Find $a^{-1} \pmod{n}$ using Extended Euclidean Algorithm

1. Use EEA to find s, t such that $as + nt = 1$
2. Then $a^{-1} \equiv s \pmod{n}$
3. Solution: $x \equiv a^{-1} \cdot b \pmod{n}$ (unique mod n)

Case 2: $\gcd(a$

Step 1: Check if $d|b$. If not, no solution!
Step 2: If yes, divide equation by d:

$$\frac{a}{d}x \equiv \frac{b}{d} \pmod{\frac{n}{d}}$$

Step 3: Now $\gcd(a/d, n/d) = 1$, so solve as in Case 1
Step 4: Get d solutions: $x_0, x_0 + \frac{n}{d}, x_0 + 2\frac{n}{d}, \ldots, x_0 + (d-1)\frac{n}{d} \bmod n$

4 Key Theorems in Number Theory

Extended Euclidean Algorithm (EEA)

For $a, b \in \mathbb{Z}^+$, can find $s, t \in \mathbb{Z}$ such that $as + bt = \gcd(a, b)$
Algorithm: Apply Euclidean algorithm, then back-substitute.

Euler's Theorem

If $\gcd(a, n) = 1$, then $a^{\phi(n)} \equiv 1 \pmod{n}$
Special case (Fermat's Little Theorem): If p is prime and $\gcd(a, p) = 1$, then $a^{p-1} \equiv 1 \pmod{p}$

Wilson's Theorem

p is prime if and only if $(p-1)! \equiv -1 \pmod{p}$

Chinese Remainder Theorem (CRT)

If $\gcd(n_1, n_2) = 1$, the system

$$x \equiv a_1 \pmod{n_1}$$
$$x \equiv a_2 \pmod{n_2}$$

has a unique solution mod $n_1 n_2$.

Algorithm:

1. Set $N = n_1 n_2$, $N_1 = n_2$, $N_2 = n_1$
2. Find M_1 such that $N_1 M_1 \equiv 1 \pmod{n_1}$
3. Find M_2 such that $N_2 M_2 \equiv 1 \pmod{n_2}$
4. Solution: $x \equiv a_1 N_1 M_1 + a_2 N_2 M_2 \pmod{N}$

Euler's Phi Function $\phi(n)$

$\phi(n) = |\{k : 1 \le k \le n, \gcd(k, n) = 1\}|$

Properties:

- If p is prime: $\phi(p) = p - 1$
- $\phi(p^k) = p^k - p^{k-1} = p^{k-1}(p-1)$
- **Multiplicative:** If $\gcd(m, n) = 1$, then $\phi(mn) = \phi(m)\phi(n)$
- $\phi(n) = n \prod_{p|n} \left(1 - \frac{1}{p}\right)$ where product is over primes dividing n

5 Combinatorics: Counting and Multisets

Basic Counting Formulas

Problem	Order Matters	Order Doesn't Matter
Without repetition	$P(n,k) = \frac{n!}{(n-k)!}$	$C(n,k) = \binom{n}{k} = \frac{n!}{k!(n-k)!}$
With repetition	n^k	$\binom{n+k-1}{k}$

Multinomial Theorem

$$(x_1 + x_2 + \cdots + x_m)^n = \sum_{k_1+k_2+\cdots+k_m=n} \binom{n}{k_1, k_2, \ldots, k_m} x_1^{k_1} x_2^{k_2} \cdots x_m^{k_m}$$

where $\binom{n}{k_1,k_2,\ldots,k_m} = \frac{n!}{k_1!k_2!\cdots k_m!}$ is the **multinomial coefficient**.

Multisets

A multiset allows repeated elements. Choosing k objects from n types with repetition:

$$\binom{n+k-1}{k} = \binom{n+k-1}{n-1}$$

Think of it as: Distributing k identical balls into n distinct bins = "stars and bars"

Multiset Applications

Problem: Number of non-negative integer solutions to $x_1 + x_2 + \cdots + x_n = k$?
Answer: $\binom{n+k-1}{k}$
Problem: Coefficient of $x_1^{a_1} x_2^{a_2} \cdots x_m^{a_m}$ in $(x_1 + x_2 + \cdots + x_m)^n$?
Answer: $\binom{n}{a_1, a_2, \ldots, a_m}$ if $a_1 + a_2 + \cdots + a_m = n$, else 0.

Ordered Partitions

Distributing n distinct objects into k labeled groups of sizes $n_1, n_2, \ldots, n_k$:

$$\binom{n}{n_1, n_2, \ldots, n_k} = \frac{n!}{n_1! n_2! \cdots n_k!}$$

6 Graph Theory Essentials

Graph Definition

A **graph** $G = (V, E)$ consists of:
- V: a finite set of vertices
- E: a set of edges, where each edge is a 2-element subset of V

Key Graph Types

- **Complete graph K_n:** Every pair of vertices is connected
- **Path graph P_n:** n vertices in a line
- **Cycle C_n:** n vertices in a closed loop
- **Bipartite graph:** $V = A \cup B$ (disjoint), all edges between A and B
- **Complete bipartite $K_{m,n}$:** All possible edges between sets of size m and n

Testing if a Graph is Bipartite

A graph G is bipartite if and only if it contains **no odd cycles**.
Algorithm (2-Coloring):
1. Start at any vertex, color it RED
2. Color all neighbors BLUE
3. Color all their neighbors RED
4. Continue... If you ever need to color a vertex two different colors, it's NOT bipartite
5. If you can 2-color the whole graph, it IS bipartite

Alternative: Try to partition vertices into two sets such that no edge has both endpoints in the same set.

Other Important Concepts

- **Subgraph:** $H = (V', E')$ where $V' \subseteq V$ and $E' \subseteq E$
- **Walk:** Sequence of vertices $v_0, v_1, \ldots, v_k$ where each consecutive pair is connected
- **Path:** Walk with no repeated vertices
- **Connected graph:** There's a path between any two vertices
- **Tree:** Connected graph with no cycles (has $|V| - 1$ edges)

Graph Isomorphism

Graphs $G_1 = (V_1, E_1)$ and $G_2 = (V_2, E_2)$ are **isomorphic** if there exists a bijection $f : V_1 \to V_2$ such that $\{u, v\} \in E_1$ iff $\{f(u), f(v)\} \in E_2$.
To prove isomorphism: Find the bijection and verify it preserves edges.
To prove NOT isomorphic: Find an invariant that differs:

- Number of vertices or edges
- Degree sequence
- Number of cycles of a given length
- Connectivity

7 Quick Problem-Solving Strategy

Exam Approach

1. **Read carefully:** Identify what topics are involved
2. **Break it down:** Split complex problems into components
3. **Choose tools:** Which theorem/algorithm applies?
4. **Show your work:** Partial credit is valuable!
5. **Check your answer:** Does it make sense?

Final Reminders for Today:

★ **Stay calm and pace yourself**
★ **Answer what you know first**
★ **Use all the time you need**
★ **Trust your preparation**

Good luck on your final exam!
– ***Yolymatics Tutorials***