You have to study all the problem sets and all the theorems discussed during lectures. Here I will just summarize SOME of the IMPORTANT topics and problems. It is NOT enough to study only these topics and problems.

- How to negate a mathematical proposition.

e.g. $\neg(\forall a, P(a)) \equiv \exists a, \neg P(a)$.

$\neg(P \wedge Q) \equiv \neg P \vee \neg Q$.

$\neg(P \Rightarrow Q) \equiv P \wedge \neg Q$.

Exp. Write the negation of the following propositions

① $\forall \varepsilon > 0, \exists n \in \mathbb{N}, \ x > n \Rightarrow \left| \frac{\log x}{x} \right| < \varepsilon$.

② $\forall a, b \in \mathbb{N}$, there is a unique $(q, r) \in \mathbb{Z} \times \mathbb{Z}$,

$a = bq + r \ \wedge \ 0 \leq r < b$.

- How to work with truth table.

e.g. Write a propositional form whose truth table is a given table.

- Use truth table to check certain identities.

For example: $\chi_{A\cap B} = \chi_A \cdot \chi_B$

$\chi_{A\cup B} = \chi_A + \chi_B - \chi_A \cdot \chi_B$.

where χ_A is the characteristic function of A.

Exp. Show $\chi_{A\setminus B} = \chi_A - \chi_{A\cap B}$.

(Can you prove it without using the truth table?)

- Induction principle. (and strong induction)

e.g. • Use induction to prove inequalities:

$\forall n \in \mathbb{N},\ n \geq 4 \Rightarrow 2^n \geq n^2$.

• As you have seen during this course lots of theorems and problems are based on induction principle.

- Well-ordering principle.

e.g. . Use it to prove division algorithm.

. Use it to prove Induction principle.

- $\forall a, b \in \mathbb{N},\ \exists x, y \in \mathbb{Z},\ \gcd(a,b) = ax + by$.

- Euclid Algorithm.

e.g. Besides its proof, you have to be able to use it:

① Find an integer solution for

$$ax+by=c$$

if it has an integer solution. And use it to find all the integer solutions.

② Find all the solutions of $ax \equiv b \pmod m$ if it has a solution.

③ Prove that $\gcd(f_n, f_m) = f_{\gcd(m,n)}$, where $f_1 = f_2 = 1$ and $f_{k+1} = f_k + f_{k-1}$.

④ Prove that $\gcd(2^n-1, 2^m-1) = 2^{\gcd(n,m)} - 1$.

• Language Of Set Theory.

e.g.. What are $A \cap B$, $A \cup B$, $A \setminus B$, A^c, $P(A)$, $A \Delta B$, $\emptyset$, $a \in A$, $A \times B$, $A \subseteq B$.

• Rules, for instance:

$$A \cup (B \cap C) = (A \cup B) \cap (A \cup C).$$

$$(A \cup B)^c = A^c \cap B^c$$

$$A \setminus B = A \cap B^c$$

• Functions.

e.g. The definition of <u>function</u>, graph of a

function, a injection, a surjection, a bijection, an invertible function.

Exp. $f, g : X \to X$. If $f \circ g$ is 1-1, then g is 1-1.

If $f \circ g$ is onto, then f is onto.

Exp. X: finite set & $f, g : X \to X$.

$f \circ g$ is invertible $\iff$ f and g are invertible.

* You have to be able to check if a given function is 1-1 or onto.

Unique Factorization

e.g. Besides its proof, you have to be able to use it to prove other problems. For instance use it to prove various properties of $v_p(n)$.

In particular, you have to be able to prove

$$|ab| = \gcd(a,b) \cdot \operatorname{lcm}(a,b).$$

You have to be able to prove

$$\left.\begin{matrix} a \mid m \\ b \mid m \end{matrix}\right\} \Rightarrow \operatorname{lcm}(a,b) \mid m.$$

As another example, you should be able to show that any rational solution of

$$x^n + a_{n-1}x^{n-1} + \cdots + a_0 = 0$$

is integer (if $a_i \in \mathbb{Z}$). In particular, $\sqrt[3]{5}$ is irrational.

Main Lemma in the proof of U.F.

$$\left.\begin{array}{l} a \mid bc \\ \gcd(a,b) = 1 \end{array}\right\} \stackrel{?}{\Rightarrow} a \mid c.$$

Solve a linear equation in $\mathbb{Z}/m\mathbb{Z}$.

- $ax = b$ has a solution in $\mathbb{Z}/m\mathbb{Z}$ iff $\gcd(a,m) \mid b$.

- If $\gcd(a,m) \mid b$, then $ax = b$ has $\gcd(a,m)$- many solutions in $\mathbb{Z}/m\mathbb{Z}$.

- Use Euclid Algorithm to find the unique solution of $\frac{a}{d}x = \frac{b}{d}$ in $\mathbb{Z}/\frac{m}{d}\mathbb{Z}$ and

lift it up to d solutions of $ax = b$ in $\mathbb{Z}/m\mathbb{Z}$, where $d = \gcd(a, m)$.

- Invertible elements in $\mathbb{Z}/m\mathbb{Z}$.

  e.g. The definition of $U(\mathbb{Z}/m\mathbb{Z})$;

  The definition of $\varphi(m)$;

  $\varphi(mn) = \varphi(m) \cdot \varphi(n)$ if $\gcd(m, n) = 1$;

  Euler's theorem.

- Chinese Remainder Theorem.

  If $\gcd(m, n) = 1$, then for any $a, b \in \mathbb{Z}$ there is a unique $x \pmod{mn}$ such that

$$\begin{cases} x \equiv a \pmod{m}. \\ x \equiv b \pmod{n}. \end{cases}$$

- Wilson's theorem.

- Partition and equivalence relation

  e.g. • Definition of a partition.

  • Finer partition (eg. Under what

condition $\mathbb{Z}/n\mathbb{Z}$ is a finer partition than $\mathbb{Z}/m\mathbb{Z}$.)

- Definition of a relation, reflexive relation, symmetric relation, transitive relation, equivalence relation.
- Find # of relations, reflexive rela., symmetric relation on a set X where $|X| = n$.
- Definition of $X/\sim$ where $\sim$ is an equivalence relation.
- Prove that there is a correspondence between partitions and equivalence relations:

$$\mathbb{P} \longmapsto R_{\mathbb{P}}, \text{ where}$$
$$a R_{\mathbb{P}} b \iff \exists A \in \mathbb{P},\ a, b \in A.$$

$$R \longmapsto X/_R, \text{ where}$$
$$X/_R = \{[a]_R \mid a \in X\} \text{ and}$$

$$[a]_R = \{x \in X \mid aRx\}.$$

- Various examples of $X/_\sim$ that are given in the problem sets.

Pigeonhole Principle

How to use it in unexpected places, e.g. Examples presented in the class.

Counting Problems

- $|A \cup B| = |A| + |B| - |A \cap B|$
- $|A \times B| = |A| \cdot |B|$.
- $|A_1 \times A_2 \times \cdots \times A_n| = \prod_{i=1}^{n} |A_i|$.
- # Functions from A to B.
- # injections from A to B.
- $|P(A)|$, $|P_r(A)|$, $\binom{n}{r}$
- Pascal triangle.
- # of positive (non-negative) solutions of $x_1 + \cdots + x_m = n$.

Cardinality of infinite sets.

e.g. • What it means to say two infinite set have the same cardinality.

• Cantor's theorem: For any set X, "X is strictly smaller than its powerset $P(X)$."

[There is no surjection from X to $P(X)$.]

List of mentioned theorems

Induction Principle; Division Algorithm; $\gcd(a,b) = ax+by$; Euclid's Algorithm; Unique Factorization; Euler's thm $\varphi(mn) = \varphi(m)\varphi(n)$ if $(m,n)=1$; Chinese Remainder thm; Wilson's thm; Partitions $\longleftrightarrow$ Equivalence Relations; $|P_r(X)| = \binom{|X|}{r}$; Cantor's Thm.

List of some of the mentioned concepts/notations

$\forall, \exists, \neg, \vee, \wedge, \Rightarrow, \cup, \cap, \Delta, \setminus, \emptyset$, gcd, lcm, well-ordering principle, 1-1, onto, bijective, linear Diophantine equations, $\mathbb{Z}/m\mathbb{Z}$, $X/\sim$, $\binom{n}{r}$, Cardinality.