Inter-IIT Tech Meet Prep

Week 1: Elementary Number Theory

MathSoc IIT Delhi

Contents

1 Well-Ordering Principle and Mathematical Induction

Definition 1.1. *The Well-Ordering Principle states that every non-empty subset of the natural numbers has a least element.*

This principle forms the foundation for proofs involving induction and is equivalent to the principle of mathematical induction.

Theorem 1.2 (Principle of Mathematical Induction)**.** *Let $P(n)$ be a proposition involving a natural number n. Suppose:*

- *$P(1)$ is true (base case),*
- *For all $k \in \mathbb{N}$, if $P(k)$ is true, then $P(k+1)$ is also true (inductive step),*

then $P(n)$ is true for all $n \in \mathbb{N}$.

2 Divisibility and the Division Algorithm

Definition 2.1. *An integer a is divisible by b (denoted $b \mid a$) if there exists an integer k such that $a = bk$.*

Theorem 2.2 (Division Algorithm)**.** *Given integers a and b with $b > 0$, there exist unique integers q and r such that:*

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

3 GCD and Euclidean Algorithm

Definition 3.1. *The greatest common divisor (gcd) of two integers a and b is the largest integer that divides both.*

Theorem 3.2 (Euclidean Algorithm)**.** *The gcd of a and b can be computed by repeatedly applying the division algorithm:*

$$\gcd(a, b) = \gcd(b, a \bmod b).$$

This process terminates when the remainder becomes zero.

4 Prime Numbers and Fundamental Theorem of Arithmetic

Definition 4.1. *A prime number is a natural number greater than 1 that has no positive divisors other than 1 and itself.*

Theorem 4.2 (Infinitude of Primes)**.** *There are infinitely many prime numbers.*

Sketch. Assume finitely many primes $p_1, p_2, \ldots, p_n$. Consider $P = p_1 p_2 \cdots p_n + 1$. This number is not divisible by any p_i, hence either prime or divisible by a new prime. □

Theorem 4.3 (Fundamental Theorem of Arithmetic)**.** *Every integer greater than 1 can be uniquely written as a product of primes, up to the order of the factors.*

5 Special Number Classes

5.1 Triangular Numbers

Definition 5.1. *A triangular number is of the form $T_n = \frac{n(n+1)}{2}$.*

5.2 Square Numbers and Pythagorean Triplets

Definition 5.2. *A* ***Pythagorean triplet*** *is a triple* (a, b, c) *such that* $a^2 + b^2 = c^2$*. Primitive triplets can be generated by:*

$$a = m^2 - n^2, \quad b = 2mn, \quad c = m^2 + n^2, \quad \text{with } m > n, \text{ and } m, n \text{ coprime, not both odd.}$$

5.3 Pentagonal Numbers

Definition 5.3. *A pentagonal number is of the form* $P_n = \frac{3n^2 - n}{2}$*.*

6 Modular Arithmetic and Congruences

Definition 6.1. *We say* $a \equiv b \mod m$ *if* $m \mid (a - b)$*. This defines a congruence relation.*

6.1 Complete and Reduced Residue Systems

A complete residue system mod m is a set of integers containing one representative from each congruence class modulo m. A reduced residue system contains integers coprime to m modulo m.

6.2 Linear Congruences

To solve $ax \equiv b \mod m$, we reduce the problem using the gcd of a and m. If $\gcd(a, m) \mid b$, then solutions exist.

6.3 Chinese Remainder Theorem

Theorem 6.2. *Let* $m_1, \ldots, m_k$ *be pairwise coprime. Then the system:*

$$x \equiv a_i \mod m_i \quad (1 \leq i \leq k)$$

has a unique solution modulo $M = m_1 m_2 \cdots m_k$*.*

6.4 Congruences Modulo a Prime Number

Modular inverses exist modulo a prime p for any number not divisible by p. The set $\{1, 2, \ldots, p-1\}$ forms a multiplicative group mod p.

6.5 Euler's and Fermat's Little Theorem

Theorem 6.3 (Euler's Theorem)**.** *If* $\gcd(a, m) = 1$*, then* $a^{\phi(m)} \equiv 1 \mod m$*.*

Theorem 6.4 (Fermat's Little Theorem)**.** *If* p *is prime and* $a \not\equiv 0 \mod p$*, then* $a^{p-1} \equiv 1 \mod p$*.*

6.6 Wilson's Theorem Application

Theorem 6.5 (Wilson's Theorem)**.** *For a prime* p*,* $(p-1)! \equiv -1 \mod p$*.*

6.7 Hensel's Lemma

Theorem 6.6 (Hensel's Lemma (special case))**.** *Let* $f(x)$ *be a polynomial with integer coefficients. Suppose* x_0 *is a solution modulo* p *and* $f'(x_0) \not\equiv 0 \mod p$*. Then there exists a lift* x_1 *such that* $x_1 \equiv x_0 \mod p$ *and* $f(x_1) \equiv 0 \mod p^2$*.*

7 This Week's Problem

7.1 Euler's Totient Function

Euler's totient function, denoted by $\phi(n)$, is defined as the number of positive integers less than or equal to n that are coprime to n, i.e.,

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

Basic Properties

- If p is a prime number, then
  $$\phi(p) = p - 1,$$
  since all integers $1, 2, \ldots, p-1$ are coprime to p.

- If p is prime and $k \geq 1$, then
  $$\phi(p^k) = p^k - p^{k-1} = p^k\left(1 - \frac{1}{p}\right).$$
  This is because the only numbers not coprime to p^k are those divisible by p, and there are exactly p^{k-1} such numbers in $\{1, 2, \ldots, p^k\}$.

- If m and n are coprime, then Euler's totient function is multiplicative:
  $$\phi(mn) = \phi(m)\phi(n).$$

7.2 Problems

Problem 1: Let n have the prime factorization:

$$n = p_1^{k_1} p_2^{k_2} \cdots p_r^{k_r}.$$

Show using the above properties, that

$$\phi(n) = n\left(1 - \frac{1}{p_1}\right)\left(1 - \frac{1}{p_2}\right)\cdots\left(1 - \frac{1}{p_r}\right).$$

Problem 2: Prove that the sum of all positive integers less than n and relatively prime to n is $\frac{1}{2}n\phi(n)$ if $n > 1$.

Problem 3: Find all positive integers n such that $\phi(n)$ divides n.

Problem 4: If $\phi(mn) = \phi(m)$ and $n > 1$, prove that $n = 2$ and m is odd.

Problem 5: Given natural numbers a, b, c satisfying $\frac{a}{\phi(b)} = \frac{b}{\phi(c)} = \frac{c}{\phi(a)} = \frac{23}{10}$, prove that $a = b = c$.