SHRIHARI BHAT

shrihariabhat@gmail.com

22nd August 2013

RMO WORKSHOP THEORY

NUMBER THEORY

- **Division Algorithm:**
  Given Integers a and b with b >0 $\exists$ unique integers q and r satisfying
  $a = qb + r, 0 \le r < b$.

- **Euclidean Algorithm:**
  Let us denote Greatest Common Divisor of a and b by $\gcd(a,b)$.
  Euclidean Algorithm states that $\gcd(a,b) = \gcd(b,r)$ where r is the remainder as described in Division algorithm.

- **Bezout's Identity:**
  $\forall a,b \in N \quad \exists s,t \in Z$ such that $\gcd(a,b) = sa + tb$

- **Theorem:**
  $\gcd(a,b)lcm(a,b) = ab$

- **The Linear Diophantine Equation**
  $ax + by = c$ has solution iff $d \mid c$ where $d = \gcd(a,b)$. If x_0 and y_0 is any particular solution of this equation then other solutions are given by
  $x = x_0 + \frac{b}{d}t$ and $y = y_0 - \frac{a}{d}t$ where t is an arbitrary integer.

- **Fundamental Theorem of Arithmetic:**
  Every positive integer greater than 1 can be expressed as a product of primes and this representation is unique ignoring the order in which the factors appear.

- **Theorem (Euclid):**
  There are infinitely many primes.

- **Theorem(Dirichlet):**
  If a and b are relatively prime positive integers then the arithmetic progression a, a+b, a+2b, a+3b,….. contains infinitely many primes.

- **Congruences:**
  Let n be a positive integer. We say that $a \equiv b \pmod{n}$ (read as a congruent to b mod n) iff $n \mid (a-b)$.

- **Theorem:**
  The linear congruence $ax \equiv b \pmod{n}$ has a solution iff $d \mid b$ where d is gcd(a,n). If $d \mid b$ then it has d mutually incongruent solutions modulo n.

- **Chinese Remainder Theorem:**
  Let $n_1, n_2 ..... n_r$ be positive integers such that $\gcd(n_i, n_j) = 1$ for $i \neq j$. Then the system of r equations $x \equiv a_i \pmod{n_i}, 1 \leq i \leq r$ has a simultaneous solution which is unique modulo the integer $\prod_{i=1}^{r} n_i$.

- **Fermat's Little Theorem:**
  Let p be a prime number and if p does not divide a then $a^{p-1} \equiv 1 \pmod{p}$.

- **Wilson's Theorem:**

  If p is a prime, then $(p-1)! \equiv -1 \pmod{p}$.

- **Number Theoretic Functions:**
  $\tau(n)$ is the number of all positive divisors of n.
  $\sigma(n)$ is the sum of all these divisors.
  $\phi(n)$ is the number of positive integers not exceeding n that are relatively prime to n.

- **Computing Number Theoretic Functions:**

  If $n = \prod_{i=1}^{r} p_i^{\alpha_i}$ then

  $$\tau(n) = \prod_{i=1}^{r} (k_i + 1)$$

  $$\sigma(n) = \prod_{i=1}^{r} \left(\frac{p_i^{k_i+1} - 1}{p_i - 1} \right)$$

  $$\phi(n) = N \prod_{i=1}^{r} \left(1 - \frac{1}{p_i} \right)$$

- **Euler's Generalisation of Fermat's Theorem:**
  Let n be a natural number and $\gcd(a,n) \equiv 1$ then $a^{\phi(n)} \equiv 1 (\bmod n)$.

- **Fermat's Last Theorem(Proof is very Easy ☺)**
  The Diophantine equation $a^n + b^n = c^n, n > 2$ has no solutions.

Problems

- Find $\gcd(12378, 3054)$ using Euclidean Algorithm. Also write the gcd as a combination of a and b.

- Solve the Diophantine Equation $172x + 20y = 1000$.

- If all the terms of the arithmetic progression p,p+d,p+3d,…..,p+(n-1)d are primes then prove that the common difference d is divisible by every prime q<n.

- Find the remainder when $\sum_{i=1}^{100} i!$ is divided by 12.

- Prove that if a is an odd number and n is a natural number we have $a^{2^n} \equiv 1 (\bmod 2^{n+2})$.

- If a, b, c are natural numbers and $a \mid b^3$, $b \mid c^3, c \mid a^3$ then prove that $abc \mid (a+b+c)^{13}$.

- Solve the system of equations simultaneously using Chinese Remainder Theorem.
$$x \equiv 2 (\bmod 3)$$
$$x \equiv 3 (\bmod 5)$$
$$x \equiv 2 (\bmod 7)$$

- Find $\phi(n)$ given that $n = \prod_{i=1}^{k} p_i^{\alpha_i}$ where all p_i are prime numbers. Thus find $\phi(2013), \phi(36000)$.

- Characterize all solutions to the Pythagorean Diophantine Equation $a^2 + b^2 = c^2$

BOOK FOR REFERENCE:

Elementary Number Theory by David M Burton

Introduction to the Theory Of Numbers by Niven & Zuckerman