Number Theory

1. The Peano axioms

The entire formalization of arithmetic is based on five fundamental axioms, called **Peano axioms**, which define properties of natural numbers. These axioms are -

(i) 0 is a natural number
(ii) Every natural number has a successor, which is also a natural number
(iii) 0 is not the successor of any natural number
(iv) Different natural numbers have different successors
(v) If a set contains the number 0 and it also contains the successor of every number in S, then S contains every natural number.

The fifth axiom is also popularly known as "principal of mathematical induction"

Being extremely basic, we would rarely need them directly, unless we want to prove every theorem in arithmetic from the first principles. But being the building blocks of arithmetic, these axioms are worth knowing.

2. Fundamental Theorem of Arithmetic and the Division Algorithm

As the name rightly says, this theorem lies at the heart of all the concepts in number theory. The fundamental theorem of arithmetic states that any integer greater than 1 can be written as a product of prime numbers in a unique way (up to the ordering of prime factors in the product). For example, 18 = 2 X 3^2, 1755 = 3^3 X 5 X 13. This theorem plays very important role in almost every number theoretic algorithm, like finding prime factors, finding GCD, finding sum of divisors of a number etc to mention a few. Proving this theorem is easy - in fact, it emerges out as a corollary to the Euclid's first theorem (discussed below).

The division algorithm states that given two integers a, b (b != 0) there exist two unique integers q and r such that

a = bq + r, 0 <= r < b

q is typically called quotient, whereas r is called remainder. If r = 0, we say that b divides a, and denote it as b|a.

3. Euclid's Theorems

The two important theorems, called "Euclid's first theorem (Or Euclid's lemma)" and "Euclid's second theorem (usually simply referred as "Euclid's theorem") are as follows:
First theorem: p is a prime and $p|ab \Rightarrow p|a$ or $p \mid b$. A direct consequence of this is the fundamental theorem of arithmetic.

Second theorem: There are infinitely many primes. There are many simple proofs for this.
While it is true that there are infinitely many primes, it should also be remembered that there are arbitarily large gap between prime numbers. In other words, it is always possible to get a sequence of n consecutive composite numbers, given n.

4. GCD, LCM, Bezout's identity

The most common algorithm for finding the greatest common divisor of two numbers is the **Euclid's algorithm.** This is an extremely efficient algorithm, as the number of steps required in this algorithm is at most 5 times the number of digits of the smaller number. GCD is typically denoted using round brackets - (a, b) denotes the gcd of a and b. Similarly LCM is denoted using square brackets - [a, b] denotes the lcm of a and b.

The numbers a and b are called coprimes iff (a, b) = 1, i.e. iff [a, b] = ab.
If gcd(a, b) = d then (a/d, b/d) = 1.

GCD and LCM are related by a very simple equation: (a, b) * [a, b] = ab. This gives a very fast way to calculate LCM of two numbers.

The bezout's identity states that if d = (a, b) then there always exist integers x and y such that ax + by = d. (Of course, the theory of linear diophantine equations assures existance of infinitely many solutions, if one exists). It is also worth noting that k=d is the smallest positive integer for which ax + by = k has a solution with integral x and y.

Given a, b, finding x and y, such that ax + by = d is done by extended Euclid's algorithm, which can be implemented in recursive as well as iterative styles.

5. Integer Factorization

The most commonly used algorithm for the integer factorization is the **Sieve of Eratosthenes**. It is sufficient to scan primes upto sqrt(N) while factorizing N. Also, if we need to factorize all numbers between 1 to N, this task can be done using a single run of this algorithm - For every integer k between 1 to N, we can maintain a single pair - the smallest prime that divides k, and its highest power, say (p,a). The remaining prime factors of k are then same as that of k/(p^a).

6. Linear Congruence Equations

The equations of the form ax ≡ b (mod n) where (x is an unknown integer) are called **linear congruences**. Such a congruence will have a solution if and only if there exists an integer x such that n | (ax-b), i.e. ax -b = ny for some integer y, or in other words ax + n(-y) = b.

We already know from Bezout's identity that a linear diophantine equation like this will have a solution only if gcd of (a,n), say d, divides b. In such a case, let b = dd', a = da', n = dn', so we have: da'x + dn'(-y) = dd' where gcd(a',n') = 1

Cancelling d throughout,
$a'x + n'(-y) = d'$.

since gcd of $(a', n') = 1$, now we can use Extended Euclid's algorithm to find the solution for $a'x + n'(-y) = 1$. and then multiply this solution by d' to get a solution for $a'x + n'(-y) = d'$.

7. Chinese Remainder Theorem

Typical problems of the form "Find a number which when divided by 2 leaves remainder 1, when divided by 3 leaves remainder 2, when divided by 7 leaves remainder 5" etc can be reformulated into a system of linear congruences and then can be solved using Chinese Remainder theorem. For example, the above problem can be expressed as a system of three linear congruences: "$x \equiv 1 \pmod 2$, $x \equiv 2$ mod(3), $x \equiv 5$ mod (7)".

In general, a system of linear congruences:
$x \equiv a1 \pmod{n_1}$
$x \equiv a2 \pmod{n_2}$
$x \equiv a3 \pmod{n_3}$
....
$x \equiv ak \pmod{n_k}$

where $(n_i,n_j) = 1$ for every n_i != n_j has a unique solution modulo n where $n = n_1n_2n_3...n_k$.
Let $c_i= n/n_i$ for every i. Let d_i be the solution for the congruence cix = 1 (mod ni) such that $0 <= d_i < n_i$. (This solution can be found out using Extended Euclid's algorithm). Then the common solution to the above system of linear equations is given by
$c = a_1c_1d_1 + a_2c_2d_2 + ... + a_kc_kd_k$

A direct corollary of the Chinese Remainder theorem is as follows: Let $n = p_1{}^a{}_1 * p_2{}^a{}_2 * .... * p_k{}^a{}_k$ be the prime factorization of n. Then, for any integers a and b, we have a = b (mod n) iff a = b (mod $p_i{}^a{}_i$) for each i.
The generalization of the Chinese Remainder Theorem, which discusses the case when the ni's are not necessarily pairwise coprime is as follows - The system of linear congruences

$x \equiv a1 \pmod{n_1}$
$x \equiv a2 \pmod{n_2}$
$x \equiv a3 \pmod{n_3}$
....
$x \equiv ak \pmod{n_k}$

has a solution iff $\gcd(n_i ,n_j)$ divides $(a_i -a_j)$ for every i != j. In such a case, there is a unique solution mod n, where n is the least common multiple of n_1, n_2 ...n_k

8. Quadratic Congruences

Given q and n, if the quation $x^2 \equiv q \pmod n$ has a solution, then q is called **quadratic residue** modulo n. If this equation doesnot have a solution, then q is called "quadratic non residue" modulo

n. For example, $x^2 \equiv 9 \pmod{15}$ has a solution x = 12, hence 9 is a quadratic residue modulo 15. On the other hand, the equation $x^2 \equiv 11 \pmod{15}$ has no solution, hence 11 is a quadratic non-residue modulo 15. In simpler terms, an integer q is a quadratic residue modulo n if a square can take the form (nk + q) for some positive integer n.

Finding whether a quadratic congruence having prime number modulus has a solution or not is somewhat easy: $x^2 \equiv a \pmod{p}$ has a solution only if $a^{(p-1)/2} = 1 \pmod{p}$. In such a case, the Shank-Tonelli algorithm can be used to get the solution.

9. Divisibility

1) Definition

a) If $a \neq 0$, b are integers, we say that a *divides* b if there is an integer c such that $ac = b$. We write this as $a \mid b$. If a does not divide b we write a †b.

b) A *prime* number p is a positive integer greater than 1 whose only positive divisors are 1 and p. If the integer $n > 1$ is not prime, then we say that it is *composite.*

For example, 2, 3, 5, 7, 11, 13, 17, 19 are prime, 4, 6, 8, 9, 10, 12, 14, 15, 16, 18, 20 are composite. The number 1 is neither a prime nor a composite.

2) Divisibility Theorems

a) If a, b, c, m, n are integers with $c \mid a$, $c \mid b$, then $c \mid (am + nb)$.
Proof: *There are integers s, t with* $sc = a$, $tc = b$. *Thus* $am + nb = c(sm + tn)$, *giving* $c \mid (am + bn)$.

b) If x, y, z are integers with $x \mid y$, $y \mid z$ then $x \mid z$.

Proof: *There are integers u, v with* $xu = y$, $y v = z$. *Hence* $xuv = z$, *giving* $x \mid z$.

It should be clear that if $a \mid b$ *and* $b \neq 0$ *then* $1 \le | a | \le | b |$.

c) If N, d are positive integers, then there are unique integers q, r such that $N = dq + r$, $0 \le r < b$.

For $N = 58, d = 7$, we obtain $q = 8$ *and* $r = 2$
$58 = 7 \times 8 + 2$

d) The number of factors, including 1 and the number itself, of any natural number

$N=p_1^{\alpha_1} \cdot p_2^{\alpha_2} \cdot p_3^{\alpha_3} \cdots p_k^{\alpha_k} \cdots$, where p_1, p_2 etc. are the prime factors of N is given by
$(\alpha_1 +1)(\alpha_2 +1)(\alpha_3 +1)\cdots(\alpha_k +1)$.

3) Divisibility Formula

$x^n - y^n = (x - y)(x^{n-1} + x^{n-2}y + x^{n-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$

Thus $x - y$ always divides $x^n - y^n$.

$x^n + y^n = (x + y)(x^{n-1} - x^{n-2}y + xn^{-3}y^2 + \cdots + xy^{n-2} + y^{n-1})$

Thus if n is odd, $x + y$ divides $x^n + y^n$.

4) Divisibility results

1). An integer is divisible by 2 if and only if its units digit is divisible by 2.

2). An integer is divisible by 4 if and only if the number formed by its last two digits is divisible by 4.

3). An integer is divisible by 8 if and only if the number formed by its last three digits is divisible by 8.

4). An integer is divisible by 3 if and only if the sum of the digits is divisible by 3.

5). An integer is divisible by 5 if and only if its units digit is divisible by 5.

6). An integer is divisible by 9 if and only if the sum of the digits is divisible by 9.

7). An integer is divisible by 11 if and only if the difference between the sum of the digits in the odd places and the sum of digits in the even places is divisible by 11. For the integer 9174825 is divisible by 11 since (9+7+8+5) – (1+4+2) = 22 and 22 is divisible by 11.

10. Number of factors

1). If a number N is divided by a divisor d to give a quotient q and a remainder r, then $N = dq + r$

For example $N = 58$, $d = 7$, we obtain $q = 8$ *and* $r = 2$

$58 = 7 \times 8 + 2$

2). The number of factors, including 1 and the number itself, of any natural number

$\mathrm{N}=\mathrm{p}_1^{\alpha_1} \cdot \mathrm{p}_2^{\alpha_2} \cdot \mathrm{p}_3^{\alpha_3} \cdots \mathrm{p}_k^{\alpha_k} \cdots$, where p_1, p_2 etc. are the prime factors of N is given by

$(\alpha_1 + 1)(\alpha_2 + 1)(\alpha_3 + 1) \cdots (\alpha_k + 1)$.

11. Modulus

1) We write $a \equiv b$ (mod m) (a is congruent to b modulus m) if and only if $m \mid a - b$, which means that a and b have the same remainder upon division by m. For example 17 = 3 (mod 7) since 7 | (17 – 3). Congruences can be added, subtracted, and multiplied.

a. If $a \equiv b$ (mod m) and $c \equiv d$ (mod m) then a ± c ≡ b ± d (mod m) and $ac \equiv bd$ (mod m).

b. a ≡ b (mod m) then $a^k \equiv b^k$ (mod m) and hence $f(a) \equiv f(b)$ (mod m) for every polynomial f with integer coefficients.

2) We must be very careful with division of congruences since it is not always possible to divide congruences. For example $5{\bullet}2 \equiv 10{\bullet}2$ (mod 10), but $5 \not\equiv 10$ (mod 10).
Even more distressing, it is possible to have $ab \equiv 0$ (mod m) with $a \not\equiv 0$ (mod m) and b $\not\equiv 0$ (mod m). For example, 3 x 4 = 0 (mod 6), while clearly 3 $\not\equiv$ 0 (mod 6) and 4 $\not\equiv$ 0(mod 6).

a. Cancellation Rule: If $ac \equiv bc$ (mod m) and gcd(m, c) = 1 then $a \equiv b$ (mod m).

We will show that an integer is divisible by 9 if and only if the sum of its digits is divisible by 9

Let $n = a_k 10^k + a_{k-1}10^{k-1} + \ldots + a_1 10 + a_0$ be the decimal expansion of n.

Since $10 \equiv 1(\text{mod } 9) \Rightarrow 10^k \equiv 1(\text{mod } 9)$, so $a_j 10^j \equiv a_j (\text{mod } 9)$ Summing over $0 \le j \le k$ we get:

$n = \sum_{j=0}^{k} a_j 10^j \equiv \sum_{j=0}^{k} a_j (\text{mod } 9)$, hence, n and the sum of its digits have the same remainder when divided by 9.

In class questions

1. Prove the following result of Euler: $641 \mid \left(2^{32}+1\right)$.

2. Prove that $7 \mid \left(2222^{5555} + 5555^{2222}\right)$.

3. Find the units digit of 7^{7^7}.

4. Find infinitely many integers n such that $2^n + 27$ is divisible by 7.

5. Are there positive integers x, y such that $x^3 = 2^y + 15$?

6. Prove that $2^k - 5,\ k = 0,\ 1,\ 2,\ ...$ never leaves remainder 1 when divided by 7.

7. Let $a_1 = 4,\ a_n = 4^{a_{n-1}}$, $n > 1$. Find the remainder when a_{100} is divided by 7.

8. Prove that if p is an odd prime and if $a / b = 1 + 1/2 + \cdots + 1/\left(p-1\right)$, then p divides a.

9. Show that $2903^n - 803^n - 464^n + 261^n$ is divisible by 1897 for all natural numbers n.

10. Find how many positive integers n have the property that $\sqrt{(n!)^2 + 13}$ is an integer, where $n! = 1 \cdot 2 \cdot 3 \cdots n$.