Number Theory needed for I.S.I. and C.M.I. entrance

Srijan Chatterjee

$\mathbb{N}$=set of natural numbers $\{1,2,3 \dots \dots .\}$

$\mathbb{N} \cup \{0\}$=set of whole numbers $\{0,1,2, \dots \dots\}$

$\mathbb{Z}$=set of integers $\{\dots \dots \dots ., -2, -1,0,1,2, \dots \dots \dots\}$

$\mathbb{Q}$=set of rational numbers $\left\{\frac{p}{q} : p \in \mathbb{Z}, q \in \mathbb{N}; \gcd(p,q) = 1\right\}$

$\mathbb{R}/\mathbb{Q}$=set of irrational numbers

- Prove that, $\sqrt{m}$ is an irrational number where m is a non-square integer.
- r^r, r^i, i^r, i^i all may be both rational and irrational (r=rational, i=irrational). [try to find examples]

$$\mathbb{N} \subset \mathbb{Z} \subset \mathbb{R} \subset C$$

Well ordering principle: Any subset of natural number has a minimum element.

Mathematical induction:

A) If some statement is true at some preliminary steps, and assuming it to be true at some m^{th} stage, if we can show it to be true for $(m+1)^{th}$ stage, then it will be true for all natural numbers.

B)(Strong form) In spite of assuming it to be rue for only m, we assume it to be true for $n = 1,2, \dots \dots, m$.

Some problems on mathematical induction:

1) $1 + 2 + \cdots + n = \frac{n(n+1)}{2}$.

2) $1^2 + 2^2 + \cdots + n^2 = \frac{n(n+1)(2n+1)}{6}$

3) $1^3 + 2^3 + \cdots + n^3 = \left[\frac{n(n+1)}{2}\right]^2 = (1 + 2 + \cdots + n)^2$

4) $1 + 3 + 5 + \cdots + (2n - 1) = n^2$

5) $1.1! + 2.2! + \cdots + n.n! = (n + 1)! - 1$

6) $\sqrt{1 + \frac{1}{1^2} + \frac{1}{2^2}} + \sqrt{1 + \frac{1}{2^2} + \frac{1}{3^2}} + \cdots + \sqrt{1 + \frac{1}{n^2} + \frac{1}{(n+1)^2}} = \frac{n(n+2)}{n+1}$

7) $\frac{1}{2}.\frac{3}{4}.\frac{5}{6}\ldots\frac{2n-1}{2n} \leq \frac{1}{\sqrt{2n+1}}$

8) $\frac{1}{2}.\frac{3}{4}.\frac{5}{6}\ldots.\frac{2n-1}{2n} \leq \frac{1}{\sqrt{3n+1}}$

Divisibility:

$'a'$ divides $'b'$ is denoted by $a|b$.

Properties:

i) $a|b, b|c, then\ a|c$

ii) $a|b, a|c, then\ a|bx + cy\ [x, y \in \mathbb{Z}]$

iii) $a|b, c|d, then\ ac|bd$.

iv) $a|b, x|b, if\ \gcd(a, x) = 1, then\ ax|b$. But the reverse is not always true.

Some preliminary problems on divisibility:

1) $d = \gcd(n^2 + 20, (n + 1)^2 + 20)\ , n \in \mathbb{N}$. Show that $d|81$.

2) $d_n = \gcd(n^3 + n^2 + 1, n^3 + n + 1)\ , n \in \mathbb{N}$.Find $d_{3^{2022}}$.

3)Prove that $5|3^{2008} + 4^{2009}$

Cyclicity of numbers:

For 2, the last digits of power returns as (2,4,8,6). It is cycle of order 4. Same for 3, the cycle is (3,9,7,1)

Some Theorems:

i) $a, b \in \mathbb{Z}$, and they are distinct. Then $(a-b)|(a^n - b^n)$.

ii) $a, b \in \mathbb{Z}, a + b \neq 0, then\ (a+b)|(a^n + b^n)\ \forall n \in \mathbb{N}$.

iii) There are infinitely many primes [a prime is that number which is exactly 2 divisors]

Some problems:

1) $133|11^{n+2} + 12^{2n+1}$.

2) $k = 1^{3017} + 2^{3017} + \cdots + 200^{3017}$. Prove that $40200|k$.

3)Find all $n \in \mathbb{N}$, such that $(n-3)|(n^3 - 3)$.

Euclidean Algorithm:

Steps of divisors:

$$b = aq_1 + r_1$$
$$a = r_1q_2 + r_2$$
$$r_1 = r_2q_3 + r_3$$
$$\vdots$$
$$r_{n-2} = r_{n-1}q_n + r_n$$
$$r_{n-1} = r_nq_{n+1}$$

Then $\gcd(a, b) = r_n$.

Bezout's Lemma:

$a, b \in \mathbb{N}, \gcd(a,b) = d. Then\ \exists x, y \in \mathbb{Z}$, such that $ax + by = d$.

Some problems:

1)Suppose $ax_0 + by_0 = d$, where $d = \gcd(a,b)$. Is (x_0, y_0) unique?
2)Prove that there exists infinitely many pairs of natural numbers such that they are consecutive and each is not square free.

Necessary condition for existence of a linear Diophantine in 2 variables:

$d = \gcd(a,b)$. Now if $ax + by = c$. The necessary condition for solution to exist is $d|c$.

Congruence:

If $m|(a-b)$, then $a \equiv b(mod\ m)$.

- $a \equiv b + mk(mod\ m), \forall k \in \mathbb{Z}$
- $ca \equiv cb(mod\ m)\ \forall c \in \mathbb{Z}$
- Modulus is equivalence relation.
- $a \equiv a(mod\ m)$[reflexive]
- $a \equiv b(mod\ m) \Leftrightarrow b \equiv a(mod\ m)$[symmetric]
- $a \equiv b(mod\ m), b \equiv c(mod\ m) \Rightarrow a \equiv c(mod\ m)$
- $a \equiv b(mod\ m), c \equiv d(mod\ m) \Rightarrow a + c \equiv b + d(mod\ m), ac \equiv bd(mod\ m)$
- $a \equiv b(mod\ m) \Rightarrow a^n \equiv b^n(mod\ m)$
- $ka \equiv kb(mod\ m), \gcd(m,k) = 1 \Rightarrow a \equiv b(mod\ m)$

Fermat's Theorem:

$a, p \in \mathbb{N}, p\ is\ prime, \gcd(a,p) = 1$. Then $a^{p-1} \equiv 1(mod\ m)$

Inverse w.r.t. modulo:

$a, m \in \mathbb{N}$, suppose $ka \equiv 1(mod\ m), k \in \mathbb{Z}$. Them k is the inverse of a modulo m.

The necessary condition for existence of inverse is $\gcd(a,m) = 1$.

Wilson's Theorem:

P is prime iff $p|(p-1)! + 1$.

Order of a number modulo:

$a, m \in \mathbb{N}, \gcd(a,m) = 1$. The lowest k such that

$a^k \equiv 1(mod\ m)$ is called the order of a w.r.t. m or $Ord_m(a)$.

- If $a, m \in \mathbb{N}, a^k \equiv 1(mod\ m)$. Then $Ord_m(a)|k$.

Complete Residue system(CRS):

$m \in \mathbb{N}, \{a_1, a_2, \dots, a_n\}$ is a CRS w.r.t. m if

$a_i \not\equiv a_j(mod\ m)\ \forall i \neq j$.

Reduced Residue system(RRS):

$m \in \mathbb{N}, \{a_1, a_2, \dots, a_n\}$ is a RRS w.r.t. m if $\gcd(a_i, m) = 1\ \forall i$

$\&\ a_i \equiv a_j(mod\ m)\ \forall i \neq j$.

Euler's Totient function:

$\boldsymbol{\phi}(m) =$ number of natural numbers less than m and co-prime to m. Note that, $\emptyset(p) = p - 1$ if p is prime.

Euler's Theorem:

$a, m \in \mathbb{N}, \gcd(a, m) = 1$. Then $a^{\emptyset(m)} \equiv 1 (mod\ m)$.

Note that, fermat's theorem is a special case of this.

- Let the divisors of n be $1 = d_1 < d_2 < \cdots < d_k = n$. Then $\emptyset(d_1) + \emptyset(d_2) + \cdots + \emptyset(d_k) = n$.

Highest power of a prime p in n! :

$$\left\lfloor \frac{n}{p} \right\rfloor + \left\lfloor \frac{n}{p^2} \right\rfloor + \left\lfloor \frac{n}{p^3} \right\rfloor + \cdots$$

Pythagorean Triples:

(a, b, c) is called a Pythagorean triple if $a^2 + b^2 = c^2$. A Pythagorean triple (a, b, c) is called primitive if

$$\gcd(a, b) = 1.$$

- $\gcd(a, b) = \gcd(a, c) = \gcd(b, c)$
- For a primitive triple, c is always odd, i.e. a, b are of opposite parity.
- $4|a\ or\ 4|b, 60|abc, 3|ab$.

Some problems:

1) Let x_n denotes the n^{th} non square positive integer. Then $x_1 = 2, x_2 = 3, x_3 = 5, x_4 = 6\ etc$. For a positive real number x, denote the integer closest to it by <x> If x=m+0.5, where m is an integer, then <x>=m. Eg. <1.2> = 1, <2.8> = 3, <3.5> = 3. Show that $x_n = n + < \sqrt{n} >$

2) Let p be a prime number bigger than 5. Suppose the decimal expansion of $\frac{1}{p}$ looks like $0.\overline{a_1 a_2 \ldots a_r}$ where the line

denotes a recurring decimal. Prove that 10^r leaves a remainder of 1 on dividing by p.

3) Let a, b, c, d be integers such that $ad - bc \neq 0$. Suppose b_1, b_2 are integers both of which are multiples of $ad - bc$. Prove that there exists integers simultaneously satisfying both the equations $ax + by = b_1, cx + dy = b_2$.

4) Consider the equation $n^2 + (n+1)^4 = 5(n+2)^3$.
A) Show that, any integer of the form $3m + 1$ or $3m + 2$ cannot be a solution of this equation.
B) Does the equation have a solution in positive integers?

5) Show that, for any positive integer n, the sum of 8n+4 consecutive positive integers cannot be a perfect square.

6) A) Show that there cannot exist three prime numbers, each greater than 3, which are in arithmetic progression with a common difference less than 5.

B) Let k>3 be an integer. Show that it is not possible for k prime numbers, each greater than k, to be in arithmetic progression with a common difference less than or equal to k+1.

7) For any real number x, let $[x]$ denote the largest integer less than or equal to x. Let $N_1 = 2, N_2 = 3, N_3 = 5$ be the sequence of non-square positive integers. If $m^2 < N_n < (m+1)^2$ then show that $m = [\sqrt{n} + \frac{1}{2}]$

8) Let R and S be two cubes with sides of lengths r and s respectively, where r and s are positive integers. Show that

the difference of their volumes equals the difference of their surface areas, iff $r = s$.

9) Let m be a natural number with digits consisting entirely of 6's and 0's. Prove that m is not the square of a natural number.

10) Let N be a positive integers such that $N(N - 101)$ is the square of a positive integer. Then determine all possible values of N. [Note that 101 is prime]

11) Show that the sum of 12 consecutive integers can never be a perfect square. Give an example of 11 consecutive integers whose sum is a perfect square.

12) Consider (n>1) lotus leaves placed around a circle. A frog jumps from one leaf to another in the following manner. It starts from one selected leaf. From there, it skips exactly one leaf in the clockwise direction and jumps to the next one. Then it skips exactly two leaves in the clockwise direction and jumps to the next one. Then it skips three leaves again in the clockwise direction and jumps to the next one, and so on. Notice that the frog may visit the same leaf more than once. Suppose it turns out that if the frog continues this way, then all the leaves are visited by the frog sometime or the other. Show that n *cannot* be odd.

13) Find all positive integers n for which $5^n + 1$ is divisible by 7. Justify your answer.

14) 1.Let $m_1 < m_2 < \cdots < m_k$ be positive integers $\frac{1}{m_1}, \frac{1}{m_2}, \ldots, \frac{1}{m_k}$ are in arithmetic progression. Then prove that $k < m_1 + 2$.

2. For any integer k > 0, give an example of a sequence of k positive integers whose reciprocals are in arithmetic progression.

15) Let d be a positive integer. Prove that there exists a right-angled triangle with rational sides and area equal to d if and only if there exists an arithmetic progression x^2, y^2, z^2 of squares of rational numbers whose common difference is d.

16) Let $g: \mathbb{N} \to \mathbb{N}$ with $g(n)$ being the product of the digits of n.

A)Prove that $g(n) \leq n$ for all natural number n.

B)Find all $n \in \mathbb{N}$, for which $n^2 - 12n + 36 = g(n)$.

17) Let $a, b, c \in \mathbb{N}$ be such that

$$a^2 + b^2 = c^2 \; and \; c - b = 1.$$

Prove that

i) a is odd.

ii) 4 | b.

iii) $c | a^b + b^a$

18) If $a \equiv b (mod\ m^n)$, then prove that

$$a^m \equiv b^m (mod\ m^{n+1})$$

For $a, b, c, d \in \mathbb{N}$

19) Find the remainder when 2^{1990} is divided by 1990.

20) Prove that $\frac{k^7}{7} + \frac{k^5}{5} + \frac{2k^3}{3} - \frac{k}{105} \in \mathbb{Z}, \forall k \in \mathbb{N}$.

21) p, q are distinct primes. Prove that

$$p^{q-1} + q^{p-1} \equiv 1(mod\ pq)$$

22) Find the last 3 digits of 7^{9999}

23) Solve for $n - \emptyset(n) = 8, n \in \mathbb{N}$.

24) $\forall n \in \mathbb{N}, S(n)$ denotes number of ordered pairs (x,y) of positive integers for which $\frac{1}{x} + \frac{1}{y} = \frac{1}{n}$. Determine the set of positive integers for which $S(n) = 5$.

25) Is a there any natural number n such that when written in base ten will end with exactly 2022 zeros?

26) Prove that there exist 100 consecutive natural numbers such that exactly 3 of them are prime.

27) Prove that the positive integers n that can-not be written as a sum of r consecutive positive integers with r>1 are of the form $n = 2^l, l \geq 0$.

28) Consider a right-angled triangle with integer-valued sides a<b<c where a, b, c are pairwise co-prime. Let d=c−b. Suppose d divides a. Then
(a) Prove that $d \leq 2$.
(b) Find all such triangles (i.e. all possible triplets (a, b, c)) with perimeter less than 100.

29) Prove that every positive rational number can be expressed uniquely as a finite sum of the form

$$a_1 + \frac{a_2}{2!} + \frac{a_3}{3!} + \cdots + \frac{a_n}{n!},$$

Where a_n are integers such that $0 \leq a_n \leq n - 1\ \forall n > 1$.

30) A function $f(n)$ defined on the set of positive integers is said to be multiplicative if $f(mn) = f(m)f(n)$ whenever m and n have no common factors greater than 1. Are the following functions multiplicative? Justify your answer.

a)$g(n) = 5^k$, where k is the number of distinct primes that divide n.

b)

$$h(n) = \begin{cases} 0 \; if \; n \; is \; divisible \; by \; k^2 \; for \; some \; integer \; k > 1 \\ 1 \; otherwise \end{cases}$$

31) Suppose that a is an irrational number.

a) If there is a real number b such that $(a + b)$ & ab are rational numbers, show that a is quadratic surd. (a is a quadratic surd if it is of the form $r + \sqrt{s} \; or \; r - \sqrt{s}$ for some rationals r and s, where s is not the square of a rational number).

b) Show that there are two real numbers b_1 & b_2 such that

i) $a + b_1$ is rational but ab_1 is irrational.

ii)$a + b_2$ is irrational but ab_2 is rational.

[Hint: Consider two cases, where a is a quadratic surd and not a quadratic surd respectively.]

32) Show that $4^n + n^4$ is composite $\forall n > 1, n \in \mathbb{N}$.

33) Find a four digit number M such that the number $N = 4 \times M$ has the following properties:

a) N is also a four-digit number.

b) N has the same digits as in M, but in the reverse order.

34) Let A be the set of integers satisfying the following properties:

i) if $m, n \in A, then\ m + n \in A$.

ii) there is no prime number that divides all elements of A.

a) Suppose $n_1\ and\ n_2$ be two integers belonging to A such that $n_2 - n_1 > 1$. Show that you can find two integers m_1, m_2 in A such that $0 < m_2 - m_1 < n_2 - n_1$.

b) Hence show that there are two consecutive integers belonging to A.

c) Let $n_0, n_0 + 1 \in A$. Show that if $n \geq n_0^2$, then $n \in A$.

35) Suppose S is the set of all positive integers. For $a, b \in S$, define $a * b = \frac{lcm(a,b)}{\gcd(a,b)}$. For example, $8 * 12 = 6$. Show that exactly two of the following three properties are satisfied:

A) If $a, b \in S, then\ a * b \in S$.

B)$(a * b) * c = a * (b * c)\ \forall a, b, c \in S$.

C)There exists an element $i \in S$, such that

$$a * i = a\ \forall a \in S$$

36) Let S be the set of integers k, $1 \leq k \leq n$, such that $\gcd(k, n) = 1$. What is the arithmetic number of integers in S?

37) Let n be a positive integer. If n has odd number of divisors (including 1 and n), then show that n is a perfect square.

38) Let a and b be two non-zero rational numbers such that the equation $ax^2 + by^2 = 0$ has a nonzero solution in rational numbers. Prove that for any rational number t, there is a solution of the equation $ax^2 + by^2 = t$.

39) Let $a_1, a_2, \ldots\ldots a_n$ be integers. Show that there exist integers k and r such that the sum $a_k + a_{k+1} + \cdots\ldots\ldots a_{k+r}\ is\ divisible\ by\ n$.

40) Let $a^2 + b^2 = 1,\ c^2 + d^2 = 1, ac + bd = 0$. Prove that $a^2 + c^2 = 1,\ b^2 + d^2 = 1, ab + cd = 0$.

41) If p is a prime number and a > 1 is a natural number. Then show that the g.c.d. of the two numbers $(a - 1)$ & $\frac{a^p - 1}{a-1}$ is either 1 or p.

42) Let $n \geq 2$ be an integer. Let m be the largest integer which is less than or equal to n, and which is a power of 2. Put l_n= least common multiple of 1,2,…,n. Show that $\frac{l_n}{m}$ is odd, and that for every integer $k \leq n, k \neq m, \frac{l_n}{k}$ is even. Hence, prove that $1 + \frac{1}{2} + \frac{1}{3} + \cdots + \frac{1}{n}$ is not an integer.