4-Day Training Camp for INMO

December 17-20, 2018

Dr. M. A. Khanday

Department of Mathematics

University of Kashmir, Srinagar

khanday@uok.edu.in

URL: maths.uok.edu.in/mak.aspx

Organized by

Department of Mathematics, University of Kashmir, Srinagar

and funded by

National Board for Higher Mathematics, Department of Atomic Energy

Quotes

- The mathematics is not there till we put it there. . **Arthur Edington**
- If I were again beginning my studies, I would follow the advice of Plato and start with mathematics. **Galileo Galilei**
- The essence of Mathematics is not to make simple things complicated but vice versa. **S. Gudder**

https://www.google.co.in/url?sa=i&source=images&cd=&cad=rja&uact=8&ved=2ahUKEwjOylq25qTfAhXLWisKHf_hAGYQjhx6BAgBEAM&url=https%3A%2F%2Fblog.oureducation.in%2Fmaths-olympiad%2F&psig=AOvVaw2w8V8S_UqaWRxLbEyTvqHd&ust=1545064911477385

Number Theory

Introduction:

- Theory of Numbers is that branch of mathematics which deals with the properties of whole numbers.

History:

- Oldest branch of mathematics.
- History shows that 5700 BC Sumerians kept the calendar for counting numbers (Arithmetic's).

Z, W and N

- Set of integers

  Z = { . . ., -3, -2,-1, 0, 1, 2, 3, . . . }

- Set of Whole numbers

  W = {0, 1, 2, 3, . . . }

- Set of Natural numbers

  N = {1, 2, 3, . . . }

Note: The set of positive integers has a smallest element.

Basic Concepts

- If a and b are two integers, such that a < b, then a ≤b-1 or if a > b, then a ≥b+1.
- An integer b is said to be divisible by an integer a(≠0), if there exists an integer x, such that b = ax and is denoted by a|b.
- Exact division: We say a^k ||b if a^k divides b but a^{k+1} does not divide m.

Cont'd

- If a|b, then a|bc for every integer c.
- a|a for all a(≠0) (Reflexivity)
- If a|b and b|a, then a = b (Anti-symmetry)
- If a|b and b|c, then a|c (Transitivity).
- If a|b and a|c, then a|bx + cy for integers x and y.
- If a|b and b|a, then a = ±b.
- If a|b, a>0, b>0, then a≤ b.
- If m(≠0) and a|b, then ma|mb.
- If a|b1, a|b2, . . . , a|bn, then $a \left| \sum_{i=1}^{n} b_i x_i \right.$

Division Algorithm

- Given any two integers a and b with $a>0$, then their exists two unique integers q and r such that $b = qa + r$ where $0 \le r < a$.

Greatest common divisor

- If at least one of the integers b or c is not equal to zero, then the greatest among the common divisors of b and c is called the greatest common divisor (gcd).

Examples: $(4,18) = 2$, $(18, 24) = 6$, $(6, 27, 33) = 3$

Cont'd

- Given any two integers a and b not both zero, then there is a unique integer $d>0$ such that

  i) $d|a$, $d|b$

  ii) If $c|a$, $c|b$, then $c|d$

- If d is a gcd of two integers b and c, then their exists two integers x and y such that

$$d = (b, c) = bx + cy$$

Prime Numbers

- An integer n(>1) is said to be prime if it has no proper divisors.

Example: 2, 3, 5, 7, 11, 13, . . .

Note: 2 is the only even prime number.

Relatively prime integers: Two integers a and b are said to be relatively prime if their gcd is 1.

Example: (4, 9) =1, (5, 12) =1. (19, 87) = 1

Bezout's Identity

- Two integers a and b are relatively prime if and only their exists x and y such that ax + by =1

Properties

- If (a, b) = 1, then (a-b, a+b) = 1 or 2
- If ax + by = m, then (a, b)|m
- For any integer m, (ma, mb) = m(a, b).
- If d|a, d|b, then (a/d, b/d) = (a, b)/d.
- If d = (a, b), then (a/d, b/d) = 1
- If (a, m) = 1, (b, m) = 1, then (ab, m) =1.
- If (a, m)=1, (b, m)=1, …, (z, m) =1, then (abc… z, m)= 1
- If (a, b) =1, then (a^m, b^n) =1 for all m, n >0

khanday@uok.edu.in

Prove that 4 does not divide n^2+2 for any integer n

- For n odd, n^2 is odd and hence n^2+2 and 4 cannot divide an odd number in this case.
- For n even, n=2k for some k, then n^2+2 is always of the form $2\left(2k^2+1\right)$.
- Thus if 4 divides n^2+2, then 4 divides $2\left(2k^2+1\right)$ which implies 2 divides $\left(2k^2+1\right)$, contradiction.
- Hence 4 does not divide n^2+2 for all n.

If (a, 4)=2, (b, 4)= 2, then (a+b, 4)=?

- Clearly a = 2 times odd number Also b = 2 times odd number.
- Therefore, a+b = 2 times even number

  = 4 times odd number
- Thus (a+b, 4) = 4

For x and y odd, $x^2 + y^2$ is always even but not divisible by 4

- If x and y are odd, then x=2k+1 and y=2m+1, therefore, $x^2 + y^2$ = 2(odd number).
- Thus $x^2 + y^2$ is even but not divisible by 4.

Composite Numbers

- An integer n(>1) is said to be composite if it is not prime. In other words, if n has a divisor d such that 1<d<n.

For n odd Show that $8 \mid (n^2 - 1)$

For m, n odd show that $64 \mid (n^2 - 1)(m^2 - 1)$

- Clearly square of odd number is odd, therefore $(n^2 - 1)$ is even and the minimum positive value of $(n^2 - 1)$ is 8. thus, $8 \mid (n^2 - 1)$.

For m odd, then $8 \mid (m^2 - 1)$

Therefore,

$$64 \mid (n^2 - 1)(m^2 - 1)$$

More properties

- If $a|bc$ and $(a,b)=1$, then $a|c$
- Every integer is either of the form 2k, 2k+1
- Every integer is of the form 3k, 3k+1, 3k+2
- If an integer is of the form 6k+5, then it is necessarily of the form 3k+2 but converse need not be true.
- Square of the integer of the form 5K+1 is of the same form.
- Square of an integer is either of the form 3k, 3k+1 but not of the form 3k+2.

No two integers x and y exist such that $x+y=100$ and $(x, y)=3$

- Clearly $3|x$, $3|y$, then $3|x+y$ implies $3|100$ which is not true.
- Thus no two integers x and y exists satisfying the above two properties simultaneously.

Fundamental theorem of Arithmetic's

- Every integer $n(>1)$ can be expressed as a product of primes

Euclid's Theorem

- If p is a prime number and p|ab, then p|a or p|b.
- If $p \mid p_1 p_2 \ldots p_r$, where $p_1, p_2, \ldots, p_r$ are all primes, then $p = p_i$ for at least on i=1,2,3,…,r.
- If x and y are odd, then $x^2 + y^2$ cannot be a perfect square.

- If x and y are prime to 3, then $x^2 + y^2$ cannot be a perfect square.

- For n≥2 and a positive integer k, $(n-1)^2 \mid (n^k - 1)$ if and only if (n-1)|k.

- No cancellation is possible in fraction $\frac{a_1 + a_2}{b_1 + b_2}$ if and only if $a_1 b_2 - a_2 b_1 = \pm 1$

- If b|a and c|a and (b, c) = 1 then bc|a.

If (a, b) =1 and a+b≠0 and p is an odd prime, then $\left(a+b,\ \frac{a^p+b^p}{a+b}\right)=1\ or\ \ p$

- We have (a, b) = 1 therefore $\left(a^{p-1},\ b^{p-1}\right)=1$
- Therefore there exists x and y such that

$$a^{p-1}x+b^{p-1}y=1$$

- Now from the binomial expansion of
- $a^p+b^p=\left\{\left(a+b\right)-b\right\}^p+b^p$
- If $\left(a+b,\ \frac{a^p+b^p}{a+b}\right)=d$, then proceed….

Problems/Tutorial

- For n≥3, let $f(n) = \log_2(3)\log_3(4)\ldots\log_{n-1}(n)$ what is the value of $\sum_{k=2}^{99} f(2^k)$??
- What is the sum of all fractions of the form $\frac{3^n + 4^n}{12^n}$ as n ranges over all nonnegative integers??
- There is only one common prime divisor of 193499 , 180253 and 160921. What is it??

Hint: This prime p must be a divisor of 193499 − 180253 = 13246 = 2·6623 and of 180253−160921 = 19332 = 4·4833. Thus p must be a divisor of 6623−4833 = 1790 = 2·5·179. Since our numbers are not divisible by 2 or 5, the answer must be 179. Indeed, the three numbers factor as 23 · 47 · 179, 19 · 53 · 179, and 29·31·179.

Cont'd

- What is the largest exponent of 2 that divides 33!??
- Find the least number whose last digit is 7 and which becomes 5 times larger when this last digit is carried to the beginning of the number.
- Given two relatively prime integers m and n, both greater than 1, show that $\frac{\log_{10} m}{\log_{10} n}$ is not a rational number.
- All the 2-digit numbers from 19 to 93 are written consecutively to form the number N=192021…93. Find the largest power of 3 that divides N.

Thanks