Scribed Notes: 23

Number Theory

- **Elementary Operations:**
  - Addition
  - Subtraction
  - Multiplication
  - Division
- **Well known Number Theory**
  - Positive Integers
  - Non-negative Integers
  - Integers
  - Rational Numbers
  - Irrational Numbers
    - Transcendental Numbers
  - Imaginary Numbers
  - Complex Numbers
  - Modulo/clock Arithmetic
- **Example Of Modulo/clock Arithmetic**
  1. Let us consider January 1st as Thursday. Then according to this which day will be the current day.(17 Nov 2021)

     January 1st= Thursday → 1

     February 1st → 4 [1+31%7] (31 days in January)

     March 1st → 4 [4+28%7]

     April 1st → 0 [4+31%7] (Considering days as 0 to 6)

     May 1st → 2 [0+30%7]

     June 1st → 5 [2+31%7]

     July 1st → 0

     August 1st → 3

     September 1st → 6

October 1st → 1

November 1st → 4

November 17th → 6

Here, January 1st is Thursday and considered as the first day, then the current day that is November 17th will be Tuesday (two days before the first day).

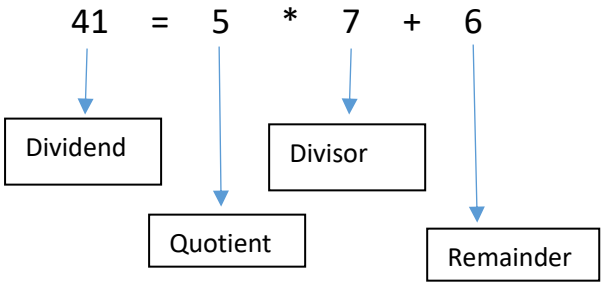
2. January 1st 2021= Friday
   January 1st 1953=?

   1st Jan 1953=x
   Therefore, 1st Jan 2021= x+68+17
   68 days were added because 365%7=1 and the difference between years 2021 and 1953 is 68.
   17 days were added because there are 17 leap years between 1953 and 2021.Hence, there will be an extra day in each year.

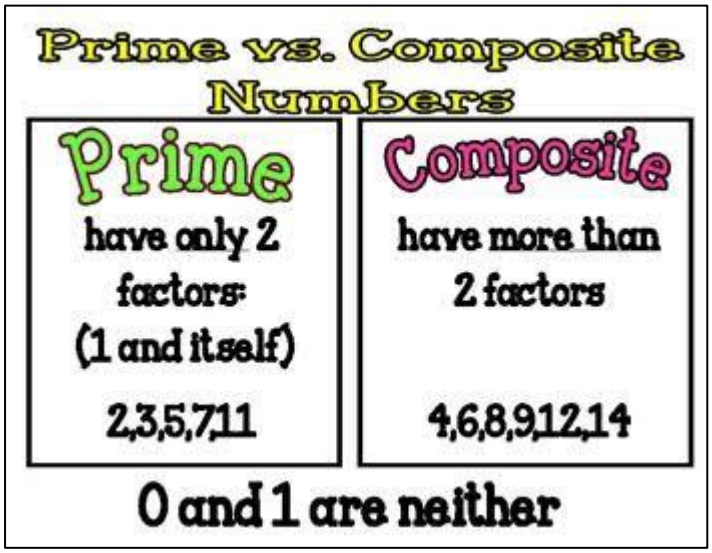
   1st Jan 2021=x+85
   Therefore, x+85%7=x+1
   Therefore, if 1st January 2021 was Friday, then 1st January 1953 will be Thursday.

- **<u>The Division Algorithm</u>**

  Example: 41/7



- **Prime Number v/s Composite Number**



- Every composite number has a unique factorization of prime numbers.

$$6 = 2 \times 3$$
$$12 = 2 \times 2 \times 3 = 2^2 \times 3$$
$$16 = 2 \times 2 \times 2 \times 2 = 2^4$$
$$250 = 2 \times 5 \times 5 \times 5 = 2 \times 5^3$$
$$510{,}510 = 2 \times 3 \times 5 \times 7 \times 11 \times 13 \times 17$$
$$42{,}059 = 137 \times 307$$

- Prove that there are infinitely many prime numbers.

  Proof by contradiction:

  - Let us assume that there are finitely many primes and label them p1. . . pn.
  - We will now construct the number P to be one more than the product of all finitely many primes:

    $$P = p1p2 \cdots pn + 1.$$

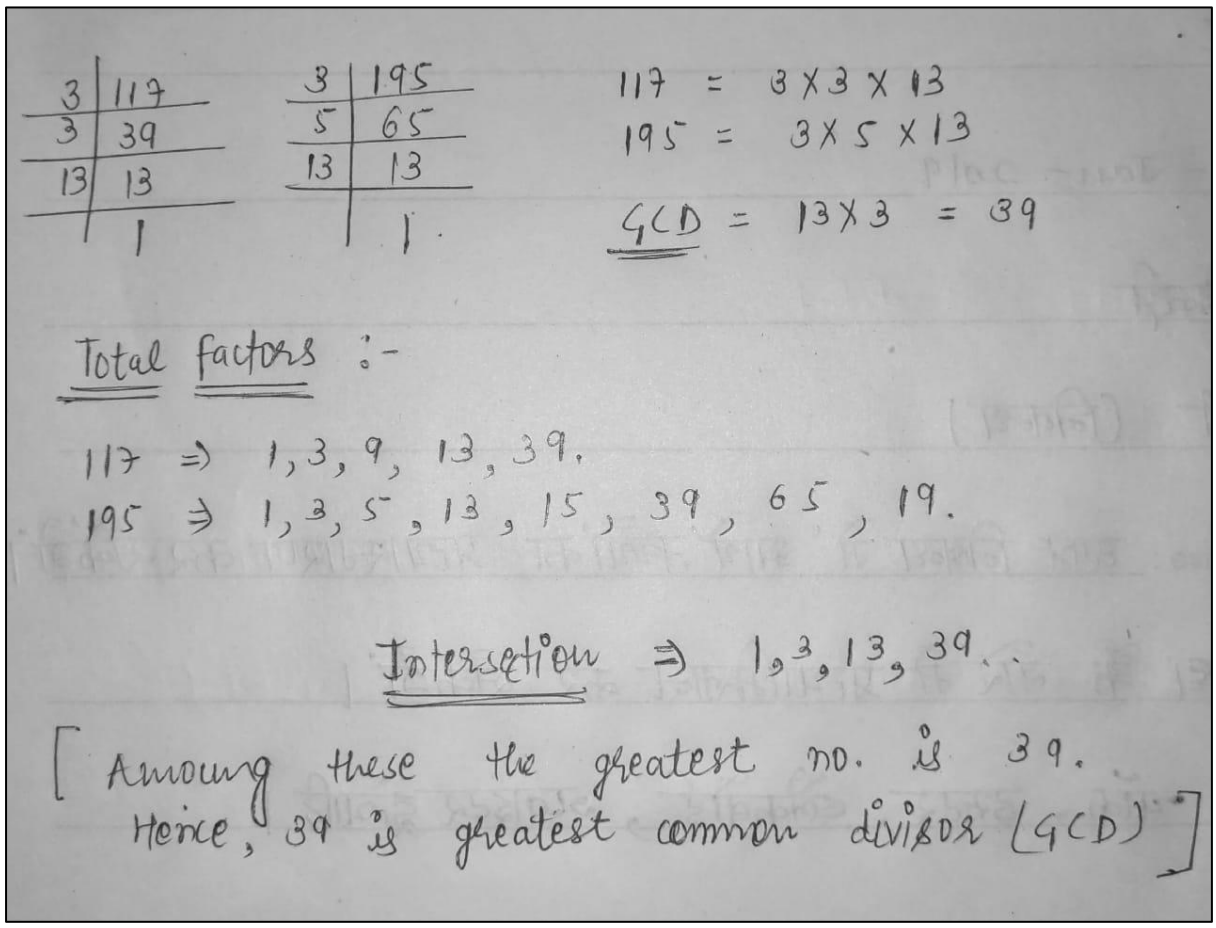
  - The number P has remainder 1 when divided by any prime pi, i = 1, . . . , n, making it a prime number as long as $P \neq 1$.

- Since 2 is a prime number, the list of pi ’s is non-empty. It follows that P is greater than one and so has two distinct divisors. It is therefore a prime number.
- It can also be seen from the definition of P that it is strictly greater than any of the pi’s. This contradicts our assumption that there are finitely many prime numbers. Therefore, there are infinitely many prime numbers.

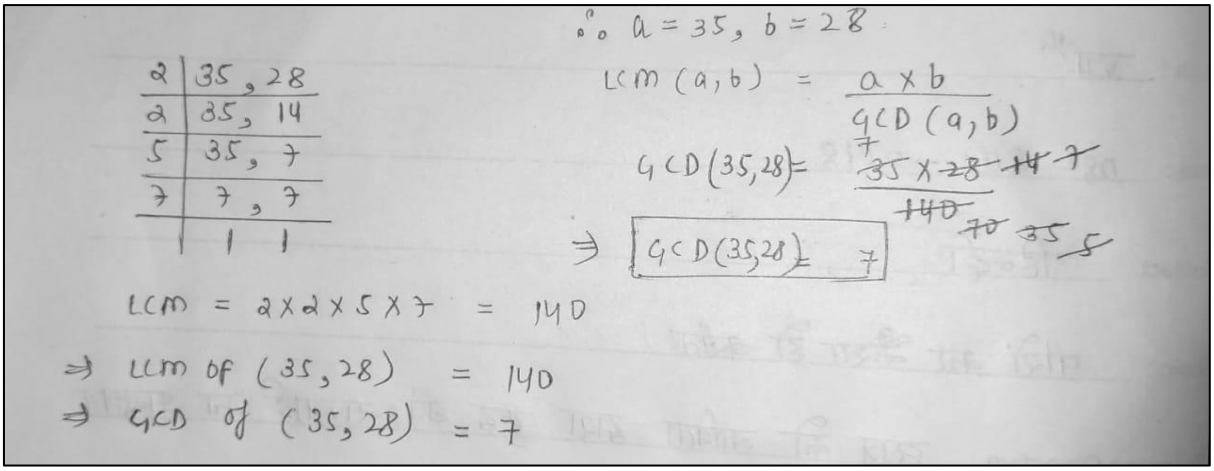
- **<u>Sieve of Eratosthenes</u>**

  $N=(\sqrt{N})^2$

- **<u>GCD (Greatest Common Divisor)</u>**



- **LCM (Least Common Multiple)**



- **<u>Relative Prime Number</u>**
  - When two numbers have no common factors other than 1.
  - In other words there is no value that you could divide them both by exactly (without any remainder).
  - 21 and 22 are relatively prime:
    - The factors of 21 are 1, 3, 7 and 21
    - The factors of 22 are 1, 2, 11 and 22

    (the only common factor is 1)
- **<u>Euler ϕ Function</u>**
  - Euler's ϕ (phi) Function counts the number of positive integers not exceeding n and relatively prime to n.
  - If p is a prime number then ϕ (p) = p-1 for any prime number.
  - Example: ϕ (117) =?

    117=13*3*3

    Number of non-relative prime multiples of 13 below 117 is 8

    Number of non-relative prime multiples of 3 below 117 is 38

    Number of non-relative prime common multiples of 3 and 13 below 117 is 2.

    Therefore,

    Total Non-relative prime multiples of 117 are 8+38-2=44

    Hence, according to Euler's ϕ (phi) Function

    Φ (117) = (117-1)-(44) = 72

    Therefore there are 72 non-relative prime multiples of 117

    1,2,4,5,7,8,10,11,14,16,17,19,20,22,23…and so on.

- **Euclid's Algorithm for GCD**
  - Multiplication is nothing but repeated addition.
  - The Euclidean Algorithm for finding GCD(A,B) is as follows:

    If A = 0 then GCD(A,B)=B, since the GCD(0,B)=B, and we can stop.

    If B = 0 then GCD (A, B) =A, since the GCD (A,0)=A, and we can stop.

    Write A in quotient remainder form (A = B·Q + R)

    Find GCD(B,R) using the Euclidean Algorithm since GCD(A,B) GCD(B,R)

    Example:

    Find GCD(195,117).

    ➔ GCD(195,117) (195/117, remainder=78)
    =GCD(78,117) (117/78, remainder=39)
    =GCD(78,39) (78/39, remainder=0)
    =GCD(0,39)
    Therefore, GCD(195,117)=39
- **Remainder Theorem**
  - Example: Find 5^{7346} mod 17.

    If p is a prime, $a^{p-1}=1$ (mod p).

    5^1 mod 17=5, 5^2 mod 17=8, 5^3 mod 17=6, 5^4 mod 17=13, 5^5 mod 17=14

    Therefore the remainder series is:

    5,8,6,13,14,2,10,16,12,9,11,4,3,15,7,1,5,8,6,13,14,2,10,16,12,9,11,4,3,15,7,1….

    Hence the cycle of numbers repeats after every 16 numbers.

    Therefore,

    7346%16=2

    As remainder is 2, the second number from the remainder series that is 8 will be the answer of our main problem.

    5^{7346} mod 17=8.

- **Chinese Theorem**

In number theory, the **Chinese remainder theorem** states that if one knows the remainders of the Euclidean division of an integer *n* by several integers, then one can determine uniquely the remainder of the division of *n* by the product of these integers, under the condition that the divisors are pairwise coprime.

Theorem:

Let p,q be coprime. Then the system of equations

$x=a(\text{mod } p)$
$x=b(\text{mod } q)$

has a unique solution for x modulo pq.

The reverse direction is trivial: given $x \in Z_{pq}$, we can reduce x modulo p and x modulo q to obtain two equations of the above form.

Proof:

Let $p1=p^{-1}(\text{mod } q)$ and $q1=q^{-1}(\text{mod } p)$. These must exist since p,q are coprime. Then we claim that if y is an integer such that

$y=aqq1+bpp1(\text{mod } pq)$
then y satisfies both equations:

Modulo p, we have $y=aqq1=a(\text{mod } p)$ since $qq1=1(\text{mod } p)$.

Similarly y=b (modq). Thus y is a solution for x.

It remains to show no other solutions exist modulo pq.

If z=a (mod p) then z−y is a multiple of p. If z=b (mod q) as well, then z−y is also a multiple of q. Since p and q are coprime, this implies z−y is a multiple of pq, hence z=y (mod pq).

This theorem implies we can represent an element of Z_{pq} by one element of Z_p and one element of Z_q, and vice versa. In other words, we have a bijection between Z_{pq} and $Z_p \times Z_q$.

For Several Equations

Theorem:

Let $m_1,...,m_n$ be pairwise coprime (that is gcd $(m_i, m_j)=1$ whenever $I \neq j$). Then the system of n equations

$$x=a_1 \pmod{m_1}$$

...

$$x=a_n \pmod{m_n}$$

has a unique solution for x modulo M where $M= m_1...m_n$.

Proof:

This is an easy induction from the previous form of the theorem, or we can write down the solution directly.

Define $b_i=M/m_i$ (the product of all the moduli except for m_i)
and $b_i'=b_i^{-1} \pmod{m_i}$. Then by a similar argument to before,

$$x=\sum_{i=1}^{n} a_i b_i b'_I \pmod{M}$$

is the unique solution.