PRIME AND COMPOSITE NUMBERS

View the lecture on YouTube: https://youtu.be/6So-0z4zsx4

View motivational speech from Adam Spencer on YouTube to understand the nature of prime numbers: https://youtu.be/B4xOFsygwr4

Definition: Any positive integer >1 is prime if and only if its factors are 1 and itself, and the positive integer that is not prime is called composite number.

If x is a positive real number then $\pi(x)$ denotes the number of primes $\leq x$.

Theorem 1: Every integer $n \geq 2$ has a prime factor.

Proof: This proof involves strong induction.

For $n = 2$, the statement is true since 2 is a prime number. Assume that all integers between 2 and $k(2 \leq x \leq k)$ has a prime factor.

TPT the integer $k+1$ also has a prime factor

(i) If $k+1$ is prime then it is a factor of itself

(ii) If $k+1$ is not prime then $k+1$ has factors between $2 \leq x \leq k \Longrightarrow (k+1)$ has a prime factor.

Hence by induction all integers $n \geq 2$ has a prime factor.

Theorem 2: Prove that there are infinitely many primes.

Proof: Assume the contradiction, that is there is only a finite number of primes i.e., $p_1, p_2, p_3 \ldots . p_n$

Now, consider an integer $N = p_1 p_2 p_3 \ldots . p_n + 1$ since $N \geq 2, N$N$ is divisible by some prime $p_i, 0 \leq i \leq n$.

Since $p_i / N \Longrightarrow p_i / (p_1 p_2 p_3 \ldots . p_n)$

$$\Longrightarrow p_i / (N - p_1 p_2 p_3 \ldots . p_n) = p_i / 1.$$

which is a contradiction that it is divided by only one term.

Hence the assumption is false.

⟹There are infinitely many primes.

Theorem 3: Prove that there are infinitely many prime of the form $4\,n+3$.

Proof: To prove this assume the contradiction. i.e.,there are only finite number of primes of the form $4\,n+3$ and let them be $p_1, p_2, p_3 \ldots . p_n$.

Let $N = 4(p_1 p_2 p_3 \ldots . p_n) - 1$, then $N \equiv -1(mod 4) \Longrightarrow N \equiv 3(mod 4)$.

Let the prime factorization of N be given as $N = q_1 q_2 q_3 \ldots . q_l$.

Since N is odd $\Longrightarrow q_1, q_2, q_3 \ldots . q_l$ are all odd.

Note that any q_i satisfies one of the residues

$q_i \equiv 1(mod 4), q_i \equiv 2(mod 4), q_i \equiv 3(mod 4), q_i \equiv 0(mod 4)$.

Since q_i is odd, $q_i \equiv 2(mod 4), q_i \equiv 0(mod 4)$.is not possible.

Therefore, we have $q_i \equiv 1(mod 4)$ or $q_i \equiv 3(mod 4)$.

Claim 1: At lease for one i, $q_i \equiv 3(mod 4)$.

To prove this claim assume the contrary that $q_i \equiv 1(mod 4)$for each $i = 1,2, \dots l$.

$q_1 q_2 q_3 \dots . q_l \equiv 1.1.1 \dots .1(mod 4)$

$N \equiv 1(mod 4)$, which is a contradiction. Hence the claim.

Claim 2: q_i is different from each of $p_1, p_2, p_3 \dots . p_n$.

To prove this assume the contradiction, ie., $q_i = p_j$ for some j.

Therefore, $p_j /(4p_1 p_2 p_3 \dots . p_n) \Longrightarrow p_j /(N + 1)$ by definition of N.

$\Longrightarrow q_i/N \Longrightarrow p_j /N$, since $q_i = p_j$.

Now, $p_j /(N + 1)$ and $p_j /N \Longrightarrow p_j /N + 1 - N \Longrightarrow p_j /1$ which is contradiction that p_j is prime. Hence the Claim.

Claim 1 and 2 contradicts the assumption that there are finite number of prime. Hence, there are infinitely many primes.

Theorem 4: For every positive integer n there are n consecutive integers that are composite.

Proof: Consider a n consecutive integers of the form

$(n + 1)! + 2, (n + 1)! + 3, \dots . (n + 1)! + n + 1$.

For any integer k,

such that $2 \leq k \leq n + 1$ and by previous theorem, we have $k/(n + 1)!$ and also k/k, therefore $k/(n + 1)! + k$ for every k .

$\Longrightarrow$ each of them is composite.

Theorem 5: Every composite number n has a prime factor $\leq \sqrt{n}$.

Proof: Consider a composite number n . Then n can be written as a product of integers.

So for $a, b \in N$, let $n = ab$ be the composite number.

If suppose $a > \sqrt{n}$, $b > \sqrt{n}$, then $n = a\, b > \sqrt{n}\sqrt{n} > n$, which is a contradiction.

Therefore, $a \leq \sqrt{n},\ b \leq \sqrt{n}$.

We know that, every positive integer ≥ 2 has a prime factor. Any such factor of a or b is also a factor of $ab = n$. So n must have a prime factor.

Important Results:

1. Let $p_1, p_2, p_3 \ldots .\, p_t$ be the prime $\leq \sqrt{n}$, then

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor - \sum_{i<j<k} \left\lfloor \frac{n}{p_i p_j p_k} \right\rfloor + \cdots + (-1)^n \left\lfloor \frac{n}{p_1 p_2 p_3 \ldots p_t} \right\rfloor$$

2. If x approaches ∞, $\pi(x)$ approaches $\frac{x}{\log x}$ for $x \geq 2$ i.e

$$\lim_{x \to \infty} \frac{\pi(x)}{x/\log x} = 1.$$

Example 1: Determine whether the following are prime or composite

a) 129 b) 1729 c) 1601 d) 1001

Solution: a) It's composite since 3 is a factor

b) Given 1729.

The prime factors $\leq \sqrt{1729}$=41.58 are 2,3,5,7,11,13,17,19,23,29,31,37 .

In this 7 is a factor of 1729 (7|1729). Therefore, it is a composite number

c) 1601. The prime factors $\leq \sqrt{1601}$=40.01 are 2,3,5,7,11,13,17,19,23,29,31,37

. In this none of the numbers divide 1601.

Therefore, 1601 is a prime number.

d) 1001. The prime factors $\leq \sqrt{1001}$=31 are 2,3,5,7,11,13,17,19,23,29,31.

In this 7 is a factor of 1001 (7|1001). Therefore, it is a composite number

Example 2: Find the number of primes ≤ 61 using $\pi(x)$.

Solution:

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_i \left\lfloor \frac{n}{p_i} \right\rfloor + \sum_{i<j} \left\lfloor \frac{n}{p_i p_j} \right\rfloor - \sum_{i<j<k} \left\lfloor \frac{n}{p_i p_j p_k} \right\rfloor + \cdots$$
$$+(-1)^n \left\lfloor \frac{n}{p_1 p_2 p_3 \ldots p_t} \right\rfloor$$

$$\pi(61) = 61 - 1 + \pi(\sqrt{61}) - \left(\frac{61}{2} + \frac{61}{3} + \frac{61}{5} + \frac{61}{7}\right)$$
$$+\left(\frac{61}{6} + \frac{61}{10} + \frac{61}{14} + \frac{61}{15} + \frac{61}{21} + \frac{61}{35}\right)$$

$$-\left(\frac{61}{30}+\frac{61}{42}+\frac{61}{70}+\frac{61}{105}\right)+\left(\frac{61}{210}\right)$$

$$= 60 + 4 - (30 + 20 + 12 + 8) + (10 + 6 + 4 + 4 + 2 + 4)$$

$$-(1 + 2 + 0 + 0) + (0)$$

$$=21.$$

Example 3: Find the number of primes ≤ 100 using $\pi(x)$.

Solution:

$$\pi(n) = n - 1 + \pi(\sqrt{n}) - \sum_i \left\lfloor\frac{n}{p_i}\right\rfloor + \sum_{i<j} \left\lfloor\frac{n}{p_i p_j}\right\rfloor - \sum_{i<j<k} \left\lfloor\frac{n}{p_i p_j p_k}\right\rfloor + \cdots$$

$$+(-1)^n \left\lfloor\frac{n}{p_1 p_2 p_3 \ldots p_t}\right\rfloor$$

$$\pi(100) = 100 - 1 + \pi(\sqrt{100}) - \left(\frac{100}{2}+\frac{100}{3}+\frac{100}{5}+\frac{100}{7}\right)$$

$$+\left(\frac{100}{6}+\frac{100}{10}+\frac{100}{14}+\frac{100}{15}+\frac{100}{21}+\frac{100}{35}\right)$$

$$-\left(\frac{100}{30}+\frac{100}{42}+\frac{100}{70}+\frac{100}{105}\right)+\left(\frac{100}{210}\right)$$

$$= 99 + 4 - (50 + 33 + 20 + 14) - (16 + 10 + 7 + 6 + 4 + 2)$$

$$= 25.$$

Example 4: Find five consecutive integers that are composite.

Solution: Here, $\mathrm{n} = 5$, We know that the consecutive composite numbers are given by $(\mathrm{n}+1)! + 2, (\mathrm{n}+1)! + 3, \ldots..(\mathrm{n}+1)! + (\mathrm{n}+1)$

For $\mathrm{n} = 5$ we have $6! + 2, 6! + 3, 6! + 4, 6! + 5, 6! + 6$

$= 722,\ 723, 724, 725, 726$ are composite.

Example 5: Find six consecutive integers that are composite.

Solution: We know that the consecutive composite numbers are given

By $(\mathrm{n}+1)! + 2, (\mathrm{n}+1)! + 3, \ldots..(\mathrm{n}+1)! + (\mathrm{n}+1)$

For $\mathrm{n} = 6$ we have $7! + 2, 7! + 3, 7! + 4, 7! + 5, 7! + 6, 7! + 7$

$= 5042,\ 5043, 5044, 5045, 504S6, 5047$ are composite.

Example 6: Find five consecutive integers < 100 that are composite numbers.

Solution: Since $5! = 120 > 100$,

We consider $4!,\ 4! + 1, 4! + 2,\ 4! + 3,\ 4! + 4,$

Therefore, 24, 25, 26, 27, 28 are 5 consecutive composite numbers < 100.

GREATEST COMMON DIVISOR

View the lecture on YouTube: https://youtu.be/IfLqUhTNQ3c

Greatest Common Divisor (GCD)

The greatest common divisor (GCD) of two integers a and b, not both zero, is the largest positive integer that divides both a and b; it is denoted by (a, b). For example, (12, 18) = 6, (12, 25) = 1, (11, 19) = 1, (−15, 25) = 5, and (3, 0) = 3.

Important Results

A positive integer d is the gcd of two positive integers a and b, if

(i) $d|a$ and $d|b$.

(ii) If $c|a$ and $c|b$ then $c|d$, where c is the positive integer .

Theorem 1: The GCD of positive integers a and b is the linear combination with respect to a and b.

Proof:

Let $S = \{xa + yb / xa + yb > 0, x, y \epsilon Z\}$.

For $x = 1$ and $y = 0$, $S = a \Rightarrow S$ is non empty.

Therefore by well ordering principle, let S has the least positive integer d.

$d = la + mb$ for some positive integers l and m.

To Prove: $d = gcd(a, b)$.

Since $d > 0$, by the division algorithm a and d , there exist an integers q and r such that

$$a = qd + r, \qquad 0 \leq r < d \qquad (1)$$

$$r = a - qd$$

$$= a - q(la + mb)$$

$$= (1 - ql)a + (-qm)b.$$

This shows r is the linear combination of a and b.