Note Title 17-08-2021

MA - 222

Lec - 8

Prime numbers

- A natural no $n \in \mathbb{N}$ ($n \geq 2$) is said to be prime if 1 & n ~~are~~ are only divisors.
- if n does not have two smaller divisors.
- If n is prime then whenever $n \mid ab$ then $n \mid a$ or $n \mid b$.

irreducible

$\mathbb{R}[x]$

$\mathbb{R}[x,y]$

$f(x)$

$x^2+2x+1 = (x+1)(x+1)$

$x^2+1 = (2x^2+2)/2$

Thm There are infinitely many primes.

— Euclid's Pf $N = p_1 \cdots p_r$ $\quad p_i \nmid N+1 \; \forall i$

— $N+1$

Lemma 1 :- Every natural no is either a prime or has a prime factor.

Lemma 2 — Two consecutive intg do not have a common factor.

Kummer $N = \prod p_i$ $(N, N-1) = 1$

$p_i \nmid N-1.$

Goldbach: **Fermat's number**

$F_n = 2^{2^n} + 1 \longleftarrow F_1 \to p_1$

$(F_m, F_n) = 1 \quad m \neq n.$

$F_2 \to p_2$

$\vdots$

p_n

Latest Pf 2005 (Saidak)

Start with $n = N_1$ $\longrightarrow$ Either a prime or has a prime factor

$n \in \mathbb{N}$ $n \geq 2$.

$N_2 = n(n+1)$. $\longrightarrow$ At least two distinct prime factors.

$N_3 = n(n+1)[n(n+1)+1]$

$= N_2(N_2+1)$ $\longrightarrow$ At least 3 distinct prime factors.

N_4 - - - .

Dirichlet:

$4k+1$
$4k+3$

Resonance 1996
Shailesh Shirali

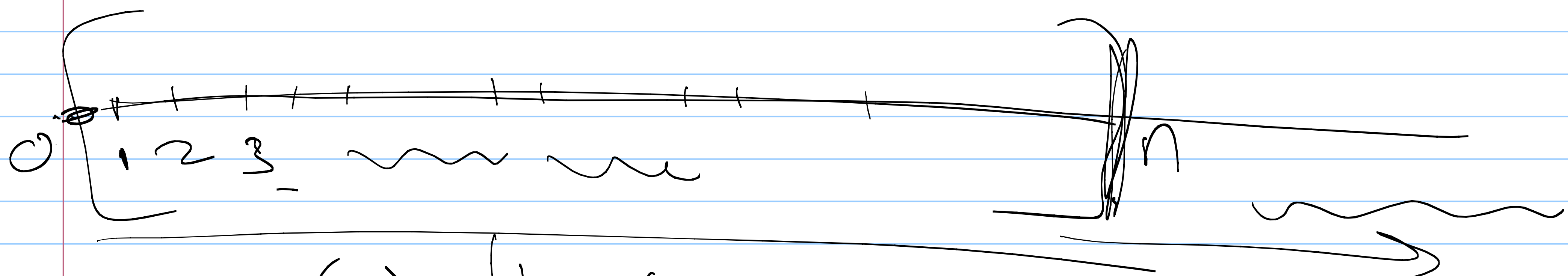
$(a,n)=1$ then there are inf. many primes of the form $nk+a$

$p \equiv a \pmod{n}$

3 7,

$7k+3$

Distribution of primes



$$\pi(n) = \left| \{ p \mid p \leq n \ \& \ \text{primes} \} \right|$$

$\pi(100) = 25$

$$\pi(n) \sim \int_2^n \frac{1}{\log x}\, dx \sim \frac{n}{\log n}$$

(Gauss) (Legendre)

$$\pi(100) = \left|\{p < 100 \mid p : \text{prime}\}\right| = \left|\{2, 3, 5, 7, 11, 13, \ldots, 97\}\right|$$

Primality testing

Given $n \in \mathbb{N}$ tell conclusively & in finitely many step whether n is prime or not.

for each $i \in \{1, \dots, n-1\}$ check if $i \mid n$.

$\log n$

$\{1, \dots, \sqrt{n}+1\}$.

$i \mid j$

nonpoly.

NP

algo

(2002)

Poly time.

Primes $\in$ P.

2

r

Miller-Rabin

Solo--- - Strassen

Fermat's test

Funda thm of Arithmetic

Thm: p : prime $p \mid ab \Rightarrow p \mid a$ or $p \mid b$.

Cor: $p \mid a_1 \cdots a_k$ then $p \mid a_i$ for some i.

Cor: If $p, q_1, \ldots, q_r$ & $p \mid q_1 \cdots q_r$

then $p = q_i$ for some i

Thm: <u>FTA</u>

Every natural no $n \in \mathbb{N}$ $(n > 1)$ can be written as a product of primes.

(OR Product of powers of distinct primes)

$$n = \prod_{i=1}^{r} p_i^{\alpha_i}$$

$p_i \neq p_j$ for $i \neq j$

$\alpha_i \geq 1$.

Congruences:

$n \in \mathbb{N}$. $a, b \in \mathbb{Z}$.

We say a is congruent to b modulo n

written as $a \equiv b \pmod{n}$ if

$$n \mid a - b$$

Properties: Define $\sim_n$ on $\mathbb{Z}$. Fix $n \in \mathbb{N}$.

$$a \sim b \text{ if } a \equiv b \pmod{n}$$

Then (Ex.) $\sim$ is an equivalence rel^n on $\mathbb{Z}$.

Thm: $a \equiv b \pmod{n}$ iff a & b leave the same remainder when divided by n.

Ex.