Bharathidasan University
Tiruchirappalli - 620 024
Tamil Nadu, India

Programme: M.Sc., Mathematics

Course Title :Theory of Numbers
COurse Code : 21M04CC

Fundametal Theorem of Arithmetic

Dr. V. Piramanantham
Professor
Department of Mathematics

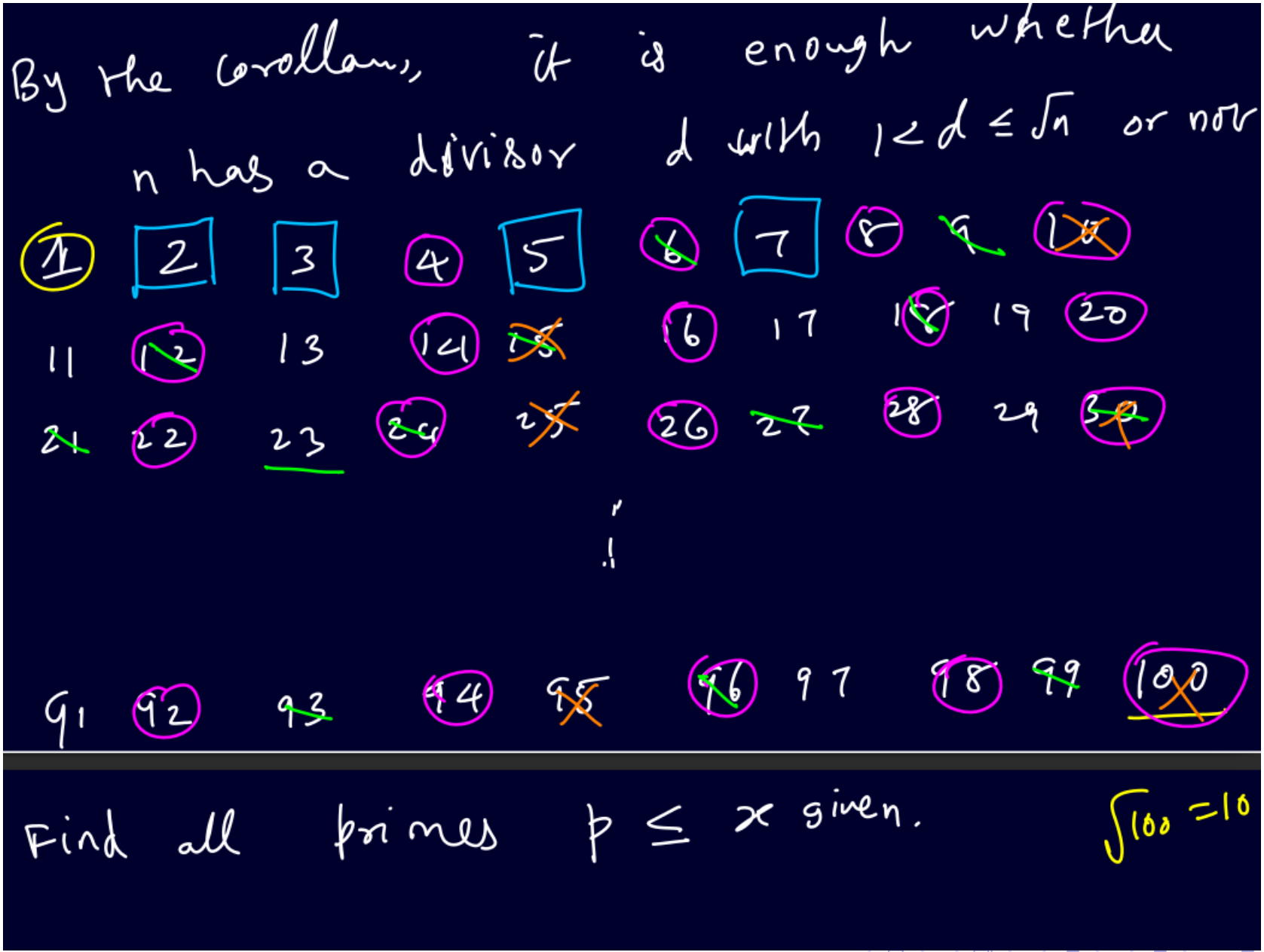
Sieve of Eratosthenes:

Result: If $n = ab$, then either $a \leq \sqrt{n}$ or $b \leq \sqrt{n}$.

Result: If there is no divisor d of n such that $1 < d \leq \sqrt{n}$, then n is prime

By the defn, to check whether a no n is prime or not, we have to verify that for all d with $1 < d < n$,

$d \mid n$ or not


By the corollary, it is enough whether
n has a divisor d with $1 < d \leq \sqrt{n}$ or not
Find all primes $p \leq x$ given.
$\sqrt{100} = 10$

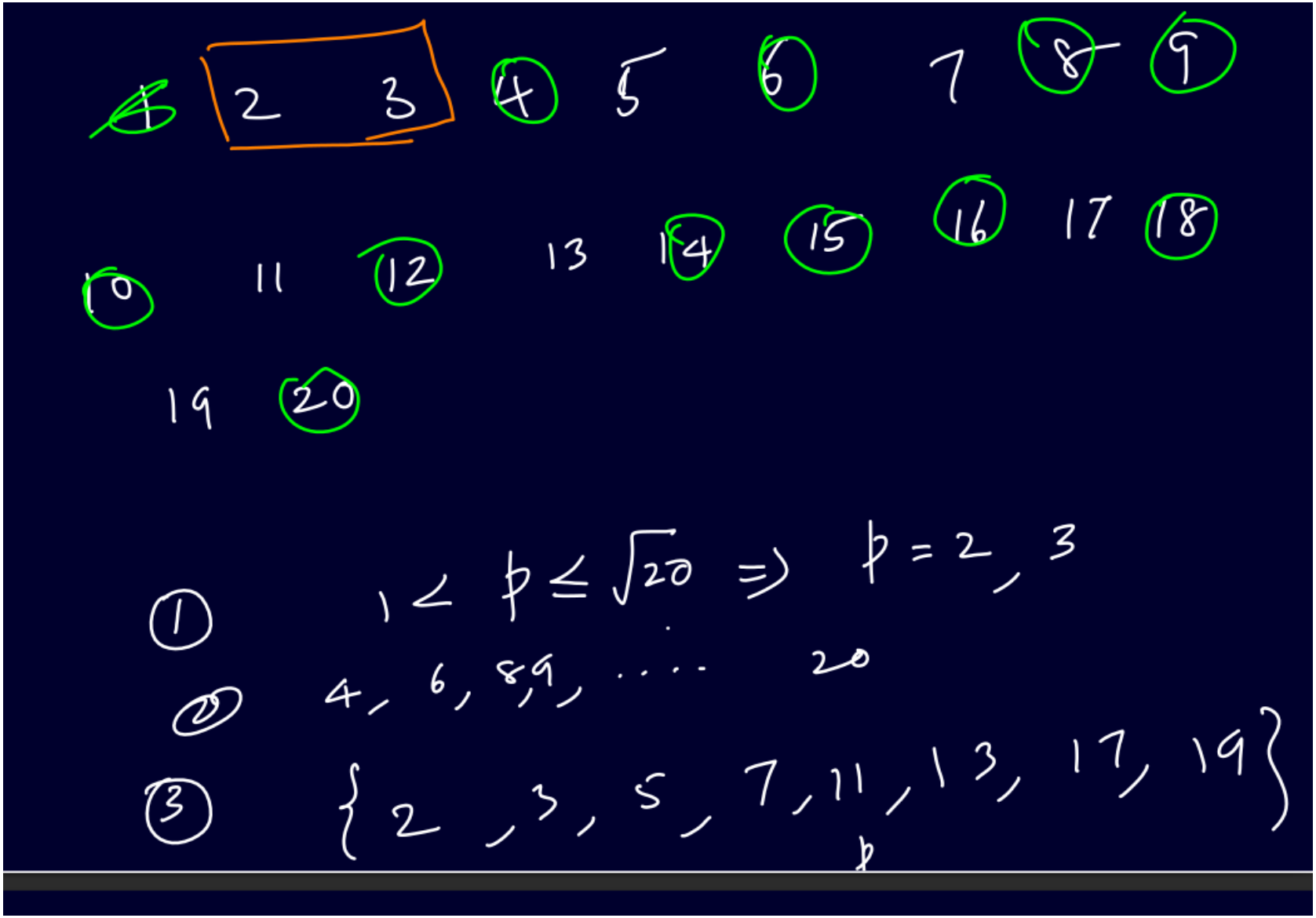
23 – prime ? $1 < d \leq \sqrt{23}$

① Select primes $p \leq \sqrt{n}$.

② Cancel all the integers multiple of any $p \leq \sqrt{n}$

③ remaining integers are primes

(list of primes $\leq n$)


1 2 3 4 5 6 7 8 9
10 11 12 13 14 15 16 17 18
19 20
① $1 < p \leq \sqrt{20} \Rightarrow p = 2, 3$
② 4, 6, 8, 9, ... 20
③ {2, 3, 5, 7, 11, 13, 17, 19}
p

Theorem 3 : The fundamental theorem of Arithmetic.

The factoring of any integer $n > 1$ into primes is unique apart from the order of prime factors.

Proof : Suppose not, there is an integer n with two different factorings.

Let $S = \{ m \in \mathbb{N} / \ m$ has two or more prime factorings $\}$

clearly $S \neq \phi$ $(\because n \in S)$.

By well-ordering principle,
S has a smallest element, say, n_0.

(ie) n_0 is the smallest integer with two different factorings

$$n_0 = p_1 p_2 \cdots p_r = q_1 q_2 \cdots q_s \quad \text{— (1)}$$

If $r=1, s=1$, $n_0 = p_1 = q_1$ is not possible.

It is clear that r & s are greater than 1.

Assume that p_1 is a common prime on both side of (1).

Then by dividing p_1 from n_0 we get two distinct factorings of n_0/p_1

This is contradiction to our assumption

that all integers smaller than n are uniquely factorable.

$\therefore$ The primes $p_1, p_2, \ldots p_r$ have no members in common with $q_1, q_2, \ldots, q_s$.

Next, without loss of generality, we assume that $p_1 < q_1$. We define the +ve int N as

$$N = (q_1 - p_1)\, q_2 q_3 \cdots q_s$$

$$= q_1 q_2 q_3 \cdots q_s - p_1 q_2 q_3 \cdots q_s$$

$$= p_1 p_2 p_3 \cdots p_r - p_1 q_2 q_3 \cdots q_s \quad \text{— (2)}$$

$$= p_1 (p_2 p_3 \cdots p_r - q_2 q_3 \cdots q_s)$$

It is clear that $N < n_0$ (by (2))

$\Rightarrow N$ has unique prime factorization.

and $N = (q_1 - p_1) q_2 q_3 \cdots q_s = p_1 (p_2 p_3 \cdots p_r - q_2 q_3 \cdots q_s)$ — (3)

But $p_1 \nmid q_1 - p_1$. p_1 is not a factor of $q_1 - p_1$

(3) gives two different factorings of N, one involving p_1 (right sides of (3)) and the other not and thus we have a contradiction

$\therefore$ Any integer $n \geq 1$ can be uniquely factored into product of primes.

$n = p_1 p_2 \cdots p_r$ — $p_1, p_2 \cdots p_r$ not necessarily distinct

$n = p_1^{\alpha_1} p_2^{\alpha_2} \cdots p_s^{\alpha_s}$ $p_1, p_2 \cdots p_s$ are distinct

$n = \prod_p p^{\alpha(p)}$ (pr) $n = \prod_p p^{\alpha}$

finite product. $\alpha = \alpha(p)$

$\alpha(p) = 0$ for all sufficiently large primes

Ex: ① If $n=1$, $\alpha(p)=0$ for all prime p

② If $a>1$, $b>1$, $a=\prod_p p^{\alpha(p)}$,

$$b=\prod_p p^{\beta(p)}$$

and $(a,b)=1$, then for every prime p

either $\alpha(p)=0$ or $\beta(p)=0$

Ex : If $a, b > 1$ and $a = \prod p^{\alpha(p)}$ & $b = \prod p^{\beta(p)}$ for every prime p, then

$$(a, b) = \prod p^{\gamma(p)}, \quad \gamma(p) = \min\{\alpha(p), \beta(p)\}$$

$$[a, b] = \prod p^{\delta(p)}$$

$$\delta(p) = \max\{\alpha(p), \beta(p)\}$$

$$(a, b)[a, b] = \prod p^{\gamma(p)} \cdot \prod p^{\delta(p)}$$

$$\gamma(p)+\delta(p) = \min\{\alpha(p), \beta(p)\} + \max\{\alpha(p), \beta(p)\}$$

$$= \alpha(p) + \beta(p)$$

$$\alpha(p)+\beta(p)$$

$$(a,b)[a,b] = \prod_{} p$$

$$\doteq \prod p^{\alpha(p)} \cdot \prod p^{\beta(p)}$$

$$\boxed{(a,b)[a,b] = ab}$$

Definition: An integer $a > 1$ is said to be square integer if $\exists$ an integer n s.t.

$$a = n^2$$

Suppose that a is a square & $a = \prod p^{\alpha(p)}$, then

$$\alpha(p) \equiv \text{even} \quad \forall p$$

If $\alpha(p) = \text{even} \quad \forall p$,

a is square

Theorem Let $a = \prod p^{\alpha}$ be the canonical factorization of a. Then

a is square $\iff$ $\alpha(p)$ is even for all primes p.

Square-free