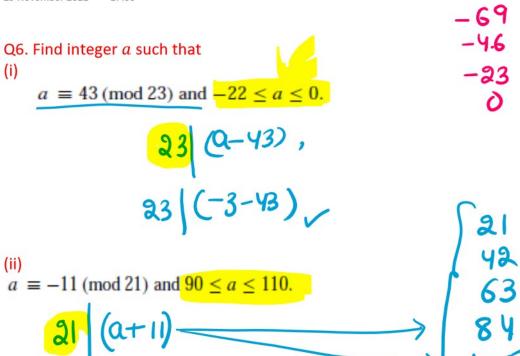
Lecture 38

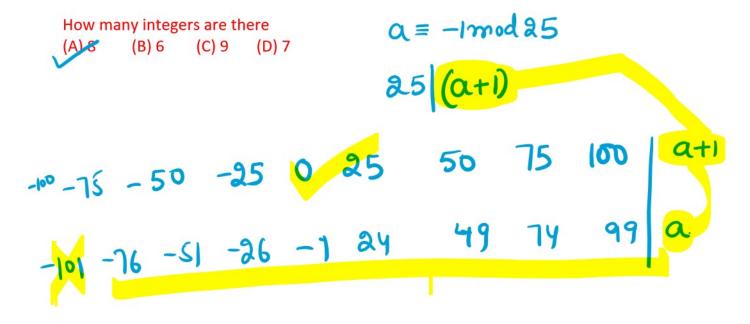
29 November 2021

17:00



Q7. List all the integers between -100 and 100 are congruent to $-1 \mod 25$.

0=94



Arithmetic Modulo m

$$\{0,1,2,...,m-1\} = \mathbb{Z}_m$$

(2) Associative

$$at_m(b+mc) = (a+mb)+mc$$

$$ai_m(b+mc) = (ai_mb)+mc$$

3 Discributive

additive identity = 0

$$Q +_m (m-a) = 0$$

$$2 \pm 5 = 0$$
 $2 \pm 4 = 1$
 $2 \pm 5 = 0$
 $2 \pm 4 = 1$
 $2 \pm 5 = 0$
 $2 \pm 4 = 1$
 $2 \pm 5 = 0$
 $2 \pm 4 = 1$
 $2 \pm 5 = 0$
 $2 \pm 7 \pm 1 = 1$
 $2 \pm 7 \pm 1 = 1$

Q8. Find the value of

$$7 + 119 \text{ and } 7 \cdot 119.$$

$$|6mod | 1 = 8 - 63 \mod 1 = 8$$

Primes and Greatest Common Divisor

Primes

An integer p greater than 1 is called *prime* if the only positive factors of p are 1 and p. A positive integer that is greater than 1 and is not prime is called *composite*.

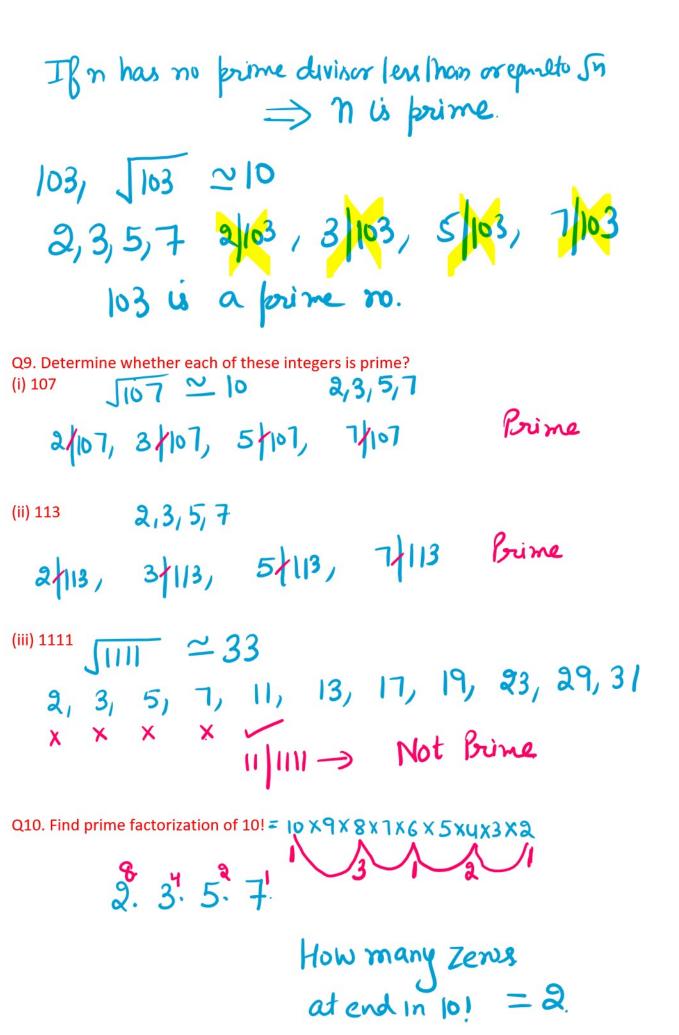
Theorem 7:

THE FUNDAMENTAL THEOREM OF ARITHMETIC Every integer greater than 1 can be written uniquely as a prime or as the product of two or more primes where the prime factors are written in order of nondecreasing size.

Theorem 8:

If n is a composite integer, then n has a prime divisor less than or equal to \sqrt{n} .

If n has no prime divisor less han or equal to In



Theorem 9: There are infinitely many primes.

Theorem 9: There are infinitely many primes.

- Mersenne primes: Primes of the form $2^p 1$, p -prime are called Mersenne primes. $7 = 2^3 1$, $3 = 2^3 1$, $3 = 2^3 1$, $3 = 2^3 1$
- Twin primes: The pair of primes that differ by 2 are called Twin primes.

$$(3,5)$$
 $(5,1)$, $(11,13)$

Greatest common divisor and Least common multiple

Let a and b be integers, not both zero. The largest integer d such that $d \mid a$ and $d \mid b$ is called the *greatest common divisor* of a and b. The greatest common divisor of a and b is denoted by gcd(a, b).

The *least common multiple* of the positive integers a and b is the smallest positive integer that is divisible by both a and b. The least common multiple of a and b is denoted by lcm(a, b).

How to find gcd and lcm using prime factorization of integers

$$a = \begin{vmatrix} m_1 & m_2 & \cdots & m_k \\ b = \begin{vmatrix} n_1 & p_2 & \cdots & p_k \\ 1 & p_2 & \cdots & p_k \end{vmatrix}$$

$$g(a(a_1b) = \begin{vmatrix} m_1 m_1 m_1 m_1 & p_2 & \cdots & p_k \\ 1 & p_2 & \cdots & p_k & \cdots & p_k \end{vmatrix}$$

$$\lim_{n \to \infty} (m_1, n_1) = \lim_{n \to \infty} (m_1, n_1) = \lim_{n \to \infty} (m_1, n_2)$$

$$\lim_{n \to \infty} (m_1, n_2) = \lim_{n \to \infty} (m_1, n_2) =$$

Q11. Find gcd and lcm of given integers

$$\begin{array}{c} (i) \ (1000, 625) \\ |000 = 2^3.5^3 \\ 625 = 5^4 \end{array}$$

$$gcd = 2.5^3 = 125$$
 $dcm = 2^3.5^4 = 5000$

(ii) (111, 201)

$$|11| = 3.37$$

 $|20| = 3.67$

$$3^{7} \cdot 5^{3} \cdot 7^{3}, 2^{11} \cdot 3^{5} \cdot 5^{9}$$

$$g(d) = 3^{5} \cdot 5^{3}$$

$$lcm = 2^{11} \cdot 3^{7} \cdot 5^{9}, 7^{3}$$

Q12. Given gcd(120, X) = 20, lcm(120, X) = 3000, then what is value of X?

Theorem 9:

Let a and b be positive integers. Then

$$ab = \gcd(a, b) \cdot \operatorname{lcm}(a, b).$$

$$(20)(3000) = (120)(x)$$

 $x = 500$

- **Relatively prime**: Two integers a, b are relatively prime if gcd(a, b) = 1.
- Pairwise prime:

The integers a_1, a_2, \ldots, a_n are pairwise relatively prime if $gcd(a_i, a_i) = 1$ whenever $1 \le n$ $i < j \le n$.

• Euler function $\phi(n)$: No. of positive integers less than or equal to n which are relatively prime to *n*.

Q13.

Determine whether the integers in each of these sets are pairwise relatively prime.

Determine whether the integers in each of these sets are

pairwise relatively prime.

Q14.

Find these values of the Euler ϕ -function.

a)
$$\phi(4)$$
.

b)
$$\phi(10)$$
.

Q15.

What is the value of $\phi(p^k)$ when p is prime and k is a positive integer?

$$\phi(b^{k}) = b^{k} - \left\lfloor \frac{b^{k}}{b} \right\rfloor$$

$$\phi(a^{0}) = a^{0} - a^{9}$$

$$= a^{9}(a-1)$$

$$= a^{9}.1$$