Lecture 38

29 November 2021 17:00

-69
-46
-23
0

Q6. Find integer a such that

(i)

$$a \equiv 43 \pmod{23} \text{ and } -22 \le a \le 0.$$

$23 \mid (a-43)$,

$23 \mid (-3-43)$ ✓

(ii)

$$a \equiv -11 \pmod{21} \text{ and } 90 \le a \le 110.$$

$21 \mid (a+11)$

21
42
63
84
105

$a = 94$

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

How many integers are there

(A) ~~8~~ (B) 6 (C) 9 (D) 7

$a \equiv -1 \bmod 25$

$25 \mid (a+1)$

-100	-75	-50	-25	0	25	50	75	100		$a+1$
$\cancel{-101}$	-76	-51	-26	-1	24	49	74	99		a

Arithmetic Modulo m

$a +_m b = (a+b) \bmod m$

addition modulo

multiplication modulo $a \cdot_m b = (ab) \bmod m$

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

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

① Closure Property $\quad a,b \in \mathbb{Z}_m$

$$a +_m b \in \mathbb{Z}_m, \quad (a \cdot_m b) \in \mathbb{Z}_m$$

② Associative

$$a +_m (b +_m c) = (a +_m b) +_m c$$

$$a \cdot_m (b \cdot_m c) = (a \cdot_m b) \cdot_m c$$

③ Distributive

$$a +_m (b \cdot_m c) = (a +_m b) \cdot (a +_m c)$$

$$a \cdot_m (b +_m c) = (a \cdot_m b) + (a \cdot_m c)$$

④ Commutative

$$a +_m b = b +_m a, \qquad a \cdot_m b = b \cdot_m a$$

⑤ Identity

$$a +_m 0 = a \qquad\qquad a \cdot_m 1 = a$$

additive identity $= 0$ $\qquad$ multiplicative identity $= 1$

⑥ Inverse

$$a +_m (m-a) = 0 \qquad\qquad a \cdot_m (a^{-1}) = 1$$

additive identity $= (m-a)$ $\qquad$ $aa^{-1} \equiv 1 \bmod m$

$$\mathbb{Z}_7 \rightarrow \{0,1,2,3,4,5,6\}$$

$$2 +_7 5 = 0 \qquad 2 \cdot_7 4 = 1$$

$2 +_m 5 = 0$ $\quad$ $2 \cdot_7 4 = 1$

$2^{-1} = 4$

$(\mathbb{Z}_m, +_m) \rightarrow$ Commutative Group.

$(\mathbb{Z}_m, +_m, \cdot_m) \rightarrow$ Commutative. Ring

Q8. Find the value of

$7 +_{11} 9$ and $7 \cdot_{11} 9$.

$16 \bmod 11 = 5$ $\quad$ $63 \bmod 11 = 8$.

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*.

Smallest Prime $\rightarrow$ 2.

Largest Prime $\rightarrow$ It exists, don't know.

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.

$103 \longrightarrow 2, \ldots \ldots 102$

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 than or equal to $\sqrt{n}$

If n has no prime divisor less than or equal to $\sqrt{n}$
$\Rightarrow$ n is prime.

$103, \sqrt{103} \simeq 10$

$2, 3, 5, 7$ $\quad 2 \nmid 103, \; 3 \nmid 103, \; 5 \nmid 103, \; 7 \nmid 103$

103 is a prime no.

Q9. Determine whether each of these integers is prime?

(i) 107 $\quad \sqrt{107} \simeq 10 \quad 2, 3, 5, 7$

$2 \nmid 107, \; 3 \nmid 107, \; 5 \nmid 107, \; 7 \nmid 107$ Prime

(ii) 113 $\quad 2, 3, 5, 7$

$2 \nmid 113, \; 3 \nmid 113, \; 5 \nmid 113, \; 7 \nmid 113$ Prime

(iii) 1111 $\quad \sqrt{1111} \simeq 33$

$2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31$

× × × × ✓

$11 \mid 1111 \rightarrow$ Not Prime

Q10. Find prime factorization of 10! $= 10 \times 9 \times 8 \times 7 \times 6 \times 5 \times 4 \times 3 \times 2$

1 3 1 2 1

$2^8 \cdot 3^4 \cdot 5^2 \cdot 7^1$

How many zeros at end in 10! $= 2$.

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.

$7 = 2^3 - 1$, $3 = 2^2 - 1$, $2^{11} - 1 =$ Not Mersenne

- **Twin primes:** The pair of primes that differ by 2 are called Twin primes.

$(3,5)$ $(5,7)$, $(11,13)$

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 $\operatorname{lcm}(a, b)$.

How to find gcd and lcm using prime factorization of integers

$$a = p_1^{m_1} \cdot p_2^{m_2} \cdots p_k^{m_k}$$

$$b = p_1^{n_1} \cdot p_2^{n_2} \cdots p_k^{n_k}$$

$$\gcd(a,b) = p_1^{\min(m_1,n_1)} \cdot p_2^{\min(m_1,n_1)} \cdots p_k^{\min(m_k,n_k)}$$

$$\operatorname{lcm}(a,b) = p_1^{\max(m_1,n_1)} \, p_2^{\max(m_1,n_1)} \cdots p_k^{\max(m_k,n_k)}$$

Q11. Find gcd and lcm of given integers

(i) (1000, 625)

$1000 = 2^3 \cdot 5^3$ $\quad$ $\gcd = 2^0 \cdot 5^3 = 125$

$625 = 5^4$ $\quad$ $\operatorname{lcm} = 2^3 \cdot 5^4 = 5000$

(ii) (111, 201)

$111 = 3 \cdot 37$ $\quad$ $\gcd = 3$

(ii) (111, 201)

$111 = 3 \cdot 37$
$201 = 3 \cdot 67$

gcd = 3
lcm = $3 \cdot 37 \cdot 67 = 7437$

(iii)

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

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

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 $\gcd(a_i, a_j) = 1$ whenever $1 \leq i < j \leq n$.

- **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.

a) 21, 34, 55 ✓
b) 14, 17, 85 ✗
c) 25, 41, 49, 64 ✓
d) 17, 18, 19, 23 ✓

Q14.

Find these values of the Euler ϕ-function.

a) $\phi(4)$. b) $\phi(10)$. c) $\phi(13)$.

$\phi(4) = 2$ 1, 3 1, 2, 3, 4

$\phi(10) = 4$ 1, 3, 7, 9

$\phi(13) = 12$ $\phi(\text{prime}) = p - 1$

Q15.

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

Home Exercise.

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

$$p^k - p^{k-1}$$

$$\phi(2^{10}) = 2^{10} - 2^9$$
$$= 2^9(2-1)$$
$$= 2^9 \cdot 1$$