MAT2440, Classwork40, Spring2025

ID:_____ Name:_____

1. Least Common Multiples.

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

a. $|\text{lcm}(a,b)$ and b. $|\text{lcm}(a,b)$.

lcm(24, 36) = 72

multiples of 24 : 24, 48, 72, 96...

multiples of 36 : 36, 72, 108, ...

2. Find lcm: **Use prime factorization.**

If $a = p_1^{a_1} p_2^{a_2} \cdots p_n^{a_n}$ and $b = p_1^{b_1} p_2^{b_2} \cdots p_n^{b_n}$, then we have

$$\text{lcm}(a,b) = p_1^{\max(a_1,b_1)} p_2^{\max(a_2,b_2)} \cdots p_n^{\max(a_n,b_n)}.$$

3. Find lcm(24, 36) by using prime factorization.

$24 = 2^3 \times 3^1$

$36 = 2^2 \times 3^2$

$\Rightarrow \text{lcm}(24,36) = 2^3 \times 3^2 = 8 \times 9 = 72$

max(3,2) = 3, max(1,2) = 2

4. Find lcm: Use the greatest common divisors.

Let a, b be positive integers. Then

$$a \cdot b = \text{gcd}(a,b) \cdot \text{lcm}(a,b)$$

$$\Rightarrow \text{lcm}(a,b) = \frac{a \cdot b}{\text{gcd}(a,b)}$$

5. Find lcm(24, 36) by gcd(24, 36).

gcd(24,36) = 12

$$\text{lcm}(24,36) = \frac{24 \cdot 36}{\text{gcd}(24,36)} = \frac{24 \cdot 36}{12} = 72.$$

1. Introduction of Linear Congruences.

Let a, b be integers and m be a positive integer. A congruence of the form

$$ax \equiv b (\text{mod } m)$$

is called a linear Congruence where x is a variable. For example, $2x \equiv 3 (\text{mod } 7)$.

Solve $ax \equiv b (\text{mod } m) \Leftrightarrow$ Find all x such that $ax \equiv b (\text{mod } m)$.

2. How to solve a linear equation $2x = 3$? $\Rightarrow$ divide by 2 on both sides

$\frac{2x}{2} = \frac{3}{2}$

$\Rightarrow x = \frac{3}{2}$

(1) Solve for $2\bar{a} = 1$: $\bar{a} = \frac{1}{2}$ which is the inverse of 2

(2) Solve for $2x = 3$: By multiplying the inverse of 2 to both sides, we have

3. Steps to solve a linear congruence $ax \equiv b (\text{mod } m)$.

$\bar{a} \cdot a \equiv 1 \pmod m$

(1) Solve for $ax \equiv 1 (\text{mod } m)$: Find $x = \bar{a}$, the **inverse of a modulo m**.

(2) Solve for $ax \equiv b (\text{mod } m)$ by multiplying $\bar{a}$ to both sides:

$$\bar{a} \cdot ax \equiv \bar{a} \cdot b (\text{mod } m) \Leftrightarrow x \equiv \bar{a} \cdot b (\text{mod } m)$$

$\bar{a} \cdot ax \equiv 1 \pmod m$

4. How to solve for $ax \equiv 1 (\text{mod } m)$?

(a) Find $x \in \mathbb{Z}$ such that $3x \equiv 1 (\text{mod } 7)$.

$x = \frac{1}{3}$ is NOT the solution, since $\frac{1}{3}$ is not $\mathbb{Z}$

How many options of x do we have $x = 0, 1, 2, 3, 4, 5, 6$

$x=0$, $3(0) = 0 \equiv 0 \pmod 7$

$x=1$, $3(1) = 3 \equiv 3 \pmod 7$

$x=2$, $3(2) = 6 \equiv 6 \pmod 7$

$x=3$, $3(3) = 9 \equiv 2 \pmod 7$

$x=4$, $3(4) = 12 \equiv 5 \pmod 7$

$x=5$, $3(5) = 15 \equiv 1 \pmod 7$

$x = 5$. that is,

5 is the inverse of 3 mod 7

(b) Find $x \in \mathbb{Z}$ such that $2x \equiv 1 (\text{mod } 4)$.

$x = 0, 1, 2, 3$

$x=0$, $2(0) = 0 \equiv 0 \pmod 4$

$x=1$, $2(1) = 2 \equiv 2 \pmod 4$

$x=2$, $2(2) = 4 \equiv 0 \pmod 4$

$x=3$, $2(3) = 6 \equiv 2 \pmod 4$

$\Rightarrow$ There is no inverse of 2 modulo 4