

Some Definitions to Recall

First, let us recall some definitions:

Definition 1. If a and b are integers, and there exists an integer q such that $b = q \cdot a$, then we say that a **divides** b , which is our preferred way of saying that b is a multiple of a , or a is a divisor of b . We often use the notation

$$a \mid b$$

to mean “ a divides b ”.

Examples:

- $4 \mid 24$ because $24 = 6 \cdot 4$
- $n \mid 2n$ because $2n = 2 \cdot n$
- $3 \mid n(n+1)(n+2)$ for any integer n (Exercise: Can you prove it?)

With this notation, we define:

Definition 2. We say that $a \equiv b \pmod{n}$ if $n \mid a - b$.

Examples:

- $11 \equiv 2 \pmod{9}$ because $9 \mid 11 - 2$
- $34 \equiv 5 \pmod{29}$ because $29 \mid 34 - 5$
- $63 \equiv 3 \pmod{6}$ because $6 \mid 63 - 3$.
- $30^{99} + 61^{100} \equiv 0 \pmod{31}$ (Exercise: Can you show why?)

Definition 3. If m and n are positive integers, we say that $d = \gcd(m, n)$, or d is the **greatest common divisor** of m and n , if d is the largest positive integer that divides both m and n .

- $\gcd(24, 36) = 12$
- $\gcd(6, 9) = 3$

Linear Congruences

For each of the following congruences, find all solutions, or show that there aren't any:

1. $x - 2 \equiv 3 \pmod{5}$

2. $12x \equiv 0 \pmod{14}$

3. $3x \equiv 0 \pmod{14}$, with the requirement that $x \not\equiv 0 \pmod{14}$.

4. $6x \equiv 1 \pmod{39}$

5. $11x \equiv 1 \pmod{29}$