

Modular Arithmetic Properties

1. Congruence (Equality Modulo):

If $a \equiv b \pmod{m}$, then $(a \% m) == (b \% m)$ and m divides $(a - b)$.

2. Addition Rule:

$$(a + b) \% m = ((a \% m) + (b \% m)) \% m$$

3. Subtraction Rule:

$$(a - b) \% m = ((a \% m - b \% m) + m) \% m$$

4. Multiplication Rule:

$$(a * b) \% m = ((a \% m) * (b \% m)) \% m$$

5. Power Rule:

$$(a^{**}b) \% m = ((a \% m)^{**}b) \% m \text{ (use modular exponentiation)}$$

6. Modular Inverse:

If $\gcd(a, m) = 1$, then there exists a^{*-1} such that $a * a^{*-1} \equiv 1 \pmod{m}$.

7. Zero Difference Rule:

If $(a - b) \% m == 0$, then $a \equiv b \pmod{m}$, and $a \% m == b \% m$.

8. Additive Inverse:

If $(a + b) \% m == 0$, then $a \equiv -b \pmod{m}$.

9. Divisibility in Modulo:

If $a \% m == 0$, then m divides a .

10. Transitivity:

If $a \equiv b \pmod{m}$ and $b \equiv c \pmod{m}$, then $a \equiv c \pmod{m}$.

11. Zero Remainder Property:

If $a \% m == 0$ and $b \% m == 0$, then $(a + b)$, $(a - b)$, and $(a * b)$ are also $0 \pmod{m}$.

12. Distribution Over Parentheses:

$$(a + b + c) \% m = ((a \% m) + (b \% m) + (c \% m)) \% m$$

13. Negative Numbers:

$$(-a) \% m = (m - (a \% m)) \% m$$

14. Equality Check:

If $a \% m == b \% m$, then $(a - b) \% m == 0$.

15. Modulo with Itself:

Modular Arithmetic Properties

$a \% a = 0$ (if $a \neq 0$).