Modular Arithmetic

Stephen Styles

September 14, 2020

Properties of Modular Arithmetic:
Let $a_1 \equiv b_1 \bmod(n)$, $a_2 \equiv b_2 \bmod(n)$, and $a \equiv b \bmod(n)$, then

- $a + k \equiv b + k \bmod(n)$ for any integer k.
- $ka \equiv kb \bmod(n)$ for any integer k.
- $a_1 + a_2 \equiv b_1 + b_2 \bmod(n)$.
- $a_1 - a_2 \equiv b_1 - b_2 \bmod(n)$.
- $a_1 a_2 \equiv b_1 b_2 \bmod(n)$.
- $a^k \equiv b^k \bmod(n)$.

The general technique when given an equation to solve with modular arithmetic is to reduce each integer to the number it's congruent to. From there we can solve the equation and find the last congruence relation.

Examples:

1. Simplify $19^5 + 14 \cdot 25 - 62 \bmod(6)$.

   Solution:

   $19^5 \equiv 1^5 \bmod(6) = 1 \bmod(6)$
   $14 \times 25 \equiv 2 \times 1 \bmod(6) = 2 \bmod(6)$
   $62 \equiv 2 \bmod(6)$

   $19^5 + 14 \times 25 - 62 \bmod(6) \equiv 1 + 2 - 2 \bmod(6) = 1 \bmod(6)$

2. Simplify $30^4 \cdot 13 + 81 \bmod(7)$.

   Solution:

   $30^4 \times 13 \equiv 2^4 \times 6 \bmod(7) = 16 \times 6 \bmod(7) \equiv 2 \times 6 \bmod(7) = 12 \bmod(7) \equiv 5 \bmod(7)$
   $81 \equiv 4 \bmod(7)$

   $30^4 \times 13 + 81 \bmod(7) = 5 + 4 \bmod(7) = 9 \bmod(7) = 2 \bmod(7)$

3. Simplify $41^3 + 55 \times 36 - 29 \bmod(3)$

Solution:

$41^3 \equiv 2^3 \bmod(3) = 8 \bmod(3) \equiv 2 \bmod(3)$
$55 \times 36 \equiv 1 \times 0 \bmod(3) = 0 \bmod(3)$
$29 \equiv 1 \bmod(3)$

$41^3 + 55 \times 36 - 29 \bmod(3) \equiv 2 + 0 - 1 \bmod(3) = 1 \bmod(3)$

Examples:

1. Simplify $23 + 42 \times 3 - 2 \bmod(9)$

2. Simplify $17^2 + 81^4 + 8 \bmod(5)$

3. Simplify $13^{13} + 87 - 61 \times 115^3 \bmod(6)$