Modular Arithmetic
Dr. Vince

1 Introduction

Definition 1. We say $n \in \mathbb{Z}$ *divides* $m \in \mathbb{Z}$ if there exists $k \in \mathbb{Z}$ with $nk = m$. In this case, we write $n \mid m$. If no such k exists, we write $n \nmid m$.

Definition 2. Suppose $n \in \mathbb{Z}^+$. If $a, b \in \mathbb{Z}$, then we say *a is congruent to b modulo n* and write $a \equiv b \pmod{n}$ if $n \mid (a - b)$. We call n the *modulus*. If $n \nmid (a - b)$, we write $a \not\equiv b \pmod{n}$.

Example 3. $19 \equiv 7 \pmod{4}$ because $4 \mid (19 - 7) = 8$.

Example 4. $12 \not\equiv 17 \pmod{4}$ because $4 \nmid (12 - 17) = -5$.

Congruence can be though of as having the same remainder upon division by n. Notice $19 \div 4$ and $7 \div 4$ both result in a remainder of 3. Notice $12 \div 4$ has a remainder of 0, while $17 \div 4$ has a remainder of 1.

Theorem 5 (Properties)**.** *Properties: Suppose $a \equiv c \pmod{n}$ and $b \equiv d \pmod{n}$. Then*

(1) $a \pm b \equiv c \pm d \pmod{n}$.

(2) $ab \equiv cd \pmod{n}$.

(3) $a^k \equiv b^k \pmod{n}$ *for* $k \in \mathbb{Z}^+$.

(4) If $\gcd(a, n) = 1$, *then* $ab \equiv ac \pmod{n}$ *implies* $b \equiv c \pmod{n}$.

Example 6. Find 6271 mod 9.

Solution: Method 1: We find the remainder upon division by 9 and get 7. Thus, 6271 mod $9 \equiv 7$.

Method 2: $6271 = 6300 - 29 \equiv -29 \equiv -2 \pmod 9$.

Method 3: For 9, the divisibility test also works as a remainder test, so $6271 \equiv 6+2+7+1 \equiv 7 \pmod 9$.

$\square$

Example 7. Find $172 + 2719 - 187$ mod 10.

Solution: By the first property, we can reduce each term modulo 10 before adding and subtracting, so

$$172 + 2719 - 182 \equiv 2 + 9 - 7 \equiv 4 \pmod{10}$$

$\square$

Example 8. Find $19^{45} \cdot 70 + 8^3$ mod 6

Solution: We can reduce modulo 6 before combining values:

$$19^{45} \cdot 70 + 8^3 \equiv 1^{45} \cdot (-2) + 2^3 \equiv -2 + 8 \equiv 0 \pmod 6$$

$\square$

Example 9. Find 267^{14} mod 13

Solution: Reduce first, then make the calculation in smaller steps, reducing as needed. Notice you cannot reduce the exponent by the modulus directly.

$$\begin{aligned} 267^{14} &\equiv (260+7)^{14} \equiv 7^{14} \pmod{13} \\ &\equiv (7^2)^7 \equiv 49^7 \equiv (-3)^7 \pmod{13} \\ &\equiv ((-3)^3)^2(-3) \equiv (-27)^2(-3) \equiv (-1)^2(-3) \equiv 10 \pmod{13} \end{aligned}$$

In the above, we made use of the fact that $27 \equiv 1$ to help simplify the calculation.

$\square$

2 Practice

(1) $718 \bmod 5$

(2) $124,758 \bmod 20$

(3) $1,203 \bmod 9$

(4) $2,675 \bmod 11$

(5) $12,498 \bmod 8$

(6) $89,432 \bmod 16$

(7) $942 \bmod 7$

(8) $23,417 \bmod 12$

(9) $4,891 \bmod 13$

(10) $7,346 \bmod 15$

(11) $45,629 \bmod 17$

(12) $67,381 \bmod 19$

(13) $17 + 24 \bmod 6$

(14) $43 - 29 \bmod 8$

(15) $15 \times 7 \bmod 9$

(16) $82 + 19 \bmod 11$

(17) $37 - 14 \bmod 5$

(18) $12 \times 9 \bmod 15$

(19) $64 + 27 \bmod 10$

(20) $53 - 18 \bmod 7$

(21) $8 \times 13 \bmod 12$

(22) $91 + 34 \bmod 14$

(23) $2^{10} \bmod 3$

(24) $3^9 \bmod 5$

(25) $2^{12} \bmod 7$

(26) $5^6 \bmod 8$

(27) $4^9 \bmod 9$

(28) $7^5 \bmod 11$

(29) $6^7 \bmod 13$

(30) $8^{23} \bmod 15$

(31) $(15 + 29) \cdot 4 \bmod 7$

(32) $12^3 - 5 \cdot 17 + 41 \bmod 11$

(33) $8 \cdot 13^2 + 25 \div 5 \bmod 10$

(34) $(23 - 17)^3 \cdot 4 + 19 \bmod 8$

(35) $5 \cdot 2^7 - 3^4 \div 9 \bmod 6$

(36) $11^5 - 3^4 + 14 \cdot 6 \bmod 13$