11 More Properties of Congruences

The Inverse of a Modulo m

Theorem 11.1. *Let $m \geq 2$. If a and m are relatively prime ($\gcd(a, m) = 1$), then there exists a unique integer a^{-1} such that*

$$aa^{-1} \equiv 1 \pmod{m} \quad \textit{and} \quad 0 < a^{-1} < m.$$

Proof. Since $\gcd(a, m) = 1$. Then there exist integers s and t such that

$$as + mt = 1. \Rightarrow as - 1 = m(-t),$$

$\Rightarrow m \mid (as - 1) \Rightarrow as \equiv 1 \pmod{m}$. Thus, $a^{-1} = s \mod m$ satisfies $0 < a^* < m$ and we have:

$$aa^{-1} \equiv 1 \pmod{m}.$$

To prove uniqueness, Let there exists an integer c such that $ac \equiv 1 \pmod{m}$ and $0 < c < m$. From this, we have:

$$ac \equiv aa^{-1} \pmod{m} \Rightarrow c \equiv a^{-1} \pmod{m}.$$

Proving the uniqueness. □

Example 11.1. Let $m = 15$ and $a = 2$. We find the integer a^{-1} such that $a \cdot a^{-1} \equiv 1 \pmod{15}$.

$$2 \cdot 0 \not\equiv 1 \pmod{15}, \quad 2 \cdot 1 \not\equiv 1 \pmod{15}, \quad 2 \cdot 2 \not\equiv 1 \pmod{15},$$
$$2 \cdot 3 \not\equiv 1 \pmod{15}, \quad 2 \cdot 4 \not\equiv 1 \pmod{15}, \quad 2 \cdot 5 \not\equiv 1 \pmod{15},$$
$$2 \cdot 6 \not\equiv 1 \pmod{15}, \quad 2 \cdot 7 \not\equiv 1 \pmod{15}, \quad 2 \cdot 8 \equiv 1 \pmod{15},$$

because $15 \mid (16 - 1)$. Thus, we can take $a^{-} = 8$.

Remark 11.1. We call a^{-1} the inverse of a modulo m.

Theorem 11.2. *Let* $m > 0$. *If* $ab \equiv 1 \pmod{m}$, *then both* a *and* b *are relatively prime to* m, *i.e.,* $\gcd(a, m) = 1$ *and* $\gcd(b, m) = 1$.

Corollary 11.1. A number a has an inverse modulo m if and only if a and m are relatively prime, i.e., $\gcd(a, m) = 1$.

Theorem 11.3. *Let* $m > 0$. *If* $\gcd(c, m) = 1$, *then* $ca \equiv cb \pmod{m}$ *implies* $a \equiv b \pmod{m}$.

Theorem 11.4. *If* $c > 0$ *and* $m > 0$, *then*

$$a \equiv b \pmod{m} \iff ca \equiv cb \pmod{cm}.$$

Theorem 11.5. *If* $m > 0$ *and* $a \equiv b \pmod{m}$, *then*

$$\gcd(a, m) = \gcd(b, m).$$

11.1 Finding Modular Inverses Using the Extended Euclidean Algorithm

Given an integer a and a modulus m, the modular inverse of a modulo m is an integer x such that:

$$ax \equiv 1 \pmod{m} \tag{8}$$

The modular inverse exists if and only if $\gcd(a, m) = 1$. We use the **Extended Euclidean Algorithm** to compute it.

Example 11.2. Find the inverse of 7 modulo 20.

Sol. We apply the Euclidean algorithm:

$$20 = 2 \times 7 + 6$$

$$7 = 1 \times 6 + 1$$

$$6 = 6 \times 1 + 0$$

Since $\gcd(7, 20) = 1$, an inverse exists.

Now, we work backward:

$$
\begin{aligned}
1 &= 7 - 1 \times 6 \\
&= 7 - 1(20 - 2 \times 7) \\
&= 7 - 20 + 2 \times 7 \\
&= 3 \times 7 - 1 \times 20
\end{aligned}
$$

Thus, $7^{-1} \equiv 3 \pmod{20}$. □

Example 11.3. Find the inverse of 11 modulo 26.

Sol. Using the Euclidean algorithm:

$$
\begin{aligned}
26 &= 2 \times 11 + 4 \\
11 &= 2 \times 4 + 3 \\
4 &= 1 \times 3 + 1 \\
3 &= 3 \times 1 + 0
\end{aligned}
$$

Since $\gcd(11, 26) = 1$, an inverse exists.

Working backward:

$$
\begin{aligned}
1 &= 4 - 1 \times 3 \\
&= 4 - 1(11 - 2 \times 4) \\
&= 3 \times 4 - 1 \times 11 \\
&= 3(26 - 2 \times 11) - 1 \times 11 \\
&= 3 \times 26 - 7 \times 11
\end{aligned}
$$

Thus, $11^{-1} \equiv -7 \equiv 19 \pmod{26}$. □

Example 11.4. Find the inverse of 17 modulo 43

Sol. Using the Euclidean algorithm:

$$43 = 2 \times 17 + 9$$
$$17 = 1 \times 9 + 8$$
$$9 = 1 \times 8 + 1$$
$$8 = 8 \times 1 + 0$$

Since $\gcd(17, 43) = 1$, an inverse exists.

Working backward:

$$\begin{aligned} 1 &= 9 - 1 \times 8 \\ &= 9 - 1(17 - 1 \times 9) \\ &= 2 \times 9 - 1 \times 17 \\ &= 2(43 - 2 \times 17) - 1 \times 17 \\ &= 2 \times 43 - 5 \times 17 \end{aligned}$$

Thus, $17^{-1} \equiv -5 \equiv 38 \pmod{43}$. □

11.2 Exercises of More Properties of Congruences

Exercises

1. Show that the inverse of 2 modulo 7 is not the inverse of 2 modulo 15.
2. Let $m > 0$. If $ab \equiv 1 \pmod{m}$, then both a and b are relatively prime to m.
3. If $c > 0$ and $m > 0$, then $a \equiv b \pmod{m} \iff ca \equiv cb \pmod{cm}$.
4. If there exists a^-1 find for each following

   (a) $11^{-1} \mod 43$, (b) $29^{-1} \mod 78$, (c) $6^{-1} \mod 19$.