

CSCI 124

Discrete Structures II: Existence of Multiplicative Inverse

Poorvi L. Vora

In this module, we see the relationship between the gcd and the multiplicative inverse *mod* m .

Recall **Definition:** The greatest common divisor of two positive integers m and n is the largest integer that divides both m and n . It is denoted (m, n) or $\gcd(m, n)$.

In other words,

$$g = (m, n) \Leftrightarrow \begin{cases} g|m, g|n \\ x|m, x|n \Rightarrow x|g \end{cases}$$

Definition: m and n are said to be relatively prime if $(m, n) = 1$.

As we saw in class, we need a lemma before we can completely prove the main result, which is:

Theorem: Let $x \in \mathbb{Z}_m$ for some positive integer m . $x^{-1} \text{ mod } m \text{ exists} \Leftrightarrow (m, x) = 1$

We first show the lemma:

Lemma: $(m, n) = 1 \Rightarrow \exists s, t \in \mathbb{Z}$ such that $sm + tn = 1$

Proof:

Suppose $(m, n) = 1$.

Consider all integers of the form $Am + Bn$ for integers A and B . That is, consider $S = \{y | y = Am + Bn, A, B \in \mathbb{Z}\}$.

Let $g = A_0m + B_0n$ be the smallest positive value in S . We would like to show that $g = (m, n) = 1$, and hence that $\exists s = A_0 \in \mathbb{Z}, t = B_0 \in \mathbb{Z}, s.t. sm + tn = g = 1$.

Consider any arbitrary value in $S, y = Am + Bn$.

Let $r = y \text{ rem } g$. That is,

$$\begin{aligned} r &= Am + Bn - q_y g \text{ for some } q_y \in \mathbb{Z} \\ &= (A - q_y A_0)m + (B - q_y B_0)n \end{aligned}$$

Notice that $A - q_y A_0 \in \mathbb{Z}$ and $B - q_y B_0 \in \mathbb{Z}$ and hence $r \in S$.

However, g is the smallest positive integer in S , and $0 \leq r < g$.

Hence

$$\begin{aligned} r &= 0 \\ &\Rightarrow g|y, \forall A, B \\ &\Rightarrow g|m \quad (A = 1, B = 0), \quad \text{and } g|n \quad (A = 0, B = 1) \end{aligned}$$

As g is a common divisor of m and n , $g|(m, n) = 1 \Rightarrow g = (m, n)$.

$$(m, n) = g = 1 \Rightarrow \exists s = A_0, t = B_0, \text{ s.t. } sm + tn = g = 1$$

□

Now we can prove the main theorem.

Theorem: Let $x \in \mathbb{Z}_m$ for some positive integer m . $x^{-1} \text{ mod } m \text{ exists} \Leftrightarrow (m, x) = 1$

Proof:

\Rightarrow Let $x \in \mathbb{Z}_m$ for some positive integer m , and suppose $\exists x^{-1} \in \mathbb{Z}_m$ such that $xx^{-1} = 1 \text{ mod } m$. Let $g = (m, x)$.

Then $x = q_x g$ and $m = q_m g$. Hence:

$$\begin{aligned} xq_m &= q_x g q_m = q_x m \equiv 0 \pmod{m} \\ &\Rightarrow x^{-1} x q_m \equiv x^{-1} 0 \pmod{m} \\ &\Rightarrow q_m \equiv 0 \pmod{m} \\ &\Rightarrow q_m = m \end{aligned}$$

Because $1 \leq q_m \leq m$. Hence $g = 1$.

\Leftarrow Suppose $(m, x) = 1$. Then, by the lemma, $\exists s, t \in \mathbb{Z}$, such that $sm + tx = 1$.

$$\begin{aligned} sm + tx &= 1 \\ &\Rightarrow tx \equiv 1 \pmod{m} \\ &\Rightarrow t \equiv x^{-1} \pmod{m} \\ &\Rightarrow x^{-1} = t \pmod{m} \end{aligned}$$

hence $\exists x^{-1} \in \mathbb{Z}_m$.

Example: How many elements in \mathbb{Z}_{10} are invertible? What are the invertible elements?

The invertible elements are those that are relatively prime to 10. These elements are: 1, 3, 7, 9. The number of invertible elements is 4.

Example: How many distinct keys for the affine cipher exist over \mathbb{Z}_{10} ?

There are 4 invertible elements, hence 4 values of a . There are 10 values of b . Hence there is a total of 40 possibilities for the key.