

CSCI 162/284

Cryptography: GCD and Multiplicative Inverses *mod m*

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

Examples: $(6, 9) = 3$, $(12, 36) = 12$, $(5, 9) = 1$.

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

The following theorem characterizes all the elements with multiplicative inverses in \mathbb{Z}_m . Essentially, exactly those elements a such that $\gcd(m, a) = 1$ are invertible.

There are two parts to showing this. The first is to show that, if the element a has an inverse *mod m*, then $\gcd(a, m) = 1$. The second is the other direction: to show that, if $\gcd(a, m) = 1$, then a^{-1} exists. The first is easier than the second.

The proof sketch of the second part is as follows. The formal proof is provided later.

Suppose $\gcd(m, a) = 1$. Consider the collection of all integers that are combinations of m and a , that is, are of the form $Sm + Ta$. Consider the smallest positive integer in this collection, call it g . Examine the remainders when the numbers in the collection are divided by g .

We can see that the remainders are also in the collection. However, because g is the smallest positive integer in the collection, and the remainders are smaller than g and non-negative, they are all zero. Hence g divides all numbers in the collection. In particular, it divides m and a , which also belong to the collection. (m corresponds to $S = 1$ and $T = 0$, and a to $S = 0$ and $T = 1$.) Hence g is a common factor of a and m . However, as $\gcd(a, m) = 1$, $g = 1$ is the only possible positive common factor.

Hence $g = 1$ is in the collection, and can be expressed in the form $sm + at$; that is, $sm + at = 1$. Looking at this equation *mod m*, we get that $at \equiv 1 \pmod{m}$, and that $a^{-1} \pmod{m}$ exists.

Theorem: a has a multiplicative inverse *mod m*, denoted $a^{-1} \pmod{m} \Leftrightarrow \gcd(m, a) = 1$

Proof:

\Rightarrow

Suppose a^{-1} exists. Then, there exists integer t such that $at \equiv 1 \pmod{m}$. That is, there exist integers s, t such that $at + sm = 1$. A common factor of a and m would divide both terms on the left hand side of the equation, and hence would also divide the right hand side. But, as the right hand side is 1, the only positive integer divisor of it can be 1, hence the only positive common factor of a and m is 1. Hence $\gcd(a, m) = 1$.

\Leftarrow

Suppose $\gcd(m, n) = 1$.

Consider all integers of the form $Sm + Ta$ for integers S and T .

Let $g = S_0m + T_0a$ be the smallest such positive integer. We show that $g = 1$, and hence that $\exists t = T_0, s = S_0$ such that $sm + ta = g = 1$. Looking at this equation *mod m*, we see that it implies that $at \equiv 1 \pmod{m}$, that is, that

$a^{-1} \bmod m$ exists. (In fact, $t = a^{-1} \bmod m$). We proceed as follows.

Consider any arbitrary integer $x = Sm + Ta$.

Let $r = x \bmod g$ be the remainder when x is divided by g . It is the unique non-negative integer smaller than g such that $x = qg + r$. Then,

$$\begin{aligned} r &= x - qg \quad q \in \mathbb{Z} \\ &= Sm + Ta - qg \\ &= (S - qS_0)m + (T - qT_0)a \end{aligned}$$

and r is also a combination of m and a .

However, g is the smallest positive integer of that form, and r is smaller than g .

Hence

$$\begin{aligned} r &= 0 \\ &\Rightarrow g \mid Sm + Ta, \forall S, T \\ &\Rightarrow g \mid m, g \mid n \quad (S = 1, T = 0; S = 0, T = 1) \end{aligned}$$

But, $\gcd(a, m) = 1$, hence $g = 1$.

Hence there exists $S = S_0$ and $T = T_0$ such that $S_0m + T_0a = 1$. That is, $T_0a \equiv 1 \bmod m$, and $a^{-1} \bmod m$ exists (in fact, its value is T_0). \square