

CSCI 124/224

Discrete Structures II: GCD

Poorvi L. Vora

Recall that we showed, in the module on Groups, that x has a multiplicative inverse *modulo* m if and only if $\exists a, b \in \mathbb{Z}$ s.t. $ax + bm = 1$. In this module, we see that this is related to a very familiar concept, the GCD. We also see how we may find out if such a and b exist.

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,

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

Here $a|b$ is notation for “ a divides b ”. Recall that $a|b \Rightarrow b = ka$ for some $k \in \mathbb{Z}$.

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

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

Theorem: $(m, n) = 1 \Leftrightarrow \exists a, b$, s.t. $am + bn = 1$

Proof:

\Rightarrow

Suppose $(m, n) = 1$.

Consider all integers of the form $Am + Bn$ for integers A and B .

Let $g = A_0m + B_0n$ be the smallest such integer. We show that $g = (m, n) = 1$, and hence that $\exists a = A_0, b = B_0$, s.t. $am + bn = g = 1$.

Consider any arbitrary integer $x = Am + Bn$.

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

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

and r is also a combination of m and n .

However, g is the smallest non-negative integer of that form, and r is smaller than g .

Hence

$$\begin{aligned} r &= 0 \\ &\Rightarrow g|Am + Bn, \forall A, B \\ &\Rightarrow g|m, g|n \end{aligned}$$

Also,

$$x|m, x|n \Rightarrow x|A_0m + B_0n = g$$

Hence,

$$(m, n) = g = 1 \Rightarrow \exists a = A_0, b = B_0, \text{ s.t. } am + bn = g = 1$$

\Leftarrow

Suppose $\exists a, b$, s.t. $am + bn = 1$. Then,

$$(m, n)|m, (m, n)|n \Rightarrow (m, n)|1 \Rightarrow (m, n) = 1$$

1 Condition for the Existence of an Inverse in \mathbb{Z}_m

The theorem above immediately provides a necessary and sufficient condition for the existence of inverses in \mathbb{Z}_m .

Corollary $x \in \mathbb{Z}_m$ is invertible $\Leftrightarrow (x, m) = 1$.

Proof:

From above theorem and the theorem in the module on groups, the above corollary follows. \square

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.

In the next section, we describe an algorithm to determine the gcd of two given elements. It can easily be used to determine if the value a of the affine cipher is invertible over \mathbb{Z}_m .

2 $(m, n) = (n, m \text{ rem } n)$

The euclidean algorithm for the gcd of two elements is thought to be the oldest existing algorithm. It is recursive. It uses the following idea:

Theorem: $(m, n) = (n, m \text{ rem } n)$

Proof: Let $g = (m, n)$, and $r = m \text{ rem } n$, then

$$m = r + q_m n, q_m \in \mathbb{Z} \quad (1)$$

Because $g = (m, n)$, the following are known:

$$g|m, g|n \quad (2)$$

$$x|m, x|n \Rightarrow x|g \quad (3)$$

$$(1), (2) \Rightarrow g|r \quad (4)$$

$$y|r, y|n \Rightarrow y|m \text{ (from (1))} \Rightarrow y|g \text{ (from (3))} \quad (5)$$

$$(4), (5) \Rightarrow g = (n, r)$$

3 The Euclidean Algorithm

The euclidean algorithm is as follows:

$gcd(m, n)$ /* $m > n$ */

$(a, b) := (m, n)$ /* Initialize */

while $(b \neq 0)$ $(a, b) := (b, a \text{ rem } b)$

return(a)

Example Use the euclidean algorithm to determine $gcd(79, 551)$.

$$(a, b) = (551, 79)$$

$$(a, b) = (79, 77)$$

$$(a, b) = (77, 2)$$

$$(a, b) = (2, 1)$$

$$(a, b) = (1, 0)$$

return(1)

Example Use the euclidean algorithm to determine $gcd(632, 5056)$.

$$(a, b) = (869, 632)$$

$$(a, b) = (632, 237)$$

$$(a, b) = (237, 158)$$

$$(a, b) = (158, 79)$$

$$(a, b) = (79, 0)$$

return(79)

In each recursion, $gcd(a, b)$ stays the same while a and b change. Further, at each step, we decrease both a and b , and neither is ever negative. Hence the algorithm will end some time, in fact, in at most n steps. Finally, at the last but one

recursion, because $a \text{ rem } b$ is zero, a is a multiple of b and hence $\gcd(a, b) = b$. At the last recursion, $(a, b) = (b, 0)$ and the returned value a is the correct \gcd (it is the value of b from the previous recursion).

Thus we now have a means of determining if a given element in \mathbb{Z}_m is invertible, and hence can be used for the value of a in the affine cipher. However, we need the value of a^{-1} for a decryption. In the next section, we study an extension of the euclidean GCD algorithm to find the inverse of an invertible element in \mathbb{Z}_m .