

CSCI 124

Discrete Structures II: Euclidean Algorithm

Poorvi L. Vora

In this module, we observe that an element $x \in \mathbb{Z}_m$ has a multiplicative inverse $\text{mod } m$ if and only if $\text{gcd}(x, m) = 1$. The module also presents the euclidean algorithm for finding $\text{gcd}(x, m)$.

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 $\text{gcd}(m, n)$.

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 $(m, n) = 1$.

Example: The invertible elements in \mathbb{Z}_{10} are those that are relatively prime to 10. How many elements in \mathbb{Z}_{10} are invertible? What are the invertible elements?

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 . we will prove it is correct later.

1 The Euclidean Algorithm

The euclidean algorithm is as follows:

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

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

```
while (b ≠ 0) (a, b) := (b, a rem b)
```

```
return(a)
```

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

$$\begin{aligned}(a, b) &= (551, 79) \\(a, b) &= (79, 77) \\(a, b) &= (77, 2) \\(a, b) &= (2, 1) \\(a, b) &= (1, 0) \\&\text{return}(1)\end{aligned}$$

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

$$\begin{aligned}(a, b) &= (869, 632) \\(a, b) &= (632, 237) \\(a, b) &= (237, 158) \\(a, b) &= (158, 79) \\(a, b) &= (79, 0) \\&\text{return}(79)\end{aligned}$$

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 $a \bmod b$ 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 module, we will study an extension of the euclidean GCD algorithm to find the inverse of an invertible element in \mathbb{Z}_m .