Integers modulo n – Multiplicative Inverses

Paul Stankovski

Recall the Euclidean algorithm for calculating the greatest common divisor (GCD) of two numbers.

If you have an integer a, then the multiplicative inverse of a in $\mathbb{Z}/n\mathbb{Z}$ (the integers modulo n) exists precisely when $\gcd(a, n) = 1$. That is, if $\gcd(a, n) \neq 1$, then a does not have a multiplicative inverse.

The multiplicative inverse of a is an integer x such that

$$a \cdot x \equiv 1 \pmod{n},$$

or equivalently, an integer x such that

$$a \cdot x = 1 + k \cdot n$$

for some k. If we simply rearrange the equation to read

$$a \cdot x - k \cdot n = 1,$$

then the equation can be read as "The integer a has a multiplicative inverse x if and only if 1 (one) can be written as a linear combination of a's and n's".

We proceed by example.

Example 1. If $n = 36$ and $a = 2$, then $\gcd(a, n) = \gcd(2, 36) = 2$, so 2 *does not* have an inverse in $\mathbb{Z}/36\mathbb{Z}$. In this case, the notation 2^{-1} does not make any sense. □

Example 2. If $n = 36$ and $a = 5$, then $\gcd(a, n) = \gcd(5, 36) = 1$, so 5 *does* have an inverse in $\mathbb{Z}/36\mathbb{Z}$, and the notation 5^{-1} makes sense in this case.

To calculate the multiplicative inverse, calculate the GCD, proceeding until you get remainder 1 (one). In this case it is a simple one-liner.

$$36 = 7 \cdot 5 + 1$$

Note that you have just written 1 (one) as a linear combination of 5's and 36's. Rearranging, we get

$$5 \cdot (-7) = 1 + (-1) \cdot 36.$$

Comparing this with

$$a \cdot x = 1 + k \cdot n,$$

it can be seen that $x = -7$ and $k = -1$ is a solution. We do not care about the value of k, but the multiplicative inverse of 5 is clearly $x = -7$.

Does it make sense to have a negative value when we are working with the integers modulo n? Well, yes, as we are free to add or remove multiples of 36, -7 is just another way of writing 29. Therefore we have $5^{-1} = 29$. $\square$

Example 3. If $n = 36$ and $a = 17$, then $\gcd(a, n) = \gcd(17, 36) = 1$, so 17 *does* have an inverse in $\mathbb{Z}/36\mathbb{Z}$, and the notation 17^{-1} makes sense.

To calculate the multiplicative inverse, apply Euclid's algorithm, proceeding until you get remainder 1 (one).

$$36 = 2 \cdot 17 + 2, \tag{1}$$
$$17 = 8 \cdot 2 + 1. \tag{2}$$

Rearranging Eq. (2), we get

$$1 \cdot 17 + (-8) \cdot 2 = 1. \tag{3}$$

Here, you have not (yet) written 1 (one) as a linear combination of 17's and 36's, but as a linear combination of 17's and 2's. However, Eq. (1) gives us a way to write 2's as a linear combination of 17's and 36's, so we can substitute the 2's according to

$$1 \cdot 36 + (-2) \cdot 17 = 2.$$

Substitution into Eq. (3) gives us

$$1 \cdot 17 + (-8) \cdot \Big(1 \cdot 36 + (-2) \cdot 17\Big) = 1, \tag{4}$$

which simplifies to

$$17 \cdot 17 + (-8) \cdot 36 = 1.$$

Again, rearranging and comparing with

$$a \cdot x = 1 + k \cdot n,$$

it can be seen that $x = 17$ and $k = 8$, so 17 is its own inverse. It is correct to write $17^{-1} = 17$. $\square$

In the general case, applying the Euclidean algorithm may produce many rows/equations. When calculating the multiplicative inverse, you will then need to substitute several times – once per additional row.

To summarize all of this, calculating the multiplicative inverse of a in $\mathbb{Z}/n\mathbb{Z}$ is quite easy (mechanical) if you remember the general trick. Use Euclid's algorithm to express 1 (one) as a linear combination of a's and n's.