Finding Multiplicative Inverses Modulo *n*

Two unequal numbers being set out, and the less being continually subtracted in turn from the greater, if the number which is left never measures the one before it until an unit is left, the original numbers will be prime to one another. Euclid*, The Elements, Book VII,* Proposition 1.

It is not necessary to do trial and error to determine the multiplicative inverse of an integer modulo *n*. If the modulus being used is small (like 26) there are only a few possibilities to check (26); trial and error might be a good choice. However, some modern public key cryptosystems use very large moduli and require the determination of inverses.

We will now examine a method (due to Euclid [c. 325 – 265 BC]) that can be used to construct multiplicative inverses modulo *n* (when they exist).

Euclid's *Elements*, in addition to geometry, contains a great deal of number theory – properties of the positive integers (whole numbers). The Euclidean algorithm is Proposition II of Book VII of Euclid's *Elements*. Euclid's question was this: given two lengths (which are positive integers) what is the largest (integer) length that can be used to measure both of them? For example, if the two given lengths are 14 and 21, the largest length that measure both of them is 7; 14 is 2×7 and 21 is 3×7. If the two lengths are 24 and 40, the *greatest common measure* is 8. If the two lengths are 7 and 25, the greatest common measure is 1. Etc.

Euclid describes a process for determining the greatest common measure of two lengths. In terms of number theory, he is describing how to find what is now called the **greatest common divisor** (gcd) of two positive integers.

The Euclidean Algorithm to Find the Greatest Common Divisor

Let us begin with the two positive integers, say, 13566 and 35742.

Divide the smaller into the larger:

$$35742 = 2 \times 13566 + 8610$$

Divide the remainder (8610) into the previous divisor (35742):

$$13566 = 1 \times 8610 + 4956$$

Continue to divide remainders into previous divisors:

$$8610 = 1 \times 4956 + 3654$$

$$4956 = 1 \times 3654 + 1302$$

$$3654 = 1 \times 1302 + 1050$$

$$1302 = 1 \times 1050 + 252$$

$$1050 = 4 \times 252 + 42$$

$$252 = 6 \times 42$$

The process stops when the remainder is 0.

The greatest common divisor of 13566 and 35742 is 42.

gcd(13566, 35742)=42.

Why the Euclidean Algorithm Works

To see why the algorithm works, we follow the division steps backwards.

First, notice that 42 is indeed a common divisor of 13566 and 35742.

> Because $252 = 6 \times 42$, 42 divides 252.
>
> $1050 = 4 \times 252 + 42$. Because 42 divides both 42 and 252, it divides the right-hand side; therefore, 42 divides the left-hand side 1050.
>
> $1302 = 1 \times 1050 + 252$. Because 42 divides 252 and 1050, it divides the right-hand side; therefore, it divides the left-hand side 1302.
>
> $3654 = 2 \times 1302 + 1050$. Because 42 divides 1050 and 1302, it divides the right-hand side; therefore, it divides the left-hand side 3654.
>
> $4956 = 1 \times 3654 + 1302$. Because 42 divides 1302 and 3654, it divides the right-hand side; therefore, it divides the left-hand side 4956.
>
> $8610 = 1 \times 4956 + 3654$. Because 42 divides 3654 and 4956, it divides the right-hand side; therefore, it divides the left-hand side 8610.
>
> $13566 = 1 \times 8610 + 4956$. Because 42 divides 4956 and 8610, it divides the right-hand side; therefore, it divides the left-hand side 13566.
>
> $35742 = 2 \times 13566 + 8610$. Because 42 divides 8610 and 13566, it divides the right-hand side; therefore, it divides the left-hand side 35742.

So, 42 is a common divisor of 13566 and 35742.

Now, we must see that it is the *greatest* common divisor. We do this by showing that 42 can be written in terms of 13566 and 35742 as follows:

Begin near the bottom of the divisions. Because $1050 = 4 \times 252 + 42$,

$$42 = 1 \times 1050 - 4 \times 252$$

Because $1302 = 1 \times 1050 + 252$, $252 = 1 \times 1320 - 1 \times 1050$. Substitute this for 252 in the expression above for 42.

$$\begin{aligned} 42 &= 1 \times 1050 - 4 \times 252 \\ 42 &= 1 \times 1050 - 4 \times (1 \times 1302 - 1 \times 1050) \\ 42 &= 5 \times 1050 - 4 \times 1302 \end{aligned}$$

Because $3654 = 2 \times 1302 + 1050$, $1050 = 1 \times 3654 - 2 \times 1302$. So,

$$\begin{aligned} 42 &= 5 \times 1050 - 4 \times 1302 \\ 42 &= 5 \times (1 \times 3654 - 2 \times 1302) - 4 \times 1302 \\ 42 &= 5 \times 3654 - 14 \times 1302 \end{aligned}$$

Because $4956 = 1 \times 3654 + 1302$, $1302 = 1 \times 4956 - 1 \times 3654$. So,

$$\begin{aligned} 42 &= 5 \times 3654 - 14 \times 1302 \\ 42 &= 5 \times 3654 - 14 \times (1 \times 4956 - 1 \times 3654) \\ 42 &= 19 \times 3654 - 14 \times 4956 \end{aligned}$$

Because $8610 = 1 \times 4956 + 3654$, $3654 = 1 \times 8610 - 1 \times 4956$. So,

$$\begin{aligned} 42 &= 19 \times 3654 - 14 \times 4956 \\ 42 &= 19 \times (1 \times 8610 - 1 \times 4956) - 14 \times 4956 \\ 42 &= 19 \times 8610 - 33 \times 4956 \end{aligned}$$

Because $13566 = 1 \times 8610 + 4956$, $4956 = 1 \times 13566 - 1 \times 8610$. So,

$$\begin{aligned} 42 &= 19 \times 8610 - 33 \times 4956 \\ 42 &= 19 \times 8610 - 33 \times (1 \times 13566 - 1 \times 8610) \\ 42 &= 52 \times 8610 - 33 \times 13566 \end{aligned}$$

Because $35742 = 2 \times 13566 + 8610$, $8610 = 1 \times 35742 - 2 \times 13566$. So,

$$\begin{aligned} 42 &= 52 \times 8610 - 33 \times 13566 \\ 42 &= 52 \times (1 \times 35742 - 2 \times 13566) - 33 \times 13566 \\ 42 &= 52 \times 35742 - 137 \times 13566 \end{aligned}$$

What is important here is that the gcd of 35742 and 13566 can be expressed as a combination of them by reversing the division portion of the Euclidean algorithm. So, any common divisor of 35742 and 13566 must divide the right-hand side of $42 = 52 \times 35742 - 137 \times 13566$ and, therefore, must divide 42. This implies that 42 is the *greatest* common divisor.

Relatively Prime

A pair of positive integers is said to be *relatively prime* if their greatest common divisor is 1. 3 and 5 are relatively prime because gcd(3, 5) = 1. 4 and 15 are relatively prime because gcd(4, 15) = 1. But, 6 and 33 are not relatively prime because gcd(6, 33) = 3.

Finding Multiplicative Inverses Modulo *n*

Any positive integer that is less than *n* and relatively prime to *n* has a multiplicative inverse modulo *n*. This is a consequence of the Euclidean algorithm. We will see in the example below why this must be so. Any positive integer that is less than *n* and not relatively prime to n does not have a multiplicative inverse modulo *n*.

gcd(15, 26) = 1; 15 and 26 are relatively prime. Therefore, 15 has a multiplicative inverse modulo 26. Using the Euclidean algorithm, we will construct the multiplicative inverse of 15 modulo 26.

First, do the "forward part" of the Euclidean algorithm – finding the gcd.

$$26 = 1 \times 15 + 11$$

$$15 = 1 \times 11 + 4$$

$$11 = 2 \times 4 + 3$$

$$4 = 1 \times 3 + 1$$

So, gcd(15, 26) = 1.

Now, do the "backward part" of the algorithm (this is often called the “extended Euclidean algorithm)– expressing 1 as a combination of 15 and 26.

$$1 = 4 - 1 \times 3$$

$$1 = 4 - 1 \times (11 - 2 \times 4)$$
$$1 = 3 \times 4 - 1 \times 11$$

$$1 = 3 \times (15 - 1 \times 11) - 1 \times 11$$
$$1 = 3 \times 15 - 4 \times 11$$

$$1 = 3 \times 15 - 4 \times (26 - 1 \times 15)$$

$$1 = 7 \times 15 - 4 \times 26$$

So, $1 = 7 \times 15 - 4 \times 26$.

Finally, "go mod 26." Because $26 = 0 \bmod 26$, when we "go mod 26," the equation $1 = 7 \times 15 - 4 \times 26$ becomes the congruence $1 = 7 \times 15 \bmod 26$. So, the inverse of 15 modulo 26 is 7 (and the inverse of 7 modulo 26 is 15).

gcd(6, 26) = 2; 6 and 26 are not relatively prime. Therefore, 6 does not have a multiplicative inverse modulo 26. For, assume that it did; say, *m* is the multiplicative inverse of 6 modulo 26. Then we would have that $6m = 1 \bmod 26$. This means that 6*m* is equal to 1 plus a multiple of 26: 6*m* = 1 + 26*k*. But, 2 divides 6 and 2 divides 26; therefore, if the equation is correct, 2 divides 1. Of course, this is false; therefore, the assumption that 6 has a multiplicative inverse modulo 26 must be false. A similar argument would work for any integer that is not relatively prime to 26.

1, 3, 5, 7, 9, 11, 15, 17, 19, 21, 23, 25 are relatively prime to 26 and, therefore, have inverses modulo 26. 2, 4, 6, 8, 10, 12, 13, 14, 16, 18, 20, 22, 24 are not relatively prime to 26 and, therefore, do not have inverses modulo 26.

Exercises

1. Determine each of the following greatest common divisors. You need not use the Euclidean algorithm to find the gcds. Which of the pairs are relatively prime?

2a. gcd(6, 15)
2b. gcd(6, 16).
2c. gcd(8, 17).
2d. gcd(6, 21).
2e. gcd(15, 27).

2. Determine each of the following greatest common divisors. Which of the pairs are relatively prime?

3a. gcd(37, 3120).
3b. gcd(24, 138).
3c. gcd(12378, 3054).
3d. gcd(314, 159).
3e. gcd(306, 657).

3. For each of the gcds in exercise 2, write the gcd as a combination of the two given integers.

4. Find the multiplicative inverse of 37 modulo 3120.

5. Find the multiplicative inverse of 19 modulo 26.

6. Does 24 have a multiplicative inverse modulo 138 Explain.

7. What integers modulo 16 have multiplicative inverses? Determine the inverses.

8. What integers modulo 7 have multiplicative inverses? Determine the inverses.

9. What integers modulo 14 have multiplicative inverses? Determine the inverses.

10. What integers modulo 9 have multiplicative inverses? Determine the inverses.