Modulo Inverses

P. Reany

June 21, 2023

Abstract

We show how to find the inverse of an integer modulo some other integer. We assume the reader knows about the Euclidean Algorithm and modulo arithmetic.

1 Introduction

The Euclidean Algorithm is used to find the the greatest common denominator (GCD) of two integers. If the GCD of two integers is unity, 1) they are said to be *relatively prime*, and 2) we can find the multiplicative inverse of one of the integers with respect to the other.

Say we have two relatively prime integers a and b, and we want to know the multiplicative inverse of a modulo b. We are guaranteed by Bézout's Lemma that there exist integers x and y, such that

$$ax + by = 1\,. \tag{1}$$

Now, if we reduce this equation modulo b we get

$$ax \equiv 1 \pmod{b}\,. \tag{2}$$

Hence, x is the multiplicative inverse of $a \pmod{b}$. And that deals with the issue of existence.

2 Problem 1

Somewhere in my travels, I found this problem: Find $27^{-1} (\text{mod } 392)$. So, let's find it. In a moment we will show that 27 and 392 are relatively prime and hence there exist integers x and y, such that

$$27x + 392y = 1\,. \tag{3}$$

And, on reducing this modulo 392, we get

$$27x \equiv 1 \pmod{392}\,, \tag{4}$$

and x is the inverse of 27 in this modulo number system.

So we use the Euclidean Algorithm to show that 27 and 392 are relatively prime:

$$392 = 14 \cdot 27 + 14\,, \tag{5a}$$
$$27 = 1 \cdot 14 + 13\,, \tag{5b}$$
$$14 = 1 \cdot 13 + 1\,. \tag{5c}$$

According to the Euclidean Algorithm, the last remainder 1 is the GCD of 392 and 27, which proves that an inverse exists. Next, we want to solve these last three equations for the remainders, like such:

$$14 - 1 \cdot 13 = 1\,, \tag{6a}$$
$$27 - 1 \cdot 14 = 13\,, \tag{6b}$$
$$392 - 14 \cdot 27 = 14\,. \tag{6c}$$

The way forward is to efficiently eliminate the lower remainders (bigger than unity) by substitution. The value of 13 in (6a) can be removed by substituting the value of 13 from (6b), yielding

$$14 - 1 \cdot [27 - 1 \cdot 14] = 1\,, \tag{7}$$

which simplifies to

$$2 \cdot 14 - 27 \equiv 1\,. \tag{8}$$

And to eliminate the 14 in (8), we use of the 14 on the RHS of (6c), yielding

$$2 \cdot [392 - 14 \cdot 27] - 27 = 1\,, \tag{9}$$

which simplifies to

$$2 \cdot 392 - 29 \cdot 27 = 1\,. \tag{10}$$

And if we reduce this equation modulo 392, we get

$$(-29) \cdot 27 \equiv 1 \pmod{392}\,. \tag{11}$$

In some sense we are finished because $-29 \equiv 27^{-1} (\text{mod } 392)$. However, it is standard to convert -29 to its equivalent positive value, which we can obtain by adding 392 to -29 to get 363. Therefore,

$$363 \equiv 27^{-1} \pmod{392}\,. \tag{12}$$

3 Problem 2

Find 7^{-1} mod 26. Or, put more algebraically, find x in the equation

$$7x \equiv 1 \pmod{26}\,. \tag{13}$$

Well, clearly 7 and 26 are relatively prime, but will go through the Euclidean Algorithm, anyway, to get the remainders and their equations.

So, we use the Euclidean Algorithm to show that 26 and 7 are relatively prime:

$$26 = 3 \cdot 7 + 5\,, \tag{14a}$$
$$7 = 1 \cdot 5 + 2\,, \tag{14b}$$
$$5 = 2 \cdot 2 + 1\,. \tag{14c}$$

Done. As before, we want to solve these last three equations for the remainders, like such:

$$26 - 3 \cdot 7 = 5\,, \tag{15a}$$
$$7 - 1 \cdot 5 = 2\,, \tag{15b}$$
$$5 - 2 \cdot 2 = 1\,. \tag{15c}$$

First, we get rid of the 2 in (15c) by substitution from (15b).

$$5 - 2 \cdot [7 - 5] = 1\,, \tag{16}$$

which simplifies to

$$3 \cdot 5 - 2 \cdot 7 = 1\,. \tag{17}$$

And we can get rid of the 5 in this last equation by use of (15a).

$$3 \cdot [26 - 3 \cdot 7] - 2 \cdot 7 = 1\,, \tag{18}$$

which simplifies to

$$3 \cdot 26 - 11 \cdot 7 = 1\,. \tag{19}$$

Next, we reduce this equation modulo 26, yielding

$$-11 \cdot 7 \equiv 1 \pmod{26}\,. \tag{20}$$

But, as before, we can replace a negative number by a positive one:

$$-11 \equiv 15 \pmod{26}\,. \tag{21}$$

Lastly, we have that

$$15 \cdot 7 \equiv 1 \pmod{26}\,, \tag{22}$$

implying that

$$7^{-1} \equiv 15 \pmod{26}\,. \tag{23}$$

And we are finished.

Note: When the modulus n of the number system is small, it can be faster to just try an exhaustive search for the inverse. For example, to find 3^{-1} mod 10, we have only 8 numbers to try, that is, 2–9 (where we ignored 0 and 1). Going through the numbers, we quickly find that $3 \cdot 7 \equiv 1 \pmod{10}$. Therefore, $3^{-1} \equiv 7 \bmod 10$. Done.