

# Lecture 6.5: Finding Modular Inverses

<http://book.imt-decal.org>, Ch. 3 (in progress)

Introduction to Mathematical Thinking

October 22nd, 2018

Suraj Rampure

# Announcements

- Midterm grades coming out tonight, on Gradescope!
- Sorry for the delay on posting last week's lecture video (was travelling all week), it will be posted alongside the video for today

Today: ~20 minute mini-lecture on Euclid's Extended GCD Algorithm (referred to in the homework).  
Remaining time will be taking up problems from HW 6 (due Wednesday 6:30PM).

## Review: Modular Inverses

We say  $y$  is the modular inverse of  $x$  in mod  $m$  if

$$x \cdot y \equiv 1 \pmod{m}$$

This inverse exists iff  $\gcd(x, m) = 1$ .

**For example:** The inverse of 3 in mod 5 is 2, because:

$$3 \cdot 2 \equiv 6 \equiv 1 \pmod{5}$$

However, the inverse of 10 in mod 12 doesn't exist, because there is no solution to

$$10x \equiv 1 \pmod{12}$$

$$\begin{aligned} 3x &= 14 \\ \underbrace{3^{-1}} \cdot 3x &= 3^{-1} \cdot 14 \\ x &= 3^{-1} \cdot 14 \\ &= \frac{14}{3} \end{aligned}$$

The problem of finding the inverse of  $a$  in  $\text{mod } m$  reduces to finding integers  $x, y$  that satisfy the equation

$$x \equiv a^{-1} \pmod{m}$$

$$\underline{ax + my = 1}$$

This equation states that the product  $ax$  is 1 away from some multiple of  $y$ .

If we were to take " $\text{mod } m$ " on both sides, we would end up with  $ax \equiv 1 \pmod{m}$ .

Here,  $x$  represents the inverse of  $a$ .

$$\gcd(a, m) = 1$$

e.g. Inverse of 3 in  $\text{mod } 5$ :

$$(2, -1)$$

$$2 \equiv -3 \pmod{5}$$

$$3x + 5y = 1$$

$$(-3, 2)$$

$$3(\underline{2}) + 5(-1) = 1 \Rightarrow 3^{-1} \equiv 2 \pmod{5}$$

$$\begin{aligned} x = -3 &\rightarrow 3(-3) + 5(2) \\ y = 2 &= -9 + 10 \\ &= 1 \end{aligned}$$

How can we find  $x, y$ ? For small numbers, Guess and Check. In general – Euclid's Extended GCD Algorithm (today!)

$$\gcd(10, 12) = 2$$

Inverse of 10 in mod 12:

$$10x + 12y = 1$$

But, since 10 and 12 share factors:

$$5x + 6y = \frac{1}{2}$$

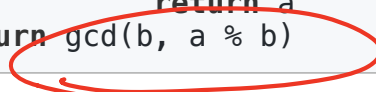
We want integer solutions for  $x, y$ . However, this equation implies that the sum of two integers is a fraction! Not possible.

**Takeaway:** The inverse of  $a$  in mod  $m$  exists iff  $\gcd(a, m) = 1$ . More formal proof of this in the homework.

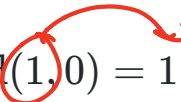
Goal: Find integer solutions to  $ax + my = 1$  (i.e. a linear combination of  $a, m$  that sums to 1).

Euclidean algorithm:

```
# Assumes a > b
def gcd(a, b):
    if b == 0:
        return a
    return gcd(b, a % b)
```



e.g.

$$\gcd(26, 15) = \gcd(15, 11) = \gcd(11, 4) = \gcd(4, 3) = \gcd(3, 1) = \gcd(1, 0) = 1$$


How can we use this process to find coefficients  $x, y$ ?

$$\underbrace{\gcd(n, 1)} = \underbrace{\gcd(1, 0)}$$

$$l = ax + my$$

$$n = d \cdot q + r$$

division algo.

At each step, let's use the **division algorithm**, and rearrange for the **remainder**:

$$(1) \gcd(26, 15) \Rightarrow 26 = 1 \cdot 15 + 11 \Rightarrow 11 = 26 - 1 \cdot 15$$

$$(2) \gcd(15, 11) \Rightarrow 15 = 1 \cdot 11 + 4 \Rightarrow 4 = 15 - 1 \cdot 11$$

$$(3) \gcd(11, 4) \Rightarrow 11 = 2 \cdot 4 + 3 \Rightarrow 3 = 11 - 2 \cdot 4$$

$$(4) \gcd(4, 3) \Rightarrow 4 = 1 \cdot 3 + 1 \Rightarrow 1 = 4 - 1 \cdot 3$$

$$l = 26 \cdot x + 15 \cdot y$$

We know that if  $\gcd(a, b) = 1$ , there will be some step in the process where we have  $\gcd(\text{some number}, 1)$ .

We can now plug in (3) into (4), then (2) into that result, and then (1) into that result. What do you observe?

$$l = a - b \cdot c$$

$$\begin{aligned}
 1 &= 4 - 1 \cdot \textcircled{3} \\
 &= 4 - 1 \cdot (11 - 2 \cdot 4) = 3 \cdot \textcircled{4} - 11 \\
 &= 3 \cdot (15 - 1 \cdot 11) - 11 = 3 \cdot 15 - 4 \cdot 11 \\
 &= 3 \cdot 15 - 4 \cdot (26 - 1 \cdot 15) = 7 \cdot 15 - 4 \cdot 26
 \end{aligned}$$

$3 = 11 - 2 \cdot 4$   
 $4 = 15 - 1 \cdot 11$

This tells us both that  $15 \equiv 7^{-1} \pmod{26}$  and  $-4 \equiv 3 \equiv 26^{-1} \pmod{7}$ .



$$9x + 14y = 1$$

rearrange for remainder

Determine  $9^{-1} \pmod{14}$ , using the Extended Euclidean algorithm.

$$\begin{array}{r} 14, 9 \\ \hline \end{array}$$

division  
algo

$$14 = 1 \cdot 9 + 5 \rightarrow$$

$$5 = 14 - 1 \cdot 9$$

$$\begin{array}{r} 9, 5 \\ \hline \end{array}$$

$$9 = 1 \cdot 5 + 4 \rightarrow$$

$$4 = 9 - 1 \cdot 5$$

$$\begin{array}{r} 5, 4 \\ \hline \end{array}$$

$$5 = 1 \cdot 4 + 1 \rightarrow$$

$$1 = 5 - 1 \cdot 4$$

$$\begin{array}{r} 4, 1 \\ \hline \end{array}$$

$$1 = 5 - 1 \cdot (9 - 1 \cdot 5) = 2 \cdot 5 - 9$$

$$5 - 1(9) - (-1)(5) \leftarrow$$

$$= 2 \cdot (14 - 1 \cdot 9) - 9$$

$$5 - 9 - (-5) = 2 \cdot 5 - 9$$

$$= 2 \cdot 14 - 3 \cdot 9$$

$$9x + 14y = 1$$

$$x \equiv 9^{-1} \pmod{14}$$

$$-3 \equiv 9^{-1} \pmod{14}$$

$$11 \equiv 9^{-1} \pmod{14}$$

$$11 \cdot 9 \equiv 99 \equiv 98 + 1$$

$$\equiv 1 \pmod{14}$$

$$\therefore 11 \text{ is } 9^{-1} \pmod{14}$$