311 Mod

Kaiyu Zheng

October 28, 2016

1 Multiplicative Inverse

Definitions Multiplicative inverse of integer a is an integer x such that $ax = 1$. (x is a's reciprocal). Multiplicative inverse of a **mod** x, where $a \in \mathbb{Z}$, is an integer x, such that $ax \equiv 1 \pmod{m}$.

> **Intuition:** the only difference between normal multiplicative inverse and the modular one is simply the extra "mod m" after ax.

$$\begin{aligned} ax \equiv 1 \pmod{m} &\leftrightarrow ax \bmod m = 1 \bmod m \\ &\leftrightarrow ax \bmod m = 1 \end{aligned}$$

Compute modular multiplicative inverse By the definition of modular multiplicative inverse, we just need to solve for x in $ax \equiv 1 \pmod{m}$. Can we come up with our own way? (Instead of memorizing the method provided in lecture.) Let's try!

First, we know $ax \equiv 1 \pmod{m}$. By definition of modular congruence, $ax = km + 1$ for integer k. This means that ax and km are **consecutive integers**. We know that *consecutive integers are co-prime* (Proof found: `https://proofwiki.org/wiki/Consecutive_Integers_are_Coprime`). Therefore, $gcd(ax, km) = 1$.

By Bézout's Identity, $gcd(ax, km) = p(ax) + q(km)$ where p, q are integers. Now, suppose we have two integers s and t, such that $s = px$, and $t = qk$, then we can write $gcd(ax, km) = sa + tm = 1$. Here is a theorem that will help us proceed: **If 1 is a linear combination of a and b, then $gcd(a, b) = 1$.** Here is a proof: `http://www.math.fsu.edu/~wooland/mad2104/integers/proofPDFs/dDaspbt1.pdf`.

> **Note:** This proof uses the fact that "if $d \mid a$, and $d \mid b$, then d divides the linear combination of a and b. Here is a proof of this fact:

Proof.

$$\begin{aligned} & d \mid a, a = kd, \text{ for some } k \in \mathbb{Z}) \\ \Rightarrow\ & d \mid b, b = jd, \text{ for some } j \in \mathbb{Z}) \\ \Rightarrow\ & sa + tb = skd + tjd = d(sk + tj) \\ \Rightarrow\ & d|(sk + tj) \\ \Rightarrow\ & d|(s(a/d) + t(b/d)) \text{ Because } d \neq 0 \\ \Rightarrow\ & s(a/d) + t(b/d) = md \\ \Rightarrow\ & (sa + tb)/d = md \\ \because\ & md \text{ is an integer} \\ \Rightarrow\ & d|(sa + tb). Basically, sa + tb = (md)d \end{aligned}$$

□

Thus, we have $gcd(a, m) = 1$. Therefore, a and m are coprime.

> **Corollary:** If you can compute the modular multiplicative inverse of a mod m, then it must be the case that a and m are coprime.

At this point, we can apply Extended Euclidean Algorithm to compute s, t. The process here is supposed to be familiar to you. First, you write down a series of equations that basically illustrates the fact that $gcd(x, y) = gcd(y, x \bmod y)$. Next, we use backwards substitution repeatedly to write $gcd(x, y)$ as the the sum of sx and ty for two integers s, t.

After applying Extended Euclidean Algorithm, what we obtain is s and t, which satisfies $gcd(a, m) = sa + tm$. Here is a key point to observe: $sa \bmod m = 1$. This is because, first, apparently, $sa + tm = 1$, and $1 \bmod 1 = 1$. Thus, $(sa + tm) \bmod m = 1 \bmod m$. Then, because tm is a multiple of m, $(sa + tm) \bmod m = sa \bmod m$.

Because $sa \bmod m = 1$, we have $sa \equiv 1 \pmod m$. This means that s is just (one of) the x that we want to find. Why one of? Notice that for an integer k,

$$(s + km)a \bmod m = (sa + kam) \bmod m = sa \bmod m$$

Thus, every integer x that satisfies $x = s + km$ will also solve $ax \equiv 1 \pmod m$. Just for the sake of consistency, we prefer to do an extra mod over the s that we got from Extended Euclidean Algorithm, so that $0 <= x < m$ when $k = 0$.

One other key point we want to get from the above is that, as long as you solved $ax \equiv 1 \pmod m$, you can solve for y in $uy \equiv v \pmod m$ for any integer u and v, using the Additivity and Multiplicity of Congruence. This idea is illustrated in the modular table. The entire point of that table is to display the property that I described here.

2 Multiplicity of Congruence

When we discussed about the algorithm to compute modular exponentiation, we encountered this property of modular congruence.

$$(a \bmod m)(b \bmod m) \equiv ab \pmod m$$

Call this property P. According to the Multiplicity of Congruence, if for $c, d \in \mathbb{Z}$, $c \equiv a \pmod m$ and $d \equiv b \pmod m$, we have $cd \equiv ab \pmod m$. Now we want to derive P based on the Multiplicity of Congruence.

Proof. We have $c \equiv a \pmod m$ and $d \equiv b \pmod m$. Now, let $c = a \bmod m$. Let $d = \bmod m$. Because, $c \bmod m = (a \bmod m) \bmod m = a \bmod m$, and similarly, $d \bmod m = (b \bmod m) \bmod m = b \bmod m$, c and d satisfy $c \equiv a \pmod m$ and $d \equiv b \pmod m$. By Multiplicity of Congruence, we know $cd \equiv ab \pmod m$. That is exactly $(a \bmod m)(b \bmod m) \equiv ab \pmod m$. □

3 Algorithm to compute Modular Exponentiation fast

In lecture, we are presented with an algorithm to compute $a^e \bmod m$ fast. The algorithm goes as follows: Write e in binary, with n digits $(b_{n-1}...,b_1b_0)_2$. Then, we look at which digit is 1. e.g. Suppose $b_i = 1$, we use repeated squaring to compute a^{2^i}. Finally, we multiply all the a^{2^i}, where i is the digit index for which b_i is not 0, that we computed from repeated squaring, and obtain $a^e \bmod m$.

This algorithm works because

$$(e)_{10} = b_{n-1}2^{n-1} + b_{n-2}2^{n-2} + ... + b_12^1 + b_02^0$$

And we know that

$$a^{x+y} = a^x a^y$$

Therefore,

$$a^e \bmod m = a^{b_{n-1}2^{n-1}+b_{n-2}2^{n-2}+...+b_12^1+b_02^0} \bmod m = a^{b_{n-1}2^{n-1}} \cdots a^{b^02^0} \bmod m$$

The *repeated squaring* process is demonstrated in the lecture slide. Essentially,

$$a^{2^n} = (a^{2^{n-1}} \bmod m)^2 \bmod m$$

We have seen examples in section. So I will not repeat examples here. You can come up with examples yourselves and apply this idea.

4 Problem 1 on section worksheet

You will eventually get the solution to the section worksheet. I will clarify several steps in the solution.

After applying Multiplicity of Congruences, we obtain

$$\sum_{i=0}^{m}(x_i \bmod 9)(10^i \bmod 9) \equiv 0 \pmod 9$$

If we treat $a = 10 \bmod 9$, and $b = 10$, and because $10 \bmod 9 \equiv 10 \pmod 9$, then based on rule [***], we have $(10 \bmod 9)^i \equiv 10^i \pmod 9$. Therefore, $10^i \bmod 9 = (10 \bmod 9)^i \bmod 9$. So equivalently we have,

$$\sum_{i=0}^{m}(x_i \bmod 9)((10 \bmod 9)^i \bmod 9) \equiv 0 \pmod 9$$

Then, by Multiplicity of Congruence (blame the solution for skipping this step), we have,

$$\sum_{i=0}^{m} x_i((10 \bmod 9)^i) \equiv 0 \pmod 9$$

Another step I want to explain from [Definition of mod] to the first [Simplifying]. In my opinion, it is unnecessary, because we know $(1 \bmod 9)^i = 1^i = 1$. Therefore, we can directly get the final step.