Modular Arithmetic Handout

November 14, 2022

(1) In class I find myself saying something like this a lot:

> "And this number is 5 times *something*, we don't care what- it's divisible by 5."

In this handout we'll learn a method for systematically ignoring multiples of some number. Here is the key definition:

Definition 1.1. Let $m \geqslant 1$ be a fixed integer. If $a, b \in \mathbb{Z}$ we say that a **is congruent to** b **modulo** m if $a - b$ is divisible by m. In this case we write:

$$a \equiv b \bmod m$$

which is read aloud as 'a is equivalent/congruent to b mod m'.

Example 1.2. Here are some examples.

$$\begin{aligned} 2 &\equiv 10 \bmod 8 && \text{because } 2 - 10 = -8 = 8 \cdot (-1) \\ 12 &\equiv -3 \bmod 5 && \text{because } 12 - (-3) = 15 = 5 \cdot 3 \\ 4 + 3 &\equiv 4 \bmod 3 && \text{because } 4 + 3 - 4 = 3 = 3 \cdot 1 \end{aligned}$$

Exercise 1.3. Write down a few integers which are congruent to 1 modulo 17. Try to have both positive and negative examples.

Exercise 1.4. Prove that $a \equiv b \bmod m$ if and only if a and b leave the same remainder upon division by m.

Warning 1.5. In computer science 'a mod m' *means* the remainder of a upon division by m. That is not what it means in mathematics. That remainder is just one of many different numbers which are equivalent to a modulo m.

Despite the warning, when we say something like

> "Compute 14658 modulo 7"

we usually mean to find this remainder, or some small number equivalent to 14657 modulo 7. The remainder is sometimes called the **standard representative**. In this example, we have

$$14657 \equiv 6 \bmod 7$$

But another reasonable answer (sometimes more useful) is:

$$14657 \equiv -1 \bmod 7$$

(2) The thing that makes 'working modulo m' so convenient is that we can do arithmetic in this world. Let's do an example before we see the general result.

Example 2.6. We'll work modulo 12. Then $15 \equiv 3 \bmod 12$ and $-16 \equiv 8 \bmod 12$. Let's compute products and sums and see what happens:

$$\begin{aligned} 15 \cdot (-16) &= -240 \\ &= 12 \cdot (-20) \equiv 0 \bmod 12 \\ 3 \cdot 8 &= 24 \\ &= 12 \cdot 2 \equiv 0 \bmod 12 \end{aligned}$$

We got the same answer, modulo 12; but the second calculation was a lot easier. How about sums?

$$\begin{aligned} 15 + (-16) &= -1 \\ 8 + 3 &= 11 \\ &\equiv -1 \bmod 12 \end{aligned}$$

Again, the same answer modulo 12. Below we'll see this is no accident.

Lemma 2.7. *Let a, a', b, and b' be integers and let $m \geqslant 1$ be an integer. Suppose that*

$$\begin{aligned} a &\equiv a' \bmod m \\ b &\equiv b' \bmod m \end{aligned}$$

Then

$$\begin{aligned} a + b &\equiv a' + b' \bmod m \\ ab &\equiv a'b' \bmod m \end{aligned}$$

and, for any $n \geqslant 0$,

$$a^n \equiv (a')^n \bmod m$$

Proof. By assumption, we can find numbers q and k so that

$$a - a' = mq, \; b - b' = mk$$

Then:

$$\begin{aligned}(a+b) - (a'+b') &= a - a' + b - b' \\ &= mq + mk \\ &= m(q+k)\end{aligned}$$

hence m divides $(a+b) - (a'+b')$. By definition, that means

$$a + b \equiv a' + b' \bmod m,$$

which proves the first claim.

For the second claim, compute:

$$\begin{aligned}ab - a'b' &= ab - ab' + ab' - a'b' \\ &= a(b-b') + (a-a')b' \\ &= a(mk) + (mq)b' \\ &= m(ak + qb')\end{aligned}$$

Thus m divides $ab - a'b'$. By definition, that means

$$ab \equiv a'b' \bmod m$$

and that completes the proof.

The third claim is a homework exercise! □

Exercise 2.8. Immediately compute the remainder of

$$11^{167253947}$$

upon division by 12.

(3) The next phenomenon is a neat thing gained by working modulo a number.

Example 3.9. The integer 5 has no *multiplicative inverse* that's an integer. In other words: there is no integer n such that

$$5 \cdot n = 1$$

On the other hand, if we work modulo 11, then

$$5 \cdot 9 = 45 \equiv 1 \bmod 11$$

So sometimes there are multiplicative inverses when working modulo some number.

Here's the general story.

Proposition 3.10. *Let $m \geqslant 1$ be fixed and suppose a is an integer. Then a has a multiplicative inverse modulo m if and only if* $\gcd(a, m) = 1$ *(i.e. if and only if a and m are relatively prime).*

Proof. We want to solve the 'equation':

$$ax \equiv 1 \bmod m$$

There is a solution if and only if there is a number x where

$$ax - 1$$

is divisible by m. In other words, there is a solution if and only if we can find x and z such that

$$ax - 1 = mz$$

In other words, if and only if

$$ax - mz = 1$$

has a solution. Substituting $y = -z$, this is true if and only if

$$ax + my = 1$$

has a solution. We have already seen that's true if and only if $\gcd(a, m) = 1$. □

This actually gives us a procedure for finding multiplicative inverses!

- Given a and m, run the Euclidean algorithm.
- If $\gcd(a, m) \neq 1$, then there is no multiplicative inverse, so you can stop.
- Otherwise, run the *reverse* Euclidean algorithm to find x and y with

  $$ax + my = 1$$

  Then x is an example of a multiplicative inverse for a, modulo m.

Exercise 3.11. Find multiplicative inverses for...

(i) 17 modulo 124

(ii) 24 modulo 25 (there's a trick to do this fast, can you spot it?)

(iii) 60 modulo 77

(4) We end with a trick for computing powers of an integer modulo some other integer. It's very useful!

Theorem 4.12 (Euler's theorem)**.** *Let $\phi(m)$ denote the number of positive integers less than m which are relatively prime to m. Suppose a is relatively prime to m. Then*

$$a^{\phi(m)} \equiv 1 \bmod m$$

Before giving the proof, we'll give a corollary and a few examples.

Corollary 4.13 (Fermat's little theorem)**.** *Let p be prime and a a number relatively prime to p. Then*

$$a^{p-1} \equiv 1 \bmod p$$

Example 4.14. Let's compute 4^{56} modulo 7. We have:

$$\begin{aligned} 4^{56} &= 4^{54} \cdot 4^2 \\ &= (4^6)^9 \cdot 4^2 \\ &\equiv 1^9 \cdot 4^2 \bmod 7 \\ &\equiv 16 \bmod 7 \\ &\equiv 2 \bmod 7 \end{aligned}$$

Notice that, in order to compute 4^{56} modulo 7, we become interested in computing 56 modulo $6 = 7 - 1$.

Ok, now for the proof. I recommend actually following along with the entire proof for a specific (small) value of m and a.

Proof of Euler's Theorem. Let's set $k = \phi(m)$ so we don't have to keep writing it. Consider the positive numbers

$$n_1, n_2, ..., n_k$$

which are less than m and relatively prime to m. I claim that the numbers

$$an_1, an_2, ..., an_k$$

are, modulo m, just a reordering of the numbers $n_1, ..., n_k$. In other words, I claim that the function:

$$g : \{n_1, ..., n_k\} \to \{n_1, ..., n_k\}$$

given by

$$g(n_i) = \text{the remainder of } an_i \text{ upon division by } m$$

is a bijection. (Notice the function is well-defined: the product of two numbers relatively prime to m is again relatively prime to m).

To see that g is a bijection, choose a multiplicative inverse b for a modulo m (which we can do by the assumption that a is relatively prime to m). Then define

$$h : \{n_1, ..., n_k\} \to \{n_1, ..., n_k\}$$

by

$$h(n_i) = \text{the remainder of } bn_i \text{ upon division by } m$$

Notice that g and h are composition inverse to one another:

$$g(h(n_i)) \equiv g(bn_i) \equiv abn_i \equiv n_i \bmod m$$

and similarly

$$h(g(n_i)) \equiv n_i \bmod m$$

Two numbers between 0 and m are congruent modulo m if and only if they are equal, therefore

$$g(h(n_i)) = n_i = h(g(n_i))$$

This completes the proof of the claim that

$$an_1, ..., an_k$$

is a reordering, modulo m, of the original numbers. But then the products are congruent:

$$(an_1) \cdot (an_2) \cdots (an_k) \equiv n_1 \cdots n_k \bmod m$$

Rewriting the left hand side we get:

$$a^k (n_1 \cdots n_k) \equiv n_1 \cdots n_k \bmod m$$

The number $n_1 \cdots n_k$ is relatively prime to m, so it has a multiplicative inverse c, modulo m. Multiplying both sides by c we learn that

$$a^k \equiv 1 \bmod m$$

Since we defined k as $\phi(m)$ at the beginning, we are done. □