CSci 2312
Discrete Structures II: Understanding Modular Arithmetic

Poorvi L. Vora

In this module, we try to get a feel for the subject of modular arithmetic.

Consider the following result (shown in the text, which we also prove in class, but assume for now that it is true):

$$x \equiv_m y \Leftrightarrow (x \; rem \; m) = (y \; rem \; m)$$

That is, two integers are congruent modulo m if and only if their remainders on division by m are the same.

That is, whether you say that:

(a) two integers are congruent modulo m, or

(b) their remainders are the same on division by m,

you are saying the same thing.

Now recall from class and the notes on Modular Arithmetic I that congruence modulo m is an equivalence relation. What does that mean? Well, among other things it means that the set of all integers can be broken up (it is referred to as *partitioned*) into equivalence classes, and each integer belongs to exactly one equivalence class. All integers in one class are equivalent to one another. What one feature characterizes the class? The remainder on division by m. For this reason, when we consider the equivalence classes modulo m, we may consider each class to be represented by the corresponding remainder, as every integer in that equivalence class will have the same remainder. For example, consider the numbers $3, 6, 9$ modulo 3. They each have a remainder of zero when divided by 3 and are hence congruent modulo 3 as you can check:

$$3 \mid (6-3) \; \Rightarrow 3 \equiv 6 \; (mod \; 3)$$

etc. Similarly, $-1, 2, 5, 8, -4$ are all congruent modulo 3 as well. Notice that you can add any multiple of the modulus to get numbers that are congruent to each other.

Similarly, consider the following result (also shown in the text, which we also prove in class, but assume for now that it is true):

If $a \equiv b \; mod \; m$ and $c \equiv d \; mod \; m$, then:

$$(a + c) \equiv (b + d) \; mod \; m$$

$$(a \times c) \equiv (b \times d) \; mod \; m$$

That is, from the above example, we can see that any value from $3, 6, 9$ when added to any value from $-1, 2, 5, 8, -4$ results in values that are congruent modulo 3. For example (check this),

$$3 + (-1) \equiv 6 + (-1) \equiv 9 + (-4) \equiv 6 + 5 \; (mod \; 3)$$

Similarly with multiplication (check this too)

$$6 \times (-1) \equiv 3 \times (5) \equiv 9 \times 5 \equiv 6 \times 2 \, (mod \, 3)$$

Taken together with the earlier result, this means that

If $a \; rem \; m = b \; rem \; m$ and $c \; rem \; m = d \; rem \; m$, then

$$(a + c) \; rem \; m = (b + d) \; rem \; m$$

and

$$(a \times c) rem \; m = (b \times d) \; rem \; m$$

That is, when two numbers have the same remainder, if you are going to add or multiply and then take remainders, it doesn't matter which number you use. You can replace one number with another one with the same remainder, if you are going to finally take a remainder. So, for all of our above examples, we see that:

$$(3 + (-1)) \; rem \; 3 = 2$$

and

$$(6 + (-1)) \; rem \; 3 = 5 \; rem \; 3 = 2$$

and

$$(9 + (-4)) \; rem \; 3 = 5 \; rem \; 3 = 2$$

and so on. You can do the same thing with multiplication (try it).

In particular, this means that we can perform arithmetic on the remainders as follows:

$\mathbb{Z}_m = \{0, 1, 2, ..., m - 1\}$ is the set of all remainders on division by m. One can add the remainders "modulo m" which means to add them and then take the remainder on division by m, as we did above. We can similarly multiply the remainders modulo m, by multiplying and then taking the remainder.

$$(2 + 3) \; rem \; 4 = 1$$

$$(2 \times 9) \; rem \; 12 = 6$$

You should always provide a result that is a valid remainder. Note that you cannot say $(-6) \; rem \; 5 = 6$ in the same way that you cannot say that $-1 = 1$.

Consider:

$$(2 \times 5) \; rem \; 9 = 1 \Rightarrow (2 \times 5) \equiv 1 (mod \, 9)$$

$$(2 \times 14) \; rem \; 9 = 1 \Rightarrow (2 \times 14) \equiv 1 (mod \, 9)$$

$$(2 \times -4) \; rem \; 9 = 1 \Rightarrow (2 \times -4) \equiv 1 (mod \, 9)$$

Did you just get confused by

$$(2 \times -4) \; rem \; 9 = 1$$

Well, to understand this, note that the remainder when you divide -8 by 9 is not 8. In fact, $-8 = (-1)9 + 1$ and hence the remainder is 1 and hence $(2 \times -4) \; rem \; 9 = 1$. You can get to this answer another way too, by first looking at the remainder when -4 is divided by 9 and getting a positive number there. The equivalence class that -4 belongs to modulo 9 is not the class of 4 because $4 \not\equiv -4 \; (mod \; 9)$ because $-4 - 4 = -8$ is not a multiple of 9. That is, $+4$ and

-4 do not have the same remainder when divided by 9. In fact, $-4 = (-1)9 + 5$ and hence the remainder when -4 is divided by 9 is 5 and not 4. That would give us: $2 \times -4 = 2 \times 5 = 10 = 1 \ mod \ 9$.

For modulus m, in order to deal with numbers that are larger than $m - 1$ or smaller than 0, you can add as many multiples of the modulus as you wish when adding and multiplying modulo m, because adding multiples of m does not change the remainder. So, for the above problem you could do:

$$2 \times -4 = -8 \equiv -8 + 9(mod\ 9) \equiv 1\ (mod\ 9)$$

or

$$-4 \equiv -4 + 9(mod\ 9) \equiv 5\ (mod\ 9)$$

Hence

$$2 \times -4 \equiv 2 \times 5(mod\ 9) \equiv 10(mod\ 9) \equiv 10 - 9(mod\ 9) \equiv 1\ (mod\ 9)$$

Similarly,

$$2 \times (-3) \equiv (-6)\ (mod\ 5) \equiv -6 + 5(mod\ 5) \equiv -1(mod\ 5) \equiv -1 + 5(mod\ 5) \equiv 4\ (mod\ 5)$$

or

$$-3 \equiv -3 + 5(mod\ 5) \equiv 2\ (mod\ 5)$$

Hence

$$2 \times (-3) \equiv 2 \times 2(mod\ 5) \equiv 4\ (mod\ 5)$$