Math 112 lecture for Wednesday, Week 3

Modular arithmetic

(Supplemental reading: Example 2.3.10 in Swanson.)

Fix $n \in \mathbb{Z}$, and recall $\mathbb{Z}/n\mathbb{Z}$, the integers modulo n. Its elements are the equivalence classes[1], for the equivalence relation defined by $a \sim b$ if $a - b = kn$ for some $k \in \mathbb{Z}$.

Example. The elements of $\mathbb{Z}/5\mathbb{Z}$ are the equivalence classes for the integers modulo 5:

$$\begin{aligned}
[0] &= \{\dots, -15, -10, -5, 0, 5, 10, 15, \dots\}\\
[1] &= \{\dots, -14, -9, -4, 1, 6, 11, 16, \dots\}\\
[2] &= \{\dots, -13, -8, -3, 2, 7, 12, 17, \dots\}\\
[3] &= \{\dots, -12, -7, -2, 3, 8, 13, 18, \dots\}\\
[4] &= \{\dots, -11, -6, -1, 4, 9, 14, 19, \dots\}
\end{aligned}$$

Note that the equivalence classes *partition* $\mathbb{Z}$: each element of $\mathbb{Z}$ is in exactly one of these sets. We know that must be the case since we are working with an equivalence relation. Also, recall that the equivalence classes do not have unique names. For instance, $[1] = [6] = [-14]$. Any two elements of the same equivalence class may serve as representatives for the equivalence class. We have chosen the "standard representatives" in this case.

There are exactly n equivalence classes for $\mathbb{Z}/n\mathbb{Z}$:

$$\mathbb{Z}/n\mathbb{Z} = \{[0], [1], \dots, [n-1]\}.$$

This follows from a standard result of elementary number theory (which we will assume without proof): Each integer a has a unique remainder $r \in \{0, 1, \dots, n-1\}$ upon divison by n. It follows that $a = r + kn$, and $[a] = [r]$. For instance, in the above example, note that the equivalence class [2] consists of all those integers whose remainer upon division by 5 is equal to 2. To find the remainder upon division by 5, we can add or subtract 5s until we get to a number between 0 and 4. The difference between that number and the original number will be some multiple of 5, and hence the two numbers will be equivalent (and therefore belong to the same equivalence class).

Definition. The numbers $0, \dots, n-1$ are called the *standard representatives* for the elements of $\mathbb{Z}/n\mathbb{Z}$.

[1] Recall that if $\sim$ is an equivalence relation on a set A, then the *equivalence class* for an element $a \in A$ is the subset of A defined by $[a] := \{x \in A : x \sim a\}$.

Important notation. Again, fix $n \in \mathbb{Z}$ and let $\sim$ be the equivalence relation on $\mathbb{Z}$ defined by $a \sim b$ if $a - b = nk$ for some $k \in \mathbb{Z}$. Then, if $a \sim b$, we write

$$a = b \bmod n$$

and say *a is equal to b mod (or modulo) n.*

Example. We have

$$28 = 22 \bmod 3, \quad 33333 = 0 \bmod 3, \quad 7 = 12 \bmod 5, \quad 134 = 4 = 9 = -6 \bmod 5.$$

Note that 28 and 22 both have a remainder of 1 upon division by 3. Therefore, they both equal 1 modulo 3. In general, two numbers are the same modulo n if and only if they have the same remainder upon division by n.

Modular addition and multiplication

It turns out the addition and multiplication modulo n have a pleasant and extremely useful property:

Proposition 1. Let $a, a', b, b', n \in \mathbb{Z}$ and suppose that

$$a' = a \bmod n \quad \text{and} \quad b' = b \bmod n.$$

Then

$$a' + b' = a + b \bmod n \quad \text{and} \quad a'b' = ab \bmod n.$$

Proof. Since $a = a' \bmod n$ and $b = b' \bmod n$, there are integers k and ℓ such that

$$a' = a + kn \quad \text{and} \quad b' = b + \ell n.$$

We then have

$$a' + b' = (a + kn) + (b + \ell n) = (a + b) + (k + \ell)n.$$

Thus, $(a' + b') - (a + b)$ is a multiple of n. This means

$$a' + b' = a + b \bmod n.$$

Similarly,

$$a'b' = (a + kn)(b + \ell n) = ab + (a\ell + kb + k\ell n)n.$$

So $a'b'$ and ab differ by a multiple of n. Thus,

$$a'b' = ab \bmod n.$$

□

Example. We have

$$2 + 4 = 1 \bmod 5 \quad \text{and} \quad 2 \cdot 4 = 3 \bmod 5.$$

Now, pick some random integers equivalent to 2 and 4 modulo 5, say 12 and 119, respectively: $2 = 12 \bmod 5$ and $4 = 119 \bmod 5$. Compare the following calculation with the one we just did:

$$12 + 119 = 131 = 1 \bmod 5 \quad \text{and} \quad 12 \cdot 119 = 1428 = 3 \bmod 5.$$

The point is: *it doesn't matter which representatives we pick for equivalences classes when doing arithmetic modulo n.*

Here is another example: it turns out that $6^{1234} = 1 \bmod 5$. There are two ways to see this—one much harder than the other. The first way would be to multiply 6 by itself 1234 times to find

$6^{1234} =$ 1732379250784311705176250882257708301496015396192567495371732614880
75240087116999452906823658984674936277681968054843690376499837328271076188
92950671536262244116264008289021109533978483211716495053443450915238047414
79399403475492481577374563714344875179653434497389873227035019055954428562
02239768057394177746236499587948233358542816161605304301756593416958294262
67436091119516786850894185683803656555920650357615681847409321547653080745
25500549643420339660570902440119972233854360573349265714550130678661859347
15478704632375895211716581542338320112691541351494637861640278807937804211
27793326220084212196058493788813758464496146785479978670277715864316234965
21692936194869871189110975700858236818633323144274142613679161190931094133
86088693223875438333744161644675543387797815167697133683764821601345219541
06460251863121190470356204284374365775568691856593528119100968955782261714
64048835337975361593424475051581642484227301745969638555856404916265709727
645696 = 1 mod 5.

The other is to first note that $6 = 1 \bmod 5$, and use the fact that multiplication "plays nicely" (to paraphrase Proposition 1) with equivalence modulo 5:

$$6^{1234} = 1^{1234} = 1 \bmod 5.$$

In fact, $6^n = 1 \bmod 5$ for any $n \in \mathbb{N}$. Here is a similar example: since $4 = -1 \bmod 5$, we have

$$4^{1234567} = (-1)^{1234567} = -1 = 4 \bmod 5,$$

and

$$4^{1234568} = (-1)^{1234568} = 1 \bmod 5,$$

Definition (Addition and multiplication for $\mathbb{Z}/n\mathbb{Z}$). For each $[a], [b] \in \mathbb{Z}/n\mathbb{Z}$, define

$$[a] + [b] := [a+b] \quad \text{and} \quad [a][b] = [ab].$$

The first thing to notice in the expression $[a]+[b] = [a+b]$ is that the $+$ on the right-hand side and the $+$ on the left-hand side are different. The $+$ on the right-hand side is ordinary addition of integers. The $+$ on the left-hand side is a new operation: it defines how to add not integers but equivalence classes of integers. The meaning of the $+$ on the left-hand side is a new thing which we are just now defining. It says this: in order to add two equivalence classes: (i) choose any representative integers for those classes, say a and b, (ii) add the representatives as integers, $a+b \in \mathbb{Z}$, and then (iii) take the equivalence class of the result, $[a+b]$. Similar remarks hold for multiplication.

Since addition and multiplication depend on the representatives a and b that we choose for the equivalence classes, we need to make sure that the resulting sum $[a+b]$ does not depend on that choice. So suppose that a' and b' are different choices for these equivalence classes. In other words, suppose that

$$[a] = [a'] \quad \text{and} \quad [b] = [b'].$$

We need to make sure that

$$[a] + [b] = [a'] + [b'] \quad \text{and} \quad [a][b] = [a'][b'].$$

Now, by the definition given just above, $[a] + [b] := [a+b]$ and $[a'] + [b'] := [a' + b']$, and similarly for multiplication.[2] So we need to check that

$$[a+b] = [a'+b'] \quad \text{and} \quad [ab] = [a'b'].$$

Proposition 1 comes to the rescue: since $[a] = [a']$, we have $a = a' \bmod n$, and similarly, $b = b' \bmod n$. Proposition 1 then says $a + b = a' + b' \bmod n$ and $ab = a'b' \bmod n$. In other words, $a+b$ and $a'+b'$ are both representatives of the same equivalence class and similarly for ab and $a'b'$, as desired.

Example. Here are addition and multiplication tables for $\mathbb{Z}/4\mathbb{Z}$. **Note:** For ease of notation in the tables below, we use standard representatives to represent equivalence classes. In other words, we will write a instead of $[a]$ where $a \in \{0, 1, 2, 3\}$:

$+$	0	1	2	3
0	0	1	2	3
1	1	2	3	0
2	2	3	0	1
3	3	0	1	2

$\cdot$	0	1	2	3
0	0	0	0	0
1	0	1	2	3
2	0	2	0	2
3	0	3	2	1

.

[2] The notation := means "is defined by".