Some examples with modular arithmetic

Sean Fitzpatrick

December 4, 2015

We discussed modular arithmetic in class, but only very briefly. This will provide you with a few more examples involving calculations in modular arithmetic. Since the book does a good job of explaining how to use modular arithmetic to explain divisibility tests (and since we discussed this earlier on in the course) I'll skip that material and look at other examples.

First, let's recall the definitions: for any natural number $n \geq 2$, we define an equivalence relation on $\mathbb{Z}$ by

$$a \sim b \leftrightarrow a \equiv b \pmod{n}.$$

In other words, we're working with the familiar relation of congruence modulo n. We refer to the equivalence classes with respect to this relation as **congruence classes**. Thus, for any $k \in \mathbb{Z}$, we define

$$[k] = \{m \in \mathbb{Z} | m \equiv k \pmod{n}\}.$$

As we discussed in class, the Division Algorithm provides us with canonical representatives for these congruence classes. For any $m \in \mathbb{Z}$, we know that there exist unique integers $q, r \in \mathbb{Z}$, with $r \in \{0, 1, \ldots, n-1\}$, such that $m = nq + r$, and of course,

$$m = nq + r \leftrightarrow m \equiv r \pmod{n} \leftrightarrow m \sim r \leftrightarrow m \in [r].$$

This gives us the partition of $\mathbb{Z}$ into congruence classes as follows:

$$\mathbb{Z} = [0] \cup [1] \cup \cdots \cup [n-1].$$

A common construction in mathematics (and by common, I mean occurring in almost every branch of mathematics, if not all), is the following: given an equivalence relation $\sim$ on a set A, we obtain a new set, often denoted by $A/\sim$, and referred to as the **quotient** of A with respect to the equivalence relation, defined as follows: we choose elements $a_1, a_2, \ldots, a_n \in A$ with the property that $a_i \not\sim a_j$ for all $i \neq j$, and such that for all $a \in A$, $a \sim a_k$ for some $k \in \{1, \ldots, n\}$. It follows that

$$A = [a_1] \cup [a_2] \cup \cdots \cup [a_n]$$

is a partition of A into **distinct** equivalence classes, and we define $A/\sim$ to be the set of these classes:

$$A/\sim = \{[a_1], [a_2], \cdots, [a_n]\}$$

Remark: For simplicity, I'm assuming that there are finitely many distinct equivalence classes, but this need not be the case. For example, one can consider the relation on $\mathbb{R}$ given by $x \sim y$ if and only if $x - y = 2\pi k$ for some $k \in \mathbb{Z}$. This is an equivalence relation, and in this case, the set of distinct equivalence classes is given by $\mathbb{R}/{\sim} = \{[x] : 0 \leq x < 2\pi\}$, where $[x] = \{y \in \mathbb{R} : y = x + 2\pi k \text{ for some } k \in \mathbb{Z}\}$. One can show that $\mathbb{R}/{\sim}$ is topologically equivalent to the circle.

For the case of the partition of $\mathbb{Z}$ into congruence classes, we obtain the set $\mathbb{Z}_n = \mathbb{Z}/{\sim}$ given by

$$\mathbb{Z}_n = \{[0], [1], \ldots, [n-1]\}.$$

It's often the case that the original set A comes equipped with some sort of structure (algebraic, geometric, topological, etc.), and the natural question one should ask in this situation is wheteher or not the quotient $A/{\sim}$ inherits some version of this structure. In the case of the integers, we have algebraic structure: the set $\mathbb{Z}$ comes equipped with two algebraic operations – addition, and mulitplication. So we check to see if these two operations define similar operations on the quotient, and indeed they do!

Given congruence classes $[k], [l] \in \mathbb{Z}_n$, we define their **sum** $[k] \oplus [l]$ and **product** $[k] \odot [l]$, by

$$\begin{aligned} &[k] \oplus [l] = [k + l] \quad \text{and} \\ &[k] \odot [l] = [k\dot{l}], \end{aligned}$$

respectively, where the addition and mulitplication on the right-hand sides above are the addition and multiplication of $\mathbb{Z}$. As mentioned in class, it is necessary to ensure that these operations are **well-defined**: to perform the addition and multiplication on the right, we need to choose *representatives* of each congruence class, which we then add or multiply, and then we determine the congruence class of the resulting sum or product. In other words, if $k_1 \sim k_2$ and $l_1 \sim l_2$, (so that $[k_1] = [k_2]$ and $[l_1] = [l_2]$) we need to make sure that $[k_1] \oplus [l_1] = [k_2] \oplus [l_2]$. But this is something that we already verified, since we provced a theorem stating that if $k_1 \equiv k_2 \pmod{n}$ and $l_1 \equiv l_2 \pmod{n}$, then $(k_1 + l_1) \equiv (k_2 + l_2) \pmod{n}$, and $(k_1 \cdot l_1) \equiv (k_2 \cdot l_2) \pmod{n}$.

Now that we know addition and multiplication of congruence classes makes sense, we can try doing the computations for a few examples. To make sure you understand the operations, make sure you can verify that the following addition and multiplication tables are correct:

Addition and multiplication in $\mathbb{Z}_3$

$\oplus$	[0]	[1]	[2]
[0]	[0]	[1]	[2]
[1]	[1]	[2]	[0]
[2]	[2]	[0]	[1]

$\odot$	[0]	[1]	[2]
[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]
[2]	[0]	[2]	[1]

Addition and multiplication in $\mathbb{Z}_4$

$\oplus$	[0]	[1]	[2]	[3]
[0]	[0]	[1]	[2]	[3]
[1]	[1]	[2]	[3]	[0]
[2]	[2]	[3]	[0]	[1]
[3]	[3]	[0]	[1]	[2]

$\odot$	[0]	[1]	[2]	[3]
[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]
[2]	[0]	[2]	[0]	[2]
[3]	[0]	[3]	[2]	[1]

Addition and multiplication in $\mathbb{Z}_5$

$\oplus$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[1]	[2]	[3]	[4]
[1]	[1]	[2]	[3]	[4]	[0]
[2]	[2]	[3]	[4]	[0]	[1]
[3]	[3]	[4]	[0]	[1]	[2]
[4]	[4]	[0]	[1]	[2]	[3]

$\odot$	[0]	[1]	[2]	[3]	[4]
[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]
[2]	[0]	[2]	[4]	[1]	[3]
[3]	[0]	[3]	[1]	[4]	[2]
[4]	[0]	[4]	[3]	[2]	[1]

Addition and multiplication in $\mathbb{Z}_6$

$\oplus$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[1]	[2]	[3]	[4]	[5]
[1]	[1]	[2]	[3]	[4]	[5]	[0]
[2]	[2]	[3]	[4]	[5]	[0]	[1]
[3]	[3]	[4]	[5]	[0]	[1]	[2]
[4]	[4]	[5]	[0]	[1]	[2]	[3]
[5]	[5]	[0]	[1]	[2]	[3]	[4]

$\odot$	[0]	[1]	[2]	[3]	[4]	[5]
[0]	[0]	[0]	[0]	[0]	[0]	[0]
[1]	[0]	[1]	[2]	[3]	[4]	[5]
[2]	[0]	[2]	[4]	[0]	[2]	[4]
[3]	[0]	[3]	[0]	[3]	[0]	[3]
[4]	[0]	[4]	[2]	[0]	[4]	[2]
[5]	[0]	[5]	[4]	[3]	[2]	[1]

One thing to observe is that in all four examples, the addition and multiplication inherit the same properties that they have for $\mathbb{Z}$: both addition and multiplication are *commutative* and *associative*, the element [0] still acts as an identity element with respect to addition (that is $[0] \oplus [k] = [k]$ for any k), and [1] still acts as an identity element with respect to multiplication ($[1] \odot [k] = [k]$ for any $[k]$). Not everything is the same, however.

You'll notice that the addition table follows the same pattern for all four sets, and indeed has all the same properties as addition in $\mathbb{Z}$. (The remaining algebraic axiom for addition is that for any $[k] \in \mathbb{Z}_n$, there exists an element $[l] \in \mathbb{Z}_n$ such that $[k] \oplus [l] = [0]$: the existence of additive inverses.) However, the multiplication tables for $\mathbb{Z}_3$ and $\mathbb{Z}_5$ are very different from the multiplication tables for $\mathbb{Z}_4$ and $\mathbb{Z}_6$. In all of them we see that $[0] \odot [k] = [0]$ for any k, which we would expect, but the sets $\mathbb{Z}_4$ and $\mathbb{Z}_6$ have what are called *zero divisors*: elements not equal to [0] that we can multiply to get [0]. One of the fundamental properties of multiplication in $\mathbb{Z}$ is that for any $a, b \in \mathbb{Z}$, if $ab = 0$, then either $a = 0$ or $b = 0$. However, we can see that in $\mathbb{Z}_6$, for example, we have $[2] \neq [0]$ and $[3] \neq [0]$, but $[2] \odot [3] = [0]$.

The reason that things look different for $\mathbb{Z}_4$ and $\mathbb{Z}_6$ is that 4 and 6 are not *prime*: both of them have positive factors other than 1 and themselves. If we look at $\mathbb{Z}_p$ when p is a prime, however, something interesting happens: not only do we avoid zero divisors (in this case, if $ab \equiv 0 \pmod{p}$, we can conclude that either a or b must be a multiple of p), but we have *mulitplicative inverses*! Just like for the sets of rational and real numbers, for any element $[k] \in \mathbb{Z}_p$, with $[k] \neq [0]$, there exists some $[l] \in \mathbb{Z}_p$ such that $[k] \odot [l] = [1]$. (Thus, in a sense, $[l] = [k]^{-1}$, which means that it makes sense to "divide by $[k]$".) You can see that this is the case for both $\mathbb{Z}_3$ and $\mathbb{Z}_5$.

All of these properties and results come up often enough in mathematics that they're given special names. For each $n \geq 2$, we say that the set $\mathbb{Z}_n$ is a **group** with respect to the $\oplus$ operation, since the operation is associative, there is an identity element for the operation ($[0]$), and every element has an inverse with respect to this operation.

Adding multiplication into the picture makes $\mathbb{Z}_n$ into what is called a **ring**. In general, rings can have zero divisors, like you see with $\mathbb{Z}_4$ and $\mathbb{Z}_6$. Many mathematicians find rings interesting, since the multiplication is required to follow fewer rules than what you see for the rational or real number systems, and this leads to a lot of variety and different algebraic weirdness that can happen. (Mathematicians find weirdness very interesting.) When n is a prime, the condition that every non-zero element has an inverse with respect to multiplication makes $\mathbb{Z}_n$ into what's called a **field**. There are many, many, examples of different types of groups, rings, and fields. (And if you're interested in finding out about them, you should take Math 3400 next year.)

The fact that multiplication behaves differently in $\mathbb{Z}_n$ depending on whether or not n is a prime means that problems like trying to solve an equation can look very different. Consider, for example, the equation

$$[2] \odot [x] \oplus [1] = [3].$$

In $\mathbb{Z}_5$, we can solve this equation as follows. First, using the fact that $[1] \oplus [4] = [0]$, we add $[4]$ to both sides, giving us

$$([2] \odot [x] \oplus [1]) \oplus [4] = [3] \oplus [4].$$

On the right, we use the fact that $[3] \oplus [4] = [2]$, and on the left, we use associativity to write

$$([2] \odot [x] \oplus [1]) \oplus [4] = [2] \odot [x] \oplus ([1] \oplus [4]) = [2] \odot [x] \oplus [0] = [2] \odot [x],$$

since $[1] \oplus [4] = [0]$, and adding $[0]$ to anything does nothing. This leaves us with the equation $[2] \odot [x] = [2]$. Now, we use the fact that $[3] \odot [2] = [1]$, and that multiplying by $[1]$ does nothing, to solve. Multiplying both sides of the remaining equation by $[3]$, we have

$$[3] \odot ([2] \odot [x]) = ([3] \odot [2]) \odot [x] = [1] \odot [x] = [x]$$

on the left, and $[3] \odot [2] = [1]$ on the right. The solution is therefore $[x] = [1]$.

Now, let's look at what would happen in $\mathbb{Z}_6$. Coming back to the original equation $[2] \odot [x] \oplus [1] = [3]$, in $\mathbb{Z}_6$ we would get rid of the $[1]$ on the left by adding $[5]$ to both sides. On the right-hand side, we get $[3] \oplus [5] = [8] = [2]$, so we once again end up with the equation

$[2] \odot [x] = [2]$. However, if we tried to solve the equation $[2] \odot [x] = [2]$ in $\mathbb{Z}_6$, we run into a problem: there is no element $[k] \in \mathbb{Z}_6$ such that $[k] \odot [2] = [1]$! All is not lost, however: we realize that the equation is asking us for any $[x] \in \mathbb{Z}_6$ such that $[2] \odot [x] = [2]$, and looking at the multiplication table for $\mathbb{Z}_6$, we see that there are two such elements: $[x] = [1]$, and $[x] = [4]$. So there is a solution, but it's not unique. And things can be even worse! If we had [4] on the right-hand side instead of [3], we'd end up with the equation $[2] \odot [x] = [3]$, and looking at the multiplication table for $\mathbb{Z}_6$, we see that there is no solution at all!

With this example to refer to, you should try Problem 2 from Section 7.4 in the textbook. Note that some of the equations are quadratic. Just like over the real numbers, a quadratic equation might have one solution, two solutions, or no solutions at all, even in $\mathbb{Z}_p$, where p is a prime. (Looking at the left-to-right diagonal in each multiplication table will tell you which elements of $\mathbb{Z}_n$ are of the form $[k] = [l]^2$ for some $[l]$. For example, in $\mathbb{Z}_5$, only [1] and [4] can be obtained as the square of another element.