2.3: Integers Modulo n

Recall the 'bumpy' hexagon, which had rotational symmetry but no reflection symmetry. The group of symmetries of the bumpy hexagon is called \(\mathbb{Z}_6\). In this section, we'll consider the general case, \(\mathbb{Z}_n\), which we can initially think of as the group of symmetries of a 'bumpy' \(n\)-sided polygon.
There are many different ways in which \(\mathbb{Z}_n\) appears in mathematics; it's a very important group! We now describe a number of different ways in which it arises.

1. Well, first we have the group of symmetries of the 'bumpy' \(n\)-sided polygon. By the exercise at the end of the last section, we know this is a group.

2. For our second definition, we'll define the 'remainder by \(n\)' operation: for any integer \(a\), define \(a \mod n\) to be the remainder of \(a\) when divided by \(n\). For example, \(5 \mod 3 = 2\), because the remainder of \((5)\) when divided by \((3)\) is \((2)\). (You should check that for any integer \(k\), \(((kn) \mod n=0))\). This operation is usually called 'modulus' or 'mod.' So \(12 \mod 5\) is read 'twelve modulo 5' or 'twelve mod 5.' (And is equal, of course, to two!)

Let \(\mathbb{Z}_n\) be the set of numbers \(\{0,1,2,\ldots,n-1\}\) (which contains \(n\) elements). We define an operation \(+_n\) on these numbers by the following rule: For any \(a,b\in \mathbb{Z}_n\), \((a+_nb)=(a+b) \mod n\). For example, \(\mathbb{Z}_5\) is the set \(\{0,1,2,3,4\}\). Here, for example, \((4+_53)=(4+3) \mod 5=7 \mod 5=2\). You should write down an addition table for \(\mathbb{Z}_5\).

Usually, we don't write \(+_n\) for the addition. From now on, whenever you see an expression like \((4+3)\), you will have to be mindful of the context! If we consider \((4)\) and \((3)\) as plain old integers, the answer is \((7)\). If they are integers mod \((5)\), then the answer is \((2)\)!

3. The next definition is really just an easy way to think of the second definition. Imagine a distant planet where the clock has \(n\) hours on it instead of \(12\) (or \(24\)). Then, just as our hours 'wrap around' the circle beyond \((12)\) o'clock, the hours wrap around at \((n)\). Now if we imagine the clock is numbered \((0)\) through \((n-1)\) instead of \((1)\) to \((n)\), we have exactly the situation of \(\mathbb{Z}_n\).

4. Our last definition will identify \(\mathbb{Z}_n\) with the \(n\)-th roots of unity, which are complex numbers. Recall that any complex number may be written as \(re^{i\theta}\), where \(r\) is a positive real number and \(\theta\) is any angle. Now let \(n\) and \(k\) be some positive integers, and consider the complex number \(x_k=e^{\frac{k}{n}2i\pi}\). Then we can see that \((x_k^n) = (e^{\frac{k}{n}2i\pi})^n = e^{k2i\pi} = 1\). Then we call \(x_k\) an \(n\)th root of unity, because raising it to the \(n\)th power gives us \(1\) (aka, unity).

Now we need an operation on the roots of unity: We can just use multiplication of complex numbers! Consider \(x_{k+1} = e^{\frac{k}{n}2i\pi}\). Because angles only matter up to adding/subtraction \(\frac{2\pi}{n}\), we see that the multiplication here 'wraps around' just like the addition in \(\mathbb{Z}_n\). In fact, we can see this directly by drawing the \(n\)th roots of unity in the complex plane! They are just \(n\) points evenly spaced around the unit circle, and their multiplication exactly matches the addition in \(\mathbb{Z}_n\) on the extra-terrestrial clock.

All of these are somehow the same; but there's a question of how to formally show that two groups are the same. What do we mean by the same? This is an important question to consider, which we will come back to later. For now, an exercise.

Exercise 2.2.0
Write out tables for \(n=5\) and \(n=6\) for:

1. composition of the rotations of the 'bumpy' \(n\)-gon,
2. addition in \(\mathbb{Z}_n\),
3. addition of hours on an extraterrestrial clock with \(n\) hours,
4. and for multiplication of the \(n\)-th roots of unity.

In what ways are all of these groups the same? In what ways are they different?

Contributors

- Tom Denton (Fields Institute/York University in Toronto)