Introduction to Modular Arithmetic: 19 XI 2015

We want to begin to cement the ideas introduced in the past 2 weeks by doing a few examples. BTW: Without wishing to encourage 'calculators', you may at some stage wish to download the following free software onto any PC or Mac you have at school/home:

http://www.mirrorservice.org/sites/www.sagemath.org/index.html

This will help you learn this stuff much faster - there are phenomenal online manuals (and help forums in google groups etc etc) giving starting commands so that you can get going with modular arithmetic on much bigger numbers and test out your conjectural ideas much more effectively .... In fact it is an easy programming language as well as a calculator, so you may find it very very interesting ...

But!!!! I still insist that mental arithmetic is the best way as far as you can .... So first please practice A LOT of these examples by hand ....

Introductory concepts

Recall that we write $\mathbb{Z}$ for the integers, or whole numbers (positive and negative, together with zero). If we write $\mathbb{N}$ for the *natural numbers*[1] (0,) 1, 2, 3, etc then we see that

$$\mathbb{Z} = \mathbb{N} \cup \{0\} \cup -\mathbb{N},$$

where $-\mathbb{N}$ means the set of all the numbers which are the negatives of those in $\mathbb{N}$.

OK so remember that a *modulus* $\mathbf{m} \in \mathbb{N}$ is like the top number on a clock. We generally equate $\mathbf{m}$ to zero, so the numbers in the system become simply

$$0, 1, 2, 3, \ldots, (\mathbf{m} - 2), (\mathbf{m} - 1).$$

[So for example with a normal 12-hour clock in our world we would have a zero at the top rather than a 12.] Then when we pass $\mathbf{m}$, we start all over again, and so on ad infinitum. Hence the analogy we discussed of a multi-storey car park spiralling off up into the sky and down into the ground, circling around on itself indefinitely in both directions: this represents the (also infinite in both directions) number line being wrapped around itself again and again.

Notice that in this image, directly **above** the point zero (first floor and above ....) there lie all the *positive* multiples of $\mathbf{m}$, in increasing order; and directly **below** zero (basement and below ...) lie all of the *negative* multiples of $\mathbf{m}$, in *decreasing* order. Similarly, if we designate 3 to lie $3/\mathbf{m}$ times the way around the first ramp going up, then the integers $3 + \mathbf{m}$, $3 + 2\mathbf{m}$, $3 + 3\mathbf{m}$ etc all lie directly above 3 on the next levels up; and the integers $3 - \mathbf{m}$, $3 - 2\mathbf{m}$, $3 - 3\mathbf{m}$ etc drill down into the ground, again directly *below* 3.

We recall that the way to find out what any given $n \in \mathbb{Z}$ corresponds to *modulo* $\mathbf{m}$ is to divide n by $\mathbf{m}$ and then throw that bit away and just keep the remainder r. That is, we use the *Euclidean algorithm* to find the unique numbers $a, r \in \mathbb{Z}$ such that

$$n = a\mathbf{m} + r, \text{ with } 0 \leq r < \mathbf{m}.$$

Note the requirement that $0 \leq r < \mathbf{m}$: without this, we could get an infinite number of different remainders. This property, that a Euclidean algorithm exists in the integers, is actually very special. For example, it often does NOT exist in the number systems I hope we shall be studying soon[2]. [While we're on that topic, if we set $\mathbf{m} = 12$ and make $n = 9$, what is n divided by 3? What is 3 times 7? What's going on? :)]

So for example if $\mathbf{m} = 17$ and $n = 141$ then we see that $141 = 17 * 8 + 5$; so we say "141 is *congruent to* 5 *modulo* 17", and write this as:

$$141 \equiv 5 \mod 17, \text{ or more simply: } 141 \equiv 5 \ (17).$$

Notice that in some sense we are doing the exact opposite of what one normally does when dividing two numbers: normally we are interested in the closest whole number to the result of the division, which in this example would have been 8. But in this type of mathematics (the branch called Number Theory) we often don't care about the 8, and just look at the remainder 5.

One very clever notation for this system of numbers (which actually means something in formal mathematical terms as well, which we shall get to later) is

$$\mathbb{Z}/\mathbf{m}\mathbb{Z}.$$

[1] I put zero in brackets because no-one can ever seem to decide whether or not $0 \in \mathbb{N}$ ...

[2] Massive healthy equivalent of a mars bar to anyone who can **explain** an example to us all ... ie not just copy it off the internet :)

That is to say, we take the set $\mathbb{Z}$ and we declare all of the multiples of $\mathbf{m}$ inside $\mathbb{Z}$ to be zero. But this set of all multiples of $\mathbf{m}$ is simply the set $\mathbf{m}\mathbb{Z}$. So this notation really says what we have just done with the modulus in our example above, namely: any multiple of $\mathbf{m}$ is unimportant; we merely look at what is left over when we count in the integers and set every multiple of $\mathbf{m}$ to zero. So we may view this thing $\mathbb{Z}/\mathbf{m}\mathbb{Z}$ as a set of objects of the form:

$$\{\ 0+\mathbf{m}\mathbb{Z}\ , 1+\mathbf{m}\mathbb{Z}\ , 2+\mathbf{m}\mathbb{Z}\ , \ldots, (\mathbf{m}-2)+\mathbf{m}\mathbb{Z}\ , (\mathbf{m}-1)+\mathbf{m}\mathbb{Z}\ \}\,.$$

This is very similar to what we do with fractions of integers (ie *rational numbers*, denoted $\mathbb{Q}$), which explains why many people find them very difficult to work with. They are actually not just "one number", but *equivalence classes* of infinite sets of numbers which we deem to be the same "number": so $1/1 = 2/2 = 3/3 = \ldots$ and this equivalence class $\{1/1, 2/2, 3/3, \ldots\}$ is just called the rational number 1. Similarly, $3/5 = 6/10 = 9/15 = 12/20 = \ldots$ and this equivalence class $\{3/5, 6/10, 9/15, 12/20, -12/-20, \ldots\}$ is just called 3/5 (or 300/500, or whatever you want – the point is that all of these fractions are "the same" ...) We will return to this idea many times in the course of this study.

By the way, since some of you seemed to be intrigued by the ideas of infinity and dimensions and things like that .... we call the "size" of a set its *cardinality.* So the set $\{1, 2, 3, 5, 89\}$ has cardinality 5. For infinite sets there is also a notion of cardinality, but it is quite tricky. Clearly the natural numbers $\mathbb{N}$ have cardinality equal to what we normally think of as "infinity". Let's just agree for now to write ∞ for that. But then what is the cardinality of $\mathbb{Z}$? And of $\mathbb{Q}$? And of the *real numbers* $\mathbb{R}$? Or the *complex numbers* $\mathbb{C}$? If you are inspired by this, please look up the so-called *Continuum Hypothesis* ....

Finally, just a reminder that the negative integers enter into this in a very natural way, namely one just goes around the clock backwards. So -1 is the same as $(\mathbf{m}-1)$, -2 is the same as $(\mathbf{m}-2)$, and so on. What is $-\mathbf{m}$? That's right .... zero again.

Modular Arithmetic Exercises #1

So let's do a couple of practise exercises on this stuff so far.

Exercise 1. *For* $\mathbf{m} = 5, 6, 11, 15$ *work out the patterns on the "modulo* $\mathbf{m}$ *clockface" which occur when we start at zero and count up by 1, then by 2, then by 3, etc. That is, we are using only addition to generate something like the "mod* $\mathbf{m}$ *times tables".*

As we observed, negative numbers can be done in a particularly simple way using the positive numbers and so anything $\geq \mathbf{m}/2$ can be done using something you have already done for earlier numbers $\leq \mathbf{m}/2$.

Exercise 2. *Do the same as the first exercise but for multiplication, ie powers (or* exponentials*) – that is take a bunch of your favourite moduli and draw the patterns which occur when you start with 2,* 2^2*,* 2^3*, ...; and then 3,* 3^2*,* 3^3*, etc .....*

Remember the tricks this time when we use negative numbers ... the picture is much more complicated (to recall the example from last session, try the powers of ± 2 (and for that matter of ± 1 and ± 3) when $\mathbf{m} = 9$).

And finally here is the famous unsolved question which we mentioned briefly at the end of the last session.

Unsolved Problem 1. *Let* $\mathbf{m}$ *be any* **prime** modulus. How do we find a *multiplicative generator* for $\mathbb{Z}/\mathbf{m}\mathbb{Z}$? That is to say, a number $g \in \mathbb{N}$ between 2 and $(\mathbf{m}-1)$ such that the powers of g give you EVERY number $1, 2, 3, 4, \ldots, (\mathbf{m}-1)$?