Modular Arithmetic 1

Telling the Time

This part of the notes is going to focus on a particular method of arithmetic (working with numbers) which is sometimes known as 'clock arithmetic'. To give it its proper name, it is **modular arithmetic**, or **arithmetic modulo** n.

Consider this example. Working with a 12 hour clock, if it is 10AM and I ask you what time it is in 5 hours, what would you respond with? You might say it would be 3PM. But $10 + 5 = 13 \neq 3$.

Similarly, if it is Tuesday today and I ask you what day it is in 13 days, what would you respond with? Presumably you would say it would be Monday. If we think of Tuesday as the second day of the week, then we've done the sum $2 + 13$ and somehow ended up with Monday, or 1, instead of 15.

In each of these examples we're actually calculating remainders. On a 12 hour clock we are working **modulo** 12 and when thinking about days of the week we are working **modulo** 7. In the first example we have added 10 and 5 to get 15 and then worked out the remainder upon dividing by 12, which gets us 3. In the second example we have added 2 (Tuesday) and 13 to get 15 again, but this time we have worked out the remainder upon dividing by 7, which gets us 1 (Monday).

(Note that the videos below briefly refer to an old version of the notes. You'll probably not even notice it!)

Video Visit the URL below to view a video:

`https://www.youtube.com/embed/GdalwCcGaPY`

Video Visit the URL below to view a video:

`https://www.youtube.com/embed/KnECaLL66io`

The Rules of Modular Arithmetic

If n is a positive integer and a is any integer, the remainder when a is divided by n is written

If n is a positive integer and a is any integer, then we can write

$$a = q \times n + r,$$

where both q and r are also integers and $0 \leq r < n$. Here q is called the **quotient** and r is called the **remainder**. This section is really all about remainders, so we will introduce some notation. If we have n, a, q, and r as above, then we will write

$$a \mod n = r.$$

Sometimes we will write

$$a \pmod{n} = r.$$

Essentially, the mod operation tells you to just think about the remainder.

For example,

$$\begin{aligned} 7 \mod 5 &= 2, \\ 10 \mod 5 &= 0, \\ (-2) \mod 5 &= 3. \end{aligned}$$

In the first case $7 = 1 \times 5 + 2$; in the second case $10 = 2 \times 5 + 0$; and in the third case $-2 = -1 \times 5 + 3$. This operation is called 'reducing a modulo (or mod) n'.

The set of all possible remainders is written $\mathbb{Z}_n$. So

$$\mathbb{Z}_n = \{0, 1, 2, \ldots, n-1\}.$$

For example,

$$\begin{aligned} \mathbb{Z}_2 &= \{0, 1\}, \\ \mathbb{Z}_5 &= \{0, 1, 2, 3, 4\}. \end{aligned}$$

Addition and multiplication can be defined on $\mathbb{Z}_n$. They are done by adding or multiplying in the usual way and then taking the remainder upon division by n. For example, in $\mathbb{Z}_5$, we have:

$$\begin{aligned} 1 + 3 &= 4, \\ 2 + 3 &= 5 = 0, \\ 4 + 3 &= 7 = 2 \end{aligned}$$

and

$$\begin{aligned} 1 \times 3 &= 3, \\ 2 \times 3 &= 6 = 1, \\ 4 \times 3 &= 12 = 2. \end{aligned}$$

As mentioned at the start of this section, we use addition modulo 12 and 7 in everyday life. (Also modulo 24 if you work to a 24 hour clock.)

We can also subtract. In ordinary arithmetic, $-x$ is the number that gives 0 when it is added to x. Then $y - x$ is defined in terms of addition by $y - x = y + (-x)$. The same applies in modular arithmetic. Modulo n, we get $-x = n - x$, because $x + (n - x) \mod n = n \mod n = 0$. For example, in $\mathbb{Z}_5$, we have

$$-4 = 1,$$
$$2 - 4 = 2 + 1 = 3.$$

(Some of these equations will seem odd but keep the time and date examples in mind!)

Raising an element of $\mathbb{Z}_n$ to a power is defined as repeated multiplication, just as normal in $\mathbb{Z}$. For example, in $\mathbb{Z}_5$, we have

$$2^0 = 1,$$
$$2^1 = 2,$$
$$2^2 = 4,$$
$$2^3 = 8 = 3,$$
$$2^4 = 16 = 1,$$
$$2^5 = 32 = 2.$$

Division isn't so simple. (We'll get to that later.)

When we add or multiply integers and then reduce mod n, we can also reduce mod n first. This can result in working with smaller numbers and so make the calculations simpler. The rules are:

$$(a + b) \mod n = (a \mod n) + (b \mod n),$$
$$(a \times b) \mod n = (a \mod n) \times (b \mod n),$$
$$(a^k) \mod n = (a \mod n)^k.$$

Here the arithmetic operations on the left hand sides of the equations are operations in $\mathbb{Z}$, and on the right hand sides they are operations in $\mathbb{Z}_n$, and k is a non-negative integer.

For an example, we'll think about finding $5^{19} \mod 7$ without using a calculator. So what we are really doing is finding the remainder of the very large number 5^{19} when it is divided by 7.

$5^1 \mod 7 = 5$

$5^2 \mod 7 = 25 \mod 7 = 4$

$5^4 \mod 7 = (5^2)^2 \mod 7 = (5^2 \mod 7)^2 \mod 7 = 4^2 \mod 7 = 16 \mod 7 = 2$

$5^8 \mod 7 = (5^4)^2 \mod 7 = 2^2 \mod 7 = 4$

$5^{16} \mod 7 = (5^8)^2 \mod 7 = 4^2 \mod 7 = 2.$

So after all of that,

$$5^{19} \mod 7 = 5^16 \times 5^2 \times 5^1 = 2 \times 4 \times 5 = 5.$$

Often when we are working with a particular modulus, then we might drop the notation until the very end. For example, the previous calculation then becomes the following, which you may find easier to read.

$$5^1 = 5$$

Month	**Days**	**Days** mod 7
January	31	3
February (leap year)	29	1
February (non-leap year)	28	0
March	31	3
April	30	2
May	31	3
June	30	2
July	31	3
August	31	3
September	30	2
October	31	3
November	30	2
December	31	3

$$\begin{aligned} 5^2 &= 25 = 4 \\ 5^4 &= (5^2)^2 = (5^2)^2 = 4^2 = 16 = 2 \\ 5^8 &= (5^4)^2 = 2^2 = 4 \\ 5^{16} &= (5^8)^2 = 4^2 = 2 \mod 7. \end{aligned}$$

A more formal way to define the modulo operation is like this. The notation $a \equiv b \pmod{n}$ or $a = b \pmod{n}$ really means that n divides $a - b$, or, in other words, that $a = b$ in $\mathbb{Z}_n$.

Video Visit the URL below to view a video:

`https://www.youtube.com/embed/OsZ3tvdOLq4`

Days of the Week

If today is Monday 25 November 2020, what day of the week is 21 December this year? One way of working this out is to see in how many days' time this is, work out the number of complete weeks and then count the days forward.

Thus, starting after 23 November, there are 7 days left in November and then 21 days to the required date in December, making 28 days altogether. This is 4 complete weeks, which means that 21 December is also on a Monday.

All we have done here really is addition modulo 7, and this idea can be extended over longer time periods.

For example, knowing that 1 January 2006 was a Sunday, on what day of the week was 22 August 2006? We have to calculate the number of days, modulo 7, that 22 August is after 1 January. (Note that we don't count 1 January itself.)

Putting in the remaining $30 = 2 \mod 7$ days of January, the complete months, and then $22 = 1 \mod 7$ for August, we have

$$2 + 0 + 3 + 2 + 3 + 2 + 3 + 1 = 16 = 2 \mod 7.$$

Hence, counting on two days on from Sunday, 22 August was on a Tuesday that year.

Concept Checks

Test Yourself Visit the URL below to try a numbas exam:
`https://numbas.mathcentre.ac.uk/question/100687/modular-arithmetic-quotient-and-remainder/embed/`