Modular arithmetic

Peter Rowlett

Some quantities we deal with every day come in cycles. If it's currently 10pm and I ask what the time will be in five hours, what would you say? Hopefully you would say 3am, not 15pm. You know $10 + 5 \neq 3$, but you have mapped $10 + 5 \to 3$ nonetheless.

We can define consistent rules to deal with this kind of quantity. These have many applications beyond time, including in cryptography, data storage, barcodes, ISBN numbers assigned to books, and even magic tricks.

1 Divisors

One property of elements of the set $\mathbb{Z}$ is that $\forall m, n \in \mathbb{Z}\ (m + n \in \mathbb{Z})$ – adding two integers produces another integer. Similarly, $\forall m, n \in \mathbb{Z}\ (m - n \in \mathbb{Z})$ and $\forall m, n \in \mathbb{Z}\ (mn \in \mathbb{Z})$. What about $\frac{m}{n}$? Is it true that $\forall m, n \in \mathbb{Z}\ (\frac{m}{n} \in \mathbb{Z})$?

In fact, we can say $\exists m, n \in \mathbb{Z}\ (\frac{m}{n} \notin \mathbb{Z})$ – sometimes, dividing one integer by another produces a non-integer. For example, choose $m = 7$ and $n = 5$. Then $\frac{7}{5}$ is not an integer.

For $m, n \in \mathbb{Z}$, we say n *divides* m if $\exists q \in \mathbb{Z}\ (m = qn)$. In this case we say m is *divisible* by n and write $n|m$. We also say n is a *divisor* of m. If n does not not divide m, we write $n \nmid m$

2 Modular arithmetic

If $n \nmid m$ for some $m \in \mathbb{Z}$ and $n \in \mathbb{N}$, we can think about remainders. By the definition above, if $n \nmid m$ then this means we cannot write $m = qn$ for some $q \in \mathbb{Z}$. Then it must be the case that we can find $q, r \in \mathbb{Z}$ so that

$$m = qn + r.$$

Here, q is called the *quotient* and r is called the *remainder*.

In modular arithmetic, we don't care about the value of q and so we write $m = r \pmod{n}$, saying "m equals r modulo n". We can also answer "Find $m \pmod{n}$" with r.

Note that since $m - r = qn$, we can also say $n|(m - r)$.

If $x, y \in \mathbb{Z}$ have the same remainder when dividing by $n \in \mathbb{N}$, then we say that x and y are *equivalent modulo* n. We can write this $x \pmod{n} = y \pmod{n}$, though for convenience we usually write either $x \pmod{n} = y$ or $x = y \pmod{n}$.

2.1 Examples

1. $15 = 0 \pmod 5$ because $15 = 3 \times 5 + 0$.
2. $16 = 4 \pmod{12}$ because $16 = 1 \times 12 + 4$.
3. $-73 = 27 \pmod{10}$ because $-73 = (-8) \times 10 + 7$ and $27 = 2 \times 10 + 7$, so both are equivalent modulo 10.

To find $261 \pmod 8$ using a calculator, divide 261 by 8 to get 32.625. If $261 = 8q + r$, we see immediate that $q = 32$. The remainder is represented in decimal form by the fractional part 0.625. We find the reminder by multiplying $0.625 \times 8 = 5$, so $261 = 5 \pmod 8$.

3 Arithmetic

3.1 Addition

Theorem 3.1. *Let $x, y, r, s \in \mathbb{Z}$ and $n \in \mathbb{N}$ so that $x = r \pmod n$ and $y = s \pmod n$. Then*

$$x + y = r + s \pmod n.$$

This is a theorem and we can prove it directly.

Proof. By assumption we have that $x = kn + r$ and $y = ln + s$ for some $k, l \in \mathbb{Z}$. Then,

$$\begin{aligned} x + y &= kn + r + ln + s \\ &= (k + l)n + (r + s). \end{aligned}$$

We have expressed $x + y$ in the form of a quotient $k + l$ times n plus a remainder $r + s$. We therefore have $x + y = r + s \pmod n$, as required. □

(Notice I told LaTeX that this is a proof, and it has ended it with the end of proof/QED symbol □.)

Replacing y with $-y$ in theorem 3.1 we can also deal with subtraction.

3.2 Multiplication

Theorem 3.2. *Let $x, y, r, s \in \mathbb{Z}$ and $n \in \mathbb{N}$ so that $x = r \pmod n$ and $y = s \pmod n$. Then*

$$xy = rs \pmod n.$$

Proof. By assumption we have that $x = kn + r$ and $y = ln + s$ for some $k, l \in \mathbb{Z}$. Then,

$$\begin{aligned} xy &= (kn + r)(ln + s) \\ &= kln^2 + kns + lnr + rs \\ &= (kln + ks + lr)n + rs. \end{aligned}$$

We have expressed xy using the quotient $kln + ks + lr$ and the remainder rs. We can therefore write $xy = rs \pmod{n}$, as required. □

3.3 Example

Find the last digit of 8^7.

Obviously we could just put 8^7 into a calculator. Hopefully it is equally obvious that we are expected to do something more clever.

Note that the last digit of a number is the remainder on division by 10. Thus we need to work mod 10.

Let's start with $8^2 = 64$. Since $64 = 4 \pmod{10}$, we can say $8^2 = 4 \pmod{10}$.

We can use this to work out 8^3, since

$$8^3 \pmod{10} = 8^2 \times 8 \pmod{10} = 4 \times 8 \pmod{10} = 32 \pmod{10} = 2 \pmod{10}.$$

We can also work out 8^4, since

$$8^4 \pmod{10} = (8^2)^2 \pmod{10} = 4^2 \pmod{10} = 16 \pmod{10} = 6 \pmod{10}.$$

Since $8^7 = 8^3 \times 8^4$, we can say

$$8^7 \pmod{10} = 2 \times 6 \pmod{10} = 12 \pmod{10} = 2 \pmod{10}.$$

So the last digit of 8^7 is 2.

3.4 Example

What are the last two digits of 7^{2018}? This time it is harder to simply pop it into a calculator, since the answer has 1704 digits.

Asking for the last two digits means we are working mod 100.

Since $7^2 = 49$ and $7 \times 49 = 343 = 43 \pmod{100}$, it follows that $7^4 = 7 \times 43 = 301 = 1 \pmod{100}$.

Since $4 \times 504 = 2016$, we can say $7^{2016} = (7^4)^{504} = 1^{504} \pmod{100} = 1 \pmod{100}$.

We were interested in $7^{2018} = 7^2 \times 7^{2016}$, so we can conclude

$$7^2 \times 7^{2016} = 49 \times 1 \pmod{100} = 49 \pmod{100},$$

so the last two digits of 7^{2018} are 49.