Numbers and Codes

Richard Earl
Mathematical Institute
University of Oxford
http://www.maths.ox.ac.uk/

Modular Arithmetic

You may well be familiar with some ideas of modular, or clockwork, arithmetic already. Modular arithmetic is essentially the study of remainders. For example, you will no doubt be happy with the following equations which hold for odd and even numbers:

$$\begin{aligned} \text{even} + \text{even} &= \text{even}, \ \ \text{even} + \text{odd} = \text{odd}, \ \ \text{odd} + \text{odd} = \text{even}, \\ \text{even} \times \text{even} &= \text{even}, \ \ \text{even} \times \text{odd} = \text{even}, \ \ \text{odd} \times \text{odd} = \text{odd}. \end{aligned}$$

Note that it doesn't matter which odd number or even number we have in mind for these equations to hold true — whatever odd numbers we multiply (e.g. 3 and 5 or 7 and 9) their product (15 or 63) will be odd.

The above equations give the rules of mod 2 arithmetic.

mod 2 Arithmetic

mod 2 arithmetic is the study of remainders when we divide by 2. If we divide a whole number by two then we will have a remainder that is either 0 or 1 depending on whether that number was even or odd. Instead of talking about even and odd, we could talk about *"0"-type numbers* and *"1"-type numbers*, and the equations above would become

$$\begin{aligned} 0+0 &= 0, \quad 0+1=1, \quad 1+1=0, \\ 0\times 0 &= 0, \quad 0\times 1=0, \quad 1\times 1=1. \end{aligned}$$

Most of these calculations look familiar to us from normal arithmetic except for the equation "1" + "1" = "0" which looks decidedly odd. Normally of course the answer is 2, but here 2 is a "0"-type number.

mod 3 Arithmetic

If we divide a number by 3 then the possible remainders are 0,1 and 2 with

- the "0"-type numbers are multiples of 3;
- the "1"-type numbers include 7,10,1,-5;
- the "2"-type numbers include 8,2,11,-1.

Let's take two "2"-type numbers, say 5 and 8, or 11 and 2; their products 40 and 22 are both "1"-type numbers. In fact, it is easy to check that the product of two "2"-type numbers is always a "1"-type number — that is, in mod 3 arithmetic $2 \times 2 = 1$.

The rules of mod 3 arithmetic are

$$\begin{aligned} 0+0 &= 0, \quad 1+1=2, \quad 2+2=1, \quad 0+1=1, \quad 0+2=2, \quad 1+2=0, \\ 0\times 0 &= 0, \quad 1\times 1=1, \quad 2\times 2=1, \quad 0\times 1=0, \quad 0\times 2=0, \quad 1\times 2=2, \end{aligned}$$

and again these rules apply no matter what example of a "0"-, "1"-, "2"-type we choose.

Proof

How would we *prove* that $2 \times 2 = 1$ in mod 3? We certainly cannot check this by multiplying all the different "2"-type numbers together.

Note that every whole number n can be written as one of

$$3k, \qquad 3k+1, \qquad 3k+2,$$

where k is a whole number, depending on whether n has type "0", "1" or "2".

If we multiply two "2"-type numbers, $3k_1 + 2$ and $3k_2 + 2$ we get

$$(3k_1 + 2)(3k_2 + 2) = 9k_1k_2 + 6k_1 + 6k_2 + 4 = 3(3k_1k_2 + 2k_1 + 2k_2 + 1) + 1.$$

We see that the product is a "1"-type number, whatever "2"-type numbers we multiply.

The General Case

Generally, if we are doing arithmetic $\bmod n$, (where $n \geqslant 2$), then there are n possible remainders, namely

$$0, 1, 2, 3, \ldots, n-1.$$

Again, we can work out how two types, say "i" and "j" add, simply by looking at the type of $i+j$, and we may subtract and multiply them in a similar fashion.

Rather than writing "i"-type each time we will denote this by $i \pmod n$.

So we have

$$\begin{aligned}
a \pmod n + b \pmod n &= \text{remainder when } a+b \text{ is divided by } n, \text{ written } a+b \pmod n. \\
a \pmod n - b \pmod n &= \text{remainder when } a-b \text{ is divided by } n, \text{ written } a-b \pmod n. \\
a \pmod n \times b \pmod n &= \text{remainder when } a \times b \text{ is divided by } n, \text{ written } ab \pmod n.
\end{aligned}$$

Examples

$$
\begin{aligned}
3 \pmod 7 + 5 \pmod 7 &= \text{remainder when } 8 \text{ is divided by 7} = 1 \pmod 7,\\
3 \pmod 7 - 5 \pmod 7 &= \text{remainder when } -2 \text{ is divided by 7} = 5 \pmod 7,\\
3 \pmod 7 \times 5 \pmod 7 &= \text{remainder when } 15 \text{ is divided by 7} = 1 \pmod 7.
\end{aligned}
$$

More concisely, the above examples might be written as

$$
\begin{aligned}
3 + 5 &= 8 = 1 \pmod 7,\\
3 - 5 &= -2 = 5 \pmod 7,\\
3 \times 5 &= 15 = 1 \pmod 7,
\end{aligned}
$$

because in the sense of $\mod 7$ arithmetic, 8 equals 1, and -2 equals 5.

Problems

1. Calculate $3 \times 5 \pmod 8$
2. Calculate $2 - 5 \pmod 6$
3. Calculate $2 + 6 \pmod 7$
4. Calculate $2 \times 3 \pmod 6$
5. Can you make sense of $1 \div 2 \pmod 5$?
   (Such a number would need to solve $2x = 1 \pmod 5$).
6. Can you make sense of $3 \div 2 \pmod 5$?
7. Can you make sense of $3 \div 2 \pmod 6$?
8. Prove that the product, of two numbers which end in 6, also ends in 6.
9. You are told a number:
   - leaves remainder 3 when divided by 4,
   - leaves remainder 2 when divided by 5.

   What is the remainder when this number is divided by 20?

Answers

1. $3 \times 5 = 15 = 7 \pmod 8$
2. $2 - 5 = -3 = 3 \pmod 6$
3. $2 + 6 = 8 = 1 \pmod 7$
4. $2 \times 3 = 6 = 0 \pmod 6$
5. As $2 \times 3 = 6 = 1 \pmod 5$ then $1 \div 2 = 3 \pmod 5$
6. As $3 \div 2 = 3 \times (1 \div 2) = 3 \times 3 = 9 = 4 \pmod 5$
7. There is no solution to $2x = 3 \pmod 6$ and so $3 \div 2 \pmod 6$ is meaningless.
8. If a number ends in 6 it is of the form $10k + 6$. Note that the product

   $(10k_1+6)(10k_2+6) = 100k_1k_2+60k_1+60k_2+36 = 10(10k_1k_2+6k_1+6k_2+3)+6,$

   of two such numbers, also ends in 6.
9. Write the number as $20k + r$ where $0 \leqslant r < 20$. We see $r = 7$ as

$$\begin{aligned} 20k + r = 3 \pmod 4 &\implies r = \ 3, 7, 11, 15 \text{ or } 19; \\ 20k + r = 2 \pmod 5 &\implies r = \ 2, 7, 12 \text{ or } 17. \end{aligned}$$

Points of Algebra

Note that modular arithmetic has some properties which don't normally occur.

For example, if two "normal" numbers x and y multiply to give 0, then it has to be the case that one (or both) of x, y is zero. But, in modular arithmetic, we find products like

$$\begin{aligned} 3 \times 5 = 15 = 0 &\quad \mod 15, \\ 4 \times 3 = 12 = 0 &\quad \mod 6. \end{aligned}$$

Here, we have examples of non-zero numbers which multiply to give zero.

In the same way that we can't divide by 0 normally, we can't divide by 2, or 3, or 4 in $\mod 6$ arithmetic. It doesn't make sense to write $1 \div 2$ as there is no number that solves $2x = 1 \mod 6$.

We can make sense of dividing by 1 and 5 though, because they have no common factor with 6 as $1/1 = 1 \mod 6$ and $1/5 = 5 \mod 6$.

Powers

We've seen that it is possible to add, subtract, multiply and sometimes divide in modular arithmetic. So repeated multiplication, that is taking powers is also possible. In fact, in many ways taking powers is easier in modular arithmetic than in standard arithmetic; normally powers, such as 2^k, become larger and larger as k increases, whilst in modular arithmetic the answer always has to remain between 0 and $n-1$.

Q: What is the last digit in 2^{1000}?

2^{1000} is a huge number, 302 digits long, too big for most calculators, and so the question looks rather difficult at first glance. But if we investigate the problem by trying to spot a pattern in the behaviour of powers of 2.

k	1	2	3	4	5	6	7	8	9
2^k	2	4	8	16	32	64	128	256	512
Last Digit	2	4	8	6	2	4	8	6	2

It seems then that the last digits of the powers of 2^k repeat every four powers, forever going through a cycle $2, 4, 8, 6$; so after 1000 powers we will be at the end of the 250^{th} cycle. So 2^{1000} ends in a 6.

A Check

A program like *Mathematica* can calculate, fairly quickly, 2^{1000} and produces the answer which is

10,715,086,071,862,673,209,484,250,490,600,018,105,614,048,117,055,336,074,437,503,
883,703,510,511,249,361,224,931,983,788,156,958,581,275,946,729,175,531,468,251,
871,452,856,923,140,435,984,577,574,698,574,803,934,567,774,824,230,985,421,074,
605,062,371,141,877,954,182,153,046,474,983,581,941,267,398,767,559,165,543,946,
077,062,914,571,196,477,686,542,167,660,429,831,652,624,386,837,205,668,069,376

and so we can see straight away that the number ends in 6; but it wouldn't be hard difficult, say by increasing k to a million or a billion or more in order to produce a number that Mathematica couldn't calculate, but having spotted a pattern we would be able to calculate it's last digit.

From the point of view of modular arithmetic we have calculated $2^{1000} \pmod{10}$ as the last digit of a number (written in decimal) is just that number $\bmod 10$.

A Proof

But without being able to calculate 2^{1000}, we could still prove that 2^{1000} ends in a 6 as follows. Note that:

- $6 \times 6 = 36 = 6 \mod 10$;
- so any product of numbers ending in 6, will also end in 6;
- in particular for any power of 6, we have $6^k = 6 \mod 10$;
- $2^4 = 16 = 6 \mod 10$;
- $2^{1000} = \left(2^4\right)^{250} = 16^{250} = 6^{250} = 6 \mod 10$.

Generally we know:

$$2^n = \begin{cases} 2 \mod 10 & \text{if } n = 1 \mod 4; \\ 4 \mod 10 & \text{if } n = 2 \mod 4; \\ 8 \mod 10 & \text{if } n = 3 \mod 4; \\ 6 \mod 10 & \text{if } n = 0 \mod 4. \end{cases}$$

Problems

1. Work out the remainder when each of $2, 4, 8, 16, 32, 64$ is divided by 7.
2. Can you work out what the remainder is when 2^{1000} is divided by 7?
3. What is the last digit in 1999^2? What about in 1999^3?
4. Write down each of $0^2, 1^2, 2^2, 3^2, 4^2, 5^2, 6^2, 7^2$ in $\mod 8$ arithmetic.
5. How many solutions are there of

   $$x^2 = 1 \mod 8?$$

   How many solutions does a quadratic equation normally have?
6. Expand the brackets of

   $$(x-1)(x-7) \text{ and } (x-3)(x-5)$$

   in $\mod 8$ arithmetic.

Answers

1. The remainders, when 2^n $(1 \leqslant n \leqslant 6)$ are divided by 7, are $2, 4, 1, 2, 4, 1$ respectively.

2. As $1000 = 333 \times 3 + 1$ then 2^{1000} leaves remainder 2 when divided by 7.

3. Note that

   $1999^2 = 9^2 = 81 = 1 \pmod{10}$ and $1999^3 = 9^2 \times 9 = 1 \times 9 = 9 \pmod{10}$.

   So 1999^2 and 1999^3 end in 1 and 9 respectively.

4. The squares n^2 $(0 \leqslant n \leqslant 7)$ are $0, 1, 4, 1, 0, 1, 4, 1 \pmod{8}$ respectively.

5. From the above, $x^2 = 1 \pmod{8}$ has four solutions: $1, 3, 5, 7 \pmod{8}$.

   With real numbers, quadratics have 0,1 or 2 roots.

6.

$$\begin{aligned}(x-1)(x-7) &= x^2 - 8x + 7 = x^2 - 1 \pmod{8};\\ (x-3)(x-5) &= x^2 - 8x + 15 = x^2 - 1 \pmod{8}.\end{aligned}$$