Modular arithmetic

1 Congruence

Two numbers x and y are said to be *congruent modulo 100* when $x - y$ is a multiple of 100. For example $13568 \equiv 290068 \pmod{100}$, because

$$13568 - 290068 \quad = \quad -2765 \times 100$$

It's like saying "if you don't care about 100s, then 13568 and 290068 are the same". The number 100 is called the *modulus*; other numbers can be used instead.

A calendrical example: Wednesday 5 October 2022 and Wednesday 15 March 2023 are congruent modulo a week. A musical example: Low C and High C are congruent modulo an octave.

The congruence relation is preserved by addition, subtraction and multiplication. In other words, if we have

$$\begin{aligned} a &\equiv x \pmod{n} \\ b &\equiv y \pmod{n} \end{aligned}$$

then we have

$$\begin{aligned} a + b &\equiv x + y \pmod{n} \\ a - b &\equiv x - y \pmod{n} \\ a \times b &\equiv x \times y \pmod{n} \end{aligned}$$

The first of these says that, if we want to know the last two digits of $a + b$, we need only know the last two digits of a and those of b. Let's prove this.

Suppose $a \equiv x \pmod{n}$ and $b \equiv y \pmod{n}$. Unpacking this, we see that $a - x = pn$ and $b - y = qn$, for integers p and q. Now $(a + b) - (x + y) = pn - qn = (p - q)n$. So we conclude $a + b \equiv x + y \pmod{n}$.

2 Commutative rings of modular arithmetic

Let's think about the set

$$[0 \mathinner{..} 10) \quad = \quad \{0, 1, 2, 3, 4, 5, 6, 7, 8, 9\}$$

For any integer x, there is a unique element of $[0 \mathinner{..} 10)$ that's congruent to $x \pmod{10}$. Namely, $x \bmod 10$. Don't get confused by the two uses of the word mod here!

Now we define operations. For any two numbers a, b in the range $[0 \mathinner{..} 10)$, let's define

$$\begin{aligned} a \ +_{10}\ b &\stackrel{\text{def}}{=} (a + b) \bmod 10 \\ a \ -_{10}\ b &\stackrel{\text{def}}{=} (a - b) \bmod 10 \\ a \ \times_{10}\ b &\stackrel{\text{def}}{=} (a \times b) \bmod 10 \end{aligned}$$

For example,

$$7 \ +_{10}\ 9 \quad = \quad ?$$

It's obvious that $+_{10}$ is commutative, but associativity is not so obvious, so let's prove this. For any a, b, c in the range $[0 \mathinner{..} 10)$, give the name x to $(a + b) + c$, which is the same as $a + (b + c)$. Now we have

$$\begin{aligned} a \ +_{10}\ b &\equiv a + b \\ (a \ +_{10}\ b) \ +_{10}\ c &\equiv (a \ +_{10}\ b) + c \\ &\equiv (a + b) + c \\ &= x \end{aligned}$$

So $(a +_{10} b) +_{10} c$ is the unique element of $[0 \mathinner{..} 10)$ that's congruent to x. By the analogous argument, so is $a +_{10} (b +_{10} c)$. So they must be equal.

In the same way, we can prove all the commutative ring laws. In summary, the set $[0 \mathinner{..} 10)$, together with the operations $+_{10}$ and $\times_{10}$, constitutes a commutative ring. We call it $\mathbb{Z}_{10}$, the commutative ring of arithmetic modulo 10.

It is closely linked to the commutative ring $\mathbb{Z}$, as follows. For any integers a and b, we have

$$\begin{aligned}(a+b) \bmod 10 &= (a \bmod 10) +_{10} (b \bmod 10)\\(a-b) \bmod 10 &= (a \bmod 10) -_{10} (b \bmod 10)\\(a \times b) \bmod 10 &= (a \bmod 10) \times_{10} (b \bmod 10)\end{aligned}$$

This means, for example, that we can find the units digit of $a \times b$ by taking the units digit of a and b, multiplying them, and taking the units digit. Even if a or b is negative.

We can replace 10 by 100 and all this still holds. Thus, we can find the tens-and-units digits of $a \times b$ by taking the tens-and-units digits of a and b, multiplying them, and taking the tens-and-units digits. Even if a or b is negative. *This is why we can perform integer multiplication in complement notation,* which is precisely what happens in Java.

In fact, this works for any positive natural number m. We have a commutative ring $\mathbb{Z}_m$ of arithmetic modulo m, and it is linked to the commutative ring $\mathbb{Z}$ just as before.

3 Multiplicative inverses

Modular arithmetic has many fascinating theorems. Here's one of them: in the commutative ring $\mathbb{Z}_m$, an element a has a multiplicative inverse iff a is coprime to m. I'm not going to prove this, but I want to give you an intuition for why it's true, by looking at some examples.

We know that 7 is coprime with 10. So in $\mathbb{Z}_{10}$, what's the multiplicative inverse of 7? The answer is 3, because $3 \times_{10} 7 = 1$. To get some intuition, let's start at 0 and keep adding 7, to get the following list:

$$0, 7, 4, 1, 8, 5, 2, 9, 6, 3, 0$$

After ten steps, we get back to 0. Before that, we get no repetitions, since 7 and 10 are coprime. Therefore every number must appear, including 1.

To put this differently, imagine a country where a week has 7 days, indexed by $[0 \mathinner{..} 7)$, and a month has 10 days, indexed by $[0 \mathinner{..} 10)$. Over a cycle of 7×10 days, each pair appears exactly once. So there's just one day that is weekday 0 and monthday 1. This gives $7m = 10n + 1$, so $7m \cong 1(\mod m)$, so m is the desired multiplicative inverse.

On the other hand, 4 is not coprime with 10. It clearly has no multiplicative inverse in $\mathbb{Z}_{10}$, because $4 \times_{10} 5 = 0$ and yet $4 \neq 0$ and $5 \neq 0$.

The way of finding multiplicative inverses given above is woefully inefficient! There is a more efficient method using the so-called "extended Euclidean algorithm", which you might be interested to read about.

4 Fields of modular arithmetic

We saw that the commutative ring $\mathbb{Z}$ is not a field. What about $\mathbb{Z}_m$? There are three cases to consider: either m is 1, or composite or prime.

If $m = 1$, then $\mathbb{Z}_1$ isn't a field, since it satisfies $0 = 1$. If m is composite, say $m = ab$, then $\mathbb{Z}_m$ isn't a field, because $ab = 0$ but $a \neq 0$ and $b \neq 0$.

If m is a prime, then $\mathbb{Z}_m$ is a field, because every nonzero element is coprime with m. Finite fields have important applications in cryptography.

5 Other intervals

Now suppose we work modulo 300, but instead of taking the range $[0 \mathinner{..} 300)$, we take some other range of the same size, let's say $[-100 \mathinner{..} 200)$. For any integer a, there's a unique element in this range that's congruent to a mod 300: let's call it $f(a)$. For example,

$$f(507) \quad = \quad ?$$

Again we can define an addition operation: for any a, b in the range $[-100, 200)$, we define

$$\begin{array}{rcl} a \;+'\; b & \stackrel{\text{def}}{=} & f(a+b) \\ a \;-'\; b & \stackrel{\text{def}}{=} & f(a-b) \\ a \;\times'\; b & \stackrel{\text{def}}{=} & f(a \times b) \end{array}$$

For example,

$$44 \;+'\; 177 \quad = \quad ?$$

As before, we get a commutative ring.

It is linked to the commutative ring $\mathbb{Z}$ as follows. For any integers a and b, we have

$$\begin{array}{rcl} f(a+b) & = & f(a) \;+'\; f(b) \\ f(a-b) & = & f(a) \;-'\; f(b) \\ f(a \times b) & = & f(a) \;\times'\; f(b) \end{array}$$

In summary, although we are not using the interval $[0 \mathinner{..} 300)$, we are in a very similar situation.

This is analogous to the Java `int` type. The range of its values $[-2^{31} \mathinner{..} 2^{31})$, which forms a commutative ring that is linked to $\mathbb{Z}$. Just like $[0 \mathinner{..} 2^{32})$, it's not a field, because $2^{16} \;\times'\; 2^{16} = 0$.