

Modular Arithmetic

We all know how to do arithmetic with the integers $\mathbb{Z} = \{\dots - 2, -1, 0, 1, 2, \dots\}$. One could write $2 + 12$ and everyone would be able to figure out that the answer is 14.

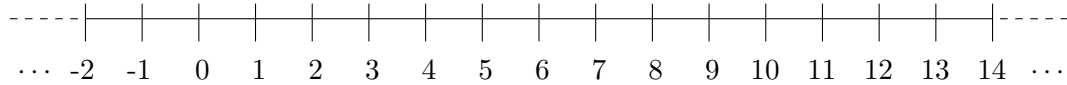


Figure 1: The integer number line

If a person were to see $2 + 12 = 2$, she would likely think that someone had made a typographical error. However, we all make this same kind of calculation every day! Sceptical? Look at a clock.

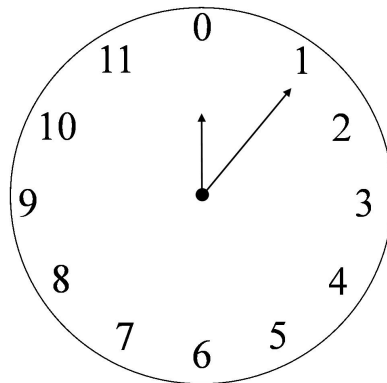


Figure 2: Clock arithmetic: the integers modulo 12

Most people think of time in twelve hour segments, from 12 a.m. to 12 p.m. and then back to 12 a.m. If John says “I got up at 8 o’clock and didn’t go to bed again for fourteen hours”, we would understand that to mean that John woke up at 8 a.m. and went to bed again at 10 p.m. So we have performed the calculation $8 + 14 = 10$. In other words, we have let $12 = 0$ in our calculation. Of course, writing $12 = 0$ does not make much sense under the well-established rules of arithmetic! Thus, mathematicians use another symbol to say that *12 is equivalent to 0*, and write $12 \equiv 0$. So we might write $8 + 14 \equiv 8 + (2 + 12) \equiv 8 + (2 + 0) \equiv 10$.

Having said all this, it does not seem to be a big leap to consider “clocks” with a different number of hours. Mathematicians call this number the *modulus*. Figure 3 shows an example of a 7-hour “clock”, so this would be integers *modulo 7*. In our last example, we would say that *14 is equivalent to 2 modulo 12*. We can also write $14 \equiv 2 \pmod{12}$.

Example 1. • $5 \equiv 5 \pmod{7}$

- $12 \equiv 5 + 7 \equiv 5 + 0 \equiv 5 \pmod{7}$
- $5 + 12 \equiv 5 + 5 \equiv 10 \equiv 3 + 7 \equiv 3 \pmod{7}$

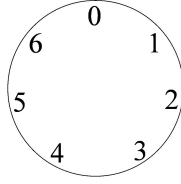


Figure 3: The integers modulo 7

Example 2. • $32 \equiv 2(16) \equiv 0 \pmod{16}$

- $3 - 17 \equiv -14 \equiv 2 \pmod{16}$
- $8(16) \equiv 8(5 + 11) \equiv 8(5) \equiv 40 \equiv 7 \pmod{11}$
- $9(12) \equiv 9(0) \equiv 0 \pmod{12}$

We can make what we learnt from the examples a bit more concrete. We saw in Example 2 that $-14 \equiv 2 \pmod{16}$. Sometimes it can be difficult to tell when two numbers are equivalent. We would like to be able to write down, in general, what makes two numbers equivalent for some modulus.

Definition 1. If a and b are two integers, and $a - b$ is divisible by m (i.e. $\frac{a-b}{m}$ is also an integer), then a and b are said to be *congruent modulo m* , and we write

$$a \equiv b \pmod{m}.$$

Example 3. Show that $-14 \equiv 2 \pmod{16}$.

So $a = -14$, $b = 2$, and $m = 16$. Then

$$\frac{a - b}{m} = \frac{-14 - 2}{16} = \frac{-16}{16} = -1,$$

and -1 is an integer. This makes sense, since

$$-14 \equiv 2 - 16 \equiv 2 - 0 \equiv 2 \pmod{16}.$$