Graeme Turner
g3turner@uwaterloo.ca

Day 1: Introduction to Modular Arithmetic

We begin with a throwback to simpler days: long division, from elementary school! Once upon a time, you would be asked to calculate the remainder of 25 ÷ 7 using long division. You would write

$$\begin{array}{rr} & 3\ \text{r}\,4 \\ 7 \big) & 25 \\ & -21 \\ \hline & 4 \end{array}$$

and conclude that $\frac{25}{7} = 3 + \frac{4}{7}$, where 4 is the **remainder** of the division of 25 by 7. Alternatively, multiplying this equation by 7, we write $25 = 3 \cdot 7 + 4$. The remainder tells us that 25 is 4 more than the greatest multiple of 7 that is equal to or less than 25 (in this case, that's 21, which shows up in the long division.)

In general, for any integers n and d, where $d \neq 0$, we can write

$$n = qd + r$$

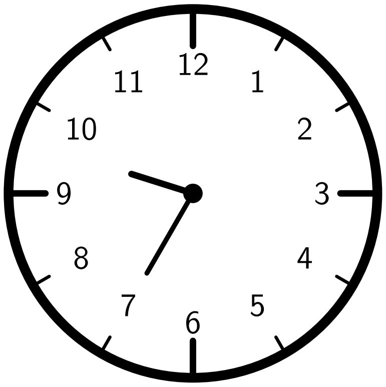
where $0 \leq r < d$ using long division. Here, r is the **remainder** of the division of n by d. This is known as the **Division algorithm**. It is the first step in the *Euclidean algorithm*, which can be used to find the greatest common divisor of two numbers n and d (more on this later!) It's also the cornerstone of *modular arithmetic* (the "math of remainders") and this branch of mathematics lies at the foundation of what is used to protect your data when you swipe your debit/credit card or input a password online!

It's interesting that something as simple as grade-school long division can end up being so powerful. Over the next few weeks, we'll unlock some of the magic behind the math of remainders!

Keeping long division in mind, let's talk about time on analog clocks.

"Clock Arithmetic"

Exhibit A: a plain old clock. In our workings, instead of writing things like "1 o'clock", we'll write 1h.



Say the current time is $10h$. What time will it be after 5 hours have elapsed? Visually, you count 5 numbers ahead from 10: 11 ... 12 ... 1 ... 2 ... 3! It'll be $3h$ when 5 hours have passed. Mathematically speaking, we've just decided that

$$10h + 5h = 3h.$$

Writing an equation like this seems like a quick way to fail Algebra class! Normally, you would collect the coefficient of h, and write $10h + 5h = 15h$. *Aside: looks a lot like international/24h time, huh?*

So what's going on? Well, $15h$ is $3h$ more than $12h$, so we write $15h = 3h$ as $15 = 1 \cdot 12 + 3$. In other words, what determines the number the hour hand lands on is the **remainder** from division by 12.

Let's take this further. Suppose we start at $2h$. We then wait for 15 hours, and then 18 hours. What time is it on the clock? Two approaches arise:

(a) Let's use what we did before. $2h + 15h + 18h = 35h$. Since $35 = 24 + 11 = 2 \cdot 12 + 11$, the time is $11h$.

(b) Waiting for 15 hours has the same effect on the clock as waiting 3 hours as $15h = 3h$. Similarly, $18h = 6h$. Therefore, the time is $2h + 3h + 6h = 11h$.

In mathematics, the above demonstrates that addition in our "clock arithmetic" is **well-defined:** no matter if we take remainders before or after addition, we get the same result! Our shortcuts from option **(b)** produced the same result as option **(a)**.

How about multiplication? Is it also well-defined? Consider starting at $12h$ (or $0h$ if you prefer). Suppose you wait for 13 hours, 13 times in a row. That's a total wait time of 169 hours! As it turns out,

$$\begin{array}{r} 14 \\ 12\,\overline{)\,169} \\ \underline{120} \\ 49 \\ \underline{48} \\ 1 \end{array}$$

so $169 = 14 \cdot 12 + 1$, thus $169h = 1h$. We could have instead used the remainders from the start: $13h = 1h$, so waiting $1h$ thirteen times gives us $13h$, which is $1h$. In essence, $13h \cdot 13h = 1h \cdot 1h = 1h$ (don't square the h). So yes, multiplication is well-defined!

Finally, let's examine the roles of $12h = 0h$ and $1h$ a little more closely. If we add $12h$ to any time, we don't change it as we simply add a full revolution around the clock in the same way that adding 0 to any number does not change it. So $0h$ seems to be more appropriate, especially since it's the remainder when dividing by 12. Multiplying any time by 1 does not change it, and multiplying by 12 produces a multiple of $12h$, which yields $0h$. This makes $0h$ the **additive identity** of our "clock arithmetic", and $1h$ our **multiplicative identity**.

We're now ready to be more formal than working with "clock arithmetic" and define the integers modulo n. When we see the word "modulo", we think "remainder after division by". For example, 25 is 4 modulo 7, and 18 is 6 modulo 12.

Integers Modulo n

Definition: Let n be a positive integer. We define

$$\mathbb{Z}_n = \{0, 1, 2, 3, ..., n-1\},$$

the set of all possible remainders from division of an integer by n, to be the **integers modulo n**. We say that integers a and b are **congruent modulo n** if a and b have the same remainder after division by n, and we write $a \equiv b \pmod{n}$.

As we saw with the clock, addition and multiplication modulo n are defined by taking the remainder modulo n after the operation has been completed, and taking remainders as often as you wish throughout the process will not affect the result!

In defining the integers modulo n, we've defined a new (and finite!) number system. As a recap, here are the other number systems (all of them infinite!) which you should be familiar with:

- **Integers:** $\mathbb{Z} = \{..., -3, -2, -1, 0, 1, 2, 3, ...\}$. The set of all whole numbers, including 0, and their negatives. We can add/subtract/multiply any two integers and we will get an integer result. This doesn't hold true for division in many cases. For example, $\dfrac{1}{2}$ is not an integer.
- **Rational Numbers:** $\mathbb{Q} = \left\{\dfrac{a}{b} \;\middle|\; a, b \in \mathbb{Z} \text{ and } b \neq 0\right\}$. The set of all fractions of integers where the denominator is non-zero. Now, along with addition/subtraction/multiplication, we have division as well.
- **Real Numbers:** $\mathbb{R}$. The set of all rational and irrational numbers. Here, we can always solve the equation $x^2 = a$ whenever a is *non-negative* (i.e. we can take square roots). We can take n^{th} roots depending on the scenario. We can also take *logarithms*: we can solve the equation $a^x = b$ whenever $a > 0$, $a \neq 1$, and $b > 0$.
- **Complex Numbers:** $\mathbb{C} = \{a + bi \mid a, b \in \mathbb{R},\ i^2 = -1\}$. Okay, maybe you haven't used these ones a lot... or possibly at all... but we're not leaving them out! Logarithms are a little more complicated here (understatement!) but we CAN take n^{th} roots of **any** number, positive or negative, real or complex! This property allows $\mathbb{C}$ to be considered **algebraically closed** - no polynomial with complex coefficients is irreducible over the complex numbers! There are several deep rabbit holes to fall into from these last two exclamations, so let's move on.

Now, back to $\mathbb{Z}_n$. We now have many more things to be curious about: subtraction, division, square roots, and logarithms. We'll treat each of these throughout this series.

Let's start with subtraction. In our familiar number systems, subtracting by a number x is the same as adding its negative. This makes $-x$ the **additive inverse** of x - adding x to $-x$ results in the *additive identity* 0.

Think back to our clock, which is modelled perfectly by $\mathbb{Z}_{12}$. How many hours need to pass after $3h$ to get to a multiple of $12h$? Nine hours! So $-3 \equiv 9 \pmod{12}$. It's no coincidence that $9 = 12 - 3$. For any $k \in \mathbb{Z}_n$, we have the formula $\boxed{-k \equiv n - k \pmod{n}}$ So in $\mathbb{Z}_{12}$, $-2 \equiv 10 \pmod{12}$, $-5 \equiv 7 \pmod{12}$, $-6 \equiv 6 \pmod{12}$, and so on. To subtract, we simply add the negative.

What about division? In $\mathbb{Q}$ and $\mathbb{R}$ (and $\mathbb{C}$, technically), for a non-zero number x, dividing by x is the same as multiplying by its reciprocal x^{-1}. The reciprocal is the unique number such that $x \cdot x^{-1} = 1$, the *multiplicative identity.* In modular arithmetic we don't usually write $\frac{1}{x}$, but we will instead write x^{-1} as "x inverse". In the integers, the only numbers which have integer inverses are 1 and -1. How does this work modulo n?

Again, we'll start with $\mathbb{Z}_{12}$. The multiplicative inverse of 1 is 1, since $1 \cdot 1 = 1$. This will be true in any version of $\mathbb{Z}_n$. But what about $x = 2$? Well,

$$\begin{array}{llll}
2 \cdot 1 \equiv 2 \pmod{12} & 2 \cdot 2 \equiv 4 \pmod{12} & 2 \cdot 3 \equiv 6 \pmod{12} & 2 \cdot 4 \equiv 8 \pmod{12} \\
2 \cdot 5 \equiv 10 \pmod{12} & 2 \cdot 6 \equiv 0 \pmod{12} & 2 \cdot 7 = 14 \equiv 2 \pmod{12} & 2 \cdot 8 = 16 \equiv 4 \pmod{12} \\
2 \cdot 9 = 18 \equiv 6 \pmod{12} & 2 \cdot 10 = 20 \equiv 8 \pmod{12} & 2 \cdot 11 = 22 \equiv 10 \pmod{12} & 2 \cdot 12 \equiv 2 \cdot 0 \equiv 0 \pmod{12}
\end{array}$$

So, it appears that 2 does **not** have a multiplicative inverse modulo 12. Take note as well that the products actually repeated... think about why this is happening!

We'll break here for the first problem set. This set is meant to help build your intuition in working with integers modulo n.