\( \mathbb{N} = \{0, 1, 2, \ldots\} \)
\( \mathbb{Z} = \{0, \pm 1, \pm 2, \ldots\} \)
\( \mathbb{Q} = \{ \frac{a}{b} : a, b \in \mathbb{Z}, b \neq 0 \} \).

Similarly \( \mathbb{R} \) and \( \mathbb{C} \) are the sets of real and complex numbers respectively. This course is largely about arithmetic in \( \mathbb{Z} \) and some related algebras. We can add subtract and multiply in \( \mathbb{Z} \) but we cannot divide there. For example, we cannot solve \( 2x = 1 \) in \( \mathbb{Z} \). Some kind of division is possible, for example non-zero cancellation: \( 2x = 4y \) implies that \( x = 2y \).

**Definition:** We say that \( a \mid b \) in \( \mathbb{Z} \) if there exists \( x \in \mathbb{Z} \) such that \( b = ax \). Note that \( a \mid b \) is not the same as \( a/b \).

**Clock arithmetic.**

\( \mathbb{Z}_7 = \{0, 1, 2, 3, 4, 5, 6\} \) Addition (and then multiplication) are defined as in ordinary arithmetic except that we remove multiples of 7 until we get back to the set \( \mathbb{Z}_7 \). So \( 3 + 6 = 8 = 8 - 7 = 1 \) and \( 3.6 = 18 = 18 - 2.7 = 4 \) and \( 3^4 = 81 = 81 - 11.7 = 4 \). We have that if \( x \) is any element of \( \mathbb{Z}_7 \), then \( -x \) is the unique element such that \( x + (-x) = 0 \). Hence we have \( -3 = 4 \) because \( 3 + 4 = 0 \) and in general

\[
\begin{array}{ccccccc}
 x & 0 & 1 & 2 & 3 & 4 & 5 \\
-x & 0 & 6 & 5 & 4 & 3 & 2 & 1
\end{array}
\]

Multiplicative inverses are a bit more difficult. Whatever \( \frac{1}{2} \) is, call it \( x \) it has the property that \( 2x = 1 \in \mathbb{Z}_7 \). Hence \( \frac{1}{2} = 4 \).

We have

\[
\begin{array}{ccccccc}
 x & 0 & 1 & 2 & 3 & 4 & 5 & 6 \\
 x^{-1} & * & 1 & 4 & 5 & 2 & 3 & 6
\end{array}
\]

There is a more complicated notation \( \equiv \pmod{n} \) for modular arithmetic but I don’t want us to be bothered by that here. We’ll use equality and remember that we are dealing with mod 7 or 12 or 911, for example, when that’s the situation.

**Problem:** Evaluate \( 2 \frac{3}{4} - 1 \frac{3}{5} \in \mathbb{Z}_7 \).

This is shorthand for

\[
2 + 3 \times \frac{1}{4} - 1 - 3 \times \frac{1}{5} = 2 + 3.2 - 1 - 3.3 = -2 = 5.
\]

It is also possible to calculate this as follows
\[
\frac{3}{4} - 1\frac{3}{5} = \frac{11}{4} - \frac{8}{5} = \frac{55 - 32}{20} = \frac{23}{20} = \frac{2}{6} = \frac{1}{3} = 5.
\]

That this is the same answer as before is no accident, but we won’t go into showing why that is here.

We then did similar calculations in \(Z_{11}\) and \(Z_{12}\). Only division is at all difficult. In \(Z_{11}\) we find

\[
\begin{array}{cccccccccccc}
    x & 0 & 1 & 2 & 3 & 4 & 5 & 6 & 7 & 8 & 9 & 10 \\
    x^{-1} & * & 1 & 6 & 4 & 3 & 9 & 2 & 8 & 7 & 5 & 10 \\
\end{array}
\]

It turns out that there are only four units in \(Z_{12}\), namely \(\{1, 5, 7, 11\}\).

The algebras \(Z\) and \(Z_n\) are examples of rings. We won’t define that concept more precisely here. We say that and element \(x\) is a unit in a ring \(R\) if there exists \(y \in R\) such that \(xy = 1\). We write the set of all units in \(R\) as \(R^*\). So we have

\[
Z_7^* = \{1, 2, 3, 4, 5, 6\}
\]
\[
Z_{11}^* = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}
\]
\[
Z_{12}^* = \{1, 5, 7, 11\}
\]
\[
Z^* = \{1, -1\}.
\]

Students should make sure that they can do modular arithmetic using their calculators.

Now we take a prime, say 911 and the last three digits of someone’s telephone number - in this case 671 and ask: What is \(671^{-1} \in Z_{911}\)? (if it exists)?