We fix a positive integer \( n \) for the duration of this short note.

## 1 Euclidean division

We first recall the Euclidean division by \( n \):

Let \( n \in \mathbb{N} \). For every \( a \in \mathbb{Z} \) there are unique \( q \in \mathbb{Z} \) and \( r \in \{0, \ldots, n-1\} \) such that

\[
a = qn + r.
\]

\( q \) is called the quotient and \( r \) the remainder (in the division of \( a \) by \( n \)).

We denote by \( \bar{a} \) the remainder of \( a \) in the division by \( n \), i.e. the element \( r \in \{0, \ldots, n-1\} \) such that \( a = qn + r \) for some \( q \in \mathbb{Z} \).

- We say that \( a \) and \( b \) are equal modulo \( n \) (some people say that \( a \) is congruent to \( b \) modulo \( n \)), and write \( a \equiv b \pmod{n} \) if there is \( k \in \mathbb{Z} \) such that \( a = b + kn \).

  In other words, \( a \equiv b \pmod{n} \) if \( a \) and \( b \) differ by a multiple of \( n \).

- It follows easily that \( a \equiv b \pmod{n} \) if and only if \( a \) and \( b \) have the same remainder in the division by \( n \).

  In other words \( a \equiv b \pmod{n} \) if and only if \( \bar{a} = \bar{b} \).

## 2 The set \( \mathbb{Z}/n\mathbb{Z} \)

The set \( \mathbb{Z}/n\mathbb{Z} \) is the set of all possible remainders in the division by \( n \), so:

\[
\mathbb{Z}/n\mathbb{Z} = \{0, 1, \ldots, n-1\}.
\]

It can be equipped with two operations, a sum and a product, defined as follows:

\[
x + y = \overline{x+y};
x \cdot y = \overline{x \cdot y}.
\]

1This is not a great notation since \( \bar{\cdot} \) does not indicate the dependence on \( n \), but it does not matter here since \( n \) is fixed.
In other words: you do the usual computation in $\mathbb{Z}$, then take the remainder.

We recall part of Theorem 1.9, Chapter 3 from MATH10040, Numbers and Functions (the proof is not hard at all):

**Theorem 2.1.** Let $a, b, a', b' \in \mathbb{Z}$. Then

1. $\overline{a + b} = \overline{a} + \overline{b}$ and $\overline{ab} = \overline{a}\overline{b}$ in $\mathbb{Z}/n\mathbb{Z}$.

2. If $\overline{a} = \overline{a'}$ and $\overline{b} = \overline{b'}$ then $\overline{ab} = \overline{a'b'}$.

It follows from the first part of this result that if you have to compute a complicated expression involving sums and products in $\mathbb{Z}/n\mathbb{Z}$, you can replace any part of it by its remainder modulo $n$, and you will get the same final result.

**Example 2.2.** For instance, in $\mathbb{Z}/5\mathbb{Z}$:

$$2 \cdot 4 \cdot 3 + 4 = \overline{8} \cdot \overline{3} + 4 = \overline{9} + 4 = 4 + 4 = \overline{8} = 3,$$

but also

$$2 \cdot 4 \cdot 3 + 4 = \overline{24} + 4 = 4 + 4 = 3,$$

and also

$$2 \cdot 4 \cdot 3 + 4 = \overline{28} = 3.$$

It can also be checked rather easily that properties (1) to (6) in our definition of field are true for $\mathbb{Z}/n\mathbb{Z}$. Such objects, with properties (1) to (6), are called (commutative) rings. You will see more about them in the second semester, in the course Groups, Rings and Fields. The terminology ring comes from the fact that they are modelled after $\mathbb{Z}/n\mathbb{Z}$, and that the sum makes $\mathbb{Z}/n\mathbb{Z}$ look a bit like a ring:
The only property of fields that \( \mathbb{Z}/n\mathbb{Z} \) may not have is property (7): that every non-zero element has an inverse.

**Example 2.3.** Consider \( \mathbb{Z}/6\mathbb{Z} \). In it we have \( 2 \cdot 3 = \bar{6} = 0 \). If every non-zero element had an inverse, \( 2 \) would have an inverse in \( \mathbb{Z}/3\mathbb{Z} \) and we would have \( 2^{-1} \cdot 2 \cdot 3 = 2^{-1} \cdot 0 \), so \( 3 = 0 \) in \( \mathbb{Z}/3\mathbb{Z} \), which is false.

### 3 When is \( \mathbb{Z}/n\mathbb{Z} \) a field?

Observe that the example above with \( \mathbb{Z}/6\mathbb{Z} \) works because 6 can be written as the product of two integers greater than one. You could in the same way show that if \( n = a \cdot b \) with \( a, b \in \mathbb{N}, a, b > 1 \), then \( \mathbb{Z}/n\mathbb{Z} \) is not a field.

It turns out that this is the only thing preventing \( \mathbb{Z}/n\mathbb{Z} \) to be a field:

**Theorem 3.1.** \( \mathbb{Z}/n\mathbb{Z} \) is a field if and only if \( n \) is a prime number.

To prove it, we need the following result (which we admit, the proof is not very complicated, but is not “on topic” for this course).

**Theorem 3.2** (Bézout’s identity). Let \( a, b \in \mathbb{Z} \) and let \( d = \gcd(a, b) \). Then there are \( u, v \in \mathbb{Z} \) such that \( d = ua + vb \).

**Proof of theorem 3.1.** “⇒” Assume that \( n = ab \) with \( a, b \in \mathbb{N}, a, b > 1 \). Then, using that every non-zero element has an inverse in \( \mathbb{Z}/n\mathbb{Z} \), we obtain a contradiction as in the example above with \( \mathbb{Z}/6\mathbb{Z} \).

“⇐” Let \( a \in \mathbb{Z}/n\mathbb{Z}, a \neq 0 \) in \( \mathbb{Z}/n\mathbb{Z} \), so \( a \in \{1, \ldots, n-1\} \). Since \( n \) is prime, it follows that \( \gcd(a, n) = 1 \), and by Bézout’s theorem there are \( u, v \in \mathbb{Z} \) such that \( ua + vb = 1 \). We compute the remainder in the division by \( n \) on both sides, i.e. we apply the map \( \bar{\cdot} \):

\[
\bar{ua + vn} = \bar{1}
\]

then using theorem 2.1

\[
\bar{u}a + \bar{v}n = 1
\]

\[
\bar{u} \cdot a + \bar{v} \cdot 0 = 1
\]

\[
\bar{u} \cdot a = 1,
\]

which shows that \( \bar{u} \) is the inverse of \( a \) in \( \mathbb{Z}/n\mathbb{Z} \). 

\( \Box \)