Worksheet #1 : \( \mathbb{Z}/n\mathbb{Z} \) – The integers mod \( n \)

In the first lecture we saw that a code \( C \) over an alphabet \( A \) is just a subset of \( A^n \) for some fixed \( n \geq 1 \). If we require that the code satisfy some additional requirements then it becomes possible to apply algebraic tools in the study of codes. Many interesting families of codes have been discovered in this way. The first requirement along these lines is that the alphabet \( A \) should be a field. The aim of this worksheet is to review the construction and properties of the ring \( \mathbb{Z}/n\mathbb{Z} \) and, in particular, the fact that it is a field when \( n \) is prime.

---

Fix an integer \( n \geq 1 \). If \( a, b \in \mathbb{Z} \) and \( n \) divides \( a - b \) then we write \( a \equiv b \) mod \( n \) (and say that “\( a \) is congruent to \( b \) mod(ulo) \( n \)”).

**Q1.** Check that \( \equiv \) mod \( n \) is an equivalence relation. That is, it satisfies the following three conditions.

(i) \( a \equiv a \) mod \( n \) \( \forall a \in \mathbb{Z} \).

(ii) \( a \equiv b \) mod \( n \) \( \iff \) \( b \equiv a \) mod \( n \) \( \forall a, b \in \mathbb{Z} \).

(iii) \( a \equiv b \) mod \( n \) and \( b \equiv c \) mod \( n \) \( \Rightarrow \) \( a \equiv c \) mod \( n \) \( \forall a, b, c \in \mathbb{Z} \).

Let \([a] = \{b \mid b \equiv a \mod n\}\). Then \([a]\) is called the equivalence class of \( a \) mod \( n \).

**Q2.**

(i) Show that \([0] = n\mathbb{Z} = \{an \mid a \in \mathbb{Z}\}\).

(ii) When does \([a] = [b]?)

(iii) Show that for all \( a \) and \( b \in \mathbb{Z} \), either \([a] = [b]\) or \([a] \cap [b] = \emptyset\).

(iv) Part (iii) above implies that the equivalence classes form a partition of \( \mathbb{Z} \). How many disjoint equivalence classes mod \( n \) are there? Describe them explicitly when \( n = 5 \).

**Q3.** Let \( \mathbb{Z}/n\mathbb{Z} = \{[a] \mid a \in \mathbb{Z}\}\). What is the size of \( \mathbb{Z}/n\mathbb{Z} \)? List the elements when \( n = 5 \).

\( \mathbb{Z} \) is not just a set, it has the algebraic structure of a commutative ring. (If you haven’t encountered “rings” before then your HW is to look this up. Try the library or online.

We define addition and multiplication operations on \( \mathbb{Z}/n\mathbb{Z} \) as follows:

\[
[a] + [b] = [a + b]
\]

\[
[a][b] = [ab].
\]

Since \([a] = [a']\) does not imply that \( a = a' \), it is not clear that these operations are well defined (i.e. the right-hand side in each of the definitions above would seem to depend on the choice of equivalence class representatives \( a \) and \( b \)).

**Q4.** Show that if \([a] = [a']\) and \([b] = [b']\) then \([a + b] = [a' + b']\) and \([ab] = [a'b']\). (It follows
that the operations above are well defined.

If you have not done so before then you should check that \( \mathbb{Z}/n\mathbb{Z} \) is also a commutative ring with respect to the operations above.

The element \([1] \in \mathbb{Z}/n\mathbb{Z}\) is a multiplicative identity element (or 1) for this ring. If \( R \) is any ring with a 1 then an element \( x \in R \) will be called a unit if there exists \( y \in R \) such that \( xy = yx = 1 \). Such an element \( y \) is called the inverse of \( x \).

Q5. Verify the following statements.

(i) If a ring \( R \) has a multiplicative identity then it is unique.

(ii) If \( x \in R \) is a unit, then the inverse \( y \) of \( x \) is uniquely determined.

(iii) The set \( U(R) \) consisting of all the units in \( R \) forms a group under multiplication.

(iv) The additive identity element \( 0 \in R \) is never a unit. (Except when \( R \) is the trivial ring containing only one element.)

Q6. Find \( U(\mathbb{Z}/n\mathbb{Z}) \) when \( n = 3, 4, 5, 6, 7 \).

Q7. Let \( a \in \mathbb{Z} \) and \( d = \text{gcd}(a, n) \), then there exist integers \( r \) and \( s \) such that \( d = ra + sn \).
(Recall or look up the proof of this result. It can be found in most introductory books on abstract algebra or number theory.)

(i) Pick \( a \) and \( n \) and then use the Euclidean algorithm to find \( r \) and \( s \) such that the above equation holds.

(ii) Show that if \( \text{gcd}(a, n) = 1 \) then \([a] \in \mathbb{Z}/n\mathbb{Z}\) is a unit.

(iii) Prove the converse of the statement in (ii).

Combining (ii) and (iii) we see that \( U(\mathbb{Z}/n\mathbb{Z}) = \{[a] \mid \text{gcd}(a, n) = 1\} \). In particular when \( n = p \) is prime then every nonzero element of \( \mathbb{Z}/p\mathbb{Z} \) is a unit. Thus \( \mathbb{Z}/p\mathbb{Z} \) is a field. We will often denote this field by \( \mathbb{F}_p \), and we will refer to it as the field with \( p \) elements. (Note: We can say “the” because one can prove that any other field with \( p \) elements must be isomorphic to it.)

In fact if \( p \) is prime and \( q = p^n \) with \( n \geq 1 \) then there exists a unique field \( \mathbb{F}_q \) with \( q \) elements. When \( n > 1 \) the construction is a little more complicated. (Warning: \( \mathbb{F}_q \) is not \( \mathbb{Z}/q\mathbb{Z} \) when \( n > 1 \) since the latter ring is not even a field!)

Q8. Show that if \( n \) is not prime then \( \mathbb{Z}/n\mathbb{Z} \) is not a field.