Lecture 31, Nov. 7

31.1 Definition (Representative)**.** For $x, a \in S$ with $\sim$m when $x \in [a]$, that is when $[x] = [a]$, we say that x is a representative of the equivalence class $[a]$.

31.2 Definition. Let $n \in \mathbb{Z}^+$. Define a relation on $\mathbb{Z}$ as follows. For $a, b \in \mathbb{Z}$, we define

$$\begin{aligned} a \sim b \Longleftrightarrow & n \mid (a-b) \\ \Longleftrightarrow & a - b = kn \text{ for some } k \in \mathbb{Z} \\ \Longleftrightarrow & a = b + kn \text{ for some } k \in \mathbb{Z} \end{aligned}$$

More commonly, we write

$$a = b \mod n$$

when $a \sim b$, and we say that a is equal (or equivalent or congruent) to b modulo n.

Note that this relation is an equivalence class because for $a, b, c \in \mathbb{Z}$,

1. $a \sim a$ since $a = a + 0 \cdot n$
2. if $a \sim b$, say $a = b + k \cdot n$ with $k \in \mathbb{Z}$, then $b = a + (-k) \cdot n$, so $b \sim a$
3. if $a \sim b$, and $b \sim c$, say $a = b + kn$ and $b = c + ln$ with $k, l \in \mathbb{Z}$, then $a = c + (l + k)n$, so $a \sim c$

31.3 Definition. We define the set of integers modulo n to be the quotient set

$$\mathbb{Z}_n = \mathbb{Z}/\sim = \{[a] \mid a \in \mathbb{Z}\}$$

where

$$\begin{aligned} [a] =& \{x \in \mathbb{Z} \mid x \sim a\} \\ =& \{x \in \mathbb{Z} \mid x = a \mod n\} \\ =& \{x \in \mathbb{Z} x = a + kn \text{ for some } k \in \mathbb{Z}\} \\ =& \{\cdots, a - 2n, a - n, a, a + n, a + 2n, \cdots\} \end{aligned}$$

Remark. Note that for $n \in \mathbb{Z}^+$ and for $a, b \in \mathbb{Z}$, we have $a = b \mod n$ if and only if a and b have the same remainder when divided by n. That is if $a = qn + r$ with $0 \leq r < n$ and $b = pn + s$ with $0 \leq s < n$, then $a = b \mod n \Longleftrightarrow r = s$

Proof. Suppose $a = qn + r$ with $0 \leq r < n$ and $b = pn + s$ with $0 \leq s < n$. Suppose that $a = b \mod n$, so that $n \mid (a - b)$. We have $a - b = (q - p)n + (r - s)$. Since $n \mid (a - b)$, we have $n \mid (r - s)$. If $r \neq s$ so $r - s \neq 0$ then since $n \mid (r - s)$ we have $n \leq |r - s|$. But since $0 \leq r < n$ and $0 \leq s < n$, we have $r - s < n - s \leq n - 0 = n$, and $s - r < n - r \leq n - 0 = n$, so $|r - s| < n$, giving a contradiction. Thus $r = s$.

Conversely Suppose that $r = s$, then $a - b = (q - p)n + (r - s) = (q - p)n$, so $n \mid (a - b)$, hence $a = b \mod n$. $\square$

Since the possible remainders r with $0 \leq r < n$ are $0, 1, 2, \cdots, n-1$, it follows that

$$\mathbb{Z}_n = \{[0], [1], \cdots, [n-1]\}$$

and the elements listed in the set are distinct (so that $\mathbb{Z}_n$ has exactly n elements).

Often, for $n \in \mathbb{Z}^+$ and $a \in \mathbb{Z}$ we shall write the element $[a]$ in $\mathbb{Z}_n$ simply as $a \in \mathbb{Z}_n$. So for $a, b \in \mathbb{Z}$ we have

$$\begin{aligned} & a = b \mod n \text{ in } \mathbb{Z} \\ \iff & a = b \text{ in } \mathbb{Z}_n \end{aligned}$$

31.4 Theorem. *For $n \in \mathbb{Z}$ with $n \geq 2$, $\mathbb{Z}_n$ is a ring using the following operations: for $a, b \in \mathbb{Z}$ we define*

$$[a] + [b] = [a + b]$$

and

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

The zero and identity elements in $\mathbb{Z}_n$ are $[0]$ and $[1]$.

Let us verify that the operations are well-defined.

Proof. We need to show that for $a, b, c, d \in \mathbb{Z}$, if $a = c \mod n$ and $b = d \mod n$, then $a + b = c + d \mod n$ and $ab = cd \mod n$.

Let $a, b, c, d \in \mathbb{Z}$, Suppose $a = c \mod n$ and $b = d \mod n$, say $a = c + kn$ and $b = d + ln$, then $a + b = (c + d) + (l + k)n$, so $a + b = c + d \mod n$, and $ab = cd + (cl + kd + kln)n$, so $ab = cd \mod n$. □

It is easy to check that the axioms are satisfied.

For example, for $a, b, c \in \mathbb{Z}$,

$$\begin{aligned} [a] + [0] =& [a + 0] \\ =& [a] \end{aligned}$$

$$\begin{aligned} [a][1] =& [a \cdot 1] \\ =& [a] \end{aligned}$$

$$\begin{aligned} [a]([b] + [c]) =& [a][(b + c)] \\ =& [a(b + c)] \\ =& [ab + ac] \\ =& [ab] + [ac] \\ =& [a][b] + [a][c] \end{aligned}$$

31.5 Theorem (Units Modulo n)**.** *For $a, n \in \mathbb{Z}$ with $n \geq 2$.*

$$[a] \text{ is invertible in } \mathbb{Z}_n \iff gcd(a,n) = 1 \text{ in } \mathbb{Z}$$

Proof. Suppose $[a]$ is a unit in $\mathbb{Z}_n$. Choose $s \in \mathbb{Z}$ so that $[a][s] = 1$. Then $[as] = 1$ and $as = 1 \mod n$. Say $as = 1 + kn$ with $k \in \mathbb{Z}$, then $as + nt = 1$ with $t = -k$. Thus $gcd(a, n) = 1$.

Conversely, suppose $gcd(a, b) = 1$. Use the Euclidean Algorithm with Back Substitution to find $s, t \in \mathbb{Z}$ such that $as + nt = 1$.Then $as = 1 - nt$. Thus $[as] = [1]$ in $\mathbb{Z}_n$, so $[a][s] = 1$. So $[a]$ is invertible with $[a]^{-1} = [s]$ in $\mathbb{Z}_n$. □

31.6 Example. Determine whether 125 is a unit in $\mathbb{Z}_{471}$ and, if so, find 125^{-1}.