INTEGERS MOD n

PETER MAYR (MATH 2135, CU BOULDER)

1. Divisibility

Definition. Let $n \in \mathbb{N}, a \in \mathbb{Z}$.

(1) Then $n|a$ (n **divides** a) if there exists $q \in \mathbb{Z}$ such that $a = qn$ (that is, a is a **multiple** of n).
(2) a, b are **congruent modulo** n (written $a \equiv b \mod n$ or $a \equiv_n b$) if $n|a - b$.

Lemma 1. *Let $a, b, c, d \in \mathbb{Z}$, $n \in \mathbb{N}$ with $a \equiv b \mod n$ and $c \equiv d \mod n$. Then*

(1) $a + c \equiv b + d \mod n$,
(2) $-a \equiv -b \mod n$,
(3) $a \cdot c \equiv b \cdot d \mod n$.

Proof. Exercise. $\square$

2. Integers modulo n

One particular important equivalence relation is $\equiv_n$ on $\mathbb{Z}$ for $n \in \mathbb{N}$. The class of $a \in \mathbb{Z}$ is the set of all integers that are congruent to a modulo n, that is,

$$[a] = \{a + zn \ : \ z \in \mathbb{Z}\}.$$

Note $[n] = [0]$ and $[-1] = [n-1]$. Moreover each integer a is in exactly one class modulo n, that is, the classes form a **partition** of $\mathbb{Z}$.

The set of classes

$$\mathbb{Z}_n := \{[0], [1], [2], \ldots, [n-1]\}$$

is called the **integers modulo** n.

Define $+, -, \cdot$ on $\mathbb{Z}_n$ by

$$\begin{aligned} [a] + [b] &:= [a + b] \\ -[a] &:= [-a] \\ [a] \cdot [b] &:= [a \cdot b] \end{aligned}$$

Date: September 9, 2019.

These operations are well-defined (independent of the choice of representatives for each class) by Lemma 1 and satisfy the same laws as $+, -, \cdot$ on $\mathbb{Z}$: associativity, commutativity, distributivity, etc.

3. Computing in $\mathbb{Z}_n$

By the above definitions one can add, multiply and subtract in $\mathbb{Z}_n$ just like in $\mathbb{Z}$. However results should be reduced modulo n and written in the form $[0], [1], \ldots, [n-1]$.

Example. In $\mathbb{Z}_5$:
$[3] + [4] = [7] = [2]$
$-[3] = [-3] = [2]$
$[3] \cdot [3] = [9] = [4]$

Dividing in $\mathbb{Z}_n$ means solving an equation $[a] \cdot [x] = [b]$ for $[x]$. For small numbers the solution can often be guessed.

Example. (1) In $\mathbb{Z}_3$ solve $[2] \cdot [x] = [1]$.
The solution could be $[x] = [0], [1]$ or $[2]$. Note
$[2] \cdot [0] = [0]$,
$[2] \cdot [1] = [2]$,
$[2] \cdot [2] = [1]$
Hence $[x] = [2]$.

(2) In $\mathbb{Z}_4$ solve $[2] \cdot [x] = [1]$. Trying all 4 options we see
$[2] \cdot [0] = [2] \cdot [2] = [0]$ $\quad$ $[2] \cdot [1] = [2] \cdot [3] = [2]$
Hence $[2] \cdot [x] = [1]$ has no solution in $\mathbb{Z}_4$.

In any case if a solution exists, it can be found by the Extended Euclidean Algorithm and Bezout coefficients:

Example. Solve $[8] \cdot [x] = [1]$ in $\mathbb{Z}_{37}$.
This amounts to solving $8x + 37y = 1$ for $x, y \in \mathbb{Z}$. The Euclidean algorithm yields $x = 14$. Hence $[8] \cdot [14] = [1]$ and $[x] = [14]$ solves the original equation.

Using the Extended Euclidean Algorithm one can show that in general:

Theorem 2. $(\mathbb{Z}_n, +, \cdot)$ *is a field iff* n *is prime.*