HW: Exercises 2.9.2, 2.9.4, 2.9.5, 2.9.8
Read §2.10 for Monday

Two goals:

1) Generalize the arithmetic of "evens and odds"
i.e. if we denote evens by $\bar{0}$ and odds by $\bar{1}$, we get the addition and multiplication tables:

$+$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{1}$
$\bar{1}$	$\bar{1}$	$\bar{0}$

$\times$	$\bar{0}$	$\bar{1}$
$\bar{0}$	$\bar{0}$	$\bar{0}$
$\bar{1}$	$\bar{0}$	$\bar{1}$

we'd like to generalize from 2 to n.

2) Make concrete what we did last time with cosets and equivalence relations

§ Congruence mod n and its arithmetic

Fix a positive integer n, and define an equivalence relation on $\mathbb{Z}$ by

$$a \sim b \Leftrightarrow n \mid (a-b) \Leftrightarrow (a-b) \in n\mathbb{Z}$$

This is clearly an equivalence relation:

- $a \sim a$
- $a \sim b \Rightarrow b \sim a$
- $a \sim b$ and $b \sim c \Rightarrow a \sim c$

We introduce the notation

$$a \equiv b \pmod{n}$$

a synonym for $a \sim b$ with n explicit, meaning "a congruent to b mod n"
For $a \in \mathbb{Z}$, write $\bar{a}$ to denote the equivalence class of n. Then

$$\bar{a} = a + n\mathbb{Z}$$
$$= \{a + bn \mid b \in \mathbb{Z}\}$$

In the language from last time $\bar{a}$ is a coset of $\mathbb{Z}$:

$$\begin{array}{ccc} H & \subset & G \\ \shortparallel & & \shortparallel \\ n\mathbb{Z} & & \mathbb{Z} \end{array} \rightarrow a + H = a + n\mathbb{Z}$$

ex: if $n = 12$, $2 \equiv 26 \pmod{12} \Rightarrow \bar{2} = \overline{26}$

<u>observation</u>: There are n distinct cosets of $n\mathbb{Z}$ (equivalence classes mod n):

$$\bar{0}, \bar{1}, \bar{2}, \ldots, \overline{n-1}$$

- why? By the division algorithm, $a \in \mathbb{Z} \Rightarrow a = nq + r$, where $\overset{q}{n}, r \in \mathbb{Z}$ and $0 \le r < n$. in other words, $\bar{a} = \bar{r}$.
- $\bar{a} = \bar{b}$ and $0 \le a, b \le n \Rightarrow |a-b| \le n-1$; $|b-a| \in n\mathbb{Z} \Rightarrow |a-b| = 0 \Rightarrow a = b$.

<u>notation</u>: for a set of equivalence classes we will use $\mathbb{Z}/n\mathbb{Z}$ (or $\mathbb{Z}/n$)

We now consider the map (reduction mod n):

$$\mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$
$$a \mapsto \bar{a}$$

We can do arithmetic in $\mathbb{Z}/n\mathbb{Z}$ by defining

$$\bar{a}+\bar{b} = \overline{a+b}$$
$$\bar{a}\cdot\bar{b} = \overline{a\cdot b}$$

Is this well-defined? Yes! It is easy to verify that

$$\bar{a}_1 = \bar{b}_1 \quad \bar{a}_2 = \bar{b}_2$$
$$\Rightarrow \overline{a_1+a_2} = \overline{b_1+b_2}$$
$$\Rightarrow \overline{a_1 a_2} = \overline{b_1 b_2}.$$

<u>observation</u>: $(\mathbb{Z}/n\mathbb{Z}, +)$ is a group

- associative, because $(\mathbb{Z},+)$ is associative:

$$(\bar{a}+\bar{b})+\bar{c} = \overline{a+b+c} = \bar{a}+(\bar{b}+\bar{c})$$

- identity $\bar{0}$
- inverses $-\bar{a} = \overline{n-a} = \overline{(-a)}$

In the language from before, then:

The set of cosets of $n\mathbb{Z} \subset \mathbb{Z}$ forms a group.

rmk: In fact this will be true whenever $H \subset G$ is normal.

<u>another observation</u>: $\mathbb{Z}/n\mathbb{Z} = \langle \bar{1} \rangle$ is a cyclic group of order n; since all cyclic groups of order n are isomorphic we see that a) there is always a cyclic group of order n, and b) all cyclic groups can be written in the form $\mathbb{Z}/n\mathbb{Z}$, for some n.

<u>notation</u>: When we use $+$ for our group operation, we write $n\cdot g$ for $\overbrace{g+\cdots+g}^{n \text{ times}}$, rather than g^n.

<u>further observation</u>: Addition and multiplication on $\mathbb{Z}/n\mathbb{Z}$ distribute:

$$\bar{a}(\bar{b}+\bar{c}) = \bar{a}\bar{b}+\bar{a}\bar{c}$$

This property is inherited from $\mathbb{Z}$.

Example of the usefulness of modular arithmetic:

Q: Compute the last two digits in 2^{1000}.

A: All we have to do is compute 2^{1000} mod 100:

$$2^{10} = 1024 \equiv 24 \pmod{100}$$
$$2^{200} = (2^{10})^2 = 24^2 = 576 \equiv 76 \pmod{100}$$
$$76^2 = 5776 \equiv 76 \pmod{100}$$
$$\Rightarrow 76^n \equiv 76 \pmod{100} \qquad \text{by induction}$$
$$\Rightarrow 2^{1000} \equiv 76 \pmod{100}$$

Remark: $(\mathbb{Z}/n\mathbb{Z}, \cdot)$ is <u>not</u> a group, for $\bar{0}$ cannot possibly have an inverse.

But we do have a subset of $\mathbb{Z}/n\mathbb{Z}$ that gives a group under multiplication; namely:

$$(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \exists\, \bar{c} \in \mathbb{Z}/n\mathbb{Z} \text{ s.t. } \bar{a}\cdot\bar{c} = \bar{1}\}$$

This satisfies the properties of a group

- Associativity inherited from $\mathbb{Z}$
- Identity $\bar{1}$
- Inverses by construction

To understand $(\mathbb{Z}/n\mathbb{Z})^\times$, we review gcd's:

if $m, n \in \mathbb{Z}$ (not both zero), then

$\gcd(m,n)$ = largest positive ~~number~~ integer dividing m and n

= unique positive integer d s.t. $d | m, n$, and if e is another integer dividing m and n, then $e | d$.

lemma: $m\mathbb{Z} + n\mathbb{Z} = \{mr + ns \mid r, s \in \mathbb{Z}\} = \gcd(m,n)\mathbb{Z}$

pf: $m\mathbb{Z} + n\mathbb{Z}$ is a subgroup of $\mathbb{Z}$, and so equals $d\mathbb{Z}$ for some (positive) integer d. Then $m \in m\mathbb{Z} + n\mathbb{Z} = d\mathbb{Z} \Rightarrow d | m$; similarly $d | n$. Furthermore if $e | m, n$, then since $mr + ns = d \in d\mathbb{Z}$, e must divide d. ☒

We now use this fact for the following

proposition: $(\mathbb{Z}/n\mathbb{Z})^\times = \{\bar{a} \in \mathbb{Z}/n\mathbb{Z} \mid \gcd(a,n) = 1\}$

pf: LHS $\supset$ RHS

if $\gcd(a,n) = 1$, then by the lemma $a\mathbb{Z} + n\mathbb{Z} = \mathbb{Z}$. Thus $\exists\, r, s \in \mathbb{Z}$ such that

$$\begin{aligned} &ar + ns = 1 \\ &\Rightarrow ar - 1 \in n\mathbb{Z} \\ &\Rightarrow \bar{a} \cdot \bar{r} = \bar{1} \\ &\Rightarrow \bar{a} \in (\mathbb{Z}/n\mathbb{Z})^\times. \end{aligned}$$

RHS $\supset$ LHS:

$$\begin{aligned} \bar{a} \cdot \bar{c} = \bar{1} &\Rightarrow ac - 1 = nb \\ &\Rightarrow 1 = ac - nb \in a\mathbb{Z} + n\mathbb{Z} = \gcd(a,n)\mathbb{Z} \end{aligned}$$ ☒

example: $(\mathbb{Z}/p\mathbb{Z})^\times = \{\bar{1}, \bar{2}, \ldots, \overline{p-1}\}$

another example: more generally $|(\mathbb{Z}/p^e\mathbb{Z})^\times| = p^e - p^{e-1}$, as the only things not relatively prime to p are $1 \cdot p, 2 \cdot p, 3 \cdot p, \ldots, p^{e-1} \cdot p$.

Next time we will look at the set of cosets of $H \subset G$, denoted G/H, when H is a normal subgroup of G. We'll see that there is a natural homomorphism

$$f: G \to G/H$$

with full image, whose kernel equals H.

Today we verified this fact in the case of $\mathbb{Z}$ by the map

$$\text{red}: \mathbb{Z} \to \mathbb{Z}/n\mathbb{Z}$$

We showed that this map is a surjective homomorphism with kernel $n\mathbb{Z} \trianglelefteq \mathbb{Z}$