Recap Math 351 Feb 14-19

- The integers can be grouped into mod-n equivalence classes, if $n \in \mathbb{Z}^+$.
- The standard representative of an equivalence class is an integer between 0 and n-1 (inclusive)
- If you add elements of two equivalence classes (mod n), then the sums are always in the same equivalence class, so adding equivalence classes makes sense. We say addition of equivalence classes is well defined.
- The same is true for multiplication, so we also accept multiplication of equivalence classes.
- There are several ways to write an equivalence class mod n: $[a]_n$, $[a]$, a (where a is an integer)
- The set whose elements are equivalence classes mod n is called $\mathbb{Z}_n$.

Examples: If $n = 6$, then

$[2]_6 = \{2, 8, 14, \dots, -4, -10, \dots\} = \{2+6k \mid k \in \mathbb{Z}\} = [8]_6 = [-4]_6 = [2] = 2$

↑ standard name; ↑ all the integers in the equivalence class; less simplified; lazy; ↑ other acceptable names for the equiv. class

$[5]_6 = \{5, 11, 17, \dots, -1, -7, \dots\} = \{5+6k \mid k \in \mathbb{Z}\} = [11]_6 = [-1]_6 = [5] = 5$

$[2]_6 + [5]_6 = \{2+5, 2+11, \dots 8+5, 8+11, \dots\} = \{2+6k+5+6j \mid j,k \in \mathbb{Z}\} = [2+5]_6 = [8+11]_6 = \dots$

$[2]_6 \cdot [5]_6 = \{2 \cdot 5, 2 \cdot 11, \dots, 8 \cdot 5, 8 \cdot 11, \dots\} = \{(2+6k)(5+6j) \mid j,k \in \mathbb{Z}\}$

$= [2 \cdot 5]_6 = [8 \cdot 11]_6 = [10]_6 = [4]_6$

$[7]_6 = [1]_6$

Equations mod-n can (should?) be solved by testing each element in $\mathbb{Z}_n$. Sometimes there are more solutions than you expect:

Example $2 \cdot x = 6 \pmod 8$ $\quad \mathbb{Z}_8 = \{0, 1, 2, 3, 4, 5, 6, 7\}$

$2 \cdot 0 = 0$
$2 \cdot 1 = 2$
$2 \cdot 2 = 4$
$2 \cdot 3 = 6$ ← solution!
$2 \cdot 4 = 8 = 0$
$2 \cdot 5 = 10 = 2$
$2 \cdot 6 = 12 = 4$
$2 \cdot 7 = 14 = 6$ ← another solution?!

$x = 3, 7$

A note on notation.
If I were being careful I would write:
$[2]_8 \cdot [7]_8 = [14]_8 = [6]_8$

or

$2 \cdot 7 \equiv 14 \equiv 6 \pmod 8$

I am almost never careful I am typical in my not-careful-ness

You can find inverses in the same way:

The additive inverse of $3 \in \mathbb{Z}_8$ is x s.t.

$3 + x = 0$
$\rightarrow x = 5$

think $x = -3 \equiv 5 \pmod 8$
or
$3 + x = 8 \rightarrow x = 5$

or try $3+0$, $3+1$, $3+2$, etc.

the additive inverse of $[3]_8$ is $[5]_8$

Note: every element of $\mathbb{Z}_n$ has a unique additive inverse

The multiplicative inverse of $3 \in \mathbb{Z}_8$ is x s.t. $3x = 1$

try: $3 \cdot 0 = 0$ $\quad 3 \cdot 1 = 3$ $\quad 3 \cdot 2 = 6$ $\quad 3 \cdot 3 = 9 = 1$ ✱

(also: $3 \cdot 4 = 12 = 4$, $3 \cdot 5 = 15 = 7$, $3 \cdot 6 = 18 = 2$, $3 \cdot 7 = 21 = 5$)

The multiplicative inverse of $[3]_8$ is $[3]_8$.

More about multiplicative inverses:

The multiplicative inverse of $6 \in \mathbb{Z}_8$ is x s.t.

$6x = 1$

try: $6 \cdot 0 = 0$, $6 \cdot 1 = 6$, $6 \cdot 2 = 12 = 4$, $6 \cdot 4 = 24 = 0$, $6 \cdot 5 = 30 = 6$

$6 \cdot 6 = 36 = 4$, $6 \cdot 7 = 42 = 2$.

$[6]_8$ does not have a multiplicative inverse.

Theorem 19 (proved in class)

If $\gcd(a, n) = 1$ then $[a]_n$ has a multiplicative inverse

If $\gcd(a, n) = d > 1$ then $[a]_n$ does not have a multiplicative inverse

---

Example: $\gcd(3, 8) = 1$

$[3]_8$ has a multiplicative inverse

$\gcd(6, 8) = 2$

$[6]_8$ does not have a multiplicative inverse

If a number u has a multiplicative inverse, it is called a unit

List all the units in $\mathbb{Z}_{14}$: ~~0~~, 1, ~~2~~, 3, ~~4~~, 5, ~~6~~, ~~7~~, ~~8~~, 9, ~~10~~, 11, ~~12~~, 13

never a unit

$\gcd(2, 14) = 2$, $\gcd(4, 14) = 2$, $\gcd(6, 14) = 2$, $\gcd(7, 14) = 7$

$\gcd(8, 14) = 2$, $\gcd(10, 14) = 2$, $\gcd(12, 14) = 2$

U_n is the set of all units in $\mathbb{Z}_n$:

$U_{14} = \{1, 3, 5, 9, 11, 13\}$

Notice: $U_5 = \{1, 2, 3, 4\}$. When n is prime, U_n is the non-zero elements of $\mathbb{Z}_n$