PLP - 30

TOPIC 30—INTEGERS MODULO n

Demirbaş & Rechnitzer

INTEGERS MODULO n

PARTITION AND EQUIVALENCE CLASSES

- The equivalence relation "$\equiv \pmod{n}$" gives a partition of $\mathbb{Z}$:

$$\{[0], [1], [2], \ldots, [n-1]\}$$

- These equivalence classes are called the **integers mod n**
- They have nice arithmetic properties

THEOREM:

Let $n \in \mathbb{N}$ and let $a, b \in \{0, 1, \ldots, n-1\}$.

If $x \in [a]$ and $y \in [b]$ then

$$x + y \in [a+b] \qquad \text{and} \qquad x \cdot y \in [a \cdot b]$$

ARITHMETIC MODULO n

$$(x \in [a]) \wedge (y \in [b]) \implies (x + y \in [a + b]) \wedge (x \cdot y \in [a \cdot b])$$

Scratch work

- Since $x \in [a], y \in [b]$ we know that $n \mid (x - a)$ and $n \mid (y - b)$, so

$$x = a + nk \qquad \text{and} \qquad y = b + n\ell$$

- This means that

$$x + y = a + b + n(k + \ell) \qquad xy = ab + n(bk + a\ell) + n^2 k\ell$$

- Which gives

$$n \mid ((x + y) - (a + b)) \qquad \text{and} \qquad n \mid (x \cdot y - a \cdot b)$$

PROOF

PROOF.

Let n, a, b, x, y be as stated. Then since $x \in [a]$ and $y \in [b]$, we know that

$$x = a + nk \qquad \text{and} \qquad y = b + n\ell \qquad \text{for some } k, \ell \in \mathbb{Z}$$

From this we have

$$x + y = a + b + n(k + \ell) \qquad xy = ab + n(bk + a\ell) + n^2 k\ell$$

and so

$$n \mid ((x + y) - (a + b)) \qquad \text{and} \qquad n \mid (x \cdot y - a \cdot b)$$

This shows that $x + y \in [a + b]$ and $x \cdot y \in [a \cdot b]$ as required.

MODULAR ARITHMETIC

DEFINITION:

Let $n \in \mathbb{N}$ and consider the equivalence classes of congruence modulo n.

The **integers modulo n** is the set

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

The elements of $\mathbb{Z}_n$ can be added and multiplied by the rule

$$[a] + [b] = [a+b] \qquad [a] \cdot [b] = [a \cdot b]$$

Quiz

① $[2]_7$ and $[5]_7$

bcus

$$[a]_n + [b]_n = [0]_n$$

$$[a+b]_n = [0]_n$$

so, $[2+5]_7 = [0]_7$

$$[7]_7 = [0]_7$$

b

② $[a]_n [b]_n = [1]_n$

$$[a \cdot b]_n = [1]_n$$

so, $[6 \cdot 6]_7 = [1]_7$

$$[36]_7 = [1]_7$$

c

And

$$[4 \cdot 4]_5 = [1]_5$$

$$[16]_5 = [1]_5$$

d