Discrete Math

Lecture 30

The Division "Algorithm" (& Friends)

- Tells about dividing (no fractions)
- not an algorithm

The Division "Algthm"

$$\forall\, a, b \in \mathbb{Z},\ b \neq 0,\ \exists!\ q, r \in \mathbb{Z}$$

$$a = q \cdot b + r$$

where $0 \leq r < |b|$

ex) $a = 55 \quad b = 4$

$$55 = \underline{q} \cdot 4 + \underline{r}$$

$$= \underline{13} \cdot 4 + \underline{3}$$

note: $0 \leq 3 < 4$ ✓

(note: $55 = \underline{14} \cdot 4 + \underline{(-1)}$

but $r = -1 < 0$ so this doesn't count!)

ex | $a = 24 \quad b = 8$

$24 = q \cdot 8 + r$

$24 = \underline{3} \cdot 8 + \underline{0}$

$r = 0 \iff b \mid a \iff a = m \cdot b$

ex | $a = 8, \quad b = 24$

$8 = q \cdot 24 + r$

$q = 0, \quad r = 8$

$8 = 0 \cdot 24 + 8$ ✓

An interesting / important consequence of the Division "Algorithm":

we always have exactly $|b| - 1$ possible remainders!

ex| $a = 15$ $b = 7$

$15 = q \cdot 7 + r$

$q = 2$, $\boxed{r = 1}$

$a = 21$, $b = 7$

$21 = q \cdot 7 + r$

$q = 3$, $\boxed{r = 0}$

When dividing by 7, which remainders are possible?

$0 \leq r < 7$

$|b| - 1$

$r \in \{0, 1, 2, 3, 4, 5, 6\}$

ex| what are the possible remainders when we divide by 3?

↳ If $a \in \mathbb{Z}$, and its remainder (when divided by 3) is not 0 and not 2, then what can we say?

possible remainders are: $\{0, 1, 2\}$

so a has a remainder of 1 (when divided by 3)

$a, b = 3$

$$a = q \cdot 3 + 1$$

$$a = \text{a mult. of } 3 + 1$$

The Division "Algorithm"

The Well-Ordering Principle is used on a set $\{a - q \cdot b \geq 0 : q \in \mathbb{Z}\}$