LECTURE 2

(Monday SEP. 30, 2019)

Numbers.

Set of all integers (possibly negative):

$$\mathbb{Z} = \{0, \pm 1, \pm 2, \pm 3, \ldots\}.$$

"zahlen"

has addition & multiplication.

Note: $\mathbb{Z}$ with $+$ is a group — check axioms:

- $(a+b)+c = a+(b+c)$
- $a+0 = a = 0+a$
- $a+(-a) = 0 = (-a)+a$

... inherited from $\mathbb{R}$. "subgroup".

However, $\mathbb{Z}$ with $\bullet$ is not a group. Even $\mathbb{Z} \setminus \{0\}$ is still not a group:

$$\frac{1}{a} \text{ is not in } \mathbb{Z} \text{ unless } a = \pm 1.$$

Recall:

Definition. Let $a, b \in \mathbb{Z}$. We say a divides b (or that b is divisible by a) if there's a $q \in \mathbb{Z}$ such that

$$\boxed{b = qa}$$

Notation: When this happens we write $a \mid b$.

Ex: For any $a \in \mathbb{Z}$, $\quad 1 \mid a$ and $a \mid a$.

$$(a = \underset{q}{\underbrace{a}} \cdot 1) \qquad (a = \underset{q}{\underbrace{1}} \cdot a)$$

– we say $a > 1$ is a <u>prime number</u> if $\{1, a\}$ are the only <u>positive</u> divisors.

note that $(-1) \mid a$ since $a = \overset{q}{\overbrace{(-a)}}(-1)$.

$2, 3, 5, 7, 11, 13, \ldots$ (∞ many)

<u>"transitive"</u>

Exc: $(a, b, c \in \mathbb{Z})$ $\quad a \mid b$ and $b \mid c \implies a \mid c$.

(sketch: $b = q_1 a$ and $c = q_2 b$

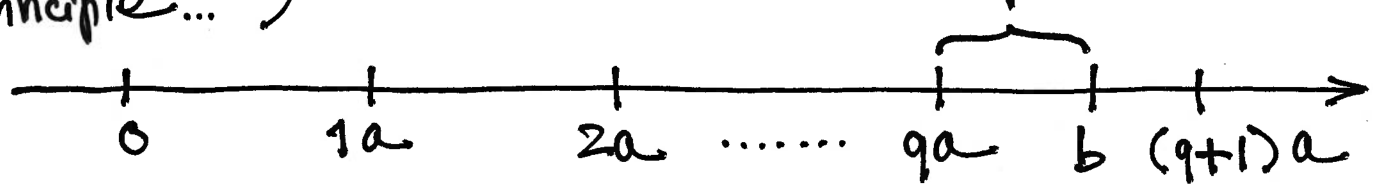
$\implies c = q_2(q_1 a) = \underbrace{(q_2 q_1)}_{\in \mathbb{Z}} a$)

<u>Theorem</u> ("Division with remainder")

Given any two $a, b \in \mathbb{Z}$ with a <u>positive</u>, there are uniquely determined $q, r \in \mathbb{Z}$ satisfying the following two conditions simultaneously:

$$\begin{cases} (1) \; b = qa + r \quad \underline{\text{and}} \\ (2) \; 0 \leq r < a. \end{cases}$$

(well-ordering principle...)



EX ($a=10$, $b=2019$) $\quad 2019 = \underset{q}{201}\cdot 10 + \underset{r}{9}$

— Compare:

$2019 = 200\cdot 10 + 19$ — too big

$\quad = 202\cdot 10 + (-1)$ — too small.

Observe: $d\mid a$ and $d\mid b \iff d\mid a$ and $d\mid r$
($d\in\mathbb{Z}$)

— Can use this to find the "greatest common divisor" $GCD(a,b)$.

Euclid's Algorithm.

EX Find $GCD(\underset{a}{221}, \underset{b}{323})$.

$$\begin{cases} 323 = 1\cdot 221 + 102 \\ 221 = 2\cdot 102 + \boxed{17} \\ 102 = 6\cdot 17 + 0. \end{cases}$$

Shows $GCD(\,,\,) = 17$.

Back-substitution allows us to express $GCD(a,b)$ as a linear combination $ax+by$ for suitable $x,y\in\mathbb{Z}$:

$$17 = 221 + (-2)\cdot 102 = 221 + (-2)(323-221)$$
$$= (-2)\cdot 323 + 3\cdot 221 \qquad \boxed{x=3,\ y=-2}.$$

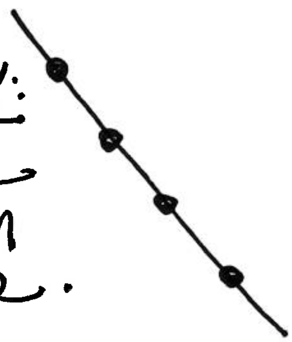
Warning: there are ∞ many solutions (x,y)

Why? $GCD(a,b) = ax + by$

$$= a\underbrace{(x+tb)}_{} + b\underbrace{(y-ta)}_{}$$

another solution ($t \in \mathbb{Z}$ varies)

GEOMETRY: ~ lattice points on a line.



[**Def.** We say $a, b \in \mathbb{Z}$ are coprime when $GCD(a,b) = 1$.

(i.e., no common factor > 1)

$\longrightarrow$ in this case: $1 = ax + by$ for suitable coefficients $x, y \in \mathbb{Z}$.

Application: p = prime number.

Suppose $p \mid ab$. Then: $p \mid a$ or $p \mid b$.

(possibly p divides both)

Why? Assume $p \nmid a$, show $p \mid b$.

$GCD(a,p) = 1 = ax + py$.

(divides p so is 1 or p)

Multiply by b on both sides:

$$b = \underbrace{(ab)x}_{} + \underbrace{p(by)}_{}$$

— both terms are p-multiples.

Ex. This fails if p not prime: $6 \mid 2 \cdot 3$, but $6 \nmid 2$ and $6 \nmid 3$.

"<u>least</u> <u>common</u> <u>multiple</u>":

$$\mathrm{LCM}(a,b) = \frac{ab}{\mathrm{GCD}(a,b)}.$$

<u>EX</u>: $\mathrm{LCM}(221, 323) =$

$$\frac{221 \cdot 323}{17} = 13 \cdot 323 = \boxed{4199}.$$

- Recall: Can read off GCD and LCM from <u>prime</u> <u>factorizations</u> of a, b.

<u>EX</u>. $a = p^5 q^7$ and $b = p^8 q^3$

($p \neq q$ primes)

Then:

$$\mathrm{GCD}(a,b) = p^{\min(5,8)} q^{\min(7,3)} = p^5 q^3$$

$$\mathrm{LCM}(a,b) = p^{\max(\ )} q^{\max(\ )} = p^8 q^7.$$