Group Theory

3rd class

① GCD's

Recall: Given integers a, b (not both 0) we say a positive integer d is a gcd for a & b if:

(1) $d \mid a$ & $d \mid b$

(2) $(c \mid a$ & $c \mid b) \Rightarrow c \mid d$

We showed: if d exists, then it must be unique, and we write it as

$$d = \gcd(a,b) = (a,b)$$

Thm (Euclid) Such a gcd always exists!

i.e., given any a, b as above, $\exists$ d satisfying (1) & (2)

Proof If $a > 0$ & $b = 0$ then $\rightarrow d = a$
or $a = 0$ & $b > 0$ $\longrightarrow d = b$

Also $\gcd(\pm a, \pm b) = \gcd(|a|, |b|)$

Hence, We may assume $a > b > 0$

Use long division:

$$a = b \cdot q_1 + r_1 \qquad 0 \le r_1 < b$$

$$b = r_1 \cdot q_2 + r_2 \qquad 0 \le r_2 < r_1$$

$$r_1 = r_2 \cdot q_3 + r_3 \qquad 0 \le r_3 < r_2$$

$$\vdots$$

$$r_{n-1} = r_n \cdot q_{n+1} + 0$$

$$\therefore \quad \gcd(a,b) = \gcd(b, r_1) = \gcd(r_1, r_2) = \cdots$$
$$= \gcd(r_{n-1}, r_n) = r_n \qquad \boxtimes$$

Ex $a = 126$, $b = 35$

$$126 = 35 \cdot 3 + 21$$
$$35 = 21 \cdot 1 + 14$$
$$21 = 14 \cdot 1 + 7$$
$$14 = 7 \cdot 2 + 0$$

$$\gcd(126, 35) = 7$$

Linear combinations

Given $a, b \in \mathbb{Z}$, we can form a linear combination

$$ma + nb, \quad \text{for some } m, n \in \mathbb{Z}$$

eg $a = 3$, $b = 5$ $\longrightarrow$ $2 \cdot 3 + 6 \cdot 5 = 36$
$\longrightarrow$ $2 \cdot 3 + (-1) \cdot 5 = 6 - 5 = 1$

Theorem If $d = \gcd(a,b)$, then $d = ma + nb$ for some $m, n \in \mathbb{Z}$.

Moreover, every linear comb. of a & b is a multiple of $d = \gcd(a,b)$, and so d is the smallest such linear combination.

Proof (sketch) Let $I = \{x \in \mathbb{Z} : x = ma + nb \text{ for some } m, n \in \mathbb{Z}\}$

- $I \neq \emptyset$: $a = 1 \cdot a + 0 \cdot b \in I$

- closed under addition & subtraction:

$$(ma+nb) \pm (pa+qb) = (m \pm p)a + (n \pm q)b \checkmark$$

Look now at $I \cap \mathbb{Z}_{>0}$

This set must have a ~~smallest element~~, call it d.

It turns out that $d = \gcd(a,b)$ | exercise!

Hence, $\underset{\substack{\in \\ I \cap \mathbb{Z}_{>0}}}{\gcd(a,b)} = ma+nb$ for some $m,n \in \mathbb{Z}$ $\blacksquare$

Ex $a=2$, $b=5$ $\quad \gcd(a,b) = 1 = 1\cdot 5 - 2\cdot 2$
$= 3\cdot 2 - 1\cdot 5$

In general, finding $d = \gcd(a,b) = ma+nb$ can be done via a modified long division algorithm, using matrices

Ex Back to $\boxed{a=126, \ b=35}$

We want to solve a system of the form $m\cdot 126 + n\cdot 35 = d$

$$\begin{array}{cc} a & b \\ \end{array}$$
$$\left[\begin{array}{cc|c} 1 & 0 & 126 \\ 0 & 1 & 35 \end{array}\right] \xrightarrow[r_1 - 3r_2]{} \left[\begin{array}{cc|c} 1 & -3 & 21 \\ 0 & 1 & 35 \end{array}\right]$$

$$\xrightarrow[r_2 - r_1]{} \left[\begin{array}{cc|c} 1 & -3 & 21 \\ -1 & 4 & 14 \end{array}\right]$$

$$\xrightarrow[r_1 - r_2]{} \left[\begin{array}{cc|c} 2 & -7 & 7 \\ -1 & 4 & 14 \end{array}\right]$$

$$\xrightarrow[r_2 - 2r_1]{} \begin{array}{c} \begin{array}{cc} a & b \end{array} \\ \left[\begin{array}{cc|c} 2 & -7 & 7 \\ -5 & 18 & 0 \end{array}\right] \end{array} \quad \gcd(a,b)$$

$\therefore \quad 7 = 2a + (-7)b = 2\cdot 126 - 7\cdot 35.$

when $d = \gcd(a,b) = 1$, we say that a & b are <u>coprime</u> (they have no prime factor in common)

eg: · 9 & 4 are coprime $\gcd = 1$

· 6 & 4 are not coprime $\gcd = 2$

<u>Prop</u> $\gcd(a,b) = 1 \iff \exists$ a linear combination $ma + nb = 1$

<u>Proof</u> ($\Longrightarrow$) follows from Thm above (w/ $d=1$)

($\Longleftarrow$) If $ma + nb = 1$, then 1 is the smallest <u>positive</u> linear combination of a & b

So again by Thm (part 2), $1 = \gcd(a,b)$ $\boxtimes$

<u>Equivalence relations</u>

<u>Def</u> A <u>relation</u> R on a set S is a subset $R \subseteq S \times S$.

<u>notation</u>: If $(a,b) \in R$, we write $a \sim b$ (or $a \underset{R}{\sim} b$)

(tex: \sim)

<u>eg</u>: The graph of a function $f: S \to S$ is a relation: $R = \{(x, f(x)) : x \in S\}$ that must pass the vertical line test.

<u>Def</u> An <u>equivalence relation</u> R (or $\sim$) on a set S is a relation that satisfies

(i) (reflexivity) $x \sim x$, $\forall x \in S$

(ii) (Symmetry) $\quad x \sim y \Rightarrow y \sim x \quad , \forall x,y \in S$

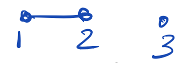
(iii) (transitivity) $\quad (x \sim y \ \& \ y \sim z) \Longrightarrow x \sim z$
$\forall x,y,z \in S$

<u>Simplest example</u> : $(S, =)$ ie $x \sim y \Leftrightarrow x = y$
ie $R = \{(x,x) : x \in S\}$

<u>Others</u> : $S = \{1,2,3\}$ $\quad R = \{(1,1),(1,2),(2,1),(2,2),(3,3)\}$

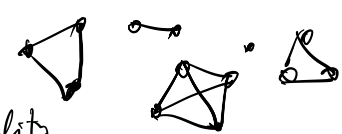
	1	2	3
1	✓	✓	
2	✓	✓	
3			✓

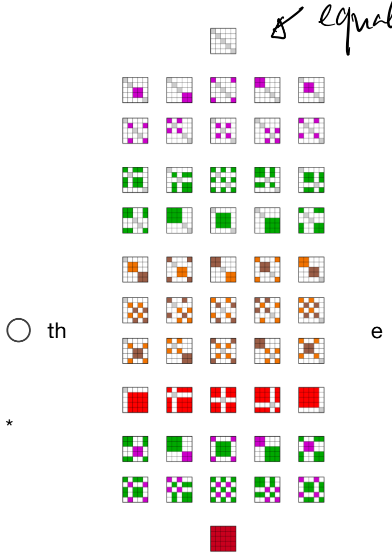
or $1 \sim 2$ etc

or 

<u>Note</u> : We can associate a graph to R, with vertex set S and edges x —— y if $x \sim y$

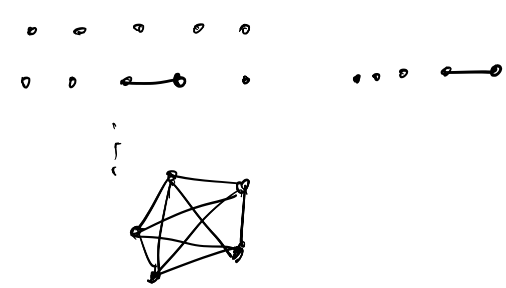
These graphs have all connected components complete graphs (or, cliques)





equality

Picture from Wikipedia of all equivalence relations on $S = \{1,2,3,4,5\}$



Not an equiv rel : (1) $R = \{(1,1),(1,2),(1,3)\}$ on $\{1,2,3\}$

(2) $(\mathbb{Z}, \leq)$ reflexive, transitive, not symm.

$a \leq a$ $\qquad$ $a \leq b, b \leq c \Downarrow a \leq c$ $\qquad$ $a \leq b \not\Downarrow b \leq a$ (unless $a=b$)

Congruence relation (mod n)

($n>0$)

Def Two integers a & b are congruent modulo n — written $a \equiv b \pmod{n}$ if $\boxed{a-b = n \cdot q}$ for some $q \in \mathbb{Z}$

e.g. $7 \equiv 2 \pmod{5}$, $8 \not\equiv 2 \pmod{5}$

Prop $\equiv$ is an equiv. relation

Proof (i) $a \equiv a \pmod{n}$: $a-a = 0 = n \cdot 0$

(ii) $a \equiv b \pmod{n} \Leftrightarrow a-b = nq$ for some q

$$\Leftrightarrow b-a = n(-q)$$
$$\Leftrightarrow b \equiv a \pmod{n}$$

(iii) $a \equiv b$ & $b \equiv c \pmod{n}$

$\Rightarrow a-b = qn$, $b-c = p \cdot n$ (for some q & p)

$\Rightarrow a-c = (a-b)+(b-c)$

$= qn + pn = (q+p) \cdot n$

$\Rightarrow a \equiv c \pmod{n}$

Def Given an equiv. rel $\sim$ on S, we write

$[x] = \{y \in S : y \sim x\}$ — equivalence class of x

---

for $\equiv$, we write

$[a]_n$ or simply $[a]$

Then $[a] = \{\dots, a-2n, a-n, a, a+n, a+2n, \dots\}$

Eg, for $n=2$ $\quad [0]_2 = \{-2, 0, 2, 4, \dots\}$ = even integers

$[1]_2 = \{-3, -1, 1, 3, 5, \dots\}$ = odd integers

The set of equivalence classes (for $\equiv \pmod n$) is

$$\mathbb{Z}_n := \{[0]_n, [1]_n, \dots, [n-1]_n\}$$

($\mathbb{Z}$ mod n) or ($\mathbb{Z}$ sub n)

This set can be thought of as all possible reminders when dividing by n

$(a = n \cdot q + r, \quad 0 \le r < n)$

reminder

The $a \equiv b \pmod{}$ $\Leftrightarrow$ $a - b = qn$ for some q

$\Leftrightarrow$ (a & b have the remainder when dividing by n)

eg: $\mathbb{Z}_5 = \{[0], [1], [2], [3], [4]\}$