11/11 Discrete

Quiz 16

1. $A = \{a, b, c\}$

$B = \{1, 2, \_\_\_ \; 8\}$

(a) How many functions

$f: A \to B$

$(f(a), f(b), f(c))$

$\quad 8 \quad\quad 8 \quad\quad 8$

$\underline{8}^3 = 512$

(b) Injective (1-1)?

$(f(a), f(b), f(c))$

$\quad 8 \quad\quad 7 \quad\quad 6$

$\underline{8 \cdot 7 \cdot 6} = 8_3 = \frac{8!}{5!}$

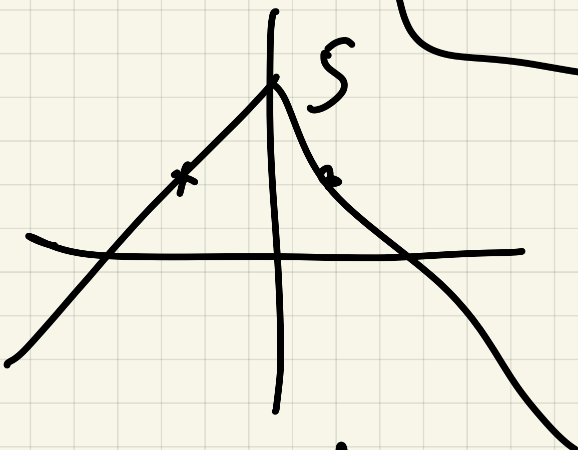
(c) NONE

$f(x) = 5 - |x|$

2. ~~f(.~~ $f: \underbrace{\mathbb{Z}}_{A} \to \underbrace{\mathbb{Z}}_{B}$

a) Show f not 1-1

$$\boxed{\begin{array}{c} f(1) = 4 = f(-1) = 4 \\ 1 \neq -1 \end{array}}$$



b) find Im f $\quad (-\infty, 5]$

$\longrightarrow \{x \in \mathbb{R} : x \leq 5\}$

$$\boxed{\{x \in \mathbb{Z} : x \leq 5\}}$$

c) f is onto?

Im $f \neq \mathbb{Z}$, no

Aside

$f: \mathbb{Z} \to \underbrace{\{x \in \mathbb{Z} : x \leq 5\}}_{B}$

(yes)

$f: \underbrace{\{x \in \mathbb{Z} : x \geq 0\}}_{A} \to \mathbb{Z}$

$f(x) = 5 - |x|$

f is 1-1

<u>Last time</u> gcd (a,b)

= greatest common divisor

Ways to compute

- By definition

- Write prime factorization

If $a = \prod p_i^{e_i}$ prime fact

$b = \prod p_i^{f_i}$

$\gcd(a,b) = \prod p_i^{\min\{e_i, f_i\}}$

$a = 2^{20} 3^{10} 5^{11} (7^0)$

$b = 2^{10} 3^5 5^{20} 7^3$

$\gcd(a,b) = 2^{10} 3^5 5^{11}$

- Via proposition 1:

If $a > b > 0$

quotient, rem

$\begin{cases} \boxed{a = bq + r} \\ 0 \leq r < b \end{cases}$

Then $\underset{\shortparallel}{\gcd(a,b)} = \underset{\shortparallel}{\gcd(b,r)}$

d $\quad$ e

pf Since $d \mid a$ and $d \mid b$,

also $d = r = a - bq$

$d \mid b$ and $d \mid r$

d common div for b, r

but e is greatest such, so

so $d \le e$.

Ex $\quad a = 10{,}010 \quad \gcd(10{,}010, 1309)$

$b = 1{,}309$

① $10010 = \underline{1309} \cdot 7 + \underline{847}$

② $1309 = \underline{847} \cdot 1 + \underline{462}$

③ $847 = \underline{462} \cdot 1 + \underline{385} \leftarrow$

④ $462 = 385 + 77$

$385 = 77 \cdot 5 + 0$

So $\gcd(10{,}010, 1309) = 77$

<u>Claim</u>: $\exists\, x, y \in \mathbb{Z}$ so that

$$10{,}010\,x + 1309\,y = 77$$

<u>Why?</u>

4

$$77 = 462 - 385$$

3

$$= 462 - (847 - 462)$$

$$= -847 + 2(462)$$

2

$$= -847 + 2(1309 - 847)$$

$$= 2(1309) - 3(847)$$

1

$$= 2(1309) - 3(10010 - 7 \cdot 1309)$$

$$= -3(10010) + 23(1309)$$

$$x = -3, \quad y = 23$$

Note: $x = -3, y = 23$

is not the only solution

$$77 = -3(10010) + 23(1309)$$

$$\underbrace{(-3+1309)}_{x'}(10010) + \underbrace{(23-10010)}_{y'}(1309)$$

Ex 2 Find $\overset{d=}{\gcd}(726, 187)$

and find $x, y \in \mathbb{Z}$:

$$d = 726x + 187y$$

① $726 = 187 \cdot 3 + 165$

② $187 = 165 \cdot 1 + 22$ ←

③ $165 = 22 \cdot 7 + 11$

④ $22 = 11 \cdot 2 + 0$

$11 = \gcd(726, 187)$

Find x, y, work backwards

3 $$11 = 165 - 7 \cdot 22$$

2 $$= 165 - 7(187 - 165)$$

$$= -7(187) + 8(165)$$

1 $$= -7(187) + 8(726 - 3 \cdot 187)$$

$$= 8(726) - 31(187)$$

so $x = 8$

$y = -31$

Prop1: Let $a, b \in \mathbb{Z}$, not both 0,

Then $\exists\, x, y \in \mathbb{Z}$:

$$\gcd(a, b) = ax + by$$

Theorem 2: Let $a, b \in \mathbb{Z}$, not both 0, Then

$\gcd(a,b)$ = smallest positive integer of form

$ax+by$, $x,y \in \mathbb{Z}$

$= \min \{ \underline{ax+by : x,y \in \mathbb{Z}, ax+by > 0} \}$

Pf: $d = \gcd(a,b)$.

Prop 1 $\Rightarrow$ $d \in \{ax+by \mid {x,y \in \mathbb{Z}, \atop ax+by>0} \}$

Why the smallest?

If ax_1+by_1 is the smallest

$d|a$, $d|b$ $\Rightarrow$ $d | \underline{a}x_1+\underline{b}y_1$,

$$d \geq ax_1 + by_1$$

$$d \leq ax_1 + by_1$$

so $$d = ax_1 + by_1$$

<u>Cor 1</u> : $a, b \in \mathbb{Z}$ are relatively prime

$$\Downarrow$$

$$\exists\, x, y \in \mathbb{Z} : xa + yb = 1$$

recall,

a, b rel prime

$\gcd(a,b) = 1$

Ex 3 Find gcd (13, 21)

① $21 = 13 + 8$

② $13 = 8 + 5$

③ $8 = 5 + 3$

④ $5 = 3 + 2$

⑤ $3 = 2 + 1$

$2 = 1 \cdot 2 + 0$

Fibonacci numbers!

If we found $x, y \in \mathbb{Z}$ via equs ① – ⑤, answer $x = -8, y = 5$

$$-\underline{8}(13) + \underline{5(21)} = 1$$

Cor 2 If e is a common divisor of a, b, then

$e \le d = \gcd(a,b)$ $\cancel{\le e}$,

but more is true:

$e | d$

__proof__: Since e is common div

$$\boxed{\begin{aligned} a &= e a_1 \\ b &= e b_1 \end{aligned}} \qquad \begin{aligned} a_1 &\in \mathbb{Z} \\ b_1 &\in \mathbb{Z} \end{aligned}$$

Then $d = \underset{=}{a}x + \underset{=}{b}y$

$$= e a_1 x + e b_1 y$$

$$= e(a_1 x + b_1 y)$$

so $e | d$

§37 Modular arithmetic

Number systems

$\mathbb{Z}$ $\quad \mathbb{Q} \quad \mathbb{R} \quad \mathbb{C}$

operation $+/-/\cdot/$

(sometimes $\div$)

Defn Let $0 < n \in \mathbb{N}$

The integers modulo n is the set

$$\mathbb{Z}_n = \{0, 1, 2, 3 \ldots n-1\}$$

Operations :

addition $a \oplus b = (a+b) \bmod n$

subtraction $a \ominus b = (a-b) \bmod n$

multiplication $a \otimes b = (a \cdot b) \bmod n$

Ex) Take, $n = 7$

$$\mathbb{Z}_7 = \{0, 1, 2, 4, 5, 6\}$$

$$4 \oplus 5 = 9 \bmod 7 = 2$$

table: for addition:

$\oplus$	0	1	2	3	4	5	6
0	0	1	2	3	4	5	6
1	1	2	3	4	5	6	0
2	2	3	4	5	6	0	1
3	3	4	5	6	0	1	2
4	4	5	6	0	1	2	3
5	5	6	0	1	2	3	4
6	6	0	1	2	3	4	5

Multiplication mod 7

	0	1	2	3	4	5	6
0	0	0	0	0	0	0	0
1	0	1	2	3	4	5	6
2	0	2	4	6	1	3	5
3	0	3	6	2	5	1	4
4	0	4	1	5	2	6	3
5	0	5	3	1	6	4	2
6	0	6	5	4	3	2	1