11/13 | Discrete

Quiz 17

1. $\underset{\text{letter}}{\underline{26}} \cdot \underbrace{\underline{10} \cdot \underline{10}}_{\text{digits}} = 2600$

2. There are more pigeons = bankers (3000) than pholes = passcodes (2600),

so PHP $\Rightarrow$ at least 2 bankers have same passcode.

Or $f: \{\text{Bankers}\} \to \{\text{passcodes}\}$

$x \longmapsto$ passcode for x

is not 1-1 because

$|\{\text{Bankers}\}| = 3000$, $|\{\text{passcodes}\}| = 2600$

3. 2601 is smallest.

Last time Modular Arithmetic

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

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

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

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

satisfy usual algebra rules:

(1) Commutative: $a \oplus b = b \oplus a$,

$a \otimes b = b \otimes a$

(2) Associative: $a \oplus (b \oplus c) = (a \oplus b) \oplus c$,

$a \otimes (b \otimes c) = (a \otimes b) \otimes c$

(3) Identity $a \otimes 1 = a$, $a \oplus 0 = a$

(4) Distributive

$a \otimes (b \oplus c) = (a \otimes b) \oplus (a \otimes c)$

Recall multiplication table for $\mathbb{Z}_7$:

$\otimes$	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

Remark:

Each nonzero column-Row contains all 7 elements of $\mathbb{Z}_7$,

so can divide by nonzero numbers:

$$x = \frac{1}{3} = 5$$

because $3 \otimes 5 = 1$

$x = 3/4 = 6$ b/c $4 \otimes 6 = 3$

i.e. $3 \oslash 4 = 6$ ← modular division

Contrast this to the case $n = 6$:

Ex: Table for $\otimes$ in $\mathbb{Z}_6$

$\otimes$	0	1	2	3	4	5
0	0	0	0	0	0	0
1	0	1	2	3	4	5
2	0	2	4	0	2	4
3	0	3	0	3	0	3
4	0	4	2	0	4	2
5	0	5	4	3	2	1

Here $3 \oslash 4$ is not defined, because there is no solution to $4 \otimes x = 3$

But $\frac{1}{5} = 5$ b/c $5 \otimes 5 = 1$

and $4/5 = \frac{1}{5} \otimes 4 = 5 \otimes 4 = 20 \equiv 2$

You can divide by 1 and 5

Defn: Let $0 \neq x \in \mathbb{Z}_n$. A reciprocal (or modular inverse) for x is $y \in \mathbb{Z}_n$: $x \otimes y = 1$

(i.e. $y = \frac{1}{x}$). If x has a reciprocal, then x is <u>invertible</u>.

The set of all invertible elements in $\mathbb{Z}_n$ is denoted $\mathbb{Z}_n^*$

(So in Ex2, $\mathbb{Z}_6^* = \{1, 5\}$)

<u>Prop1</u>: Let $a \in \mathbb{Z}_n$, $n > 0$.

① If a is invertible, then $\frac{1}{a}$ unique

② If a invertible and $b \in \mathbb{Z}_n$, $\exists c : c = b/a$ and c is unique.

<u>Proof</u>: ① If $c = \frac{1}{a}$ and $c' = \frac{1}{a}$, then $a \otimes c = 1$, $a \otimes c' = 1$, so

$c = c \otimes 1 = c \otimes (a \otimes c') = (c \otimes a) \otimes c'$

$= 1 \otimes c' = c'$, so $c = c'$,

(2) $c = b/a$ means $a \otimes c = b$,

but then $\underbrace{\frac{1}{a} \otimes a}_{} \otimes c = \frac{1}{a} \otimes b$

$$\parallel$$

$$c = 1 \otimes c$$

so $c = \frac{1}{a} \otimes b$.

Ex3 Compute $\mathbb{Z}_{10}^*$

$\mathbb{Z}_{10} = \{0, 1, 2 \dots 9\}$

$0 \notin \mathbb{Z}_{10}^*$ $2 \otimes x = 1$ has no solution,

so $2 \notin \mathbb{Z}_{10}^*$, also $4, 6, 8 \notin \mathbb{Z}_{10}^*$

$5 \otimes x = 1$ no solution, so

only need check $1, 3, 7, 9$

Now $1 \otimes 1 = 1$, $3 \otimes 7 = 1$, $9 \otimes 9 = 1$,

so $\mathbb{Z}_{10}^* = \{1, 3, 7, 9\}$.

What's the general pattern?

<u>Theorem</u> For $a \in \mathbb{Z}_n$,

a invertible $\Leftrightarrow$ a rel. prime to n

<u>Proof</u>: a invertible $\Leftrightarrow \exists x \in \mathbb{Z}_n$:

$a \otimes x = 1 \Leftrightarrow \exists b$: $ax \equiv 1 \pmod{n}$

$\Leftrightarrow \exists x \in \mathbb{Z}_n$: $n \mid 1 - ax \Leftrightarrow$

$\exists x \in \mathbb{Z}_n, y \in \mathbb{Z}$: $ny = 1 - ax \Leftrightarrow$

$\exists x, y \in \mathbb{Z}$: $1 = ax + ny \Leftrightarrow$

$\gcd(\cancel{x} a, n) = 1 \Leftrightarrow a, n$ rel. prime

<u>Ex 4</u> Find $\mathbb{Z}_{18}^*$ and inverses

$\mathbb{Z}_{18}^* = \{1, 5, 7, 11, 13, 17\}$

$\frac{1}{1} = 1$, $\frac{1}{17} = 17$, $\frac{1}{5} = 11$, $\frac{1}{7} = 13$,

$1/11 = 5$, $1/13 = 7$

Ex5 find $1/7$ and $8/7$

(a) In $\mathbb{Z}_{10}$. $\frac{1}{7} = 3$ b/c

$7 \otimes 3 = 1$.

Thus $\frac{8}{7} = 8 \otimes \frac{1}{7} = 8 \otimes 3 = 4$.

(b) In $\mathbb{Z}_{40}$. Now $|\mathbb{Z}_{40}^{\otimes}| = 16$

and brute force approach is not convenient.

But theorem suggests that solving $7 \otimes x = 1$ is same as solving $7x + 40y = 1$, we know how from §36.

① $40 = 5 \cdot 7 + 5$

② $7 = 5 \cdot 1 + 2$

(3) $5 = 2\cdot 2 + (1) = \gcd(40,7)$.

$$1 = 5 - 2\cdot 2 \stackrel{(2)}{=} 5 - 2(7-5) =$$

$$-2\cdot 7 + 3\cdot 5 \stackrel{(1)}{=} -2\cdot 7 + 3(40 - 5\cdot 7) =$$

$$\underbrace{-17}_{x}\cdot 7 + \underbrace{3}_{y}\cdot 40 = 1$$

So $x = -17 \equiv 23 \pmod{40}$,

$\therefore \frac{1}{7} = 23$.

$$8/7 = 8 \odot \frac{1}{7} = 8 \odot 23 = 184 \equiv 24 \pmod{40}$$

$\therefore 8/7 = 24$.