

Exam 3

109060013 張芯瑜

(1) If (\mathbb{Q}^+, \times) is a group, then it must satisfy four properties below:

1° (\times is a closed operation)

$$a, b \in \mathbb{Q}^+$$

$$\therefore a = \frac{p}{q} \quad (p, q \in \mathbb{N}) \quad (p, q \in \mathbb{Z} \text{ 且 } p, q > 0) \quad , \quad b = \frac{p'}{q'} \quad (p', q' \in \mathbb{N})$$

$$\Rightarrow a \times b = \frac{p}{q} \times \frac{p'}{q'} = \frac{p \times p'}{q \times q'}$$

$$\therefore pp', qq' \in \mathbb{N} \quad \therefore a \times b \in \mathbb{Q}^+ \Rightarrow \text{closed}$$

2° (there is an identity)

choose 1 to be the identity

$$\forall a \in \mathbb{Q}^+, a \cdot 1 = 1 \cdot a = a \quad \therefore e = 1$$

3° (\times is associative operation)

$$a, b \in \mathbb{Q}^+$$

$$\therefore a, b \in \mathbb{Q} \Rightarrow a \times b = b \times a$$

$\Rightarrow \times$ is associative

4° (every element in \mathbb{Q}^+ has an inverse)

$$a \in \mathbb{Q}^+, a^{-1} \cdot a = 1$$

Assume $a^{-1} \notin \mathbb{Q}^+ \Rightarrow a^{-1} = 0$, Impossible

$a^{-1} \in \mathbb{Q}^-$, Impossible $\because a^{-1} \cdot a > 0, a > 0$

$a^{-1} \notin \mathbb{Q}$, Impossible \because 無理數 \times 非0有理數
= 無理數

but $1 \in \mathbb{Q}$

$$(\Rightarrow \Leftarrow) \therefore a^{-1} \in \mathbb{Q}$$

5° By above, (\mathbb{Q}^+, \times) is a group.

$$(2) \quad 53^{723}$$

$$\equiv 53 \times (53^2)^{361} \pmod{100}$$

$$\equiv 53 \times 2809^{361} \pmod{100}$$

$$\equiv 53 \times 9^{361} \pmod{100}$$

$$\equiv 53 \times 9 \times 729^{120} \pmod{100}$$

$$\equiv 53 \times 9 \times 29^{120} \pmod{100}$$

$$\equiv 53 \times 9 \times 841^{60} \pmod{100}$$

$$\equiv 53 \times 9 \times 41^{60} \pmod{100}$$

$$\equiv 53 \times 9 \times 1681^{30} \pmod{100}$$

$$\equiv 53 \times 9 \times 81^{30} \pmod{100}$$

$$\equiv 53 \times 9 \times 6561^{15} \pmod{100}$$

$$\equiv 53 \times 9 \times 61^{15} \pmod{100}$$

$$\equiv 53 \times 9 \times 61 \times 3721^7 \pmod{100}$$

$$\equiv 53 \times 9 \times 61 \times 21^7 \pmod{100}$$

$$\equiv 53 \times 9 \times 61 \times 21 \times 441^3 \pmod{100}$$

$$\equiv 53 \times 9 \times 61 \times 21 \times 41^3 \pmod{100}$$

$$\equiv 53 \times 9 \times 61 \times 21 \times 41 \times 1681 \pmod{100}$$

$$\equiv (53 \times 9) \times (61 \times 21) \times (41 \times 81) \pmod{100}$$

$$\equiv 477 \times 1281 \times 3321 \pmod{100}$$

$$\equiv 77 \times 81 \times 21 \pmod{100}$$

$$\equiv 6237 \times 21 \pmod{100}$$

$$\equiv 37 \times 21 \pmod{100}$$

$$\equiv 777 \pmod{100}$$

$$\equiv 77 \pmod{100}$$

#

(3a)

$$\begin{aligned}
 n &= 779 = 19 \times 41 \\
 \phi(n) &= 779 \times \frac{18}{19} \times \frac{40}{41} = 720 \\
 e &= 101 \\
 ed &\equiv 1 \pmod{720}
 \end{aligned}$$

$$\begin{array}{rcl}
 \Rightarrow \begin{array}{cc} (1, 0) & 101 \\ (-49, 7) & 91 \\ \hline (50, -7) & 10 \\ (-171, 24) & 9 \\ \hline (221, -31) & 1 \end{array} & \begin{array}{cc} 720 & (0, 1) \\ 707 & (7, 0) \\ \hline 13 & (-7, 1) \\ 10 & (50, -7) \\ \hline 3 & (-57, 8) \end{array}
 \end{array}$$

$$\Rightarrow 221 \times 101 + (-31) \times 720 = 1$$

$$\therefore \underline{d = 221} \#$$

$$(3b) \quad 299^{221} \equiv 29 \pmod{779}$$

$$656^{221} \equiv 41 \pmod{779}$$

$$280^{221} \equiv 48 \pmod{779}$$

$$47^{221} \equiv 35 \pmod{779}$$

$$216^{221} \equiv 30 \pmod{779} \quad \#$$

$$(3c) \quad 29 \rightarrow "C"$$

$$41 \rightarrow "O"$$

$$48 \rightarrow "V"$$

$$35 \rightarrow "I"$$

$$30 \rightarrow "d"$$

$$\Rightarrow \underline{\text{covid}} \#$$

(4) $S = \left\{ \begin{array}{c} \text{Diagram 1} \quad \text{Diagram 2} \quad \dots \quad \text{Diagram 3} \\ \text{Diagram 4} \end{array} \right\}$

Diagram 1: A hexagon with 6 black dots at vertices. A curved line above it is labeled 2^6 .

Diagram 2: A hexagon with 6 dots, 3 black and 3 white, alternating.

Diagram 3: A hexagon with 6 white dots at vertices.

Diagram 4: A hexagon with 6 black dots at vertices, enclosed in a large bracket labeled 3^6 .

$$G_S = \{ (I), (60^\circ), (120^\circ), (180^\circ), (240^\circ), (300^\circ) \}$$

$$\frac{2^6 \times 3^6 + 2 \times 3 + 2^2 \times 3^2 + 2^3 \times 3^3 + 2^2 \times 3^2 + 2 \times 3}{6}$$

6

$$= 6^5 + 1 + 6 + 6^2 + 6 + 1$$

$$= \underline{7826} \#$$

(5) $C_p = \frac{1}{p+1} \binom{2p}{p} = \frac{(2p)!}{(p+1)!p!}$