Exam 3

109060013 張芯瑜

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

1° ($\times$ is a closed operation)

$a, b \in Q^+$ ($p, q \in \mathbb{Z}$ 且 $p, q > 0$)

$\therefore a = \frac{p}{q}$ $(p, q \in \mathbb{N})$, $b = \frac{p'}{q'}$ $(p', q' \in \mathbb{N})$

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

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

2° (there is an identity)

choose 1 to be the identity

$\forall a \in Q^+$, $a \cdot 1 = 1 \cdot a = a$ $\therefore e = 1$

3° ($\times$ is associative operation)

$a, b \in Q^+$

$\because a, b \in Q$ $\Rightarrow a \times b = b \times a$

$\Rightarrow \times$ is associative

4° (every element in Q^+ has an inverse)

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

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

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

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

but $1 \in Q$

$(\rightarrow\leftarrow)$ $\therefore a^{-1} \in Q$

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

(2) 53^{723}

$$\begin{aligned}
&\equiv 53 \times (53^2)^{361} \pmod{100} \\
&\equiv 53 \times 2809^{361} \pmod{100} \\
&\equiv 53 \times 9^{361} \pmod{100} \\
&\equiv 53 \times 9 \times 729^{120} \pmod{100} \\
&\equiv 53 \times 9 \times 29^{120} \pmod{100} \\
&\equiv 53 \times 9 \times 841^{60} \pmod{100} \\
&\equiv 53 \times 9 \times 41^{60} \pmod{100} \\
&\equiv 53 \times 9 \times 1681^{30} \pmod{100} \\
&\equiv 53 \times 9 \times 81^{30} \pmod{100} \\
&\equiv 53 \times 9 \times 6561^{15} \pmod{100} \\
&\equiv 53 \times 9 \times 61^{15} \pmod{100} \\
&\equiv 53 \times 9 \times 61 \times 3721^{7} \pmod{100} \\
&\equiv 53 \times 9 \times 61 \times 21^{7} \pmod{100} \\
&\equiv 53 \times 9 \times 61 \times 21 \times 441^{3} \pmod{100} \\
&\equiv 53 \times 9 \times 61 \times 21 \times 41^{3} \pmod{100} \\
&\equiv 53 \times 9 \times 61 \times 21 \times 41 \times 1681 \pmod{100} \\
&\equiv (53 \times 9) \times (61 \times 21) \times (41 \times 81) \pmod{100} \\
&\equiv 477 \times 1281 \times 3321 \pmod{100} \\
&\equiv 77 \times 81 \times 21 \pmod{100} \\
&\equiv 6237 \times 21 \pmod{100} \\
&\equiv 37 \times 21 \pmod{100} \\
&\equiv 777 \pmod{100} \\
&\equiv \underline{77 \pmod{100}} \ \#
\end{aligned}$$

(3a) $\begin{cases} n = 779 = 19 \times 41 \\ \phi(n) = \cancel{779 \times \frac{18}{19}} \times \frac{40}{\cancel{41}} = 720 \\ e = 101 \\ ed \equiv 1 \pmod{720} \end{cases}$

⇒ (1, 0)	101	720	(0, 1)
(-49, 7)	91	707	(7, 0)
(50, -7)	10	13	(-7, 1)
(-171, 24)	9	10	(50, -7)
(221, -31)	1	3	(-57, 8)

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

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

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

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

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

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

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

(3C) $29 \longrightarrow$ "c"

$41 \longrightarrow$ "o"

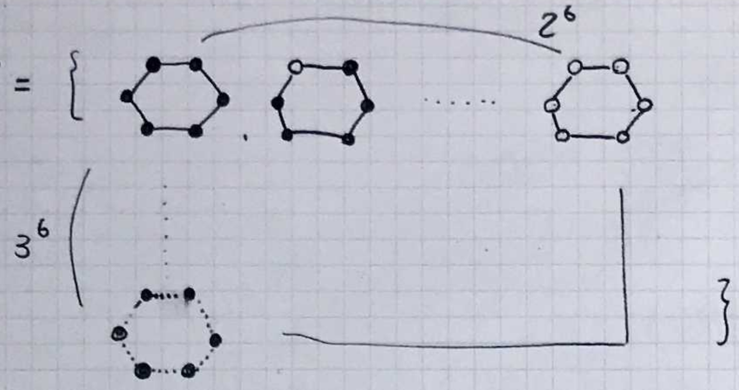
$48 \longrightarrow$ "v"

$35 \longrightarrow$ "i"

$30 \longrightarrow$ "d"

⇒ covid #

(4) $S = \{$



$\}$

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

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

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

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

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