H.W. 5

109060013 張芯瑜

(1) $\phi(1720)$

$1720 = 2^3 \times 5 \times 43$

$\Rightarrow \phi(1720) = 1720 \times \frac{42}{43} \times \frac{4}{5} \times \frac{1}{2} = \underline{672}$ #

(2a) $\gcd(j,k) = aj + bk$

$\Rightarrow n^{\gcd(j,k)} = n^{aj+bk}$

$= n^{aj} \cdot n^{bk}$

$= (n^j)^a \cdot (n^k)^b \equiv 1^a \cdot 1^b \pmod m \equiv 1 \pmod m$

#

(2b) By Fermat's Little Thm. $\Rightarrow 2^{p-1} \equiv 1 \pmod p$

while p is prime

$\because 2^n \equiv 1 \pmod n$

$\therefore n \mid 2^n - 1 \Rightarrow p \mid 2^n - 1 \Rightarrow 2^n \equiv 1 \pmod p$

$\because 2^{p-1} \equiv 1 \pmod p, \quad 2^n \equiv 1 \pmod p$

By (2a) $\longrightarrow 2^{\gcd(p-1,\, n)} \equiv 1 \pmod p$ #

(2c) $\because p$ is the smallest prime of n

$\therefore \gcd(p-1, n) = 1$

$\therefore 2^{\gcd(p-1,\, n)} \equiv 2 \pmod p \not\equiv 1 \quad (\rightarrow\!\leftarrow)$

$\Rightarrow$ Assumption wrong. $2^n \not\equiv 1 \pmod n$ for all $n > 1$

#

(3a) $n = 2^m(2^{m+1}-1)$

$$\Rightarrow (2^0 + 2^1 + \cdots + 2^m) + (2^0 + 2^1 + \cdots + 2^{m-1})(2^{m+1}-1)$$

$$= 2^m + (2^{m+1} + 2^{m+2} + \cdots + 2^{2m})$$

$$= 2^m (1 + 2^1 + 2^2 + \cdots + 2^m)$$

$$= 2^m \cdot \frac{1(1-2^{m+1})}{1-2} = 2^m(2^{m+1}-1) = n \quad \#$$

(3b) $n = 2^m Q$

$$\Rightarrow 2^{m+1} Q = 2n$$

$\because$ n is perfect num $\therefore n = 2^m(\underbrace{2^{m+1}-1}_{Q})$ by (a)

$$\Rightarrow \sigma(Q) = 2^{m+1} - 1 + 1 = 2^{m+1}$$

$$\therefore 2n = 2^{m+1} Q = \sigma(Q) \cdot (2^{m+1}-1) \quad \#$$

(4) $1°\ n = 2419 = 41 \times 59$

$\Rightarrow \phi(n) = 2419 \times \frac{40}{41} \times \frac{58}{59} = 2320$

$2°\ 211 \times k \equiv 1 \pmod{2320}$

$2320 \mid 211k - 1 \quad \Rightarrow k = 11$

$3°\ 1040^{11} \equiv 70 \pmod{2419}$

$1182^{11} \equiv 101 \pmod{2419}$

$1075^{11} \equiv 114 \pmod{2419}$

$741^{11} \equiv 109 \pmod{2419}$

$2366^{11} \equiv 97 \pmod{2419}$

$1495^{11} \equiv 116 \pmod{2419}$

$\Rightarrow \underline{(70, 101, 114, 109, 97, 116)}$ #

(5a)

$$\begin{matrix}1\\2\\3\\4\\5\\6\end{matrix} \longrightarrow \begin{matrix}4\\1\\5\\2\\6\\3\end{matrix} \quad \therefore \quad \begin{matrix} 1,2,3 \to 2,4,6 \\ 4,5,6 \to 1,3,5 \end{matrix}$$

Let a_t be the position for the card after t shuffles.

$\Rightarrow a_{t+1} \equiv 2a_t \pmod{2n+1}$

$a_t \equiv 2a_{t-1}$ (〃)

$\vdots$

$\Rightarrow a_t \equiv 2^t a_0 \pmod{2n+1}$

$\because \gcd(2, 2n+1) = 1$

$\therefore$ By Euler's Thm. $\Rightarrow 2^{\phi(2n+1)} \equiv 1 \pmod{2n+1}$

$\Rightarrow$ After $\phi(2n+1)$, $a_{\phi(2n+1)} \equiv 2^{\phi(2n+1)} a_0 \equiv a_0 \pmod{2n+1}$

the cards will rusume !!