預習測驗09

姓名：_____ 序號：____ 學號：_____ 分數：6 5 4 3 2

預習第九、十講 (211-218頁) 並完成下列問題

1. 令 p 為一質數且令 a 為模 p 下的非零元素。 那個最小的正整數 r 使得 $a^r \equiv 1 \pmod{p}$ 就稱為 a 的週期(order)； 通常以符號 $\circ(a)$ 表示之。模 p 的一個原根就是其中一 個非零元素 g 使得每一個模 p 的非零元素都是 g 的一個次冪。因此

$$g \text{ 是質數 } p \text{ 的一個原根 } \iff \circ(g) = p - 1 \text{ 。}$$

   (a) 請計算，在模 17 之下 2 與 3 的次冪：

j	1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16
2^j	2	4	8	16	15											
3^j	3	9	10	13	5											

   (b) 請問在模 17 之下 2 與 3 的週期分別是多少？

   (c) 請問 2 與 3 何者是模 17 的原根？

2. 令 $p = 601$, 則 $p - 1 = 600 = 2^3 \cdot 3 \cdot 5^2$; 請證明： $\circ(7) = 600$ ，因而 7 是質數 601 的一個原根。

   (a) 先證明：若 $r < 600$ 而且 r 整除 600 ，那麼 r 必可整除 $\{300,\ 200,\ 120\}$ 三數之一。

   (b) 費馬小定理告訴我們 $7^{600} \equiv 1 \pmod{601}$ ，證明： $\circ(7) \mid 600$。

   (c) 計算顯示 (可用連續平方法得到) $7^{300} \equiv 600,\ 7^{200} \equiv 576,\ 7^{120} \equiv 423 \pmod{601}$。
   因此得知： $\circ(7)$ 不整除 300, 200 或 120。

   (d) 若 $\circ(7) < 600$ ，由 (a) 與 (b) 得知 $\circ(7)$ 必可整除 $\{300,\ 200,\ 120\}$ 三數之一； 可惜的是，這跟實際的情況 (c) 不符；因此得證 $\circ(7) = 600$ 。

3. 固定一質數 p 。令 α 與 β為模 p之下的兩個非零整數並考慮方程式 $\alpha^x \equiv \beta \pmod{p}$; 此同餘方程式中，解 x 的問題稱之為離散對數問題。 請問同餘式 $3^x \equiv 2 \pmod{65537}$ 中 x 的解是多少？