相關定理 - Fermat 定理

Fermat 定理

- 定義：若 p 為質數，且 a 是無法讓 p 整除的正整數，則：

  $a^{p-1} \equiv 1 \bmod p$

- 譬如： a = 7, p=19 則 $7^{19-1} \equiv 1 \bmod 19$

  $7^2 = 49 \equiv 11 \bmod 19$

  $7^4 = 7^2 \times 7^2 \equiv 11 \times 11 = 121 \equiv 7 \bmod 19$

  $7^8 = 7^4 \times 7^4 \equiv 7 \times 7 = 49 \equiv 11 \bmod 19$

  $7^{16} = 7^8 \times 7^8 \equiv 11 \times 11 = 121 \equiv 7 \bmod 19$

  $a^{p-1} = 7^{18} = 7^{16} \times 7^2 \equiv 7 \times 11 = 77 \equiv 1 \bmod 19$ 得證之。

- Fermat 定理變形：

  - $a\ (a^{p-1}) \equiv a(1 \bmod p)$
  - $a^p \equiv a \bmod p$

相關定理 - Euler‘s Totient 函數

Euler's Totient 函數

- ϕ(n) 是小於 n 但與 n 成為互質之正整數的數目。

  譬如 ϕ(10) = 4，則表示小於 10 且與 10 為互質的數字共計有 4 個。

  gcb(1, 10)，gcd(3, 10), gcd(5, 10), gcd(7, 10)=1

  譬如 ϕ(9), 則 gcd(1,9)=1, 2, 3, 5, 7, 8 則 6 個

- 如果 p 為質數的話，則：ϕ(p) = p-1

  譬如：p=3，則 ϕ(3) = 3-1=2；p=19，則 ϕ(19) = 18

- 30 以前數字的 ϕ(n)

n	ψ(n)	n	ψ(n)	n	ψ(n)
1	1	11	10	21	12
2	1	12	4	22	10
3	2	13	12	23	22
4	2	14	6	24	8
5	4	15	8	25	20
6	2	16	8	26	12
7	6	17	16	27	18
8	4	18	6	28	12
9	6	19	18	29	28
10	4	20	8	30	8

相關定理 - Euler‘s Totient 函數

- 假設有兩個質數 p 與 q，而 n = pq，則：

  $\phi(n) = \phi(pq) = \phi(p) \times \phi(q) = (p-1) \times (q-1)$

- 譬如，p=3、q=7、然而 n = 21，則：

  $\phi(21) = \phi(3) \times \phi(7) = 2 \times 6 = 12$

  $= (3-1) \times (7-1)$

相關定理 - Euler 定理

Euler 定理

- 定義：如果 a 與 n 互質（gcd(a, n) = 1）的話，則：

$$a^{\phi(n)} \bmod n \equiv 1 \bmod n$$

- 意思表示：a 與 n 相互之間無法整除的話（互質），$a^{\phi(n)}$ 除以 n，所得到的餘數為 1。

  譬如，a = 3、n = 10，則 $\phi(n) = \phi(10) = 4$

  推演如下：

$$a^{\phi(n)} = 3^4 = 81 \equiv 1 \bmod 10 \equiv 1 \bmod n$$

- Euler 定理的變形：

$$a \times (a^{\phi(n)}) \equiv a \times (1 \bmod n)$$

$$a^{\phi(n)+1} \equiv a \bmod n$$