7202　關於 2^{1000}（周雲雄提供）

也許我們無法實際算出 2^{1000}，但是，是否有方法可以讓我們來計算 2^{1000} 的個位數、十位數、最高位數及次高位數？

解答：（周雲雄提供）

$$2^1 = 2$$
$$2^2 = 4$$
$$2^3 = 8$$
$$2^4 = 16$$
$$2^5 = 32$$
$$2^6 = 64$$
$$2^7 = 128$$
$$2^8 = 256$$
$$2^9 = 512$$
$$2^{10} = 1024$$
$$2^{11} = 2048$$
$$2^{12} = 4096$$

$2^{13} = 8192$

$2^{14} = 16384$

$2^{15} = 32768$

$2^{16} = 65536$

$2^{17} = 131072$

$2^{18} = 262144$

$2^{19} = 524288$

$2^{20} = 1048576$

$2^{21} = 2097152$

$2^{22} = 4194304$

$2^{23} = 8388608$

$2^{24} = 16777216$

$2^{25} = 33554432$

$2^{26} = 67108864$

$2^{27} = 134217728$

$2^{28} = 268435456$

$2^{29} = 536870912$

$2^{30} = 1073741824$

$2^{31} = 2147483648$

$2^{32} = 4294967296$

$2^{33} = 8589934592$

$2^{34} = 17179869184$

$2^{35} = 34359738368$

$2^{36} = 68719476736$

$2^{37} = 137438953472$

$2^{38} = 274877906944$

$2^{39} = 549755813888$

$2^{40} = 1099511627776$

I. 2^{1000} 的末兩位：

由上表可觀察到下列規律性：

末兩位自 2^2 起以 04, 08, 16, 32, …, 76, 52 每 20 個做一循環。

於是可馬上推出 2^{1000} 的末兩位是 76 。此種觀察算證明嗎？答案是肯定的。因爲乘法是向左進位，一旦兩個 2 的冪方的末兩位相同時，它們就進入一個循環節，而任意一個數的末兩位是介於 0 與 99 之間，故循環節的長度

最多是 100（請比較“有理數皆是循環小數”的證明）。在本題中，第一次有相同末兩位的情況發生在 2^2 及 2^{22}，故循環節長是 20，即 $2^{n+20k} \equiv 2^n \pmod{100}$，$n, k \in N$

$$n+20k \geq 2$$

在此 $a \equiv b \pmod{c}$ 表示 $c \mid (b-a)$，即 $b-a$ 是 c 的倍數。令

$$n = 20, \qquad k = 49$$

即得

$$2^{1000} \equiv 2^{20} \equiv 76 \pmod{100}$$

下面兩種證明方法為許多人所採用，本質上它們是一樣的（對觀察到的規律性做一整理）。

a. $76^2 \equiv 76 \pmod{100}$

因

$$2^{20} \equiv 76 \pmod{100}$$

故

$$2^{1000} = (2^{20})^{50} \equiv (76)^{50} \equiv 76 \pmod{100}$$

b. $2^{20} \equiv 1 \pmod{25}$

於是

$$2^{1000} \equiv (2^{20})^{50} \equiv 1^{50} = 1 \pmod{25}$$

故 2^{1000} 的末兩位是 1, 26, 51 或 76，因為 2^{1000} 是 4 的倍數，76 是唯一的可能。

注意：在 a，b 的證明中，我們使用了下面結果：

若 $x \equiv y \pmod{m}$

$u \equiv v \pmod{m}$

則 $xu \equiv yv \pmod{m}$ …………(1)

觀察法很簡單，但也有缺點。譬如它可能需要很長的時間才能算出 2^{1000} 的末四位。在這些情況時，下面的定理可能很有用。

定理 1 設 $(a, m) = 1$，

則 $a^{\varphi(m)} \equiv 1 \pmod{m}$

上式中的 $\varphi(m)$ 表示 $\leq m$ 且與 m 互質的正整數的個數。譬如說，當 p 是一個質數時，

$$\varphi(p) = p-1,$$

$$\varphi(p^n) = p^{n-1}(p-1) \cdots\cdots(2)$$

証明 設 $c_1, c_2, \cdots, c_{\varphi(m)}$ 為所有 $\leq m$ 且與 m 互質的正整數，易見

$$(ac_i, m) = 1,$$

且對不同的 i，j

$$ac_i \not\equiv ac_j \pmod{m}$$

故每一 ac_i 必與某一 c_j 同餘 $(\bmod\ m)$：

$$ac_i \equiv c_j \pmod{m}$$

且此種對應是一對一，映成。所以連乘起來時，根據(1)式

$$\prod_{i=1}^{\varphi(m)} (ac_i) \equiv \prod_{j=1}^{\varphi(m)} c_j \pmod{m}$$

即

$$\left(\prod_{i=1}^{\varphi(m)} c_i\right)\left(a^{\varphi(m)}-1\right) \equiv 0 \pmod{m}$$

因

$$(c_i, m) = 1, \ \forall i$$

於是

$$\left(\prod_{i=1}^{\varphi(m)} c_i, m\right) = 1$$

由此及上式可得到結論。

下面是定理 1 的一個簡單結果：

推論 若 p 是一個質數，且 $p \nmid a$，則

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

現在讓我們來計算 2^{1000} 的末四位，令定理中的 $a=2$，$m=5^4$，則有

$$2^{5^3(5-1)} \equiv 1 \pmod{5}$$

即 $2^{500} \equiv 1 \pmod{625}$

故 $2^{1000} \equiv 1 \pmod{625}$

即 $2^{1000} = 625k + 1$ ……………(3)

因為 2^{1000} 是 16 的倍數，且

$$625 = 16 \times 39 + 1$$

故 $k+1$ 是 16 的倍數。令 $k+1=16n$ 代入(3)，

$$\begin{aligned}2^{1000}&=625\times 16n-625+1\\&=10^4n-624\\&=10^4(n-1)+9376\end{aligned}$$

故 2^{1000} 的末四位是9376 。

有興趣的人士可找一些例子來試試定理 1 的威力。在結束本節之前，讓我們為 $\varphi(m)$ 做一補充：若 $(a, b)=1$，則

$$\varphi(ab)=\varphi(a)\varphi(b) \quad \cdots\cdots\cdots(4)$$

根據(2),(4)，函數 φ 的計算就變得相當簡單。譬如說，

$$\begin{aligned}&\varphi(840)\\&=\varphi(2^3\cdot 3\cdot 5\cdot 7)\\&=\varphi(2^3)\cdot\varphi(3)\cdot\varphi(5)\cdot\varphi(7)\\&=4\cdot 2\cdot 4\cdot 6\\&=192\end{aligned}$$

(4)式的證明應可在任何一本數論的書上找到。

Ⅱ. 2^{1000} 的最高兩位：

a. 利用計算機知 $\log 2=0.30102$（取五位小數），若考慮誤差，則有

$$0.30101<\log 2<0.30103$$

故

$$301.01<\log 2^{1000}<301.03 \quad \cdots\cdots(5)$$

上式表示 2^{1000} 有 302 位數，即

$$1\leq\frac{2^{1000}}{10^{301}}<10$$

根據(5)式，

$$0.01<\log\left(\frac{2^{1000}}{10^{301}}\right)<0.03$$

由計算機知

$$\log 1.1=0.04139>0.04$$

綜合得

$$\log 1.0\leq\log\left(\frac{2^{1000}}{10^{301}}\right)<\log 1.1$$

於是可知 2^{1000} 的最高兩位是 10 。

接下來的一個很自然的問題是我們能否算得更精確。譬如說 2^{1000} 的最高十位，或最高二十位。很明顯地，此時就是八位對數表也不適用。但是上面的方法依然正確，只要我們能很精確地計算 $\log 2$ 及 $\log x$，$1\leq x<10$ 的數值。理論上來說，這可以借助下面的方式來完成：

$$\log x=(\log_e x)/\log_e 10$$

$$\log_e(1+x)=\int_0^x\frac{1}{1+t}\,dt\ ,\ x\geq 0$$

$$\log_e(1+x)=x-\frac{x^2}{2}+\frac{x^3}{3}-\frac{x^4}{4}\cdots,$$

$$|x|<1$$

換句話說，我們必須自己製作對數表。

b. 下面的做法不使用對數表，所以也值得注意。

$$\begin{aligned}2^{1000}&=(1024)^{100}\\&=(10^3+24)^{100}\\&=10^{300}+\binom{100}{1}10^{297}\cdot 24\\&\quad+\binom{100}{2}10^{294}\cdot(24)^2\\&\quad+\cdots\cdots\cdots\end{aligned}$$

很明顯地右端前面的幾項比較重要，計算前面七項並且對其餘的項做誤差估計，也可以證明 2^{1000} 的最高兩位是 10 。

c. 有同學觀察到 2^1 到 2^{40} 的首位係以 2，4，8，1，3，6，1，2，5，1 的順序出現，因此猜測 2 的冪方的首位有循環性，且循環節長度為 10 ，於是 2^{1000} 的首位是 1 。這個答案是對的，但是方法正確嗎？

由於乘法是向左進位，現在的情況與計算末兩位時不同，基本上我們懷疑首位會有此種規律性。

假設 2 的冪方的首位每十個做一循環，那麼

$$[10^{\{(n+10)\log 2\}}]=[10^{n\log 2}] \quad \cdots(6)$$

其中 $\{x\}$，$[x]$ 分別表示 x 的小數及整數

部份。令

$$b = 10\log 2 - 3 = 0.0102 \cdots\cdots\cdots (7)$$

則(6)式表示對所有的 $n \in N$，$\{n\log 2\}$ 不會落在任何一個下面的區間

$$(-b+\log k, \log k),$$
$$2 \leq k \leq 10$$

因爲 b 是無理數（爲什麼？），我們可以引用下面定理

定理2 若 x 是無理數，則數列 $\{x\}$，$\{2x\}$，$\{3x\}$，…在區間 $(0,1)$ 上稠密。即對任意區間 $(a,b) \subseteq (0,1)$，我們都可以找到一個 $m \in N$ 使得

$$a < \{mx\} < b$$

於是得到一個矛盾。同理可知 2 的冪方的首位不可能以任意一個整數 k 做循環節長度，即它們不可能循環出現。當然 2^1 到 2^{1000} 的首位仍有可能每十個做一循環（即(6)式對 $1 \leq n \leq 990$ 成立），不過實際計算顯示

$$2^{41} = 2199023255552$$
$$2^{42} = 4398046511102$$
$$2^{43} = 8796093022204$$
$$2^{44} = 17592186044408$$
$$2^{45} = 35184372088816$$
$$2^{46} = 70368744177632$$

此種猜測的循環性在 2^{47} 時即不再成立。