「噢！數？」 拾例集　　周浩然輯

數論 － 同餘

摘要

1. 認識同餘式的基本性質：
   若　$a \equiv b(\mathrm{mod}\, m)$，則有
   (a)　$a \pm k \equiv b \pm k(\mathrm{mod}\, m)$
   (b)　$ak \equiv bk(\mathrm{mod}\, m)$
   (c)　$\frac{a}{k} \equiv \frac{b}{k}(\mathrm{mod}\, \frac{m}{(m,k)})$，特別地當 $(m,k)=1$，$\frac{a}{k} \equiv \frac{b}{k}(\mathrm{mod}\, m)$
2. 運用費馬（Fermat）小定理：
   當 p 為素數且 $(a,p)=1$ 時，$a^{p-1} \equiv 1(\mathrm{mod}\, p)$。
3. 運用歐拉（Euler）定理：
   當 $(a,m)=1$ 時，$a^{\varphi(m)} \equiv 1(\mathrm{mod}\, m)$，其中 $\varphi(m)$ 為歐拉函數。
4. 求某些整數算式的個位數字，即模十下的取值。
   (a)　$n^{4k+t} \equiv n^t$（mod 10），其中 $t=0,1,2,3$。
   (b)　$n^{m^k} \equiv n^4$（mod 10），當 m 為偶數且 k>1。
   $n^{m^k} \equiv n$（mod 10），當 m 為奇數且 k 為偶數。
   $n^{m^k} \equiv n^m$（mod 10），當 m 為奇數且 k 為奇數。
5. 解一次同餘方程或同餘方程組。
6. 認識及解中國剩餘問題：

$$\begin{cases} x \equiv b_1(\mathrm{mod}\, m_1) \\ x \equiv b_2(\mathrm{mod}\, m_2) \\ \quad\cdots \\ x \equiv b_n(\mathrm{mod}\, m_n) \end{cases}$$

，其中 $m_1, m_2, m_3, ..., m_n$ 倆倆互素。

作 $M_i = k_i m_1 ... m_{i-1} m_{i+1} ... m_n$ 及 $M_i = 1(\mathrm{mod}\, m_i)$，$i = 1,2,3,...n$。
中國剩餘問題的解為 $S \equiv b_1 M_1 + b_2 M_2 + b_3 M_3 + ... + b_n M_n$
（mod $m_1 m_2 m_3 ... m_n$）。

拾例

1. 若 n 除以 2004 時的餘數為 13，則 n^3 除以 2004 時的餘數是多少？（培正 2004 中四）

答：$n^3 \equiv 13^3 \equiv 2197 \equiv 193 \pmod{2004}$

所以餘數為 193。

2. 求 22^{33}、$22^{33^{55}}$ 的個位數字。

答：$22^{33} \equiv 2^{4\times 8+1} \equiv 2 \pmod{10}$，故其個位數字為 2。

$22^{33^{55}} \equiv 22^{33} \equiv 2 \pmod{10}$，故其個位數字亦為 2。

3. 若 $A = 19\times 199\times 1999\times\ldots\times(199\ldots999)$，當中最後一項為 1 之後有 1999 個 9。求 A 除以 1000 的餘數。

答：由於 $1999、19999、199999、\ldots \equiv -1 \pmod{1000}$

上式中有 $1999-3+1=1997$ 個數 $\equiv -1 \pmod{1000}$

故上式為 $19\times 199\times(-1)^{1997} \equiv -3781 \equiv 219 \pmod{1000}$

故餘數為 219。

4. 求 $5555^{6666}+6666^{5555}$ 除以 7 的餘數。

答：$1111 \equiv 5 \pmod 7$，

即 $5555 \equiv 5\times 5 \equiv 25 \equiv -3 \pmod 7$ 及 $6666 \equiv 6\times 5 \equiv 30 \equiv 2 \pmod 7$。

另由費馬小定理，可知 $2^6 \equiv 3^6 \equiv 1 \pmod 7$

即原式 $\equiv (-3)^{6666}+(2)^{5555} \equiv 3^{6666}+2^{5555} \pmod 7$

$\equiv 3^{6\times 1111}+2^{6\times 925+5} \equiv 1+2^5 \pmod 7$

$\equiv 33 \equiv 5 \pmod 7$

所以餘數為 5。

5. 求 2^{999} 的最末的兩位數。

答：求最末的兩位數即求 2^{999} 除以 100 的餘數。

由於 $(4,25)=1$，

2^{999} 是 4 的倍數，所以只考慮 2^{999} 除以 25 的餘數。

由於 $2^{10}+1 \equiv 1025 \equiv 0 \pmod{25}$，所以 $2^{10} \equiv -1 \pmod{25}$。

而 $2^{1000} \equiv (-1)^{100} \equiv 1 \pmod{25}$。

即 2^{1000} 的最末兩位數可能是 01、26、51、76。再由 2^{1000} 為 4 的倍數，所以其最末兩位數只可為 76。即 2^{999} 最末兩位數為 88。

6. 求 3^{999} 的最末的兩位數。

答： 由於 $100=2^2\times5^2$

$\phi(100)=100(1-\frac{1}{2})(1-\frac{1}{5})=100\times\frac{1}{2}\times\frac{4}{5}=40$

所以 $3^{1000}\equiv3^{25\times40}\equiv1(\text{mod}100)$，

即 $3^{999}\times3\equiv1(\text{mod}100)$。

由於 $201=3\times67$

故 $3^{999}\equiv67(\text{mod}100)$，即 3^{999} 最末兩位數為 67。

7. 1998^{10} 除以 10^4，所得的餘數為 b，求 b。（HKMO 1993/94 決賽團體）

答： $1998^{10}=(2000-2)^{10}$

$=2000^{10}+C_1^{10}\times2000^9\times2+...+C_9^{10}\times2000\times2^9+2^{10}$

所以 $1998^{10}\equiv2^{10}\equiv1024(\text{mod}10^4)$，故 $b=1024$。

8. 解同餘方程 $3x-9\equiv0(\text{mod}30)$。

答： 即 $x-3\equiv0(\text{mod}10)$， $x\equiv3(\text{mod}10)$。

9. 今有物不知其數，三三數之剩二，五五數之剩三，七七數之剩二，問物幾何？（孫子算經）

答： $x\equiv2(\text{mod}3)$、$x\equiv3(\text{mod}5)$、$x\equiv2(\text{mod}7)$

故 $x\equiv2\times70+3\times21+2\times15\equiv233\equiv23(\text{mod}105)$。

故該數最小值為 23，通式為 $23+105t$，其中 $t=0,1,2,...$。

10. 在 1 至 1000 之間，有多少對正整數，使它們的平方和能被 49 整除。（MMO 1940）

答： 設該兩正整數為 x,y 且 $x\geq y$。

若兩數同為 7 的倍數，正合題意。

但在 1 至 1000 之間共有 142 個 7 的倍數。

若 $x\neq y$，共有組合 $\frac{142\times141}{2}=10011$ 對，

若 $x=y$，共有組合 142 對。

由於在模七下，我們有 $\begin{cases}x^2\equiv1 & x\equiv\pm1\\ x^2\equiv4 & x\equiv\pm2\\ x^2\equiv2 & x\equiv\pm3\end{cases}$，

當中沒有兩數之和為 7 的倍數，更不會有 49 的倍數。

即 x,y 只可為 7 的倍數，故共有組合數 $10011+142=10153$。

淺問

1. 求下列各式的餘數：
   (a) $2^{100} \div 11$　　(b) $3^{1000} \div 19$

2. 試求 $10+10^2+10^3+10^4+\ldots+10^{2012}$ 除以 7 的餘數。

3. 若 $\sqrt[2003]{B}=2003$，求 B 的個位數字。（HKMO 2003/04 初賽個人）

4. 已知數列 1, 4, 8, 10, 16, 19, 21, 25, 30, 43 中相鄰的若干數之和能被 11 整除的數組共有多少組？

5. 求 243^{4002} 的最末四個位。

6. 求 1991^{2000} 除以 10^6 的餘數。

7. 求 $3^{2002}+5^{2002}$ 除以 64 時的餘數。（培正 2002 中四）

8. 求 $7\times19\times31\times\ldots\times1999$ 的最後兩位數字。（當中 7、19、31、…、1999 各數組成一個公差為 12 的等差數列。）(HKPSC 2003)

9. 解下列一次同餘方程：
   (a) $8x\equiv9(\mathrm{mod}11)$　　(b) $6x\equiv4(\mathrm{mod}8)$

10. 解下列一次同餘方程：
    (a) $3x+7\equiv10(\mathrm{mod}12)$　　(b) $6x+9\equiv8(\mathrm{mod}17)$

11. 解下列中國剩餘問題，並求其通式及最小值。
    (a) 某數以三數之，餘一；以五數之，餘二；以七數之，餘四。
    (b) 某數以三數之，餘一；以五數之，餘三；以九數之，餘六。
    (c) 某數以五數之，餘四；以六數之，餘三；以七數之，餘二。

12. 正整數 N 被 10、9、8、7、6、5、4、3 及 2 除所得的餘數依次是 9、8、7、6、5、4、3、2 及 1，求 N 的最小值。
    (HKMO 1989/90 初賽個人)(HKMO 2012/13 決賽團體)

13. 解同餘方程組 $\frac{x+2}{3}\equiv4(\mathrm{mod}11)$ 及 $\frac{5x-6}{7}\equiv8(\mathrm{mod}9)$。

詳答

1. (a) $2^{100} \div 11$

根據費馬小定理 $(2, 11) = 1$， $2^{10} \equiv 1 (\mathrm{mod} 11)$，

故 $2^{100} \equiv (2^{10})^{10} \equiv 1 (\mathrm{mod} 11)$。故餘數為 1。

(b) $3^{1000} \div 19$

根據費馬小定理 $(3, 19) = 1$，$3^{18} \equiv 1 (\mathrm{mod} 19)$，

故 $3^{1000} \equiv (3^{18})^{55} \times 3^{10} \equiv 3^{10} (\mathrm{mod} 11)$。而

3^n	1	2	3	4	5	6	7	8	9	10
餘數	3	9	27=8	24=5	15	45=7	21=2	6	18	54=16

故餘數為 16。

2. $10 \equiv 3 (\mathrm{mod} 7)$，即原式為 $x = 3^1 + 3^2 + 3^3 + 3^4 + ... + 3^{2012} (\mathrm{mod} 7)$，

但由於 $3^1 + 3^2 + ... + 3^6 \equiv 1 + 2 + 3 + 4 + 5 + 6 \equiv 0 (\mathrm{mod} 7)$，

故原式可化簡為 $x \equiv 3^{2011} + 3^{2012} \equiv 3 + 9 \equiv 12 \equiv 5 (\mathrm{mod} 7)$。

3 即求 $B = 2003^{2003} \equiv 3^{2003} (\mathrm{mod} 10)$。

留意 $3^2 \equiv 9 \equiv -1 (\mathrm{mod} 10)$，所以 $3^{2003} \equiv (-1)^{1001} \times 3 \equiv -3 (\mathrm{mod} 10)$。

故個位數字為 7。

4. 計算由第一項至第 n 項的和，組成新數列：

1, 5, 13, 23, 39, 58, 79, 104, 134, 177

再求其除以 11 的餘數，得：

1, 5, 2, 1, 6, 3, 2, 5, 2, 1

我們找到當中有三個 1、三個 2、兩個 5。指定數組 = $2 \times 3 + 1 = 7$ 組。

5. 由歐拉函數，得 $\varphi(10000)$ = $10000 \times \frac{1}{2} \times \frac{4}{5}$ = 4000

且 $(243, 10000) = 1$，故 $243^{4000} = 1 (\mathrm{mod} 10000)$。

$243^{4002} \equiv 243^2 \equiv 59049 \equiv 9049 (\mathrm{mod} 10000)$。

6. 原式 = $(1+1990)^{2000}$

= $1+C_1^{2000}(1990)+C_2^{2000}(1990)^2+C_3^{2000}(1990)^3+...+(1990)^{2000}$

= $1+2000(1990)+\frac{2000\times1999}{2}(1990)^2$

$+\frac{2000\times1999\times1998}{6}(1990)^3+...+(1990)^{2000}$

式中自第四項起，全是 10^6 的倍數，故得計算

$1+2000(1990)+\frac{2000\times1999}{2}(1990)^2$

= 1 + 3980000 + 7916239900000

= 7916243880001

故餘數為 880001。

7. $3^{2002}+5^{2002} \equiv (4-1)^{2002}+(4+1)^{2002}$ （mod 64）

$\equiv (4^{2002}-C_1^{2002}4^{2001}+C_2^{2002}4^{2000}+...+1)$

$+(4^{2002}+C_1^{2002}4^{2001}+C_2^{2002}4^{2000}+...+1) \pmod{64}$

$\equiv 2\times(4^{2002}+C_2^{2002}4^{2000}+C_4^{2002}4^{1998}+...+1) \pmod{64}$

$\equiv 2\times(C_{2000}^{2002}4^2+1) \equiv 2\times(C_2^{2002}16+1) \pmod{64}$

$\equiv 2\times(\frac{2002\times2001}{2}\times16+1) \pmod{64}$

$\equiv 1001\times2001\times32+2 \equiv 34$（mod 64）

8. 即求該乘積在模 100 的值，由於 $100=4\times25$，且（4, 25）= 1，故考慮該乘積分別除以 4 和 25 的餘數。

由於（12, 25）= 1，且該數列多於 25 項，故至少存有一項為 25 的倍數，即該乘積為 25 的倍數。

亦由於 7、19、31 等全是 $4n-1$ 型的整數，再加上該數列共有

$\frac{1999-7}{12}+1=167$ 項，即該乘積 $\equiv(-1)^{167}\equiv-1(\mathrm{mod}\,4)$。

總結，該乘積最末兩位為 75。

9. (a) 由於 $8\times7=56=5\times11+1$，故 $8\times7\equiv1(\text{mod}11)$。

$8x \equiv 9 \pmod{11}$

$56x \equiv 63 \pmod{11}$

$x \equiv 8 \pmod{11}$

(b) 原式等同 $3x\equiv2(\text{mod}4)$，

由於 $3\times3=9=2\times4+1$，故 $3\times3\equiv1(\text{mod}4)$

$3x \equiv 2 \pmod{4}$

$9x \equiv 6 \pmod{4}$

$x \equiv 2 \pmod{4}$

$x \equiv 2, 6 \pmod{8}$

10. (a) $3x+7 \equiv 10 \pmod{12}$

$3x \equiv 3 \pmod{12}$

$x \equiv 1 \pmod{4}$

$x \equiv 1, 5, 9 \pmod{12}$

(b) $6x+9 \equiv 8 \pmod{17}$

$6x \equiv -1 \pmod{17}$

$6x \equiv -18 \pmod{17}$

$x \equiv -3 \pmod{17}$

$x \equiv 14 \pmod{17}$

11. (a) $x\equiv1(\text{mod}3)$，$x\equiv2(\text{mod}5)$ 及 $x\equiv4(\text{mod}7)$。

$x\equiv15\times4+21\times2+70\times1\equiv172\equiv67(\text{mod}105)$，

最小值為 67，通式：$x=67+105n$，其中 $n=0,1,2,...$

(b) $x\equiv1(\text{mod}3)$ 和 $x\equiv6(\text{mod}9)$ 有矛盾，故無解。

(c) $x\equiv4(\text{mod}5)$，$x\equiv3(\text{mod}6)$ 及 $x\equiv2(\text{mod}7)$。

$x\equiv126\times4+175\times3+120\times2\equiv1269\equiv9(\text{mod}210)$，

最小值為 9，通式：$x=9+210n$，其中 $n=0,1,2,...$

12. N+1 可被 10、9、8、7、6、5、4、3 及 2 整除，再由於 N 取最小值，所以 $N+1=2^3\times3^2\times5\times7=2520$，所以 $N=2519$。

13. $x+2 \equiv 12 \pmod{11}$ 及 $5x-6 \equiv 56 \pmod{9}$

$x \equiv 10 \pmod{11}$ 及 $5x \equiv 62 \pmod{9}$

$x \equiv 10 \pmod{11}$ 及 $5x \equiv 35 \pmod{9}$

$x \equiv 10 \pmod{11}$ 及 $x \equiv 7 \pmod{9}$

綜合得 $x \equiv 10\times45+7\times55 \equiv 835 \pmod{99}$

$\equiv 43 \pmod{99}$