同餘的基本概念

許介彥

大葉大學　電信工程學系

兩個例子

假設今天是星期四，再過一天當然是星期五，兩天之後則爲星期六，請問：1000 天之後是星期幾？

這是一個簡單的問題。由於一個禮拜有七天，因此七天之後必爲星期四，14 天、21 天、28 天、…之後也都是星期四；由於 1000 除以 7 的餘數爲 6，因此 1000 天之後一定是某個星期四的六天之後，也就是星期三。

再看另一個例子：某艘太空船於某天傍晚六點發射升空，於幾天後的某天早上九點返回地表；幾個月之後此太空船於某天凌晨兩點再度發射升空。如果此太空船的第二次升空在空中停留的時間長短與上一次相同，那麼它再度回到地表的時間是早上或是下午的幾點鐘？

這個問題也不難。如果將一天的 24 小時看成是由 0 點至 23 點，那麼傍晚六點相當於 18 點，因此太空船的第一次升空在空中總共待了 $(24k+9-18)$ 個小時（k 爲某正整數），所以第二次升空回到地表的時間一定是凌晨兩點的 $(24k+9-18)$ 個小時之後；由於

$$\begin{aligned} 2+(24k+9-18) &= 24k-7 \\ &= 24(k-1)+17 \end{aligned}$$

因此第二次返回地表的時間一定是某天的 17 點，也就是傍晚五點。

以上兩個問題中，第一個問題的關鍵在求出 1000 除以 7 的餘數，第二個問題的關鍵在求出 $2+(24k+9-18)$ 除以 24 的餘數；這兩個問題的重點都是在餘數，至於商是多少則無關緊要。數學上，「求餘數」是相當重要的一個運算，本文將對其基本應用作一概略性的介紹。

同餘的定義

假設 a,b,m 都是整數；如果 $a-b$ 是 m 的整數倍，數學上常將 a 與 b 的關係記作

$$a \equiv b \pmod{m}$$

其中的 m 稱爲「模」（modulus）；我們將上面的式子讀作「a 與 b 對模 m 而言同餘」（"a and b are congruent modulo m."）。

舉例來說，17 與 52 對模 7 而言同餘（記作 $17 \equiv 52 \pmod{7}$），因爲 17 與 52 之差爲 7 的倍數（不論是 35 或是 −35 都是 7 的倍數）；請留意此時 17 與 52 除以 7 的餘數相同（都等於 3），這是「同餘」名稱的由來。讀者不難檢驗以下兩個式子也都是成立的：

$$21 \equiv 0 \pmod{3},$$

$$399 \equiv -1 \pmod{100}.$$

如果 $a-b$ 是 m 的倍數，$a-b$ 必定也是 $-m$ 的倍數，反之亦然，因此 $a \equiv b \pmod{m}$ 若且唯若 $a \equiv b \pmod{-m}$；我們通常將模限定爲非負整數。

模算術

同餘的記號（≡）在形狀上與一般算術運算式中的等號（=）很像，「同餘式」與「等式」在許多方面也相當類似。

舉例來說，如果

$$a \equiv b \pmod{m} \quad 且 \quad c \equiv d \pmod{m}$$

那麼以下三個式子一定都成立：

$$a+c \equiv b+d \pmod{m}$$

$$a-c \equiv b-d \pmod{m}$$

$$ac \equiv bd \pmod{m}$$

它們的證明都不難。以第一個式子爲例，由已知條件可知存在整數 s 與 t 使得

$$a = b+sm \quad 且 \quad c = d+tm$$

因此

$$a+c = (b+d)+m(s+t)$$

所以 $(a+c)$ 與 $(b+d)$ 之差爲 m 的倍數，也就是它們對模 m 而言同餘；其他兩個式子的證明也類似。由第三個式子我們又可推知如果 a 與 b 對模 m 而言同餘，下式對任意正整數 n 一定成立：

$$a^n \equiv b^n \pmod{m}.$$

雖然以上對同餘式兩邊所作的加、減、乘等算術運算看似平常，不過要將兩邊同時除以一個數時必須特別小心。如果 $k \neq 0$ 且

$$ak \equiv bk \pmod{m}$$

我們並不能像一般等式一樣直接將兩邊的 k 消掉（只有當 $\gcd(k,m)=1$ 時方可如此）；事實上，讀者不難自行證明：

$$ak \equiv bk \pmod{m}$$

若且唯若

$$a \equiv b \pmod{\frac{m}{\gcd(k,m)}}.$$

舉例來說，$6 \equiv 12 \pmod{2}$ 而且 2 與 3 互質，因此我們可以將上式兩邊的 3 約掉而得 $2 \equiv 4 \pmod{2}$，但是我們不能由上式導出 $3 \equiv 6 \pmod{2}$（此式顯然是錯的），因爲 $\gcd(2,2) = 2 \neq 1$。

和同餘式有關的另一個重要性質是：如果 k 是 m 的因數而且 $a \equiv b \pmod{m}$，那麼 $a \equiv b \pmod{k}$；道理很簡單，因爲當 $a-b$ 是 m 的倍數，$a-b$ 必定也是 k 的倍數。

求餘數方面的應用

例題一：

試求出 2^{90} 除以 11 的餘數。

解：對模 11 而言，

$$2^{90} \equiv 4^{45} \equiv 4 \cdot 4^{44} \equiv 4 \cdot 16^{22}$$

$$\equiv 4 \cdot 5^{22} \quad （因爲 16 \equiv 5）$$

$$\equiv 4 \cdot 25^{11} \equiv 4 \cdot 3^{11} \equiv 12 \cdot 3^{10}$$

$$\equiv 9^5 \equiv 9 \cdot 9^4 \equiv 9 \cdot 81^2 \equiv 9 \cdot 4^2$$

$$\equiv 9 \cdot 5 \equiv 45 \equiv 1$$

因此 2^{90} 除以 11 的餘數一定是 1。

由上面這個例子讀者不難體會模算術的「威力」。2^{90} 是一個相當大的數，如果我們打算先將 2^{90} 的值算出來然後再將其除以 11 求餘數，理論上雖然可行，實際做起來不僅計算量相當龐大而且很容易出錯（尤其如果沒有電腦或其他工具輔助的話）；有了模算術的觀念後，即使只靠紙跟筆，我們都能輕鬆地在短時間之內將此問題解決。

例題二：

求證：對任意正整數 n，$3^{2n+1} + 2^{n+2}$ 必爲 7 的倍數。

證明：對模 7 而言，

$$3^{2n+1}+2^{n+2}\equiv 3(3^2)^n+4\cdot 2^n$$
$$\equiv 3\cdot 2^n+4\cdot 2^n\equiv 2^n(3+4)$$
$$\equiv 2^n\cdot 0\equiv 0$$

因此 $3^{2n+1}+2^{n+2}$ 一定是 7 的倍數。

剛看到這個題目，許多讀者想到的方法可能是數學歸納法（不妨一試），不過利用同餘的觀念我們可以作得更快而且更漂亮。

例題三：

求出所有會使得 2^n+1 是 3 的倍數的正整數 n。

解：n 須滿足

$$2^n+1\equiv 0 \pmod 3$$
$$2^n\equiv -1 \pmod 3$$
$$(-1)^n\equiv -1 \pmod 3$$

因此 2^n+1 是 3 的倍數若且唯若 n 爲正奇數。一般而言，對任意正整數 m 及正奇數 n，$(m-1)^n+1$ 必定是 m 的倍數。

例題四：

求證：一個數字和爲 15 的整數（如 816，$8+1+6=15$）不可能是一個完全平方數。

證明：

對任意正整數 n，

$$n\equiv 0,\pm 1,\pm 2,\pm 3,\pm 4 \pmod 9$$
$$n^2\equiv 0,1,4,7 \pmod 9$$

因此 n^2 的數字和除以 9 的餘數只有 0, 1, 4, 7 等四種可能（見 [1]），然而 $15\equiv 6 \pmod 9$，因此一個數字和爲 15 的數不可能是一個完全平方數。

例題五：

試求出 9^{9^9} 的末兩個阿拉伯數字。

解：

一個數的末兩位數就是該數除以 100 的餘數。由例題三可知 $9^9\equiv -1\equiv 9 \pmod{10}$，因此存在正整數 n 使得 $9^9=10n+9$。

由二項式定理將 $(10-1)^9$ 展開得

$$(10-1)^9=10^9-C_1^9 10^8+\cdots+C_8^9\cdot 10-1$$

其中除了最後兩項之外的每一項都是 100 的倍數，因此

$$9^9\equiv 9\cdot 10-1\equiv 89 \pmod{100}$$
$$9^{10}\equiv 9\cdot 89\equiv 1 \pmod{100}$$

所以對模 100 而言，

$$9^{9^9}\equiv 9^{10n+9}\equiv (9^{10})^n\cdot 9^9\equiv 89$$

所求的末兩位數爲 8 和 9。

例題六：

求證：對任意四個整數 a,b,c,d 而言，

$$P=(a-b)(a-c)(a-d)(b-c)(b-d)(c-d)$$

一定是 12 的倍數。

證明：

我們先證明 P 一定是 4 的倍數。由於任何整數除以 4 的餘數有 0, 1, 2, 3 四種可能，因此我們可以將所有的整數依除以 4 的餘數是多少分成四類。如果 a,b,c,d 當中有某兩數屬於同一類（即除以 4 的餘數相同），此兩數的差必是 4 的倍數，因此 P 將是 4 的倍數。如果 a,b,c,d 當中沒有任何兩數屬於同一類，那麼它們除以 4 的餘數必爲 0, 1, 2, 3 四數，因此 a,b,c,d 當中有兩個奇數及兩個偶數；由於兩個奇數之差與兩個偶數之差都是偶數，此時的

P 也必定是 4 的倍數。

接著我們證明 P 一定是 3 的倍數。任何整數除以 3 的餘數有 0, 1, 2 三種可能，根據鴿籠原理，a,b,c,d 四數中必有某兩數除以 3 的餘數相同，而此兩數之差必是 3 的倍數，因此 P 是 3 的倍數。

由於 P 既是 4 的倍數又是 3 的倍數，P 一定是 12 的倍數。

重複的字尾

五位數 85222 的最後三個位數都是 2，177 的結尾則有兩個 7；以下我們將利用同餘的觀念來解決兩個與整數的重複字尾有關的問題。

例題一：

一個正整數的平方（即完全平方數）的字尾最多可以重複多少個不是 0 的數字？

解：

我們先看看哪些阿拉伯數字可以作爲一個完全平方數的個位數（也就是除以 10 的餘數）。對任意正整數 n，

$$n \equiv 0, \pm 1, \pm 2, \pm 3, \pm 4, 5 \pmod{10}$$

因此

$$n^2 \equiv 0, 1, 4, 9, 6, 5 \pmod{10}$$

所以一個平方數的個位數不可能是 2,3,7,8；由於本題不考慮字尾爲 0 的情形，因此我們只須考慮個位數爲 1,4,5,6,9 的平方數。

n 有奇數與偶數兩種可能。當 n 爲偶數，n^2 一定是 4 的倍數；當 n 爲奇數，n^2 除以 4 一定餘 1（由 $(2k+1)^2$ 展開可知），因此

$$n^2 \equiv 0, 1 \pmod{4}.$$

一個末兩位數爲 11 的數除以 4 的餘數必爲 3，因此一個平方數的末兩位數不可能是 11。同理，一個平方數的末兩位數也不可能是 55,99（除以 4 餘 3）或 66（除以 4 餘 2）；因此一個平方數的結尾如果有重複的數字，這個數字只可能是 4。我們剩下的問題是：一個平方數結尾的 4 最多可以重複幾次？

我們知道至少可以重複兩次，因爲 $12^2 = 144$ 是我們熟悉的平方數。有可能重複四次嗎？如果我們將 n 表爲 $100x + y$，其中的 y 是 n 的末兩位數，那麼當 n^2 的結尾有四個 4 時，下式將成立：

$$(100x + y)^2 \equiv 4444 \pmod{10000}$$

從而

$$(200x + y)y \equiv 4444 \pmod{10000}$$

y 顯然必是偶數，因爲 4444 與 10000 都是偶數；如果 $y = 2z$，那麼

$$4(100x + z)z \equiv 4444 \pmod{10000}$$

$$(100x + z)z \equiv 1111 \pmod{2500}$$

$$(100x + z)z \equiv 1111 \pmod{4}$$

因此 $z^2 \equiv 3 \pmod{4}$，但這是不可能的（如前所述，平方數除以 4 的餘數只可能是 0 或 1），因此一個平方數的末四位不可能全是 4。

有沒有可能有三個 4 呢？答案是肯定的，其中最小的數是 $1444 = 38^2$。

例題二：

某數列 $a_1, a_2, a_3, \ldots$ 以遞迴的方式定義如下：

$$a_n = \begin{cases} 9 & n = 0 \\ 3a_{n-1}^4 + 4a_{n-1}^3 & n > 0 \end{cases}$$

求證：對任意非負整數 n，a_n 的最後 2^n 個數字都是 9。

解：我們只要能證明對任意非負整數 n，

$$a_n \equiv -1 \pmod{10^{2^n}}$$

即可；這項工作可由數學歸納法完成。

首先，當 $n=0$ 時，$a_0=9$，此時 a_0 的結尾的確有 $2^0=1$ 個 9。接著假設所要證明的性質對某個非負整數 n 而言成立，也就是存在整數 k 使得

$$a_n = 10^{2^n}k - 1$$

那麼

$$a_{n+1} = 3a_n^4 + 4a_n^3 = a_n^3(3a_n + 4)$$
$$= (10^{2^n}k - 1)^3(3(10^{2^n}k - 1) + 4)$$

對模 $10^{2^{n+1}}$（$=10^{2\cdot 2^n}$）而言，

$$a_{n+1} \equiv (3\cdot 10^{2^n}k - 1)(3\cdot 10^{2^n}k + 1)$$
$$\equiv 9\cdot 10^{2\cdot 2^n}k^2 - 1 \equiv -1$$

也就是說，a_{n+1} 的結尾有 2^{n+1} 個 9，因此根據數學歸納法得證：對任意非負整數 n，a_n 的最後 2^n 個數字全都是 9。

在不定方程的應用

同餘的觀念對解決與不定方程有關的許多問題（例如求出某方程式所有的解或是證明某方程式無解或有無窮多解等）相當有幫助；以下我們看幾個例子。

例題一：

求出 $2^n + 7 = x^2$ 的所有整數解。

解：n 不可能是負數或 0，因此 2^n+7 一定是奇數，等號右邊的 x 一定也是奇數；又由於任何奇數的平方除以 4 一定餘 1，因此

$$2^n + 7 \equiv 1 \pmod 4$$
$$2^n \equiv 2 \pmod 4$$

n 顯然只可能是 1，此時 $x=\pm 3$；除此之外再無其他可能。

例題二：

證明 $2003 = x^2 + y^2$ 沒有整數解。

解：由於

$$x^2 \equiv 0,1 \pmod 4$$
$$y^2 \equiv 0,1 \pmod 4$$

因此

$$x^2 + y^2 \equiv 0,1,2 \pmod 4$$

但是 2003 除以 4 的餘數卻是 3，所以方程式不可能有解。

例題三：

求出 $2^m - 3^n = 1$ 的所有正整數解。

解：$3^2 \equiv 1 \pmod 8$，因此對任意正整數 k，$3^{2k} \equiv 1 \pmod 8$ 且 $3^{2k+1} \equiv 3 \pmod 8$，換句話說，對任意正整數 n，$3^n + 1 \equiv 2,4 \pmod 8$；然而對所有大於 2 的正整數 m 而言，$2^m \equiv 0 \pmod 8$，因此方程式 $2^m = 3^n + 1$ 只可能在 $m \le 2$ 時有解。

當 $m=1$，$2 = 3^n + 1$ 顯然沒有正整數解；當 $m=2$，由 $2^2 = 3^n + 1$ 得 $n=1$，因此 $(m,n)=(2,1)$ 是 $2^m - 3^n = 1$ 唯一的一組正整數解。

例題四：

求出 $5^x \cdot 7^y + 4 = 3^z$ 的所有非負整數解。

解：由於等號左邊至少是 4，因此 z 不爲 0，等號兩邊一定都是 3 的倍數。

對模 3 而言，$3^z \equiv 0$，因此

$$5^x \cdot 7^y + 4 \equiv (-1)^x \cdot 1^y + 1 \equiv 0 \pmod 3$$

我們推知 x 一定是正奇數。

對模 5 而言，

$$5^x \cdot 7^y + 4 \equiv 4 \equiv 3^z \pmod 5$$

如果我們分別計算 $3^1, 3^2, 3^3, \cdots$ 除以 5 的餘數，所得的數列爲 $3, 4, 2, 1, 3, 4, 2, 1, \cdots$，每四個數一個循環，因此 $z \equiv 2 \pmod 4$，z 可能的值爲 $\{2, 6, 10, 14, 18, \ldots\}$。

如果 z 等於 2，$5^x \cdot 7^y$ 將等於 5，由此可得方程式的一組解：$(x, y, z) = (1, 0, 2)$。

如果 $z > 2$，z 可寫爲 $2k$（$k > 1$），此時

$$5^x \cdot 7^y = 3^{2k} - 4 = (3^k - 2)(3^k + 2)$$

等號右邊的兩數之差爲 4，因此這兩數不可能同時是 5 的倍數或同時是 7 的倍數；有可能其中一個等於 5^x 而另一個等於 7^y，或者其中一個等於 $5^x \cdot 7^y$ 而另一個等於 1。

如果兩數的其中一個等於 $5^x \cdot 7^y$ 而另一個等於 1，$3^k - 2$ 與 $3^k + 2$ 兩數中一定是較小的 $3^k - 2$ 等於 1，但是這樣一來 $k = 1$，與 $k > 1$ 矛盾。

如果 $3^k - 2$ 與 $3^k + 2$ 之中有一個等於 5^x 而另一個等於 7^y，那麼存在正整數 x 與 y 使得 5^x 與 7^y 之差爲 4；以下我們將說明這是不可能的。

x 顯然一定大於 1，因爲當 x 等於 1 時，$5^1 - 4$ 與 $5^1 + 4$ 都不是 7 的正整數次方。當 $x \geq 2$，5^x 的末兩位一定是 25；如果 5^x 與 7^y 之差爲 4，7^y 的末兩位一定是 21 或 29，但是對任意正整數 y 而言，

$$7^y \equiv 7, 49, 43, 1 \pmod{100}.$$

因此，$(x, y, z) = (1, 0, 2)$ 是 $5^x \cdot 7^y + 4 = 3^z$ 唯一的一組非負整數解。

猴子與椰子

有五個人和一隻猴子一起被困在一座荒島上。某天，這五人辛苦地從島上各處收集到 n 粒椰子，打算隔天一早大家將椰子平分。

半夜裡，其中一人因爲不信任其他同伴而悄悄起身來到椰子堆旁，他爲了要安撫猴子而將一粒椰子丟給猴子，並發覺剩下的椰子數剛好可以平分成五份；這個人將屬於自己的一份搬到一個隱密的地方藏好後才安心地回去睡覺。

過了不久，另一個人也起來了，他做了和第一個人相同的事：將一粒椰子丟給猴子，剩下的椰子也剛好可以分成五等份，他也將其中一份搬到隱密的地方藏好後才回去睡覺。不止這兩個人，其他三人也都在半夜裡陸續偷偷爬起來做了相同的事。

隔天早上，當這五個人一起來到椰子堆旁邊時，他們發覺剩下的椰子剛好可以分成五等份。

請問：n 最小是多少？

這是一個有名的問題，英文常稱作 the Monkey and Coconuts problem。爲了書寫方便，我們令 $A = 4/5$，那麼第一個人留下的椰子數爲 $A(n-1)$，第二個人留下的椰子數爲

$$A\big(A(n-1)-1\big) = A^2(n-1) - A$$

第三個人留下的椰子數爲

$$A\big(A^2(n-1) - A - 1\big) = A^3(n-1) - A^2 - A$$

第四個人留下的椰子數爲

$$A^4(n-1) - A^3 - A^2 - A$$

最後一人留下的椰子數爲

$$A^5(n-1) - A^4 - A^3 - A^2 - A$$

$$= A^5(n-1) - \frac{A^5 - A}{A-1}$$

$$= A^5\left(n-1-\frac{1}{A-1}\right) + \frac{A}{A-1}$$

由題意知此數須爲 5 的倍數；由 $A = 4/5$ 得

$$\left(\frac{4}{5}\right)^5 (n+4) - 4 \equiv 0 \pmod 5$$

$$\left(\frac{-1}{5}\right)^5 (n+4) \equiv -1 \pmod 5$$

$$\frac{n+4}{5^5} \equiv 1 \pmod 5$$

因此 $$\frac{n+4}{5^5} = 5k+1$$

$$n = 5^5(5k+1) - 4$$

其中的 k 可以是任何不會使得 $n < 0$ 的整數，因此當 $k = 0$ 時 n 有最小值：

$$n = 5^5 - 4 = 3121$$

也就是說，一開始的椰子數最少爲 3121 粒。

練習題

以下是幾個與本文相關的問題，提供讀者參考。

1. 試證：如果 a 與 b 爲已知整數且對任意正整數 m，$ax + b \equiv 0 \pmod m$ 都有解，那麼方程式 $ax + b = 0$ 一定有整數解。
2. 分別求出以下兩數的的末兩個數字。
   (1) 2^{10000} (2) 9^{9^9}
3. 證明 $1599 = x_1^4 + x_2^4 + x_3^4 + \cdots + x_{14}^4$ 沒有整數解。（提示：模 16）
4. 求出 $3^m - 2^n = 1$ 的所有正整數解。
5. 下面這個數是 7 的倍數：

   888…88A999…99

   其中的 A 是某個阿拉伯數字，A 的前面及後面分別有 50 個 8 及 50 個 9。請問 A 是多少？（提示：$7 \mid 1001$）
6. 假設當 n 爲奇數時，我們定義 $n!!$ 等於 $n(n-2)(n-4)\cdots 3\cdot 1$，當 n 爲偶數時則定義 $n!!$ 等於 $n(n-2)(n-4)\cdots 4\cdot 2$。試證：$2001!! + 2002!!$ 是 2003 的倍數。
7. 以下是本文椰子與猴子問題的幾個變形，請分別求出最初的椰子數的最小值。
   (1) 島上有四人而非五人。（答案：765 粒）
   (2) 猴子有兩隻，因此每個人在半夜各丟了兩粒椰子給猴子。（答案：6242 粒）
   (3) 隔天早上這五人要分椰子時，發覺還是須先丟一粒椰子給猴子，剩下的椰子才可分成五等分。（答案：15621 粒）

結語

同餘式與等式在許多方面類似其實並不足爲奇，因爲等式可以說是同餘式在模爲 0 時的特例；當 $a \equiv b \pmod 0$，$a - b$ 爲 0 的倍數，也就是 0，因此 $a = b$。

同餘的記號是大數學家高斯（C.F. Gauss, 1777–1855）的發明，從西元 1801 年問世以來陸續爲數論引入了相當多新的定理；其基本概念雖然簡單卻很有用，值得介紹給中學學生。

參考資料

1. 許介彥（2002），神奇的數字 9，科學教育月刊，第 246 期。
2. K. H. Rosen, *Elementary Number Theory And Its Applications,* 4th edition, Addison-Wesley, 1999.