關於一個同餘問題的猜想及其證明

文 | 曾鷹　李守球　劉增榮　魏澤夫

一、問題的提出

在數學課外興趣小組活動當中，我發現了一個十分有趣的現象：4^{22} 的末兩位元數字與 4^2 的末兩位元數字相同，再試一下發現：3^{26}的末兩位元數字與 3^6 的末兩位元數字也相同！由此我產生了一個猜想：對於a,b,n均為大於1的正整數，若 $a\equiv b\ (\mathrm{mod}20)$ ，則 $n^a\equiv n^b\ (\mathrm{mod}100)$。

二、問題的解決

由於餘數問題是一種週期現象，因此我利用電腦程式設計中的迴圈語句編寫了一個程式，當在電腦上運行程式之後顯示：我提出的猜想完全正確。對此我非常興奮！興奮之餘，我覺得這僅僅是用電腦給出的證明，如何用傳統方法證明呢？我立刻開始着手新的證明，但是在證明$25|n^b(n^{a-b}-1)$時遇到了困難，在老師的幫助下，我終於完成了如下的證明：

證明：不妨設 $a\geq b$，若要證

$n^a-n^b\equiv 0\ (\mathrm{mod}100)$，則只需證 $100\mid n^b(n^{a-b}-1)$.

1. 首先證明 $4|n^b(n^{a-b}-1)$

（1）當 n 為正偶數時，設 $n=2k$，$k\in N_+$。

由 $b>1$ 且 $b\in N$ 可知，$4|(2k)^b$ ，$\therefore 4|n^b$；

（2）當n為正奇數時，設 $n=2m+1$，$m\in N$。

$\because a\equiv b(\mathrm{mod}20)$，$\therefore 20|(a-b)$，設 $a-b=20k$，$k\in N$，則$n^{a-b}=n^{20k}=(2m+1)^{20k}$

$=(4m^2+4m+1)^{10k}=[4(m^2+m)+1]^{10k}$，由同餘的性質可知 $[4(m^2+m)+1]^{10k}\equiv 1(\mathrm{mod}4)$。

$\therefore n^{a-b}\equiv 1\ (\mathrm{mod}4)$ ，$\therefore 4|(n^{a-b}-1)$。

綜合（1）,（2）可知，$4|n^b(n^{a-b}-1)$。

2. 其次證明 $25|n^b(n^{a-b}-1)$

$\because\ 2^{20}=2^{10\times2}=1024^2=(25\times41-1)^2$

$=(25\times41)^2-2(25\times41)+1$ ，$\therefore\ 2^{20}\equiv 1(\mathrm{mod}25)$。

下面證明當 n 取3至25之間的整數時，恒有 $n^{20}\equiv 1(\mathrm{mod}25)$.

（1）當 n 取 5、10、15、20、25時，由 $b>1$ 且 $b\in N$ 可知，顯然 $n^{20}\equiv 1(\mathrm{mod}25)$ ；

（2）當 $n=2k$，$2<k<13$且 $k\in N$時，由於已證出$2^{20}\equiv 1(\mathrm{mod}25)$，故 $n^{20}\equiv 1(\mathrm{mod}25)$；

（3）當 $n=3$ 時，$3^{20}=3^{5\times4}=243^4=(25\times9+18)^4$ $=25u+18^4$，其中 u 為正整數，而$18^4=324^2$ $=(25\times13-1)^2=(25\times13)^2-2\times(25\times13)+1$，故 $18^4\equiv 1\ (\mathrm{mod}25)$，$\therefore\ 3^{20}-1\equiv 0(\mathrm{mod}25)$，$\therefore\ 3^{20}\equiv 1\ (\mathrm{mod}25)$；

（4）當 $n=7$ 時，$\because 7^4=2401=25\times96+1$，$\therefore 7^4-1\equiv 0(\mathrm{mod}25)$，$\because\ 7^{20}=7^{4\times5}$，$\therefore 7^{20}\equiv 1(\mathrm{mod}25)$；

（5）當 $n=9$ 時，$\because\ 9^{20}=3^{20\times2}$，由（3）可知 $3^{20}\equiv 1\ (\mathrm{mod}25)$，$\therefore 9^{20}\equiv 1\ (\mathrm{mod}25)$；

（6）當 $n=11$ 時，$11^{20}=11^{5\times4}=161051^4=(25\times6442+1)^4$，$\therefore 11^{20}\equiv 1\ (\mathrm{mod}25)$ ；

（7）當 $n=13$ 時，$\because 13^{20}=13^{4\times5}=(25\times1142+11)^5$

$=25u+11^5$，其中 u 為正整數，

由（6）可知 $11^{20}\equiv1 \pmod{25}$，$\therefore 13^{20}\equiv 1 \pmod{25}$；

（8）當 $n=17$ 時，$\because 17^{20}=17^{4\times5}=83521^5=(25\times3340+21)^5=25t+21^5$，其中 t 為正整數。而 $21^5=4084101=25\times163364+1$，

$\therefore 17^{20}\equiv 1 \pmod{25}$；

（9）當 $n=19$ 時，$\because 19^{20}=19^{2\times10}=361^{10}=(25\times14+11)^{10}=25v+11^{10}$，其中 v 是正整數。

由於 $11^{10}=11^{5\times2}=161051^2=(25\times6442+1)^2$

$=25t+1\equiv 1 \pmod{25}$，故 $19^{20}\equiv 1 \pmod{25}$；

（10）當 $n=21$ 時，$\because 21^{20}=3^{20}\times7^{20}$，$\therefore$ 由（3）和（4）可知，$21^{20}\equiv1 \pmod{25}$；

（11）當 $n=23$ 時，$\because 23^{20}=23^{2\times10}=529^{10}$

$=(25\times21+4)^{10}=25p+4^{10}$，其中 p 為正整數。由（2）可知，$4^{10}=2^{20}\equiv1 \pmod{25}$，

$\therefore 23^{20}\equiv 1 \pmod{25}$.

綜上討論，對於任意大於1 的正整數 a,b,n，且 $a\geq b$，恆有 $n^{a-b}\equiv 1 \pmod{25}$；

$\therefore$ 若 a,b,n 均為大於1的正整數，且 $a>b$，$a\equiv b \pmod{20}$，則 $100|n^{20}(n^{a-b}-1)$。

由此便證明了：設 a,b,n 均為大於1的正整數，若 $a\equiv b \pmod{20}$，則 $n^a\equiv n^b \pmod{100}$。

教師評語： 我們非常欣賞曾鷹同學研究問題的思想方法和科學態度。他能夠細心觀察和思考，由特例提出猜想，然後用電腦驗證猜想，同時嘗試用傳統方法證明猜想。這體現了現代中學生的一個重要特徵：主動運用資訊技術解決問題，同時也體現了近代數學研究的方向──借助電腦加快研究進程，迅速接近問題的實質。

實際上，此題可以利用歐拉定理給出一個十分簡捷的證明：

證明：只需證 $n^a-n^b\equiv0 \pmod 4$ …（1）以及 $n^a-n^b\equiv0 \pmod{25}$ …（2）同時成立。

設 $a\geq b$，$\because a\equiv b \pmod{20}$，

$\therefore a=b+20k\,(k\in N)$，則 $n^a-n^b=n^b(n^{20k}-1)$。

1. 當 $2|n$ 時，易知 $n^a\equiv0 \pmod 4$，且 $n^b\equiv0 \pmod 4$ 故（1）式成立；當2不能整除 n 時，則 $n^2\equiv1 \pmod 4$，

$\therefore n^{20k}\equiv1 \pmod 4$。故（1）式得證；

2. 當 $5|n$ 時，易知 $n^b\equiv0 \pmod{25}$；當5不能整除 n 時，由歐拉函數[1] 可知 $\varphi(25)=20$，由歐拉定理[2] 知 $n^{\varphi(25)}=1 \pmod{25}$，故 $n^{20}=n^{\varphi(25)}\equiv1 \pmod{25}$，

$\therefore n^{20k}\equiv1 \pmod{25}$，故（2）式得證。

綜上，$n^a\equiv n^b \pmod{100}$ 得證。

【註釋】

1. **歐拉函數**：因為模 n 共有 n 個不同的剩餘類，即 $M_i=\{x|x\in Z, x\equiv i \pmod n\}$，$i=0, 1, \cdots, n-1$。易知，若 i 與 n 互素，則同餘類 M_i 中所有的數都與 n 互素，這樣的同餘類稱為模 n 的縮同餘類，記模 n 的縮同餘類的個數為 $\varphi(n)$，此函數稱為歐拉函數。
2. **歐拉定理**：設 n 為大於1 的整數，a 是與 n 互素的任意整數，$\varphi(n)$ 為歐拉函數，則 $a^{\varphi(n)}\equiv1 \pmod n$。

曾鷹

濠江中學學生。

李守球

濠江中學教師。

劉增榮

濠江中學教師。

魏澤夫

吉林省吉林市第一中學教師。