數論中的華林問題

本文取材自Rademacher及Toeplitz的數學欣賞（The enjogment of mathematics），凡異出版社印行。

林克瀛

將正整數的平方排成數列：1，4，9，16，25，……可看出相鄰兩數間隔越來越大。也就是說，絕大部分的整數都不是平方。但許多數却可以寫成兩個平方之和，例如 13＝9＋4，41＝25＋16。如果我們想把6寫成兩個平方之和，由於比6小的平方只有1和4，而1＋1，1＋4，4＋4都不等於6，因此至少需要三個平方，即6＝4＋1＋1。同理可證7不可能寫成三個平方之和，最少要四個平方，即7＝4＋1＋1＋1。這樣看來，似乎比較大的數需要表示成更多個平方的和。令人驚奇的是在十七世紀，法國大數學家費馬（Fermat）證明每一個正整數都可以表示成最多四個平方之和。

華林（Waring）猜想對立方，四次方等，也有類似的事實，但他未能證明，後來這些問題就稱爲華林問題。整數的立方是1，8，27，64……若把比8小的數例如7表示爲立方之和，則必須完全用1，因此7＝1＋1＋1＋1＋1＋1＋1需要七個立方。同理可知15＝8＋1＋1＋1＋1＋1＋1＋1需要八個立方，而23＝8＋8＋1＋1＋1＋1＋1＋1＋1需要九個立方。

數學家賈可貝（Jacobi）利用心算天才達司（Dahse）列出一張表，顯示出每一整數分解爲最少個立方之和。從表上看出23以後下一個需要九個立方的數是239。這張表一直算到12000，其中只有上述兩個數需要九個立方。需要八個立方的數只有 15，22，50，114，167，175，186，212，213，238，303，364，420，428，454。以後一直到12000的數都不需要八個立方。需要七個立方的數有7，14，21，42，47，49，61，77，85，87，103，……，5306，5818，8042。後來許多人繼續計算仍然找不到需要七，八，或九個立方的其他整數。

這些計算本身不能證明什麼，但它强烈暗示每一數可表示爲最多九個立方之和，並且自從某一數開始每一數只是最多八個，甚至七個立方之和。藍道 Landau 首先證實（使用很困難的數學方法）自某一數起每一數均可表示爲最多八個立方之和，後來Wieferich 證明任何數均可表示爲最多九個立方之和。

四次方也有類似的性質，它們依次是1，16，81，256，…… 所以 15 需要十五個四次方，31 需要十六個，47 需要十七個，63 需要十八個，79 需要十九個。問題是十九個四次方是否永遠足夠？許多人研究這個問題。劉維 Liouville 證明 53 個四次方一定足夠，後來此數漸漸縮小爲47，45，41，39，38，後來Wieferich 得到 37。但這個結果比由經驗所發現的 19 仍大得太多了。

德國的大數學家希爾伯Hilbert 由不同的角度來攻擊這個一般的問題。他並不嘗試改進以前的計算，而考慮整個立方，四次方，等等的問題。他一口氣證明了對任何 k 次方而言，每一整數

必可寫成最多$N(k)$個k次方之和。但是他只證明N的存在，至於N本身的大小却不知道，不過顯然k越大時N也跟著增大。

英國的哈代Hardy和李特烏Littlewood用更困難及複雜的方法來處理華林問題。他們證明從某一數起每一個數均可表示爲最多十九個四次方之和，但此一數是天文數字，因此迄今仍無法以計算機驗算比這個數小的數是否可以表示爲最多十九個四次方之和。他們還得到許多其他的結果。華林在1782年劍橋出版的一本書中提到他的猜想如下：每一個整數n均可表示爲最多

$$I=2^k+q-2$$

個k次方之和，其中q是不大於$(3/2)^k$的最大整數。當

$$n=2^kq-1$$

時，確實需要這麼多個k次方，因爲此數比3^k小，因此只能表示爲1^k及2^k之和。哈代的結果發表於1925，Dickson及Pillai在1936和以後的研究中（經過Niven的改進）證明當$k\geq 6$時上述公式中的I值的確對所有的整數n都成立，只要

$$(\frac{3}{2})^k-q<1-\frac{q}{2^k}$$

根據Lehmer，Selfridge，Stemmler等人的計算這個條件對$2\leq k\leq 200{,}000$的k值均成立。並且Makler於1957證明至多只有有限個k值不滿足上述條件，而且迄今仍找不到一個不滿足上述條件的k值。如果這些特殊的k值是存在的話，$N(k)$也已經決定了。當$k=2$，3時，I＝4，9早已證明是正確的，但當$k=4$，5時，目前只知道

$$19\leq N(4)\leq 35,$$
$$37\leq N(5)\leq 54.$$

下面我們將證明最簡單的情形，即每一整數均可寫成最多四個平方之和。證明中需用下面的代數恒等式

$$(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2 \quad \cdots\cdots (1)$$

此式對任意$abcd$之值均成立，只要展開兩端就可證明。由(1)式可知如果兩個數中，每一個都是兩個平方之和，則兩數之乘積也可寫成二個平方之和。例如$13=9+4$及$41=25+16$。由(1)式知

$$533=13\cdot 41=23^2+2^2.$$

十八世紀的瑞士大數學家奧衣勒Euler發現了下面的恒等式：

$$\begin{aligned}&(a_1^2+a_2^2+a_3^2+a_4^2)\times(b_1^2+b_2^2+b_3^2+b_4^2)\\&=(-a_1b_1+a_2b_2+a_3b_3+a_4b_4)^2\\&\quad+(a_1b_2+a_2b_1+a_3b_4-a_4b_3)^2\\&\quad+(a_1b_3-a_2b_4+a_3b_1+a_4b_2)^2\\&\quad+(a_1b_4+a_2b_3-a_3b_2+a_4b_1)^2. \quad (2)\end{aligned}$$

由上式可知若兩數均可表示爲四個平方之和，則此二數之乘積也是四個平方之和。拉格朗日Lagrange利用這個恒等式很漂亮的證明了每一整數必可表示爲最多四個平方之和。首先注意的是只要證明每一質數爲最多四個平方之和就夠了。

劉維進一步證明每一整數可表示爲最多53個四次方之和。他用了下面的恒等式：

$$\begin{aligned}&6(x_1^2+x_2^2+x_3^2+x_4^2)^2\\&=(x_1+x_2)^4+(x_1+x_3)^4+(x_2+x_3)^4\\&\quad+(x_1+x_4)^4+(x_2+x_4)^4+(x_3+x_4)^4\\&\quad+(x_1-x_2)^4+(x_1-x_3)^4+(x_2-x_3)^4\\&\quad+(x_1-x_4)^4+(x_2-x_4)^4+(x_3-x_4)^4\\&\qquad\qquad\qquad\qquad\cdots\cdots\cdots\cdots (3)\end{aligned}$$

他把任意整數寫成$n=6x+y$，使y爲0，1，2，3，4，5中的一數。再把x寫成$a^2+b^2+c^2+d^2$而得

$$n=6a^2+6b^2+6c^2+6d^2+y.$$

再把$abcd$四數分別表示爲四個平方之和而得

$$\begin{aligned}a&=a_1^2+a_2^2+a_3^2+a_4^2\\b&=b_1^2+b_2^2+b_3^2+b_4^2\\c&=c_1^2+c_2^2+c_3^2+c_4^2\\d&=d_1^2+d_2^2+d_3^2+d_4^2\end{aligned}$$

由恒等式(3)可知$6a^2$可寫成十二個四次方之和，同理可知$6b^2$，$6c^2$，$6d^2$也一樣，於是n可寫成48個四次方（其中可能有零在內）加上y。由y之定義知最多是五個四次方（即五個1）之和，於是最多只有$48+5=53$個四次方。

現在回到拉格朗日的證明（他的結果是費馬最先用更複雜的方法得到的）。在奧衣勒恒等式(2)中令$a_1=x_1$，$a_2=x_2$，$a_3=x_3$，$a_4=$

x_4，$b_1=-y_1$，$b_2=y_2$，$b_3=y_3$，$b_4=y_4$ 可得

$$(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)$$
$$=(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2$$
$$+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2$$
$$+(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2$$
$$+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2 \quad (2')$$

證明可分成幾部分，由上式立刻得到

定理一 設A及B均可寫成四個平方之和，則乘積AB亦然。

定理二 設 p 爲大於2的質數，則必可找到一個整數 m，令 $1\leq m<p$ 並且 $mp=x_1^2+x_2^2+x_3^2+x_4^2$。

證明：p 是奇數，先寫下 0^2，1^2，2^2 ……，$(p-1)^2/4$，再依次除以 p，只保留餘數，這樣得到 $(p+1)/2$ 個數 r，每一數都介在0與 $p-1$ 之間。例如 $p=11$ 時，寫下0，1，4，9，16，25。除以11的餘數 r 是0，1，4，9，5，3。在一切的情形下，所有的餘數均不相同。因爲假如有兩個餘數相同，則可在0與 $(p-1)/2$ 之間找到兩個整數，$x_1>x_2$，它們的平方除以 p 後餘數相同，於是

$$x_1^2=q_1p+r,$$
$$x_2^2=q_2p+r$$

二式相減，可得

$$x_1^2-x_2^2$$
$$=(x_1-x_2)(x_1+x_2)$$
$$=(q_1-q_2)p$$

由於 p 是質數，它必須除盡 x_1-x_2 或 x_1+x_2，但這是不可能的，因爲 x_1-x_2 和 x_1+x_2 都是比 p 小的正整數。

現在考慮 $S=p-r-1$，這樣可得 $(p+1)/2$ 個介於0及 $p-1$ 之間的數，並且各數均不相同。例如當 $p=11$ 時可得10，9，6，1，，5，7。至少有一個數 S 必須等於上述一組數 r 當中的某一數。因爲 r 用去 p 個數0，1，2，……，$p-1$ 中的 $(p+1)/2$ 個數，只剩下 $(p-1)/2$ 個數，而 S 有 $(p+1)/2$ 個。例如 $p=11$ 時，有三數1，9，5同時在 r 和 s 內。

現在把 r 和 s 中某一相同的數以 $R=S$ 表示。R 是 x^2（$0\leq x\leq(p-1)/2$）除以 p 後的餘數，$S=p-1-$（y^2 除以 p 的餘數），其中 $0\leq y\leq(p-1)/2$。也就是說

$$x^2=q_1p+R$$
$$y^2=q_2p+r$$
$$S=p-r-1$$

三式相加得

$$x^2+y^2+S=(q_1+q_2+1)p+R-1$$

由於 $R=S$，因此上式可寫成

$$x^2+y^2+1=mp$$
$$m=q_1+q_2+1$$

又因爲

$$0\leq x\leq(p-1)/2$$
$$0\leq y\leq(p-1)/2$$

可得

$$0<mp\leq\left(\frac{p-1}{2}\right)^2+\left(\frac{p-1}{2}\right)^2+1$$
$$=\frac{p^2-2p+1}{2}+1$$
$$=(p^2-2p+3)/2<p^2/2<p^2$$

因此 $0<m<p$，於是定理二得證，因爲

$1\leq m<p$，

$mp=x^2+y^2+1^2+0^2$

例如 $p=11$ 時，可取 $R=S=5$ 而得 $x=y=4$，$4^2+4^2+1^2+0^2=3\cdot11$，不過若取 $R=S=1$，則 $x=1$，$y=3$，$1^2+3^2+1^2+0^2=1\cdot11$，於是 $p=11$ 表示爲四個平方之和，這是下一定理的特殊例子。

定理三 若 p 是一個大於2的質數，及 m 是最小的正整數使 mp 表示爲四個平方之和，則 $m=1$。

由定理二已知 $m<p$，這個最小的 m 不能是偶數，因爲這樣 $x_1^2+x_2^2+x_3^2+x_4^2=mp$ 也是偶數，於是四個 x 可能全是偶數，或者二奇二偶，或者全爲奇數。在第二種情形，可以假設 x_1，x_2 爲偶，x_3，x_4 爲奇。這樣在三種情形中 x_1+x_2，x_1-x_2，x_3+x_4，x_3-x_4 四數均爲偶數，於是

$$\left(\frac{x_1+x_2}{2}\right)^2+\left(\frac{x_1-x_2}{2}\right)^2+\left(\frac{x_3+x_4}{2}\right)^2+\left(\frac{x_3-x_4}{2}\right)^2$$

$$=\frac{1}{2}\left(x_1^2+x_2^2+x_3^2+x_4^2\right)=\frac{m}{2}p$$

可知m並不是最小的數。所以m必爲奇數。欲證$m=1$，可先設$m>1$，再證明它可以減小。設$m\geq 3$及

$$mp=x_1^2+x_2^2+x_3^2+x_4^2 \quad \cdots\cdots\cdots\cdots (4)$$

把每一x_k除以m而得一餘數r_k，$0\leq r_k<m$。

如果$0\leq r_k\leq\frac{1}{2}(m-1)$，令$y_k=r_k$。

若$\frac{1}{2}(m+1)\leq r_k\leq m-1$，令$y_k=r_k-m$。

在上述兩種情形，都可寫成

$$x_k=q_km+y_k$$

$$及-\frac{m-1}{2}\leq y_k\leq\frac{m-1}{2}$$

由於$y_k=x_k-q_km$，利用(4)式可得

$$\begin{aligned}&y_1^2+y_2^2+y_3^2+y_4^2\\&=x_1^2+x_2^2+x_3^2+x_4^2\\&\quad-2m(x_1q_1+x_2q_2+x_3q_3+x_4q_4)\\&\quad+m^2(q_1^2+q_2^2+q_3^2+q_4^2)\\&=mp-2m(x_1q_1+x_2q_2+x_3q_3+x_4q_4)\\&\quad+m^2(q_1^2+q_2^2+q_3^2+q_4^2)\\&=mn\end{aligned} \qquad (5)$$

上式中n爲整數，並且$n>0$，因爲若$n=0$則$y_1=y_2=y_3=y_4=0$，於是每一n均爲m之倍數，即每一x^2均爲m^2之倍數，由(4)式知mp爲m^2之倍數，於是p是m的倍數而非質數。此外

$$mn=y_1^2+y_2^2+y_3^2+y_4^2$$

$$\leq 4\left(\frac{m-1}{2}\right)^2$$

$$<m^2,$$

所以$n<m$。

將(4)及(5)二式相乘，可得

$$\begin{aligned}m^2np&=(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2\\&\quad+y_2^2+y_3^2+y_4^2)\\&=(2')\text{ 式中的右端}\end{aligned} \qquad (6)$$

在(2′)式中右端第一個平方中的數是

$$\begin{aligned}&x_1y_1+x_2y_2+x_3y_3+x_4y_4\\&=x_1(x_1-q_1m)+x_2(x_2-q_2m)\\&\quad+x_3(x_3-q_3m)+x_4(x_4-q_4m)\\&=x_1^2+x_2^2+x_3^2+x_4^2\\&\quad-m(x_1q_1+x_2q_2+x_3q_3+x_4q_4)\\&=mp-m(x_1q_1+x_2q_2+x_3q_3+x_4q_4)\\&=mz_1\end{aligned}$$

其中z_1爲整數。同理，(2′)中第二個平方中的數是

$$\begin{aligned}&x_1y_2-x_2y_1+x_3y_4-x_4y_3\\&=x_1(x_2-q_2m)-x_2(x_1-q_1m)\\&\quad+x_3(x_4-q_4m)-x_4(x_3-q_3m)\\&=m(-x_1q_2+x_2q_1-x_3q_4+x_4q_3)\\&=mz_2\end{aligned}$$

同理可得mz_3及mz_4，代入(6)式得

$$\begin{aligned}m^2np&=m^2z_1^2+m^2z_2^2+m^2z_3^2+m_2z_4^2\\np&=z_1^2+z_2^2+z_3^2+z_4^2\end{aligned}$$

所以np可寫成四個平方之和，而且$0<n<m$，與m之定義不合，所以$m=1$。

例如$p=11$時，$x_1=4$，$x_2=4$，$x_3=1$，$x_4=0$，$m=3$，可得$y_1=1$，$y_2=1$，$y_3=1$，$y_4=0$；

$$\begin{aligned}&4\cdot1+4\cdot1+1\cdot1+0\cdot0\\&=3z_1,\ z_1=3\\&4\cdot1-4\cdot1+1\cdot0-0\cdot1\\&=3z_2,\ z_2=0\\&4\cdot1-1\cdot1+0\cdot1-4\cdot0\\&=3z_3,\ z_3=1\\&4\cdot0-0\cdot1+4\cdot1-1\cdot1\\&=3z_4,\ z_4=1\end{aligned}$$

最後得到$3^2+0^2+1^2+1^2=1\cdot11$，$n=1$。

由定理三可知每一質數均可表示爲最多四個平方之和，因爲$p=2$時，$2=1^2+1^2+0^2+0^2$。因爲由(2)式可知每一整數均可表示爲最多四個平方之和。

（本文作者現任教於清大物理系）