四個整數的平方和

國立高雄師範學院數學系 李珠矽

現在討論那些正整數可以寫成四個整數的平方和。

我們很容易驗證

引理 1（Euler 等式）：

(1) $(x_1^2+x_2^2+x_3^2+x_4^2)(y_1^2+y_2^2+y_3^2+y_4^2)$

$=(x_1y_1+x_2y_2+x_3y_3+x_4y_4)^2+(x_1y_2-x_2y_1+x_3y_4-x_4y_3)^2$

$+(x_1y_3-x_3y_1+x_4y_2-x_2y_4)^2+(x_1y_4-x_4y_1+x_2y_3-x_3y_2)^2$

由引理 1 可知，可以寫成四個整數平方和的兩個正整數的乘積仍然可以寫成四個整數的平方和，又 $1=1^2+0^2+0^2+0^2$，所以我們只須討論那一些質數可以寫成四個整數的平方和就可以了。

引理 2：對於任意質數 $p>2$，存在正整數 m，$1\le m<p$，使得 mp 可以寫成四個整數的平方和。

證明：若 $x_1^2\equiv x_2^2 \pmod p$，則 $p\mid(x_1-x_2)(x_1+x_2)$，即 $x_1\equiv\pm x_2 \pmod p$，因此 $\frac{p+1}{2}$ 個數 x^2，$0\le x\le\frac{p-1}{2}$，對模 p 互不同餘，而 $\frac{p+1}{2}$ 個數 $-1-y^2$，$0\le y\le\frac{p-1}{2}$，對模 p 互不同餘，利用鴿洞原理可知上面的 $p+1$ 個數必有二個數對模 p 同餘，即存在 x, y 使得

$$x^2\equiv-1-y^2 \pmod p，\ |x|<\frac{p}{2}，\ |y|<\frac{p}{2}.$$

所以存在整數 m 使得

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

此時

$$0<mp<\frac{p^2}{4}+\frac{p^2}{4}+1=\frac{p^2}{2}+1<p^2，\ 0<m<p。$$

引理 3：每一質數都可寫成四個整數的平方和。

證明：$2=1^2+1^2+0^2+0^2$。現在令 $p>2$，由引理 2，令 m 為使 mp 可以寫成四個整數平方和之最小正整數，則 $m<p$。我們若能證明 $m=1$，引理便得證了。令 $mp=x_1^2+x_2^2+x_3^2+x_4^2$。

如果 m 為偶數，則

$$x_1+x_2+x_3+x_4\equiv x_1^2+x_2^2+x_3^2+x_4^2\equiv mp\equiv 0\ (\bmod 2)$$

不失一般性，可設

$$x_1+x_2\equiv 0\ (\bmod 2)\ ,\ x_3+x_4\equiv 0\ (\bmod 2)$$

因此

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

此與m爲具有這性質的最小者矛盾，故m爲奇數。

如果m爲≥ 3的奇數，對$k=1,2,3,4$，令

$$y_k\equiv x_k\ (\bmod m)\ ,\ |y_k|<\frac{m}{2}$$

（這能夠作到，因爲$-\frac{m-1}{2}\leq y\leq\frac{m-1}{2}$爲模$m$的完全剩餘系）。

$$\Sigma y_k^2\equiv\Sigma x_k^2\equiv mp\equiv 0\ (\bmod m)\ ,$$
$$\Sigma y_k^2=mn\ 。$$

此時$n>0$，否則對$k=1,2,3,4$，$y_k=0$，$m\mid x_k$，故$m\mid\Sigma x_k^2$，$m^2\mid mp$，$m\mid p$，與$m<p$矛盾。而且$n<m$（因爲$mn<4\cdot\frac{m^2}{4}=m^2$）。所以

$$m^2np=(1)\text{式之右邊。}$$

(1)式右邊的第一項

$$\Sigma x_ky_k\equiv\Sigma x_k^2\equiv 0\ (\bmod m)\ ,$$

其他各項的前二數及後二數滿足

$$x_ky_l-x_ly_k\equiv x_kx_l-x_lx_k\equiv 0\ (\bmod m)\ ,$$

因此(1)式右邊的每一項都$\equiv 0$（$\bmod m$），故可得

$$np=z_1^2+z_2^2+z_3^2+z_4^2\ ,$$

但$0<n<m$，此與m爲具有此性質的最小者矛盾，所以$m=1$。

由上便可知

定理 3：每一正整數都可以寫成四個整數的平方和。

下面有另一種方法可以得到定理3的結果，在49期（三個整數的平方和）中定理2提到除了$4^m(8k+7)$外，都可寫成三個整數的平方和，而$4^m(8k+7)=[4^m(8k+7)-4^m]+(2^m)^2$，$4^m(8k+7)-4^m$可以寫成三個整數平方和，所以所有的正整數都可以寫成四個整數的平方和。 □