三個整數的平方和

李珠矽
國立高雄師範學院數學系

有那些正整數可以寫成三個整數的平方和？

因爲 $x^2+y^2+z^2$ 是一個三元二次式，所以需要先討論二次式的性質，然後藉以解答我們的問題。

定義 1.

如果 $x_1, x_2, \cdots, x_r$ 爲整數變數，而 a_{kJ} 爲滿足

$$a_{kJ}=a_{Jk},\quad 1\le k,J\le r$$

的整數係數，則

$$F=F(x_1,x_2,\cdots,x_r)=\sum_{k=1}^{r}\sum_{J=1}^{r}a_{kJ}x_kx_J$$

叫做 r 元二次式。而行列式 $|a_{kJ}|$ 稱爲 F 的判別式，以 d 表之。

定義 2.

如果 $F=\sum_{k,J}a_{kJ}x_kx_J$，$G=\sum_{k,J}b_{kJ}x_kx_J$ 爲兩個 r 元二次式，如果存在 r^2 個整數 c_{kJ} 使得 $|c_{kJ}|=1$ 且利用下面 r 個等式

1) $$x_k=\sum_{J=1}^{r}c_{kJ}y_J,\quad k=1,2,\cdots,r$$

可以把 $F(x_1,x_2,\cdots,x_r)$ 轉換成 $G(y_1,y_2,\cdots,y_r)$，則稱 F 等值於 G，以 $F\sim G$ 表之。

此時

$$\sum_{m,n}b_{mn}y_my_n=\sum_{k,J}a_{kJ}\sum_{m}c_{km}y_m\sum_{n}c_{Jn}y_n=\sum_{m,n}y_my_n\sum_{k,J}c_{km}a_{kJ}c_{Jn}$$

因爲

$$\sum_{k,J}c_{km}a_{kJ}c_{Jn}=\sum_{k,J}c_{km}a_{Jk}c_{Jn}=\sum_{J,k}c_{Jm}a_{kJ}c_{kn}=\sum_{k,J}c_{kn}a_{kJ}c_{Jm}$$

也就是 y_my_n 的係數與 y_ny_m 的係數是一樣的，也因此

$$b_{mn} = \sum_{k,j} c_{km} a_{kj} c_{jn}$$

$$b_{kj} = \sum_{m,n} c_{mk} a_{mn} c_{nj}$$

如果以 $(c_{kj})^t$ 表 (c_{kj}) 的倒置方陣，即得

(2)　　$(b_{kj}) = (c_{kj})^t (a_{kj}) (c_{kj})$

因爲

$$\begin{aligned} F(x_1, x_2, \cdots, x_r) &= (x_1, x_2, \cdots, x_r)(a_{kj})(x_1, x_2, \cdots, x_r)^t \\ &= (y_1, y_2, \cdots, y_r)(c_{kj})^t (a_{kj})(c_{kj})(y_1, y_2, \cdots, y_r)^t \\ &= (y_1, y_2, \cdots, y_r)(b_{kj})(y_1, y_2, \cdots, y_r)^t \\ &= G(y_1, y_2, \cdots, y_r) \end{aligned}$$

利用(2)很容易就可以得知～爲一個等價關係，而且當 $F \sim G$ 時，二者的判別式相同，且描述相同的整數。

定義 3.

如果對於所有不全爲0的 $x_1, x_2, \cdots, x_r$，$F(x_1, x_2, \cdots, x_r)$ 恆大於0，則稱F爲正定。

如果 $F \sim G$，且F爲正定，則G當然也是正定，因此與F等值的二次式全爲正定，也就是說所有正定的二次式形成若干個等價類。

$F(x, y) = ax^2 + 2bxy + cy^2$ 爲二元二次式，其判別式爲 $d = ac - b^2$。此二次式縮寫爲 $\{a, b, c\}$。

引理 1.

$F = \{a, b, c\}$ 爲正定的充要條件是 $a > 0$ 且 $d > 0$。

證明.

(i) $a \leq 0$，$F(1, 0) = a \leq 0$，F不爲正定。

(ii) $a > 0$，$d \leq 0$，$F(-b, a) = ab^2 - 2b^2a + ca^2 = -ab^2 + ca^2 = a(ac - b^2)$

$= ad \leq 0$，F不爲正定。

(iii) $a > 0$，$d > 0$

$$aF = a^2x^2 + 2abxy + acy^2 = (ax + by)^2 + (ac - b^2)y^2 = (ax + by)^2 + dy^2$$

由此可知，若x，y不同時爲0，則 $F(x, y) > 0$，故F爲正定。

引理 2.

每一個正定的二元二次式的等價類中至少包含一個二次式滿足

$$2|b| \le a \le \frac{2}{\sqrt{3}} d 。$$

證明.

在這個等價類中，找一個固定的二次式$F = \{a_0, b_0, c_0\}$。設a爲F所描述的最小正整數，則可以找到適當的整數r，t使得

$$a = a_0 r^2 + 2b_0 rt + c_0 t^2$$

如果$(r, t) = v > 1$，則$F(\frac{r}{v}, \frac{t}{v}) = a_0(\frac{r}{v})^2 + 2b_0(\frac{r}{v})(\frac{t}{v}) + c_0(\frac{t}{v})^2 = \frac{a}{v^2}$爲F所描述的更小的正整數，與假設不合所以$(r, t) = 1$，因此存在$u_0, s_0$使$ru_0 - s_0 t = 1$

且若　　$s = s_0 + hr$，$u = u_0 + ht$；h爲任意整數

也有　　$ru - st = 1$

現在利用$\begin{pmatrix} r & s \\ t & u \end{pmatrix}$把$F = \{a_0, b_0, c_0\}$轉換成$G = \{a_1, b, c\}$，

則$a_1 = G(1, 0) = F(r, t) = a$，且由(2)式，得

$$\begin{aligned} b &= s(a_0 r + b_0 t) + u(b_0 r + c_0 t) \\ &= s_0(a_0 r + b_0 t) + u_0(b_0 r + c_0 t) + h(r(a_0 r + b_0 t) + t(b_0 r + c_0 t)) \\ &= s_0(a_0 r + b_0 t) + u_0(b_0 r + c_0 t) + ha \end{aligned}$$

因此可以適當的取h使得

$$|b| \le \frac{a}{2}$$

又$C = G(0, 1) = F(s, u)$，依a的定義，得$a \le c$。因此，

$$a^2 \le ac = b^2 + d \le \frac{a^2}{4} + d$$

$$\frac{3}{4} a^2 \le d$$

$$2|b| \le a \le \frac{2}{\sqrt{3}} d。$$

系. 任一個判別式爲1的二元正定二次式都與$x^2 + y^2$等值。

引理3.

$F = \sum_{k,j=1}^{3} a_{kj} x_k x_j$爲正定的充要條件是

$$a_{11} > 0，b = \begin{vmatrix} a_{11} & a_{12} \\ a_{21} & a_{22} \end{vmatrix} > 0，d > 0。$$

如果F爲正定，則

(3) $$a_{11}F=(a_{11}x_1+a_{12}x_2+a_{13}x_3)^2+K(x_2,x_3)$$

$K(x_2,x_3)$爲二元正定二次式 $\{a_{11}a_{22}-a_{12}^2,\ a_{11}a_{23}-a_{12}a_{13},\ a_{11}a_{33}-a_{13}^2\}$，其判別式爲 $a_{11}d$。

證明

(3)早已成立，而$K(x_2,x_3)$的判別式爲

$$(a_{11}a_{22}-a_{12}^2)(a_{11}a_{33}-a_{13}^2)-(a_{11}a_{23}-a_{12}a_{13})^2$$
$$=a_{11}(a_{11}a_{22}a_{33}-a_{11}a_{23}^2+2a_{12}a_{13}a_{23}-a_{12}^2a_{33}-a_{13}^2a_{22})=a_{11}d$$

（i）如果$a_{11}\leq 0$，則$F(1,0,0)=a_{11}\leq 0$，F不爲正定。

（ii）如果$a_{11}>0$，很明顯，F爲正定的充要條件是$K(x_2,x_3)$爲正定。因爲如果$K(x_2,x_3)$不爲正定，則存在兩個不全爲0且都是a_{11}的倍數的整數使得$K(x_2,x_3)\leq 0$，因此我們可以找到一個整數x_1，使得

$$a_{11}x_1+a_{22}x_2+a_{33}x_3=0$$

因此對這三個整數x_1,x_2,x_3，我們有

$$a_{11}F=K(x_2,x_3)\leq 0$$

又$a_{11}>0$，因此F不爲正定。另一方面，當$K(x_2,x_3)$爲正定時，

$$a_{11}F\begin{cases}\geq K(x_2,x_3)>0, & (x_2,x_3\text{不全爲0時})\\ =(a_{11}x_1)^2>0, & (x_1\neq 0,\ x_2=x_3=0\text{時})\end{cases}$$

所以F也爲正定。

由引理1，$K(x_2,x_3)$爲正定的充要條件是

$$a_{11}a_{22}-a_{12}^2>0,\quad a_{11}d>0$$

$$b=\begin{vmatrix}a_{11} & a_{12}\\ a_{21} & a_{22}\end{vmatrix}>0,\quad d>0。$$

引理4.

如果$(c_{11},c_{21},c_{31})=1$，則可以找到六個整數$c_{12},c_{22},c_{32},c_{13},c_{23},c_{33}$使得$|c_{kj}|=1$。

證明

設$g=(c_{11},c_{21})$，則$(g,c_{31})=1$，因此存在四個整數c_{12},c_{22},u,v使得

$$c_{11}c_{22}-c_{12}c_{21}=g$$
$$gu-c_{31}v=1$$

因此

$$\begin{vmatrix} c_{11} & c_{12} & \frac{c_{11}}{g}v \\ c_{21} & c_{22} & \frac{c_{21}}{g}v \\ c_{31} & 0 & u \end{vmatrix} = c_{31}\frac{c_{12}c_{21}-c_{11}c_{22}}{g}v+(c_{11}c_{22}-c_{12}c_{21})u=-c_{31}v+gu=1。$$

引理 5.

每一個正定的三元二次式的等價類中至少包含一個二次式滿足

$$a_{11}\leq\frac{4}{3}\sqrt[3]{d},\ 2|a_{21}|\leq a_{11},\ 2|a_{31}|\leq a_{11}。$$

證明

在這個等價類中，找一個固定的二次式F。設a_{11}爲F所描述的最小正整數，則可以找到適當的c_{11}，c_{21}，c_{31}使得

$$a_{11}=F(c_{11},c_{21},c_{31})$$

因此$(c_{11},c_{21},c_{31})=1$，否則$\frac{a_{11}}{(c_{11},c_{21},c_{31})^2}$爲F所描述的更小正整數。利用引理 4 的方法，我們可以找到c_{12}，c_{22}，c_{32}，c_{13}，c_{23}，c_{33}使得$|c_{kJ}|=1$。

利用(c_{kJ})把F轉換成$G=\sum_{k,J}b_{kJ}x_kx_J$，則

$$b_{11}=G(1,0,0)=F(c_{11},c_{21},c_{31})=a_{11}$$

如果四個整數t，2v，u，v滿足$tw-uv=1$，取

$$(d_{kJ})=\begin{pmatrix}1 & r & s\\ 0 & t & u\\ 0 & v & w\end{pmatrix}$$

則對任意整數r，s，$|d_{kJ}|=1$。

現在再利用(d_{kJ})把G轉換成H，則H的y_1^2的係數爲$G(d_{11},d_{21},d_{31})=G(1,0,0)=a_{11}$，設$H=\sum_{k,J}a_{kJ}x_kx_J$，則

(4) $$a_{12}=\sum_{m,n}d_{mJ}b_{mn}d_{n2}=\sum_{n}b_{Jn}d_{n2}=ra_{11}+tb_{12}+vb_{13}$$

(5) $$a_{13}=\sum_{m,n}d_{mJ}b_{mn}d_{n3}=\sum_{n}b_{Jn}d_{n3}=sa_{11}+ub_{12}+wb_{13}$$

而且

(6)　$$b_{11}x_1+b_{12}x_2+b_{13}x_3=\sum_k b_{Jk}\sum_J d_{kJ}y_J=\sum_J y_J\sum_k b_{Jk}d_{kJ}=a_{11}y_1+a_{12}y_2+a_{13}y_3$$

由引理3，我們有

$$a_{11}G(x_1,x_2,x_3)=(b_{11}x_1+b_{12}x_2+b_{13}x_3)^2+K(x_2,x_3)$$

$$a_{11}H(y_1,y_2,y_3)=(a_{11}y_1+a_{12}y_2+a_{13}y_3)^2+L(y_2,y_3)$$

其中K與L都是正定的二元二次式，由(6)可以得知$\begin{pmatrix} t & u \\ v & w \end{pmatrix}$把$K(x_2,x_3)$轉換成$L(y_2,y_3)$。由引理3知L的判別式爲$a_{11}d$而第一個係數爲$a_{11}a_{22}-a_{12}^2$，再由引理2得

$$a_{11}a_{22}-a_{12}^2\le\frac{2}{\sqrt{3}}\sqrt{a_{11}d}$$

在(4)，(5)中我們可以選適當的r，s，使得

$$|a_{12}|\le 2a_{11}\ ,\ |a_{13}|\le 2a_{11}$$

因爲$a_{22}=H(0,1,0)$，因此$a_{11}\le a_{22}$，所以

$$a_{11}^2\le a_{11}a_{22}=(a_{11}a_{22}-a_{12}^2)+a_{12}^2\le\frac{2}{\sqrt{3}}\sqrt{a_{11}d}+\frac{a_{11}^2}{4}$$

$$a_{11}^2\le\frac{8}{3\sqrt{3}}\sqrt{a_{11}d}$$

$$a_{11}^4\le\frac{64}{27}a_{11}d$$

$$a_{11}^3\le\frac{64}{27}d$$

$$a_{11}\le\frac{4}{3}\sqrt[3]{d}$$

系。任一個判別式爲1的三元正定二次式與$x_1^2+x_2^2+x_3^2$等值。

介紹過了二次式後，現在利用上面的這些引理以及Dirichlet定理（如果(a,b)＝1，則存在無限多個ka＋b型的質數。）來解決三個整數的平方和的問題。

先看可以寫成三個整數的平方和的正整數的必要條件是什麼。對任意整數l，

$$l^2\equiv 0,1\text{或}4\ (\mathrm{mod}\ 8)$$

因此三個整數的平方和將

$$\equiv 0,1,2,3,4,5\text{或}6\ (\mathrm{mod}\ 8)$$

亦即8k＋7型的正整數無法寫成三個整數的平方和。又如果$4^{m+1}(8k+7)$可以寫成三個整數的平方和時（其中m爲非負整數），設

$$4^{m+1}(8k+7)=x^2+y^2+z^2$$

因爲x^2，y^2，z^2都$\equiv 0$或$1\ (\mathrm{mod}\ 4)$，所以當x,y,z之中有一個不爲偶數時，$x^2+y^2+z^2\not\equiv 0\ (\mathrm{mod}\ 4)$，因此x,y,z必須全爲偶數，得到

$$4^m(8k+7)=(\frac{x}{2})^2+(\frac{y}{2})^2+(\frac{z}{2})^2$$

亦即 $4^m(8k+7)$ 也可以寫成三個整數的平方和。利用數學歸納法證得，對任意非負整數 m 與 k，$4^m(8k+7)$ 都無法寫成三個整數的平方和。

其他的正整數是否全部可以寫成三個整數的平方和？下面便是充分條件的討論。

如果 $4n=x^2+y^2+z^2$，則 x，y，z 全爲偶數，所以 $n=(\frac{x}{2})^2+(\frac{y}{2})^2+(\frac{z}{2})^2$，因此只需要討論 $\equiv 1,2,3,5$ 或 $6 \pmod 8$ 即可。又由引理 5 的系，只需要證明 n 可以寫成一個判別式爲 1 的三元正定二次式即可，再由引理 3 可以知道下面四個式子中的九個未知數 $a_{11},a_{22},a_{33},a_{12},a_{13},a_{23},x,y,z$ 有解即可：

$$n=a_{11}x^2+a_{22}y^2+a_{33}z^2+2a_{12}xy+2a_{13}xz+2a_{23}yz$$

$$\begin{cases} a_{11}>0 \\ a_{11}a_{22}-a_{12}^2>0 \\ \begin{vmatrix} a_{11} & a_{12} & a_{13} \\ a_{12} & a_{22} & a_{23} \\ a_{13} & a_{23} & a_{33} \end{vmatrix}=1 \end{cases}$$

取 $a_{13}=1$，$a_{23}=0$，$a_{33}=n$，$x=y=0$，$z=1$，則上面條件變成下面三個式子中的三個未知數 a_{11}，a_{12}，a_{22} 有解即可：

$$\begin{cases} a_{11}>0 \\ b=a_{11}a_{22}-a_{12}^2>0 \\ a_{22}=bn-1 \end{cases}$$

當 $n=1$ 時必然成立，因此現在假設 $n>1$，則

$$a_{22}>b-1\geq 0$$

$$a_{11}a_{22}=a_{12}^2+b>0$$

此時 $a_{11}>0$ 必然成立，因此變成了由後二個式子中的三個未知數 a_{11},a_{12},a_{22} 有解即可。更簡單一點，只要 $b>0$，而且 $-b$ 是模 $bn-1$ 的二次剩餘即可。

(i) $n\equiv 2$ 或 $6 \pmod 8$

因 $(4n,n-1)=1$，由 Dirichlet 定理，存在一個質數

$$p=4nv+(n-1)=(4v+1)n-1$$，其中 v 爲正整數

設 $b=4v+1$，則 $b>0$ 且 $\equiv 1 \pmod 4$，又 $p=bn-1\equiv 1 \pmod 4$，故

$$(\frac{-b}{p})=(\frac{b}{p})=(\frac{p}{b})=(\frac{bn-1}{b})=(\frac{-1}{b})=1$$

(ii) $n\equiv 1,3$ 或 $5 \pmod 8$

設 $$c=\begin{cases} 1 & \text{若 } n\equiv 3 \pmod 8 \\ 3 & \text{若 } n\equiv 1 \text{ 或 } 5 \pmod 8 \end{cases}$$

則 $\frac{cn-1}{2}$ 必爲奇數，而且 $(4n, \frac{cn-1}{2})=1$，由Dirichlet 定理，存在一個質數

$$p=4nv+\frac{cn-1}{2}=\frac{1}{2}((8v+c)n-1)，其中v爲正整數$$

設 $b=8v+c$，則 $b>0$ 且 $2p=bn-1$，因此

$$\begin{cases} b\equiv 3 \pmod 8 且 p\equiv 1 \pmod 4, & 當 n\equiv 1 \pmod 8 \\ b\equiv 1 \pmod 8 且 p\equiv 1 \pmod 4, & 當 n\equiv 3 \pmod 8 \\ b\equiv 3 \pmod 8 且 p\equiv 3 \pmod 4, & 當 n\equiv 5 \pmod 8 \end{cases}$$

在任何情形下，都有 $(\frac{-2}{b})=1$，所以

$$(\frac{-b}{p})=(-1)^{\frac{-b-1}{2}\cdot\frac{p-1}{2}}(\frac{p}{b})=(\frac{p}{b})=(\frac{p}{b})(\frac{-2}{b})=(\frac{-2p}{b})$$

$$=(\frac{1-bn}{b})=(\frac{1}{b})=1$$

於是，必有一個奇數k，使得 $-b\equiv k^2 \pmod p$，又因爲 $-b\equiv k^2 \pmod 2$，故得 $-b\equiv k^2 \pmod{2p}$，所以 $-b$ 爲對模 $2p$ 的二次剩餘，亦即 $-b$ 爲對模 $bn-1$ 的二次剩餘。

由上面的討論，我們可以得到

定理2. 正整數n可以寫成三個整數的平方和的充要條件是n不爲 $4^m(8k+7)$ 型的正整數（其中m與k爲非負整數）。

口袋型電視機

冠　穎

一種7吋長，3吋寬，1吋厚的口袋型電視機將問世了。這種電視機的畫面約2吋寬，體型之大小與口袋型計算機相似，大概一、二年後會大量上市。

這是英國發明家克力夫辛克力（Clive Sinclair）所發明，他是口袋型計算機的先驅。這種電視機的原理是將電子平行於螢光幕射出去，最後使電子束彎曲折向螢光幕。第一台這種電視機今年將在美國與大衆見面。

日本的東芝電子公司則試驗一種完全固態的螢光幕，其所使用之材料像用於電子錶的液晶（liguid crystals）。這種標準型電視機厚度只有0.7吋。畫面的控制裝置能使畫面中心的影像放大兩倍。

（取材自*Science Digest*—March 1982）