$X^2+Y^2=Z^2$ 的高斯整數解

李珠矽

國立高雄師範學院數學系

如果 a，b 爲整數，我們稱 $a+b_i$ 爲高斯整數，其集合以 $\boldsymbol{Z}(i)$ 表示。

定義1 對於 $\alpha=a+b_i$，我們定義 α 的範數 $N(\alpha)$ 爲

$$N(\alpha)=a^2+b^2。$$

引理1 $N(\alpha\beta)=N(\alpha)N(\beta)$。

定義2 若 α 有乘法反元素，我們稱 α 爲單位。

引理2 $\boldsymbol{Z}(i)$ 的單位是 $\pm 1, \pm i$。

定義3 若 α 是不爲 0 也不爲單位的高斯整數，如果對每一個分解 $\alpha=\beta\gamma$，β 與 γ 之中必有一個爲單位，我們稱 α 爲不可約數。如果由 $\alpha|\beta\gamma$ 可推得 $\alpha|\beta$ 或 $\alpha|\gamma$，我們稱 α 爲質數。

引理3 若 $N(\alpha)=p$，p 爲有理質數（$\boldsymbol{Z}$ 中的質數），則 α 爲不可約數。

引理4 $\boldsymbol{Z}(i)$ 爲唯一分解整域（U.F.D.）。

引理5 α 爲不可約數的充要條件是 α 爲質數。

因爲 $N(1+i)=2$，所以 $1+i$ 爲質數。（以上的性質請參考〔1〕的 3-5）

引理6 若 $\alpha=a+b_i$，則 $N(\alpha)$ 爲奇數的充要條件是 a,b 爲一奇一偶。

引理7 若高斯整數 α 與 β 互質，且 $\alpha\beta$ 爲一平方數，則 α 與 β 都是平方數。如果 $\alpha=u^2$，$\beta=v^2$，則 u 與 v 互質。

證明 若 $\alpha\beta=w^2$，設 w 的質因數分解爲 $w=\prod_{i=1}^{r}\delta_i^{k_i}$，則 $\alpha\beta=\prod_{i=1}^{r}\delta_i^{2k_i}$。所以 $\alpha=\prod_{i=1}^{r}\delta_i^{a_i}$，$\beta=\prod_{i=1}^{r}\delta_i^{b_i}$，$a_i\geq 0$，$b_i\geq 0$，$a_i+b_i=2k_i$。如果 a_i 與 b_i 都不爲 0，則 $\delta_i|\alpha$，$\delta_i|\beta$，矛盾。所以 a_i 與 b_i 之中有一爲 0，一爲 $2k_i$，令 $a_i=2u_i$，$b=2v_i$，所以 $\alpha=\prod_{i=1}^{r}\delta_i^{2u_i}$，$\beta=\prod_{i=1}^{r}\delta_i^{2v_i}$。令 $u=\prod_{i=1}^{r}\delta_i^{u_i}$，$v=\prod_{i=1}^{r}\delta_i^{v_i}$，則 $\alpha=u^2$，$\beta=v^2$。因爲 u_i 與 v_i 之中恰有一爲 0，所以 u 與 v 互質。

如果 $x^2+y^2=z^2$ 的解互質，我們稱

這種解為原始的解。求解時，只須求出原始的解就可以了，因此下面我們只討論原始的解。

引理8　若 x, y, z 為原始的解，則 x, y, z 兩兩互質。

證明　若 δ 為質數且 $\delta | x$ 且 $\delta | y$，則 $\delta | x^2$ 且 $\delta | y^2$，故 $\delta | (x^2+y^2)$，即 $\delta | z^2$，所以 $\delta | z$，矛盾，所以 x, y 互質。同理可以證明 x, z 互質，y, z 互質。

因為 $2=-i(1+i)^2$，所以 $2|N(\alpha)$ 的充要條件是 $(1+i)|\alpha$。因此，根據引理8，$N(x), N(y), N(z)$ 至多有一個為偶數。令 $x=x_1+x_2 i$, $y=y_1+y_2 i$, $z=z_1+z_2 i$，因為

$$(x_1+x_2 i)^2+(y_1+y_2 i)^2 = (z_1+z_2 i)^2$$

所以

$$x_1^2-x_2^2+y_1^2-y_2^2 = z_1^2-z_2^2$$
$$x_1x_2+y_1y_2 = z_1z_2 \text{。}$$

如果 $N(x), N(y), N(z)$ 都是奇數，則 x_1, x_2；y_1, y_2；z_1, z_2 皆為一奇一偶，因此 $x_1^2-x_2^2+y_1^2-y_2^2 \equiv 0 \pmod 2$，$z_1^2-z_2^2 \equiv 1 \pmod 2$，矛盾。所以 $N(x), N(y), N(z)$ 之中恰有一個為偶數。若 $N(x)$ 為偶數，則 $N(y), N(z)$ 皆為奇數，所以 $y_1y_2 \equiv z_1z_2 \equiv 0 \pmod 2$，因此 $x_1x_2 \equiv 0 \pmod 2$，得 $x_1 \equiv x_2 \equiv 0 \pmod 2$，即 $2|x$。同理 $N(y)$（或 $N(z)$）為偶數，亦可得 $2|y$（或 $2|z$），由此可得

引理9　若 x, y, z 為原始的解，則 $N(x), N(y), N(z)$ 為二奇一偶，範數為偶數的數是 2 的倍數。

我們可設 z 或 x 為 2 的倍數，則 x_1, x_2, z_1, z_2 為三偶一奇，因此 z_1-x_1, z_2-x_2 與 z_1+x_1, z_2+x_2 皆為一奇一偶，故 $N(z-x)$ 與 $N(z+x)$ 都是奇數。如果存在質數 δ 使 $\delta | (z-x)$ 且 $\delta | (z+x)$，則 $\delta | 2x$ 且 $\delta | 2z$。因為 x 與 z 互質，故 $\delta | 2$，即 $\delta = 1+i$。因此 $N(z-x)$ 與 $N(z+x)$ 都是偶數，矛盾。所以 $z-x$ 與 $z+x$ 互質。又因為

$$y^2 = z^2-x^2 = (z-x)(z+x),$$

所以存在二互質的高斯整數 u 與 v，使

$$z-x = u^2$$
$$z+x = v^2,$$

由引理1，$N(u)$ 與 $N(v)$ 都是奇數。最後得到

$$x = \frac{v^2-u^2}{2}$$
$$y = uv$$
$$z = \frac{v^2+u^2}{2} \text{。}$$

反之，若 x, y, z 為上面所給的形式，則 $x^2+y^2=z^2$。如果存在質數 δ 使 $\delta | x$ 且 $\delta | y$，則 $\delta | u$ 或 $\delta | v$。又 $\delta \left| \dfrac{v^2-u^2}{2} \right.$，故 $\delta | (v^2-u^2)$，因此 $\delta | u$

且 $\delta | v$ ，矛盾。所以 x, y 互質，亦即 x, y, z 爲原始的解。

定理 x, y ($N(y)$ 爲奇數)，z 爲原始的解的充要條件是存在二互質的高斯整數 u 與 v ，使 $x=\frac{v^2-u^2}{2}$, $y=uv$, $z=\frac{v^2+u^2}{2}$，其中 $N(u)$ 與 $N(v)$ 都是奇數。

若定理中的 x, y, z 爲正整數，則 $z+x=v^2$。於是，v 必是一個整數，因此，v 可取爲正整數，$u=\frac{y}{v}$ 亦爲正整數，又 $x=\frac{v^2-u^2}{2}>0$ ，所以 $v>u$ 。反之，若 u 與 v 都是正整數且 $v>u$ ，則 u 與 v 都是奇數，因此 $v^2-u^2 \equiv 0 \pmod 4$ ，$v^2+u^2 \equiv 2 \pmod 4$ ，所以 x 爲正偶數，z 爲正奇數，而 $y=uv$ 爲正奇數。因爲 $v-u$ 與 $v+u$ 都是偶數，

$$x=\frac{v^2-u^2}{2}=2\left(\frac{v-u}{2}\right)\left(\frac{v+u}{2}\right),$$

我們令 $s=\frac{v-u}{2}$, $t=\frac{v+u}{2}$，則 s 與 t 爲一奇一偶，且 $u=t-s$, $v=t+s$。因此

$$x=\frac{v^2-u^2}{2}=2st$$

$$y=uv=(t-s)(t+s)=t^2-s^2$$

$$z=\frac{v^2+u^2}{2}=\frac{(t+s)^2+(t-s)^2}{2}$$

$$=t^2+s^2 \text{。}$$

推論 x (偶數), y, z 爲原始的畢氏三數組的充要條件是存在二互質的正整數 s 與 t ，使 $x=2st$, $y=t^2-s^2$, $z=t^2+s^2$，其中 s 與 t 爲一奇一偶且 $t>s$ 。

參考資料

〔1〕 Burton : “Abstract and Linear Algebra”, 協進出版社。