兩個整數的平方和

到底那些正整數n可以寫成兩個整數的平方和？其寫法有多少種？

李珠矽

國立高雄師範學院數學系

為了解決這個問題，我們先討論方程式

(1) $$n=x^2+y^2$$

的整數解的組數為$U(n)$。

在本文中的n, n_1, n_2, …, n_k, d, d_1及d_2都是正整數。我們以$V(n)$表示

$$x^2\equiv -1 \pmod{n}$$

在0, 1, 2, …, $n-1$之中的解的個數。首先可以利用中國餘數定理得到

引理1.

如果$(n_1, n_2)=1$，則$V(n_1n_2)=V(n_1)\cdot V(n_2)$。再利用數學歸納法得到

系：

如果$n_1, n_2, \cdots, n_k$為k個兩兩互質的正整數，則

$$V(n_1n_2\cdots n_k)=V(n_1)V(n_2)\cdots V(n_k)。$$

對任意$4r+1$型的質數p與任意正整數l，考慮滿足$0<x<p^l$且與p互質的$\varphi(p^l)$個整數x，則可以找到一個整數m滿足$0<m<p^l$，使得

$$x^2\equiv m \pmod{p^l}$$

這種m至多有$\frac{1}{2}\varphi(p^l)$個。但如果

$$x^2\equiv x_0^2 \pmod{p^l},\ p\nmid x_0$$

則$p\nmid x$，且

$$p^l\mid (x+x_0)(x-x_0)$$

因為p只能整除$x+x_0$與$x-x_0$之中的一個（否則$p\mid 2x$），因此

$$x\equiv \mp x_0 \pmod{p^l}$$

也就是說對於上述的每一個m至多有兩個解。利用pigeon-holes（鴿洞）原理可以知道上述的m恰好有$\frac{1}{2}\varphi(p^l)$個，且對於每一個這種m恰好有兩個解，而依Wilson定理及Hensel定理知，$-1\equiv p^l-1 \pmod{p^l}$是這種$m$的一個，因此

$$V(p^l)=2$$

如果$4\mid n$，則$x^2\equiv -1 \pmod 4$無解，因

此 $x^2\equiv -1 \pmod n$ 也無解，亦即

$$V(n)=0。$$

如果 n 有一個 $4r+3$ 型的質因子 p，因爲 $x^2\equiv -1 \pmod p$ 無解，因此 $x^2\equiv -1 \pmod n$ 也無解，亦即

$$V(n)=0。$$

又 $V(1)=V(2)=1$，由引理1可以得到。

引理2.

(1) 如果 $4\mid n$ 或 n 有一個 $4r+3$ 型的質因子，則 $V(n)=0$。

(2) 如果 $4\nmid n$ 且 n 沒有 $4r+3$ 型的質因子，同時 n 恰好有 s 個 $4r+1$ 型的質因子，則 $V(n)=2^s$。

以下是討論 $U(n)$ 與 $V(n)$ 的關係。

引理3.

如果

$$n>1,\ l^2\equiv -1 \pmod n$$

則

$$n=x^2+y^2,\ x>0,\ y>0,\ (x,y)=1$$
$$y\equiv lx \pmod n$$

恰有一組解。

證明：

1. 存在性（證明中〔x〕表示 x 的最大整數值）

因爲 $l^2+1\equiv 0 \pmod n$，所以 $(l,n)=1$。於差數 $lx-y$ 中，令 x,y 分別取 $0,1,2,\cdots[\sqrt{n}]$，共 $[\sqrt{n}]+1$ 個值，則得 $([\sqrt{n}]+1)^2>n$ 個差數，利用 pigeon-holes 原理，則上面的 $([\sqrt{n}]+1)^2$ 個差數中必有兩個不同的差數對模 n 同餘，設

$$lx_1-y_1\equiv lx_2-y_2 \pmod n$$

即

$$l(x_1-x_2)\equiv y_1-y_2 \pmod n$$

此時 $x_1\neq x_2$，否則 $y_1\equiv y_2 \pmod n$，而 $0\le y_1,y_2\le\sqrt{n}$，得 $y_1=y_2$；同時 $y_1\neq y_2$，否則 $l(x_1-x_2)\equiv 0 \pmod n$，因 $(l,n)=1$，得 $x_1\equiv x_2 \pmod n$，而 $0\le x_1,x_2\le\sqrt{n}$，得到 $x_1=x_2$。

現在設 $x_1>x_2$，並令 $a=x_1-x_2$，$b=y_1-y_2$，則 $0<a$，$|b|<\sqrt{n}$，因此

$$0<a^2+b^2<2n$$

而且

$$l^2a^2\equiv b^2 \pmod n$$

所以

$$a^2+b^2\equiv a^2+la^2\equiv (l^2+1)a^2\equiv 0 \pmod n$$

得到

$$n=a^2+b^2。$$

因爲 $la\equiv b \pmod n$，所以存在整數 c，使得

$$b=nc+la$$

因此

$$n=a^2+b^2=a^2+(nc+la)^2$$
$$=(l^2+1)a^2+2lacn+n^2c^2$$

兩邊同時除以 n，得到

$$1=\frac{l^2+1}{n}a^2+2lac+nc^2$$
$$=\left(\frac{l^2+1}{n}a+lc\right)a+c(nc+la)$$
$$=ua+cb$$

其中 $u=\dfrac{l^2+1}{n}a+lc$。因此 $(a,b)=1$。

如果 $b>0$，則 $x=a$，$y=b$ 便爲所求。

如果 $b<0$，取 $x=-b$，$y=a$，則

$$lx\equiv -lb\equiv -l(la)\equiv -l^2a$$
$$\equiv a\equiv y \pmod n$$

所以 x，y 便爲所求。

2. 唯一性

如果 x_1,y_1；x_2,y_2 爲兩組解，則

$$n^2=(x_1^2+y_1^2)(x_2^2+y_2^2)$$
$$=(x_1x_2+y_1y_2)^2+(x_1y_2-y_1x_2)^2$$

又

$$x_1x_2+y_1y_2\equiv x_1x_2+(lx_1)(lx_2)$$
$$\equiv(l^2+1)x_1x_2\equiv 0(\text{mod } n)$$

因爲 $x_1x_2+y_1y_2>0$ ，所以

$$x_1x_2+y_1y_2=n\ ,\ x_1y_2-y_1x_2=0$$
$$x_1n=x_1(x_1x_2+y_1y_2)-y_1(x_1y_2-y_1x_2)$$
$$=x_2(x_1^2+y_1^2)=x_2n$$

$x_1=x_2$, $y_1=y_2$。

引理4.

如果 $n>1$ ，則

$n=x^2+y^2$，$x>0$，$y>0$，$(x,y)=1$

的整數解共有 $V(n)$ 組。

證明：

如果 x, y 爲一組解，因爲 $(x, y)=1$ 所以 $(x, n)=1$，因此在 0, 1, 2, …, $n-1$ 之中存在唯一的整數 l 使得

$$y\equiv lx(\text{mod } n)$$

此時

$$0\equiv n\equiv x^2+y^2\equiv x^2+lx^2$$
$$\equiv(1+l^2)x^2(\text{mod } n)$$

所以

$$l^2+1\equiv 0(\text{mod } n)$$

亦即 l 爲 $x^2\equiv -1(\text{mod } n)$ 的一解。所以對於每一組解 x, y 有唯一的 $x^2\equiv -1(\text{mod } n)$ 的解 l 與之對應，再由引理3，l 只有 x ，y 與之對應，因此(2)共有 $V(n)$ 組整數解。

系：

$n=x^2+y^2$, $(x, y)=1$ 的整數解共有 $4V(n)$ 組。

證明：

因爲 $(x, y)=1$，則 $x\neq 0$，$y\neq 0$，現在只須把引理4中 $x>0$ ，$y>0$ 的條件去掉即可，此時整數解的組數變爲原來的4倍。又 $1=(\pm 1)^2+0^2=0^2+(\pm 1)^2$ 有 $4=4V(1)$ 組解。

引理5.

$$U(n)=4\sum_{d^2|n}V\left(\frac{n}{d^2}\right)$$

證明：

如果 x, y 爲滿足 $(x, y)=d$ 的(1)的整數解，則 $d^2|n$ 。令

$$x_1=\frac{x}{d}\ ,\ y_1=\frac{y}{d}$$

則 $(x_1, y_1)=1$ ，且

$$\frac{n}{d^2}=x_1^2+y_1^2$$

因此滿足 $(x, y)=d$ 的整數解恰好有 $4V\left(\frac{n}{d^2}\right)$ 組，其中 $d^2|n$ ，所以引理得證。

引理6.

如果 $(n_1, n_2)=1$ ，則 $\frac{U(n_1n_2)}{4}=\frac{U(n_1)}{4}\ \frac{U(n_2)}{4}$ 。

證明：

因爲滿足 $d^2|n_1n_2$ 的 d 與滿足 $d_1^2|n_1^2$, $d_2^2|n_2$ 的 d_1, d_2 的乘積 d_1d_2 形成1－1對應，所以

$$\frac{U(n_1n_2)}{4}=\sum_{d^2|n_1n_2}V\left(\frac{n_1n_2}{d^2}\right)$$
$$=\sum_{\substack{d_1^2|n_1\\ d_2^2|n_2}}V\left(\frac{n_1}{d_1^2}\ \frac{n_2}{d_2^2}\right)$$
$$=\sum_{\substack{d_1^2|n_1\\ d_2^2|n_2}}V\left(\frac{n_1}{d_1^2}\right)V\left(\frac{n_2}{d_2^2}\right)$$
$$=\sum_{d_1^2|n_1}V\left(\frac{n_1}{d_1^2}\right)\sum_{d_2^2|n_2}V\left(\frac{n_2}{d_2^2}\right)$$
$$=\frac{U(n_1)}{4}\ \frac{U(n_2)}{4}\ 。$$

利用數學歸納法可以得到。

系：

如果 $n_1, n_2, \cdots, n_k$ 爲 k 個兩兩互質的正整數，則

$$\frac{U(n_1 n_2 \cdots n_k)}{4} = \frac{U(n_1)}{4}\frac{U(n_2)}{4}\cdots\frac{U(n_k)}{4}。$$

如果 p 爲質數，則

$$V(p^m)=\begin{cases}1 & 當\ p=2,\ m=1\\ 0 & 當\ p=2,\ m>1\\ 0 & 當\ p\equiv 3\ (\mathrm{mod}\ 4),\ m>0\\ 2 & 當\ p\equiv 1\ (\mathrm{mod}\ 4),\ m>0\end{cases}$$

由引理 5，當 l 爲偶數時，

$$\frac{U(p^l)}{4}=V(p^l)+V(p^{l-2})+\cdots$$
$$+V(p^2)+V(1)$$

當 $p=2$ 時，$\frac{1}{4}U(p^l)=1$，

當 $p\equiv 1(\mathrm{mod}\ 4)$ 時，$\frac{1}{4}U(p^l)=2\cdot\frac{l}{2}+1=l+1$，

當 $p\equiv 3(\mathrm{mod}\ 4)$ 時，$\frac{1}{4}U(p^l)=1$。

當 l 爲奇數時，

$$\frac{U(p^l)}{4}=V(p^l)+U(p^{l-2})+\cdots+V(p),$$

當 $p=2$ 時，$\frac{1}{4}U(p^l)=1$，

當 $p\equiv 1(\mathrm{mod}\ 4)$ 時，$\frac{1}{4}U(p^l)=2\cdot\frac{l+1}{2}=l+1$。

當 $p\equiv 3(\mathrm{mod}\ 4)$ 時，$\frac{1}{4}U(p^l)=0$。

如果 n 的質因數分解爲

$$n=2^a p_1^{r_1}p_2^{r_2}\cdots p_k^{r_k}q_1^{s_1}q_2^{s_2}\cdots q_l^{s_l}$$

其中 $p_1, p_2, \cdots, p_k$ 爲不同的 $4r+1$ 型質數，$q_1, q_2, \cdots, q_l$ 爲不同的 $4r+3$ 型質數，a, k, l 爲非負整數，而 $r_1, r_2, \cdots, r_k, s_1, s_2, \cdots, s_l$ 爲正整數。我們利用引理 6 的系可以得到。

定理 1.

$$\frac{U(n)}{4}=\begin{cases}0 & 如果\ s_1, s_2, \cdots s_l\ 之中至少有一爲奇數\\ T(r) & 如果\ s_1, s_2, \cdots s_l\ 全爲偶數。\end{cases}$$

其中 $T(r)=(r_1+1)(r_2+1)\cdots(r_k+1)$。當 $k=0$ 時，$T(r)=1$。

因爲兩個 $4r+1$ 型或兩個 $4r+3$ 型的整數的乘積都是 $4r+1$ 型的整數，如果 n 爲 $4r+3$ 型的整數，則 $l>0$ 且 $s_1, s_2, \cdots, s_l$ 中至少有一個爲奇數，故得

系：

如果 $n=2^a m$，其中 a 爲非負整數，m 爲 $4k+3$ 型的正整數，則 $U(n)=0$。

但若 $n=2^a m$，其中 m 爲 $4k+1$ 型的正整數，$U(n)$ 並不一定 $\neq 0$。

定理 1 告訴我們當 $s_1, s_2, \cdots, s_l$ 中至少有一個爲奇數時，n 無法寫成兩個整數的平方和。其他的 n 都可以寫成兩個整數的平方和，此時 $n=x^2+y^2$ 共有 $4(r_1+1)(r_2+1)\cdots(r_k+1)$ 組解。當 x 與 y 之中有一個爲 0 時，n 爲完全平方數，而當 $x=y$ 時，n 爲一個完全平方數的二倍，此時 $T(r)$ 爲奇數，如果(1)沒有上面兩種的解時，$s_1, s_2, \cdots, s_l$ 全爲偶數，而 $r_1, r_2, \cdots, r_k$ 之中至少有一個爲奇數，此時 $T(r)$ 爲偶數。

另外問題，到底能寫成兩個整數的平方和的正整數較多，還是不能寫成兩個整數的平方和的正整數較多？因爲 $2^a m$（其中 a 爲非負整數，m 爲 $4r+3$ 型的正整數）的正整數佔了正整數的一半，由定理 1 的系可以知道不能寫成兩個整數的平方和的正整數較多。 □