第三章　可表示爲平方和的正整數

定義. 不大於正整數 n 且與 n 互質的正整數個數稱爲 n 的**歐拉函數**, 記爲 $\varphi(n)$。

對於給定的正整數 m, 若將被 m 除餘數相同的整數看成一類, 則所有整數可以分成被 m 除餘 0, 被 m 除餘 1,..., 被 m 除餘 $m-1$ 等 m 類。

定義. 令 $m \in \mathbb{N}$, A_r 表示所有型如 $qm+r$ 的整數組成的集合, 其中 $r = 0, 1, ...$ $m-1$, 則 $A_0, A_1, \ldots, A_{m-1}$ 稱爲以 m 爲除數的**剩餘類**。在 $A_0, A_1, \ldots, A_{m-1}$ 中各取一個數, 則這 m 個數 (即 $\{a_r \in A_r \mid r = 0, 1, \ldots, m-1\}$) 稱爲以 m 爲除數的一組**完全剩餘系**。如果一個以 m 爲除數的剩餘類裡面的數與 m 互質, 則稱此剩餘類爲與 m 互質的剩餘類。在所有與 m 互質的剩餘類中各取一數所組成的集合, 稱爲以 m 爲除數的**簡化剩餘系**。

顯然, 根據定義可知 m 個整數要形成以 m 爲除數的一組完全剩餘系的充分必要條件是這 m 個數兩兩被 m 除不同餘。另外, 根據歐拉函數的定義, 一組以 m 爲除數的簡化剩餘系有 $\varphi(m)$ 個數。

引理 4. 令 $m \in \mathbb{N}$, $k \in \mathbb{Z}$ 且 $\gcd(k, m) = 1$。若 $a_1, a_2, \ldots, a_m$ 是以 m 爲除數的一組完全剩餘系, 則 $ka_1, ka_2, \ldots, ka_m$ 也是以 m 爲除數的一組完全剩餘系。同樣地, 若 $b_1, b_2, \ldots, b_{\varphi(m)}$ 是以 m 爲除數的一組簡化剩餘系, 則 $kb_1, kb_2, \ldots, kb_{\varphi(m)}$ 也是以 m 爲除數的一組簡化剩餘系。

證明. 若第一個命題爲假, 則存在 $1 \le i, j \le m$, $i \ne j$ 使得 $ka_i \equiv ka_j \pmod{m}$, 因爲 $\gcd(k, m) = 1$, 所以 $a_i \equiv a_j \pmod{m}$, 矛盾。同樣地, 因爲 $k, b_1, b_2, \ldots, b_{\varphi(m)}$ 皆與 m 互質, 所以 $kb_1, kb_2, \ldots, kb_{\varphi(m)}$ 也與 m 互質, 若第二個命題爲假, 則存在 $1 \le i, j \le \varphi(m)$, $i \ne j$ 使得 $kb_i \equiv kb_j \pmod{m}$, 也就是 $b_i \equiv b_j \pmod{m}$, 矛盾。 □

定理 3. (歐拉定理) 假設 $m \in \mathbb{N}, a \in \mathbb{Z}$。若 $\gcd(a, m) = 1$, 則

$$a^{\varphi(m)} \equiv 1 \pmod{m}。$$

證明. 假設 $r_1, r_2, \ldots, r_{\varphi(m)}$ 是以 m 爲除數的一組簡化剩餘系, 則 $ar_1, ar_2, \ldots, ar_{\varphi(m)}$ 也是以 m 爲除數的一組簡化剩餘系 (引理 4), 我們有

$$\begin{aligned} (ar_1)(ar_2)\cdots(ar_{\varphi(m)}) &\equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m} \\ \Rightarrow a^{\varphi(m)}(r_1 r_2 \cdots r_{\varphi(m)}) &\equiv r_1 r_2 \cdots r_{\varphi(m)} \pmod{m}。 \end{aligned}$$

因爲

$$\gcd(r_1, m) = \gcd(r_2, m) = \cdots = \gcd(r_{\varphi(m)}, m) = 1,$$

所以 $a^{\varphi(m)} \equiv 1 \pmod{m}$。 □

定理 4. 假設 $m \in \mathbb{N}$, $a, b \in \mathbb{Z}$ 且 $\gcd(a, m) = d$。則一次同餘式 $ax \equiv b \pmod{m}$ 有解若且唯若 $d \mid b$。此外, 當 $d = 1$ 時, 此同餘式有唯一解 (在同餘的觀點下)。

證明. 若同餘式有解, 則存在 $x_0 \in \mathbb{Z}$ 使得 $ax_0 \equiv b \pmod{m}$, 換句話說, 存在 $c \in \mathbb{Z}$ 使得 $ax_0 - b = mc$。因爲 $d \mid a$ 且 $d \mid m$, 所以 $d \mid ax_0 - mc = b$。另一方面, 若 $d \mid b$, 存在 $b_1 \in \mathbb{Z}$ 使得 $b = db_1$。此外, 根據 Bézout's identity, 存在 $s, t \in \mathbb{Z}$ 使得 $as + mt = d$。我們取 $x = sb_1$, 則

$$m \mid -mtb_1 = asb_1 - db_1 = a(sb_1) - b,$$

因此 sb_1 爲同餘式的解。最後, 假設 $d = 1$。因爲 $1 \mid b$, 所以同餘式有解。假設 $x_1, x_2 \in \mathbb{Z}$ 皆是同餘式的解, 則

$$ax_1 \equiv b \equiv ax_2 \pmod{m}。$$

因 $d = 1$, 前式可化簡爲 $x_1 \equiv x_2 \pmod{m}$。也就是說, 同餘式所有的整數解在同餘的觀點下只有一種。 □

定理 5. (Wilson 定理) 一個大於 1 的正整數 n 是質數若且唯若

$$(n-1)! \equiv -1 \pmod{n}。$$

證明. 當 $n = 2$ 時, $(2-1)! \equiv -1 \pmod{2}$。現在假設 n 是奇質數。對所有的 $1 \le a \le n-1$, 因爲 $\gcd(a, n) = 1 \mid 1$, 所以一次同餘式 $ax \equiv 1 \pmod{n}$ 有解 (定理 4)。我們要證明對 a 而言, 除了 1 和 $n-1$ 之外, 其他同餘式的解都不是自己。若 $a^2 \equiv 1 \pmod{n}$, 則 $n \mid a^2 - 1 = (a-1)(a+1)$, 也就是說, $n \mid a-1$ 或 $n \mid a+1$, 所以 $a = 1$ 或 $a = n-1$。於是我們可將 $2, 3, \ldots, n-2$ 分成 $\frac{n-3}{2}$ 對, 每一對的數字相乘後被 n 除都會餘 1。我們得到

$$2 \times 3 \times \cdots \times (n-3) \times (n-2) \equiv 1 \pmod{n},$$

將兩邊同乘 $n-1$ 即得證。另一方面, 當 $(n-1)! \equiv -1 \pmod{n}$ 時, 代表 $n \mid (n-1)! + 1$, 若 n 不是質數, 則存在一個正整數 $1 < p < n$ 使得 $p \mid n$, 但 p 又整除 $(n-1)!$, 所以 $p \mid (n-1)! + 1 - (n-1)! = 1$, 矛盾, 因此 n 必須是質數。 □

引理 5. 若 p 是型如 $4m+1$ 的質數, 則 $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p}$。

證明. 對所有的 $r = 1, 2, \ldots, \dfrac{p-1}{2}$, 我們有 $p - r \equiv -r \pmod{p}$。根據 Wilson 定理,

$$\begin{aligned}
-1 \equiv (p-1)! &= \left(1 \times 2 \times 3 \times \cdots \times \frac{p-1}{2}\right)\left(\frac{p+1}{2}\right)\left(\frac{p+3}{2}\right)\cdots(p-2)(p-1) \\
&= \left(\frac{p-1}{2}\right)!\left(p - \frac{p-1}{2}\right)\left(p - \frac{p-3}{2}\right)\cdots(p-2)(p-1) \\
&\equiv \left(\frac{p-1}{2}\right)!\left(-\frac{p-1}{2}\right)\left(-\frac{p-3}{2}\right)\cdots(-2)(-1) \\
&= (-1)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod{p}。
\end{aligned}$$

因爲 $\dfrac{p-1}{2}$ 是偶數, 所以 $\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod{p}$。 □

當正整數 n 可以表示爲兩個整數的平方和 (即存在 $x, y \in \mathbb{Z}$ 使得 $x^2+y^2 = n$) 時, 對於任意整數 k, $k^2n = (kx)^2 + (ky)^2$, 所以 k^2n 亦能表示爲兩個整數的平方和。若正整數 m, n 都能表示爲兩個整數的平方和, 令 $m = a^2 + b^2$, $n = c^2 + d^2$, 則

$$mn = (a^2 + b^2)(c^2 + d^2) = (ac + bd)^2 + (ad - bc)^2,$$

所以任兩個型爲平方和的正整數乘積也可表示爲兩個整數的平方和。我們現在證明任兩個型爲平方和的正整數乘積只有兩種整數的平方和表示法。

引理 6. 若 $m = u^2 + v^2$, $p = a^2 + b^2$, 其中 $u, v, a, b \in \mathbb{N}$, 則 mp 只有以下兩種整數的平方和表示法:

$$\begin{gathered}
mp = (au + bv)^2 + (bu - av)^2 \\
\text{或 } mp = (au - bv)^2 + (bu + av)^2。
\end{gathered}$$

證明. 因爲兩個絕對值相等的整數平方後也會相等, 所以對於

$$\pm(au + bv),\ \pm(bu - av),\ \pm(au - bv),\ \pm(bu + av)$$

這些可能, 我們只各取一個來代表, 其他的組合皆視爲同一類。現在令

$$\mathbb{Z}[i] = \{a + bi \mid a, b \in \mathbb{Z}, i = \sqrt{-1}\},$$

顯然 $m, p \in \mathbb{Z}[i]$。因爲 $\mathbb{Z}[i]$ 是一個歐氏環, 根據歐氏環的唯一分解定理可知 [1],

$$m = u^2 + v^2 = (u + vi)(u - vi)$$

以及

$$p = a^2 + b^2 = (a + bi)(a - bi)$$

所形成的高斯整數乘積表示法唯一, 因此

$$mp = [(u + vi)(u - vi)][(a + bi)(a - bi)]。$$

我們有

$$\begin{aligned} mp &= [(u - vi)(a + bi)][(u + vi)(a - bi)] \\ &= [(au + bv) + (bu - av)i][(au + bv) - (bu - av)i] \\ &= (au + bv)^2 + (bu - av)^2, \end{aligned}$$

或者是

$$\begin{aligned} mp &= [(u + vi)(a + bi)][(u - vi)(a - bi)] \\ &= [(au - bv) + (bu + av)i][(au - bv) - (bu + av)i] \\ &= (au - bv)^2 + (bu + av)^2。 \end{aligned}$$

□

引理 7. 若 p 是正整數 n 的一個質因數, p 能表示爲兩個整數的平方和, n 能表示爲兩個互質整數的平方和, 則 $\frac{n}{p}$ 也能表示爲兩個互質整數的平方和。

證明. 令 $p = a^2 + b^2$, $n = x^2 + y^2$, 其中 $a, b, x, y \in \mathbb{Z}$, $\gcd(x, y) = 1$。因爲 $p \mid n = x^2 + y^2$, 所以

$$p \mid a^2(x^2 + y^2) - y^2(a^2 + b^2) = a^2x^2 - b^2y^2 = (ax - by)(ax + by)。$$

情形一: $p \mid ax - by$。因爲

$$pn = (a^2 + b^2)(x^2 + y^2) = (ax - by)^2 + (ay + bx)^2,$$

所以 p 也整除 $ay + bx$。令 $\gcd(ax - by, ay + bx) = pq$, 則

$$pq \mid [a(ax - by) + b(ay + bx)] = xp$$

且

$$pq \mid [a(ay+bx)-b(ax-by)] = yp,$$

所以 q 是 x 和 y 的公因數, 但 $\gcd(x,y)=1$, 代表 q 也必須是 1, 因此我們得到 $\gcd(ax-by, ay+bx) = p$,

$$\frac{n}{p} = \left(\frac{ax-by}{p}\right)^2 + \left(\frac{ay+bx}{p}\right)^2。$$

情形二: $p \mid ax+by$。仿照情形一的論證過程 (只有符號上的更動, 不再贅述), 我們最後會得到 $\gcd(ay-bx, ax+by) = p$,

$$\frac{n}{p} = \left(\frac{ay-bx}{p}\right)^2 + \left(\frac{ax+by}{p}\right)^2。$$

□

定理 6. 對所有的 $n \in \mathbb{N}$, n^2+1 的每一個質因數都能表示爲兩個整數的平方和。

證明. 當 $n=1$ 時, 1^2+1 唯一的質因數爲 $2 = 1^2+1^2$, 命題成立。我們假設

$$1^2+1, 2^2+1, 3^2+1, \ldots, (m-1)^2+1$$

的每一個質因數都能表示爲兩個整數的平方和, 其中 m 是某個大於 1 的正整數。現在考慮 $n=m$ 且設 p 是 n^2+1 的質因數。

情形一: $p < m$。因爲 $p \mid m^2+1$, 所以

$$p \mid m^2+1-2mp+p^2 = (m-p)^2+1。$$

又因 $1 < p \le m-1$, 根據前面的假設, p 能表示爲兩個整數的平方和。

情形二: $p = m$。若 $p=m$, 則 $p \mid m^2+1-m^2 = 1$, 矛盾, 所以情形二不會發生。

情形三: $p > m$。設 $m^2+1 = pq$。因爲 $p \ge m+1$, 若 $q \ge m$, 則

$$pq \ge m^2+m > m^2+1 = pq,$$

矛盾, 因此 $q < m$。令 $q = q_1 q_2 \cdots q_k$, 其中 $q_1, q_2, \ldots, q_k$ 皆是小於 m 的質數。根據情形一, $q_1, q_2, \ldots, q_k$ 皆可表爲兩個整數的平方和。因爲 m^2+1 爲兩個互質整數的平方和, 且 q_1 是 m^2+1 的質因數, 根據引理 7,

$$\frac{m^2+1}{q_1} = (q_2 q_3 \cdots q_k)p$$

能表示爲兩個互質整數的平方和。同理, 因爲 $\frac{m^2+1}{q_1}$ 爲兩個互質整數的平方和, 且 q_2 是 $\frac{m^2+1}{q_1}$ 的質因數, 根據引理 7,

$$\frac{m^2+1}{q_1q_2} = (q_3q_4\cdots q_k)p$$

能表示爲兩個互質整數的平方和。依此類推, 最後我們得到

$$\frac{m^2+1}{q_1q_2\cdots q_k} = p$$

能表示爲兩個互質整數的平方和。 □

定理 7. 每一個型如 $4m+1$ 的質數 p 都可表示爲兩個正整數的平方和且不計次序時表示法唯一。

證明. 因爲 $p \equiv 1 \pmod 4$, 根據引理 5, $[(\frac{p-1}{2})!]^2 \equiv -1 \pmod p$, 所以 p 是型如 n^2+1 的數的質因數 $\left(n = (\frac{p-1}{2})!\right)$, 根據定理 6, p 能表示爲兩個整數的平方和。因爲兩個絕對值相等的整數平方後也會相等, 所以我們也可以說 p 能表示爲兩個正整數的平方和。對於唯一性, 我們假設 $p = x^2+y^2$ 且 $p = a^2+b^2$, 其中 $x, y, a, b \in \mathbb{N}$, $\gcd(x,y) = \gcd(a,b) = 1$。因爲

$$p \mid a^2(x^2+y^2) - y^2(a^2+b^2) = a^2x^2 - b^2y^2 = (ax-by)(ax+by),$$

所以 $p \mid ax-by$ 或 $p \mid ax+by$。

情形一: $p \mid ax-by$。因爲 $p^2 = (ax-by)^2 + (ay+bx)^2$, 所以 p 也整除 $ay+bx$。又因 $ay+bx > 0$, 我們有

$$ay+bx \geq p \Rightarrow (ay+bx)^2 \geq p^2 \Rightarrow (ax-by)^2 = 0 \Rightarrow ax = by。$$

因爲 $\gcd(x,y) = \gcd(a,b) = 1$, 所以 $a = y$ 且 $b = x$。

情形二: $p \mid ax+by$。仿照情形一的論證過程, 最後我們會得到 $a = x, b = y$。

□

我們知道型如 $4m+1$ 的質數可唯一表示爲兩個互質正整數的平方和, 現在考慮型如 $4m+3$ 的正整數。因爲所有的整數平方之後被 4 除不是餘 0 就是餘 1, 所以對所有的 $x, y \in \mathbb{Z}$, x^2+y^2 被 4 除可能的餘數只有 $0, 1, 2$, 因此所有型如 $4m+3$ 的正整數皆無法表示爲兩個整數的平方和。

引理 8. 令 $x, y \in \mathbb{Z}$ 且 $\gcd(x,y) = 1$, 則所有型如 x^2+y^2 之正整數的奇質因數一定型如 $4m+1$。

證明. 設 $p = 2n+1$ 是 x^2+y^2 的奇質因數。因爲 $p \mid x^2+y^2$, 所以

$$x^2 \equiv -y^2 \pmod{(2n+1)}。$$

此外,

$$\begin{aligned}\gcd(x,y)=1 &\Rightarrow \gcd(x,y^2)=1\\ &\Rightarrow \gcd(x,x^2+y^2)=1\\ &\Rightarrow \gcd(x,2n+1)=1,\end{aligned}$$

根據歐拉定理, $x^{2n} \equiv 1 \pmod{(2n+1)}$。同樣地,

$$\begin{aligned}\gcd(x,y)=1 &\Rightarrow \gcd(x^2,y)=1\\ &\Rightarrow \gcd(x^2+y^2,y)=1\\ &\Rightarrow \gcd(2n+1,y)=1,\end{aligned}$$

同理 $y^{2n} \equiv 1 \pmod{(2n+1)}$。因此我們有

$$1 \equiv x^{2n} = (x^2)^n \equiv (-y^2)^n = (-1)^n y^{2n} \equiv (-1)^n \pmod{2n+1},$$

代表 n 是偶數, 令 $n = 2m$, 則 $p = 2(2m)+1 = 4m+1$。 □

我們已知兩個可表示爲平方和的正整數之乘積有兩種不同的平方和表示法, 在給定某些條件下, 當其中一個能整除另外一個時, 兩種表示法中只有一種是兩個互質整數的平方和, 而且當這兩個型如平方和的正整數互質時, 兩種表示法皆是兩個互質整數的平方和, 以下證明。

引理 9. 假設 $m = u^2+v^2$, $p = a^2+b^2$, 其中 $u,v,a,b \in \mathbb{N}$, $\gcd(u,v)=1$, p 是奇質數, $m > 2$。則

1. 當 $p \nmid m$ 時, 有兩種不同的方法將 mp 表示爲兩個互質整數的平方和。
2. 當 $p \mid m$ 時, 上述兩種表示法中只有一種是兩個互質整數的平方和。

證明. 我們先證 1。由引理 6 可知, mp 有

$$(au+bv)^2+(bu-av)^2 \text{ 和 } (au-bv)^2+(bu+av)^2$$

兩種表示法。若 $\gcd(au+bv, bu-av) \neq 1$, 令 q_1 爲 $\gcd(au+bv, bu-av)$ 的質因數, 則我們有

$$\begin{cases} au \equiv -bv \pmod{q_1} \\ bu \equiv av \pmod{q_1} \end{cases} \Rightarrow \begin{cases} a^2u \equiv -abv \pmod{q_1} \\ b^2u \equiv abv \pmod{q_1} \end{cases},$$

因此 $u(a^2+b^2) \equiv 0 \pmod{q_1}$。同樣地,

$$\begin{cases} au \equiv -bv \pmod{q_1} \\ bu \equiv av \pmod{q_1} \end{cases} \Rightarrow \begin{cases} -abu \equiv b^2 v \pmod{q_1} \\ abu \equiv a^2 v \pmod{q_1} \end{cases},$$

故 q_1 也整除 $v(a^2+b^2)$。因爲 $p \nmid m$ 且 $q_1^2 \mid pm$, 我們知 $q_1 \neq p$, 因此 $q_1 \mid u$ 且 $q_1 \mid v$, 但這與 $\gcd(u,v)=1$ 矛盾, 所以 $\gcd(au+bv, bu-av)=1$。仿照同樣的論證過程, 我們也可證得 $\gcd(au-bv, bu+av)=1$。接下來, 假設

$$mp = (au+bv)^2 + (bu-av)^2 \text{ 和 } mp = (au-bv)^2 + (bu+av)^2$$

是同一種表示法。因爲 $au+bv > au-bv$, 我們有

$$\begin{cases} au+bv = bu+av \\ bu-av = au-bv \end{cases} \Rightarrow \begin{cases} (a-b)u = (a-b)v \\ b(u+v) = a(u+v) \end{cases} \Rightarrow a = b,$$

則 $p = a^2+b^2 = 2a^2$, 與 p 是奇數矛盾, 因此 $mp = (au+bv)^2 + (bu-av)^2$ 與 $mp = (au-bv)^2 + (bu+av)^2$ 是兩種不同的表示法。

我們現在來證明 2。因爲 $p \mid m$ 且 $p \mid p$, 我們有

$$\begin{cases} u^2 \equiv -v^2 \pmod{p} \\ a^2 \equiv -b^2 \pmod{p} \end{cases} \Rightarrow a^2u^2 \equiv b^2v^2 \pmod{p},$$

也就是說, $p \mid a^2u^2 - b^2v^2 = (au-bv)(au+bv)$。

情形一: $p \mid au-bv$ 且 $p \mid au+bv$。這麼一來, $p \mid 2au$。因爲 p 是奇質數且 $0 < a < p$, 所以 $p \nmid 2$ 且 $p \nmid a$, 故 $p \mid u$。但又因 $p \mid m$, 我們得到

$$p \mid m - u^2 = v^2 \Rightarrow p \mid v,$$

與 $\gcd(u,v)=1$ 矛盾, 因此情形一不會發生。

情形二: $p \mid au-bv$ 但 $p \nmid au+bv$。因爲 $mp = (au-bv)^2 + (bu+av)^2$, 所以

$$p \mid mp - (au-bv)^2 = (bu+av)^2 \Rightarrow p \mid bu+av,$$

顯然 $au-bv$ 與 $bu+av$ 不互質。若 $\gcd(au+bv, bu-av) \neq 1$, 令 q_2 爲 $\gcd(au+bv, bu-av)$ 的質因數, 則我們有

$$\begin{cases} au \equiv -bv \pmod{q_2} \\ bu \equiv av \pmod{q_2} \end{cases} \Rightarrow \begin{cases} a^2u \equiv -abv \pmod{q_2} \\ b^2u \equiv abv \pmod{q_2} \end{cases},$$

因此 $u(a^2+b^2) \equiv 0 \pmod{q_2}$。同樣地,

$$\begin{cases} au \equiv -bv \pmod{q_2} \\ bu \equiv av \pmod{q_2} \end{cases} \Rightarrow \begin{cases} -abu \equiv b^2 v \pmod{q_2} \\ abu \equiv a^2 v \pmod{q_2} \end{cases},$$

故 q_2 也整除 $v(a^2+b^2)$。因爲情形一不會發生, 我們知 $q_2 \neq p$, 因此 $q_2 \mid u$ 且 $q_2 \mid v$, 但這與 $\gcd(u,v)=1$ 矛盾, 所以 $\gcd(au+bv, bu-av)=1$。

情形三: $p \mid au+bv$ 但 $p \nmid au-bv$。仿照情形二的論證過程, 我們也可證得 $au+bv$ 與 $bu-av$ 不互質, 而且 $\gcd(au-bv, bu+av)=1$。

所以當 $p \mid m$ 時, mp 的兩種平方和表示法只有一種是互質整數的平方和。 □