2023 年臺灣國際科學展覽會
優勝作品專輯

作品編號　**010019**

參展科別　數學

作品名稱　探討圓及橢圓上的格子點個數之連乘積表達式

得獎獎項　四等獎

就讀學校　臺北市立內湖高級中學

指導教師　林鳳美、歐登銘

作者姓名　彭士鳴、林士哲

關鍵詞　橢圓上格子點個數、唯一分解整環、黑格納數

作者簡介

我是彭士鳴，從國七就開始探索及研究數學，這次科展對數學的嚴謹更為要求，因此在證明上花了一些功夫，體會到證明美妙之處，也了解到數論代數對於數學結構是如何去研究，讓我對數學在知識上的見解也跟隨逐日增強，因而數學成為我最酷愛的科目。這次難得的盛會非常榮幸，特別感謝指導教授、指導老師及支持我的人。

我是林士哲，數學是我最感興趣的科目，從國七就開始研究數學，這次作品針對證明的嚴謹度及做研究的錯誤理解更加強，花更多時間去學會如何思考問題、分析數據及嚴謹論證，讓我受益良多。這次難得的盛會中，抱持學習的心態及擴展我的知識與國際視野，十分感謝指導教授、指導老師以及支持我的人一路上陪伴與指導。

摘要

在坐標平面上，x, y 坐標均為整數的點稱為格子點，在這篇作品中，主要探討圓及橢圓 $x^2 + sy^2 = m$ 上的格子點個數，並且此個數以連乘積表達式呈現，其中 s 為黑格納數，此時虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環為唯一分解整環(簡稱 UFD)，由此性質可得到虛二次體的整數環中任一元素的分解有唯一表示法。

首先探討質數 p 在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的分解性，是根據分解性分成四類，再由四類決定 m 的不可約元分解，進一步推導出 $x + y\sqrt{s}i, x - y\sqrt{s}i$ 可能的唯一表示法，再由唯一表示法來計數圓及橢圓上的格子點個數。

Abstract

On the coordinate plane, a lattice point is a point whose x and y coordinates are both integers. This research discusses the numbers of lattice points on circles and ellipses $x^2 + sy^2 = m$, and these numbers are presented as product formulae, where s is a Heegner number. In this case the ring of algebraic integers of imaginary quadratic field $\mathbb{Q}[\sqrt{-s}]$ is a unique factorization domain (UFD). From this property, it can be obtained that the factorization of any elements in the ring of algebraic integers of imaginary quadratic field $\mathbb{Q}[\sqrt{-s}]$ has a unique representation.

First, we discuss the factorization of the prime number p in the ring of algebraic integers of imaginary quadratic $\mathbb{Q}[\sqrt{-s}]$. It is divided into four categories according to the factorization properties. Then we determine the factorization of m into irreducibles via the four categories. Further, we derive possible unique representations of $x + y\sqrt{s}i, x - y\sqrt{s}i$ and use these unique representations to count the numbers of lattice points on circles and ellipses.

壹、前言

在專題研究中，閱讀**科學月刊** (游森棚[1])：「**圓上的格子點**」，文章中提到由數學家**勒讓德** (Legendre) 與**高斯** (Gauss) 計算圓上的格子點之個數性質：

給定圓方程式為 $x^2+y^2=m$ **，設** $N_1(m)$ **與** $N_3(m)$ **分別為** m **的奇因數中模 4 餘 1 與模 4 餘 3 的個數，則圓上恰通過** $4\left[N_1(m)-N_3(m)\right]$ **個格子點。**

對上述性質除了好奇外，更感興趣是否能推導**另一個圓上的格子點個數公式呢**？此個數是以連乘積形式呈現，於是想推廣至橢圓 $\Omega_s: x^2+sy^2=m$ (s **為黑格納數**)上的格子點個數，同樣此個數是以連乘積形式呈現。為了對連乘積表達式有進一步認識，再查閱到 J.Cilleruelo and A.C´ordoba [5]中 Corollary 4.(p5)給我們啟發：在某些特定條件下，橢圓上的格子點個數是存在連乘積表達式。我們首先探討質數 p 在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的分解性，分解性如何分類呢？在 Aleksander Skenderi [2]中有探討 $x^2+sy^2=p$ $(s=1,2,3,7)$ 有整數解的充要條件為特定型質數，進一步探討其餘黑格納數 s 的情況。我們將這些特定型質數由分解性做分類，再由分解性協助計數圓及橢圓 $\Omega_s: x^2+sy^2=m$ 上的格子點個數。

底下是本作品的研究目的：

一、探討質數 p 在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的分解性。

二、計數圓及橢圓 $\Omega_s: x^2+sy^2=m$ 上的格子點個數，並且此個數以連乘積表達式呈現。

貳、研究設備及器材

筆、紙、電腦、GeoGebra5.0 動態幾何繪圖板、Wolfram Mathematica 及 OEIS 網站。

參、研究過程或方法

一、名詞定義與先備知識

本作品主要探討圓及橢圓 $\Omega_s: x^2+sy^2=m$ 上格子點個數，其中 s 為黑格納數，並且 s 只有九個： $1,2,3,7,11,19,43,67,163$)及 $m\in\mathbb{Z}$ 來探討。

【定義 1】(整環、可逆元素、不可約元素及相伴元素)

整環 (integral domain) 是指含乘法單位元素的無零因子的**交換環**。而**無零因子**等價於 $ab=0\Rightarrow a=0$ 或 $b=0$。在有乘法單位元素 1 的環 R 中，

(i)若 a 為環 R 中**可逆元素**，則存在環 R 中元素 b 使得 $ab=ba=1$。

(ii)若 a 為環 R 中**不可約元素**，則不存在 b,c 不可逆使得 $a=bc$。

(iii)在環 R 中，a 整除 b 是指存在環 R 中元素 c 使得 $b=ac$，記作 $a\mid b$。

(iv)若 a,b 為環 R 中**相伴元素**，則 $a\mid b$ 且 $b\mid a$。

相伴元素的重要性質：a,b 為在整環中相伴元素充要條件為存在可逆元素 u 使得 $a=bu$。

【定義 2】(唯一分解整環、Unique factorization domain、UFD**)**

唯一分解整環是一個整環且滿足(i)任一非零元素可表為有限多個不可約元素相乘。

(ii)任一非零元素 m，若存在不可約元素 $p_1,p_2,\cdots,p_v$ 與 $q_1,q_2,\cdots,q_w$ 使得

$m=p_1\times p_2\times\cdots\times p_v=q_1\times q_2\times\cdots\times q_w$，則 $v=w$，並且 $q_1,q_2,\cdots,q_v$ 可重排為 $q_{\pi(1)},q_{\pi(2)},\cdots,q_{\pi(v)}$ 使得 q_j , $p_{\pi(j)}$ 為**相伴元素** $(1\le j\le v)$。

【定義 3】(代數整數)

設 α 為複數，若 α 為存在領導係數為 1 的整係數多項式之根，則稱 α 為**代數整數** (algebraic integer)。所有代數整數構成一個環，記作 A 。

【定義 4】(二次體□ $[\sqrt{-d}]$)

二次體是指有理數體□ 的二次擴體。二次體可表示為□ $[\sqrt{-d}]$，其中 d 無平方因數。

若 $d<0$，則稱其為**實二次體**。若 $d>0$，則稱其為**虛二次體**。

【定義 5】(虛二次體□ $[\sqrt{-d}]$的整數環)

虛二次體□ $[\sqrt{-d}]$的整數環是指虛二次體□ $[\sqrt{-d}]$中的代數整數，整數環即□ $[\sqrt{-d}]\cap$ A 。

【定義 6】(黑格納數、Heegner number**)**

黑格納數 **(**Heegner number**)** s 是指滿足兩個性質： s 為非平方數的正整數且虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環為唯一分解整環。由**高斯**發現此數僅有九個：$1,2,3,7,11,19,43,67,163$ 。

注意本作品中提到的 s 皆指黑格納數。

【先備定理 1】(虛二次體 $\mathbb{Q}[\sqrt{-d}]$ 的整數環)

虛二次體 $\mathbb{Q}[\sqrt{-d}]$ 的整數環為

$$\begin{cases} \mathbb{Q}[\sqrt{-d}]=\left\{a+b\sqrt{-d}\,\middle|\,a,b\in\mathbb{Z}\right\} & ,\text{其中 } d\equiv 1,2 \pmod 4 \\ \mathbb{Z}\oplus\mathbb{Z}\cdot\dfrac{1+\sqrt{-d}}{2}=\left\{\dfrac{a+b\sqrt{-d}}{2}\,\middle|\,a,b\in\mathbb{Z},\ a,b\text{為同奇數或同偶數}\right\} & ,\text{其中 } d\equiv 3 \pmod 4 \end{cases}。$$

【先備定理 2】(在整數環 $\mathbb{Z}[i]$ 及 $\mathbb{Z}[\sqrt{-2}]$ 中的可逆元素)

(i)在整數環 $\mathbb{Z}[i]$ 中的可逆元素為 $\pm 1,\pm i$ 。(ii)在整數環 $\mathbb{Z}[\sqrt{-2}]$ 中的可逆元素為 ± 1 。

【證明】設 $a+b\sqrt{-s}$ 為在 $\mathbb{Q}[\sqrt{-s}]$ 中的可逆元素，其中 $s=1,2$ 且 $a,b\in\mathbb{Z}$ ，則存在

$c+d\sqrt{-s}\in\mathbb{Q}[\sqrt{-s}]$ 使得 $\left(a+b\sqrt{-s}\right)\left(c+d\sqrt{-s}\right)=\left(c+d\sqrt{-s}\right)\left(a+b\sqrt{-s}\right)=1$ 。

推得 $\left|a+b\sqrt{-s}\right|^2\left|c+d\sqrt{-s}\right|^2=\left|c+d\sqrt{-s}\right|^2\left|a+b\sqrt{-s}\right|^2=1$ ，即

$$\left(a^2+sb^2\right)\left(c^2+sd^2\right)=1。 \qquad (1)$$

(i)當 $s=1$ 時，(1)式為 $\left(a^2+b^2\right)\left(c^2+d^2\right)=1$ ，在(1)式要有整數解且 $a^2,b^2,c^2,d^2\geq 0$ ，所以僅有 $\begin{cases}a^2+b^2=1\\ c^2+d^2=1\end{cases}$ 成立，求整數解得到 $a=\pm 1,b=0$ 或 $a=0,b=\pm 1$ ，故在整數環 $\mathbb{Z}[i]$ 中的可逆元素為 $\pm 1,\pm i$ 。

(ii)當 $s=2$ 時，(1)式為 $\left(a^2+2b^2\right)\left(c^2+2d^2\right)=1$ ，在(1)式要有整數解且 $a^2,b^2,c^2,d^2\geq 0$ ，所以僅有 $\begin{cases}a^2+2b^2=1\\ c^2+2d^2=1\end{cases}$ 成立，求整數解得到 $a=\pm 1,b=0$ ，故在整數環 $\mathbb{Z}[\sqrt{-2}]$ 中可逆元素為 ± 1 。 ■

【先備定理 3】(在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的可逆元素，參考文獻[11])

在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的可逆元素 $(s \neq 1,2)$ 為 $\begin{cases} \pm 1 \text{ 或 } \dfrac{\pm 1 \pm \sqrt{3}i}{2}, \text{其中 } s=3 \\ \pm 1 \qquad\qquad , \text{其中 } s \neq 3 \end{cases}$ 。

【證明】 設 $\dfrac{a+b\sqrt{-s}}{2}$ 為在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的可逆元素 $(s \neq 1,2)$，其中 a,b 為同偶數或同奇數，則存在在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的元素 $\dfrac{c+d\sqrt{-s}}{2}$ 使得

$$\left(\frac{a+b\sqrt{-s}}{2}\right)\left(\frac{c+d\sqrt{-s}}{2}\right)=\left(\frac{c+d\sqrt{-s}}{2}\right)\left(\frac{a+b\sqrt{-s}}{2}\right)=1 \text{。}$$

推得 $\left|\dfrac{a+b\sqrt{-s}}{2}\right|^2\left|\dfrac{c+d\sqrt{-s}}{2}\right|^2=\left|\dfrac{c+d\sqrt{-s}}{2}\right|^2\left|\dfrac{a+b\sqrt{-s}}{2}\right|^2=1$，即

$$\left(a^2+sb^2\right)\left(c^2+sd^2\right)=16 \text{。} \tag{2}$$

(i)當 $s=3$ 時，(2)式為 $\left(a^2+3b^2\right)\left(c^2+3d^2\right)=16$，在(2)式要有整數解下，有 $a^2+3b^2=1$ 或 $a^2+3b^2=4$ 或 $a^2+3b^2=16$ 等三種情況有整數解。但 a,b,c,d 為同偶數或同奇數，所以僅有 $\begin{cases} a^2+3b^2=4 \\ c^2+3d^2=4 \end{cases}$ 成立，求整數解得到 $a=\pm 2, b=0$ 或 $a=\pm 1, b=\pm 1$，故在 $\mathbb{Q}[\sqrt{-3}]$ 中的整數環中的可逆元素為 ± 1 或 $\dfrac{\pm 1 \pm \sqrt{3}i}{2}$ 。

(ii)當 $s \neq 3$ 時，(2)式為 $\left(a^2+sb^2\right)\left(c^2+sd^2\right)=16$，在(2)式要有整數解下，有 $a^2+sb^2=1$ 或 $a^2+sb^2=4$ 或 $a^2+sb^2=16$ 等三種情況有整數解。但 a,b,c,d 為同偶數或同奇數，所以僅有 $\begin{cases} a^2+sb^2=4 \\ c^2+sd^2=4 \end{cases}$ 成立，求整數解得到 $a=\pm 2, b=0$，故在 $\mathbb{Q}[\sqrt{-s}]$ 中的整數環中的可逆元素為 ± 1。 ■

【定義 7】(二次剩餘)

設 $p>0, x \in N$ 且 $\gcd(x,p)=1$，若 $x^2 \equiv a \pmod{p}$，則稱 a **為模 p 的二次剩餘**。

【定義 8】(勒讓德符號)

設 p 為奇質數且 a 為非零整數，若 $p \nmid a$ ，則**勒讓德符號**定義

$$\left(\frac{a}{p}\right)=\begin{cases} 1, \text{若} a \text{是模} p \text{的二次剩餘} \\ -1, \text{若} a \text{是模} p \text{的二次非剩餘} \end{cases}。$$

本作品探討圓及橢圓 $\Omega_s : x^2+sy^2=m$ (s 為黑格納數)上的格子點個數，首先要探討質數 p 在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的分解性，分解性在 Aleksander Skenderi [2]及 David A. Cox[3]中針對 $s=1,2,3,7$ 作探討，在本作品中我們想要進一步探討其餘黑格納數 s 的情況。

接著由質數 p 在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的分解性決定 m 中質因數分解成不可約元連乘，稱為 m **的不可約元分解**。另外從**相伴元選出代表元**，若選定每一類相伴元不可約元中的代表元，任一非零元素可”**唯一**“表為 $m=up_1\times p_2\times\cdots\times p_v$ ，其中 u 為可逆元素且 $p_j\ (1\le j\le v)$ 為代表元，稱為 m **的唯一表示法**。

【性質 1】(任一非零元素 m 有唯一表示法)

在唯一分解整環中，若已決定每一組相伴元不可約元中的代表元，則任一非零元素 m 有唯一表示法，即 $m=up_1\times p_2\times\cdots\times p_v$ ，其中 $p_j\ (1\le j\le v)$ 為代表元且 u 為可逆元素。

【證明】設 m 存在另一個表示法為 $u'p_1'\times p_2'\times\cdots\times p_w'$ ，其中 $p_j'\ (1\le j\le w)$ 為代表元且 u' 為可逆元素，則由**唯一分解整環性質**可知 $v=w$ 且存在可逆元素 u_j 使得 $p_j'=u_jp_{\pi(j)}$ 。

又 p_j', p_j 皆為代表元且 $p_j', p_{\pi(j)}$ 為相伴元，所以 $p_j'=p_{\pi(j)}$ ，即 $u_j=1$ ，故

$$m=u'p_1'\times p_2'\times\cdots\times p_v'=u'p_{\pi(1)}\times p_{\pi(2)}\times\cdots\times p_{\pi(v)}=u'(p_1\times p_2\times\cdots\times p_v)。$$

又 $m=up_1\times p_2\times\cdots\times p_v$ ，推得 $(u-u')(p_1\times p_2\times\cdots\times p_v)=0$ 。

又 $p_1, p_2,\cdots, p_v\neq 0$ ，因此， $u=u'$ 。 ■

例如：質數 $m=7$ 在虛二次體 $\mathbb{Q}[\sqrt{-3}]$ 的整數環中的不可約元分解可寫成

$$\left[\left(\frac{1+\sqrt{3}i}{2}\right)^n(2+\sqrt{3}i)\right]\times\left[\left(\frac{1-\sqrt{3}i}{2}\right)^n(2-\sqrt{3}i)\right]$$，其中 $n=1,2,3,\cdots,6$。

若選擇代表元 $p'=2+\sqrt{3}i, p''=2-\sqrt{3}i$ ，則 $m=7$ **的唯一表示法**為 $1\times\left(2+\sqrt{3}i\right)\left(2-\sqrt{3}i\right)$ ，其中1為可逆元素。

二、探討質數 p 在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的分解性

(一)質數 p 在整數環 $\mathbb{Q}[i]$ 及 $\mathbb{Q}[\sqrt{-2}]$ 中的分解性

現在要探討質數 p 在整數環 $\mathbb{Q}[i]$ 及 $\mathbb{Q}[\sqrt{-2}]$ 中的分解性，在 Aleksander Skenderi [2]中

定理 2.22：

【先備定理 4】對於奇質數 p ，

(i) $x^2+y^2=p$ 有整數解的充要條件為 $p\equiv 1 \pmod 4$。(即**費馬平方和定理**，參考文獻[13])

(ii) $x^2+2y^2=p$ 有整數解的充要條件為 $p\equiv 1,3 \pmod 8$。

(iii) $x^2+3y^2=p$ 有整數解的充要條件為 $p=3$ 或 $p\equiv 1 \pmod 3$。

(iv) $x^2+7y^2=p$ 有整數解的充要條件為 $p=7$ 或 $p\equiv 1,9,11,15,23,25 \pmod{28}$。

先備定理 4 在 Aleksander Skenderi [2]中是採用二次式方式來證明，(i)與(ii)中所指質數 p 在整數環 $\mathbb{Q}[i]$ 及 $\mathbb{Q}[\sqrt{-2}]$ 是屬於兩個非相伴元的不可約元相乘：型如

$p=(x+y\sqrt{si})(x-y\sqrt{si})\ (s=1,2)$ ，其中 x,y 為整數，稱此類質數 p 為**第 II_s 類質數**。

底下**引理 1** 的證明在參考文獻[13]找到，我們嘗試推廣證明 $s=2,3,7$ ，當 $s=2,3$ 時，演算法規律較單純，但證明到 $s=7$ 時，演算法仍有規律，但無法證明此規律，未來將重新檢視演算法中的規律並且證明。

底下**引理 1** 的證明會用到**婆羅摩笈多－斐波那契恆等式：**

對於任意實數 a,b,c,d ，滿足 $(a^2+b^2)(c^2+d^2)=(ac+bd)^2+(ad-bc)^2$ 。

【引理 1】(費馬平方和定理，David A. Cox[3]及參考文獻[13])

設 p 為奇質數，則 $x^2+y^2=p$ 有整數解若且唯若 $p\equiv 1 \pmod 4$ 。

【證明】“**必要性**”當 $x^2+y^2=p$ 有解時， x,y 必定一奇一偶。令 $x=2k_1+1, y=2k_2$ ，其中 $k_1,k_2\in$ ，則 $p=(2k_1+1)^2+(2k_2)^2=4(k_1^2+k_1+k_2^2)+1$ ，故 $p\equiv 1 \pmod 4$ 。

“**充分性**”設 $p\equiv 1 \pmod 4$ ，則由 **Wilson 定理**可知 $(p-1)!\equiv -1 \pmod p$ 。又

$$(p-1)!\equiv 1\times 2\times 3\times\cdots\times\frac{p-1}{2}\times\left(-\frac{p-1}{2}\right)\cdots\times(-3)\times(-2)\times(-1)$$
$$\equiv(-1)^{\frac{p-1}{2}}\left[\left(\frac{p-1}{2}\right)!\right]^2\equiv\left[\left(\frac{p-1}{2}\right)!\right]^2,$$

若 $\left[\left(\frac{p-1}{2}\right)!\right]\equiv r \pmod p$ ，則

當 $r\le\frac{p-1}{2}$ 時，取 $x=r\le\frac{p-1}{2}$ 使得 $x^2=r^2\equiv(p-1)!\equiv -1 \pmod p$ 。

當 $r>\frac{p-1}{2}$ 時，取 $x=p-r<p-\frac{p-1}{2}=\frac{p+1}{2}$ 使得 $x^2\equiv r^2\equiv(p-1)!\equiv -1 \pmod p$ 。

上述可知存在一整數 x 且 $0<|x|\le\frac{p-1}{2}$ 使得 $x^2+1^2\equiv 0 \pmod p$ (此 x 稱為**絕對最小剩餘**)，故存在整數 x,y,m_0 使得 $1\le m_0<p$ 且取 m_0 為最小正整數使得 $x^2+y^2=m_0p$ 。

底下要證明 $m_0=1$ 。

令 $m_0>1$ ，取正整數 e,f 且 $|e|,|f|\le\frac{m_0}{2}$ 使得 $x\equiv e \pmod{m_0}$ 且 $y\equiv f \pmod{m_0}$ ，則

$0<e^2+f^2\le\left(\frac{m_0}{2}\right)^2+\left(\frac{m_0}{2}\right)^2=\frac{m_0^2}{2}$ 且 $x^2+y^2\equiv e^2+f^2 \pmod{m_0}$ ，即存在正整數 m_1 使得

$1\le m_1\le\frac{m_0}{2}<m_0$ 且 $e^2+f^2=m_1m_0$ ，故由**婆羅摩笈多－斐波那契恆等式**可知

$$(m_0p)(m_1m_0)=(x^2+y^2)(e^2+f^2)=(ex+fy)^2+(ey-fx)^2 。$$

又 $ex+fy\equiv x^2+y^2\equiv m_0p\equiv 0 \pmod{m_0}$ 且 $ey-fx\equiv xy-yx\equiv 0 \pmod{m_0}$ ，所以

$\left(\frac{ex+fy}{m_0}\right)^2+\left(\frac{ey-fx}{m_0}\right)^2=m_1p$ 且 $1\le m_1\le\frac{m_0}{2}<m_0$ ，與 m_0 為最小正整數矛盾，故 $m_0=1$ ，

即 $x^2+y^2=p$ 。因此， $x^2+y^2=p$ 有整數解若且唯若 $p\equiv 1 \pmod 4$ 。 ■

【註】由上面證明給了啟發，提出一個演算法，此演算法可以協助檢查 $x^2+sy^2=p$ 有整數解的存在性，演算法的步驟說明如下：

Step 1：找到一整數 x_0, y_0, m_0 使得 $1\le m_0<p$ 且 $x_0^2+sy_0^2=m_0 p$ 。

Step 2：若有整數 x_k, y_k, m_k 使得 $1\le m_k<p$ 且 $x_k^2+sy_k^2=m_k p$ ，且取正整數 e_k, f_k 且

$|e_k|, |f_k| \le \frac{m_k}{2}$ 使得 $x_k\equiv e_k \pmod{m_k}$ 且 $y_k\equiv f_k \pmod{m_k}$ ，則

存在正整數 m_{k+1} 使得 $\left(\frac{e_k x_k+sf_k y_k}{m_k\cdot \gcd(e_k, f_k)}\right)^2+s\left(\frac{e_k y_k-f_k x_k}{m_k\cdot \gcd(e_k, f_k)}\right)^2=m_{k+1}p$ ，

令 $x_{k+1}=\frac{e_k x_k+sf_k y_k}{m_k}, y_{k+1}=\frac{e_k y_k-f_k x_k}{m_k}$ ，則 $x_{k+1}^2+sy_{k+1}^2=m_{k+1}p$ 。

Step 3：重複操作 *Step* 2 ，若有正整數 n 使得 $m_n=1$ 或 $m_n=4$ ，此時就能保證存在 $x^2+sy^2=p$ 或 $x^2+sy^2=4p$ 的整數解。

我們從數據發現操作有限次必得到 $m_n=1$ 或 $m_n=4$ ($s\ge 7$ 才會發生)，按照上述步驟發現 m_{k+1} 一定比 m_k 小，未來要證明此性質。進一步將質數 p 在整數環 $\mathbb{Z}[i]$ 及 $\mathbb{Z}[\sqrt{-2}]$ 、虛二次體 $\mathbb{Q}[\sqrt{-3}]$ 的整數環中的質數 p 再細分種類，將兩個相同不可約元相乘的質數 p 稱為**第 I_s 類質數**及不可分解的質數 p 稱為**第 III_s 類質數**。

【先備定理 5】(p 在整數環 $\mathbb{Z}[i]$ 中的分解性，Aleksander Skenderi [2]及參考文獻[13])

設 p 為質數，質數 p 則在整數環 $\mathbb{Z}[i]$ 中有以下三種情形：

(i) $2=-i(1+i)^2$ 。(ii)存在兩個非相伴元的不可約 $p', p''\in\mathbb{Z}[i]$ 使得 $p=p'p''$ ，此時 p 為 $p\equiv 1 \pmod 4$ 型的質數。(iii) p 為在 $\mathbb{Z}[i]$ 中不可分解，此時 p 為 $p\equiv 3 \pmod 4$ 型的質數。

【證明】(i)由於 $2=(1+i)(1+i)=-i(1+i)^2$ ，所以 $2=-i(1+i)^2$ 。

(ii)由**引理 1** 知 $x^2+y^2=p$ 有整數解的充要條件為 $p\equiv 1 \pmod 4$ 。

又 $x^2+y^2=(x+yi)(x-yi)=p$ ，其中 x,y 為非零的整數，所以 $x+yi, x-yi$ 為非相伴元的不可約，此時 p 為 $p\equiv 1 \pmod 4$ 型的質數。

(iii)由(ii)的證明可知若 p 不為 $p\equiv 1 \pmod 4$ 型的質數，則 p 為在整數環 $\mathbb{Z}[i]$ 中不可分解，此時 p 為 $p\equiv 3 \pmod 4$ 型的質數。 ■

仿照**先備定理 5** 可證明**先備定理 6 及先備定理 7**。

【先備定理 6】(p 在整數環 $\mathbb{Z}[\sqrt{-2}]$ 中的分解性，Aleksander Skenderi [2]及 David A. Cox[3])

設 p 為質數，質數 p 則在整數環 $\mathbb{Z}[\sqrt{-2}]$ 中有以下三種情形：

(i) $2=-(\sqrt{2}i)^2$ 。(ii)存在兩個非相伴元的不可約 $p', p'' \in \mathbb{Z}[\sqrt{-2}]$ 使得 $p=p'p''$ ，此時 p 為 $p\equiv 1 \pmod 8$ 型或 $p\equiv 3 \pmod 8$ 型的質數。(iii) p 為在整數環 $\mathbb{Z}[\sqrt{-2}]$ 中不可分解，此時 p 為 $p\equiv 5 \pmod 8$ 型或 $p\equiv 7 \pmod 8$ 型的質數。

【先備定理 7】(p 在虛二次體 $\mathbb{Z}[\sqrt{-3}]$ 的整數環中的分解性，Aleksander Skenderi [2])

設 p 為質數，質數 p 則在虛二次體 $\mathbb{Z}[\sqrt{-3}]$ 的整數環中有三種情形：

(i) $3=-(\sqrt{3}i)^2$ 。(ii)存在兩個非相伴元的不可約 $p', p'' \in \mathbb{Z}[\sqrt{-3}]$ 使得 $p=p'p''$ ，此時 p 為 $p\equiv 1 \pmod 6$ 型的質數。(iii) p 為在 $\mathbb{Z}[\sqrt{-3}]$ 的整數環中不可分解，此時 p 為 2 或 $p\equiv 5 \pmod 6$ 型的質數。

(二)質數 p 在虛二次體 $\mathbb{Z}[\sqrt{-s}]\,(s\geq 7)$ 的整數環中的分解性

底下探討當質數 p 在虛二次體 $\mathbb{Z}[\sqrt{-s}]\,(s\geq 7)$ 的整數環中的分解性是否如 $s=1,2,3$ 中僅分成三類呢？以 $s=11$ 為例來說明：考慮 $x^2+11y^2=p$ 有整數解，若考慮 $p\equiv 1,3,5,9,15 \pmod{22}$ 型的質數，發現並非所有 $p\equiv 1,3,5,9,15 \pmod{22}$ 型的質數使得 $x^2+11y^2=p$ 有整數解，注意到當 $p=23,31,37,59,67,71,89$ 時， $x^2+11y^2=p$ 無整數解，進一步發現：

(i)取 $x=1, y=2$ 代入 $3x^2+2xy+4y^2$ 就可求得 23，所以 23 為 $3x^2+2xy+4y^2$ 型的質數。

可由 $x^2+11y^2=4\times 23$ 整數解為 $(\pm 9, \pm 1)$ 中得到 $23=\left(\frac{9+1\cdot\sqrt{11}i}{2}\right)\left(\frac{9-1\cdot\sqrt{11}i}{2}\right)$。

(ii)取 $x=3, y=-2$ 代入 $3x^2+2xy+4y^2$ 就可求得 31，所以 31 為 $3x^2+2xy+4y^2$ 型的質數。

可由 $x^2+11y^2=4\times 31$ 整數解為 $(\pm 5, \pm 3)$ 中得到 $31=\left(\frac{5+3\sqrt{11}i}{2}\right)\left(\frac{5-3\sqrt{11}i}{2}\right)$。

從上述例子可猜測特定二次型 $ax^2+bxy+cy^2$ 的質數 p 會使得 $x^2+sy^2=p$ 無整數解，並且此質數 p 可表示為 $\left(\frac{x'+y'\sqrt{si}}{2}\right)\left(\frac{x'-y'\sqrt{si}}{2}\right)$，底下將會證明上述猜測的結果。為了更進一步瞭解，查閱文獻發現 Aleksander Skenderi [2]中**定理 2.21** 及 David A. Cox[3]中 p25，告訴我們二次剩餘與二次型 $ax^2+bxy+cy^2$ 的質數之關係，其中 a,b,c 為整數。

【定義 9】(二次型 $ax^2+bxy+cy^2$ 的判別式及 reduced)

給定二次型 $ax^2+bxy+cy^2$ $(a,b,c\in\mathbb{Z})$，(i)設 $f(x,y)=ax^2+bxy+cy^2$，則稱 b^2-4ac 為 $f(x,y)$ 的**判別式**，記作 D。(ii)設 a,b,c 滿足 $\gcd(a,b,c)=1$，滿足 $|b|\le a\le c$，並且當 $|b|=a$ 或 $a=c$ 時，$b\ge 0$，則稱為 **reduced**。

【先備定理 8】(二次型質數 p 可表為二次型 $ax^2+bxy+cy^2$ 的性質，Aleksander Skenderi [2])

設 $D\equiv 0,1 \pmod 4$ 且 D 為負整數，若 p 為奇質數，則 $\left(\frac{D}{p}\right)=1$ 若且唯若質數 p 可表為二次型 $ax^2+bxy+cy^2$，其中此二次型 $ax^2+bxy+cy^2$ 為 **reduced** 且判別式 D 為 b^2-4ac。

底下利用**先備定理 8** 來證明**引理 2**。

【引理 2】(在 $-s$ 為模 p 的二次剩餘下，二次型質數 p 的種類，Aleksander Skenderi [2])

給定 $s=3,7,11,19,43,67,163$，設 p 為奇質數，若 $\left(\frac{-s}{p}\right)=1$，則

當 $s=3,7$ 時，質數 p 可表為二次型 x^2+sy^2。

當 $s=11$ 時，質數 p 可表為二次型 x^2+11y^2 或 $3x^2+2xy+4y^2$。

當 $s=19$ 時，質數 p 可表為二次型 x^2+19y^2 或 $4x^2+2xy+5y^2$ 。

當 $s=43$ 時，質數 p 可表為二次型 x^2+43y^2 或 $4x^2+2xy+11y^2$ 。

當 $s=67$ 時，質數 p 可表為二次型 x^2+67y^2 或 $4x^2+2xy+17y^2$ 。

當 $s=163$ 時，質數 p 可表為二次型 x^2+163y^2 或 $4x^2+2xy+41y^2$ 。

【**證明**】令 $D=-4s\equiv 0 \pmod 4$ ，因為

$$\left(\frac{D}{p}\right)=\left(\frac{-4s}{p}\right)=\left(\frac{2}{p}\right)^2\left(\frac{-s}{p}\right)=(-1)^{2\times\frac{p^2-1}{8}}\left(\frac{-s}{p}\right)=(-1)^{\frac{p^2-1}{4}}\left(\frac{-s}{p}\right)=\left(\frac{-s}{p}\right)=1$$ ，所以

由**先備定理 8** 可知質數 p 可表為二次型 $ax^2+bxy+cy^2$ ，其中二次型 $ax^2+bxy+cy^2$ 為 **reduced**。

由於 $D=b^2-4ac=-4s$ ，所以 $ac=\dfrac{b^2+4s}{4}$ 。又 $|b|\le a\le c$ ，推得

$b^2=4ac-4s=4(ac-s)\ge 4(b^2-s)$ ，化簡為 $b^2\le\dfrac{4s}{3}$ ，其中 $s=3,7,11,19,43,67,163$ 。 (3)

(i)當 $b=0$ 時，(3)式顯然成立，代入 $b^2-4ac=-4s$ ，推得 $ac=s$ 。又 s 為質數且 a,c 必須滿足 $|b|\le a\le c$ ，所以 $a=1$ 且 $c=s$ ，故質數 p 為二次型 x^2+sy^2 的質數。

底下將滿足 $|b|\ge 1$ 分為奇數與偶數來討論，注意求得 a,c 必須滿足三個條件：

$$a,c\in\square \text{ 、 } \gcd(a,b,c)=1 \text{ 及 } |b|\le a\le c \qquad (4)$$

(ii)當 b 為滿足(3)式的奇數時，因為 $ac=\dfrac{b^2+4s}{4}$ 且 s 為質數，所以 $4\nmid(b^2+4s)$ ，得到 $ac\notin\square$ ，但 $a,c\in\square$ ，所以這種情況不合。

(iii)當 b 為滿足(3)式的偶數時，因為 $ac=\dfrac{b^2+4s}{4}$ 且 s 為質數，所以 $4|(b^2+4s)$ ，此時滿足 $a,c\in\square$ 。又 $ax^2-bxy+cy^2=ax^2+bx(-y)+c(-y)^2$ ，所以二次型 $ax^2-bxy+cy^2$ 的質數同於二次型 $ax^2+bxy+cy^2$ 的質數，故底下以 $b>0$ 來討論 $s=3,7,11,19,43,67,163$ 的情況：

①當 $b=2$ 時，由 $b^2=4ac-4s$ 可得 $ac=s+1$ 。

考慮 $s=3$ ，則 $ac=s+1=3+1=4$ ，推得 a,c 的正整數解中均不滿足(4)式中的條件，所以這種情況不合。

考慮 $s=7$，則 $ac=s+1=7+1=8$，推得 a,c 的正整數解中均不滿足(4)式的條件，所以這種情況不合。

考慮 $s=11$，$ac=s+1=11+1=12$，推得 a,c 的正整數解中僅有 $a=3$ 且 $c=4$ 滿足(4)式的條件，所以質數 p 可表為二次型 $3x^2+2xy+4y^2$。

考慮 $s=19$，$ac=s+1=19+1=20$，推得 a,c 的正整數解中僅有 $a=4$ 且 $c=5$ 滿足(4)式的條件，所以質數 p 可表為二次型 $4x^2+2xy+5y^2$。

考慮 $s=43$，$ac=s+1=43+1=44$，推得 a,c 的正整數解中僅有 $a=4$ 且 $c=11$ 滿足(4)式的條件，所以質數 p 可表為二次型 $4x^2+2xy+11y^2$。

考慮 $s=67$，$ac=s+1=67+1=68$，推得 a,c 的正整數解中僅有 $a=4$ 且 $c=17$ 滿足(4)式的條件，所以質數 p 可表為二次型 $4x^2+2xy+17y^2$。

考慮 $s=163$，$ac=s+1=163+1=164$，推得 a,c 的正整數解中僅有 $a=4$ 且 $c=41$ 滿足(4)式的條件，所以質數 p 可表為二次型 $4x^2+2xy+41y^2$。

②當 $b\ (\geq 4)$ 的偶數時，(3)式推得 $16\leq b^2\leq \frac{4s}{3}$，顯然 $s=3,7,11$ 不滿足上述不等式，所以底下僅探討 $s=19,43,67,163$ 的情況。

考慮 $s=19$，代入(3)式得 $16\leq b^2\leq \frac{76}{3}$，求得 $b=4$、5。由 $b^2=4ac-4s$ 且 $a,c\in$ □ 可得 $ac=23$，推得 a,c 的正整數解中均不滿足(4)式的條件，所以這種情況不合。

考慮 $s=43$，代入(3)式得 $16\leq b^2\leq \frac{172}{3}$，求得 $b=4$、5、6 或 7。由 $b^2=4ac-4s$ 且 $a,c\in$ □ 可得 $ac=47$ 或 $ac=52$，推得 a,c 的正整數解中均不滿足(4)式的條件，所以這種情況不合。

考慮 $s=67$，代入(3)式得 $16\leq b^2\leq \frac{268}{3}$，求得 $b=4$、5、6、7、8 或 9。

由 $b^2=4ac-4s$ 且 $a,c\in$ □ 可得 $ac=71$ 或 $ac=76$ 或 $ac=83$，推得 a,c 的正整數解中均不滿足(4)式的條件，所以這種情況不合。

考慮 $s=163$，代入(3)式得 $16\leq b^2\leq \frac{652}{3}$，求得 $b=4,5,6,\cdots,14$。由 $b^2=4ac-4s$ 且

$a,c\in$□ 可得 $ac=167$ 或 $ac=172$ 或 $ac=179$ 或 $ac=188$ 或 $ac=199$ 或 $ac=212$，推得 a,c 的正整數解中均不滿足(4)式的條件，所以這種情況不合。

由以上討論故得證。 ■

由**引理 2** 知當 $s\geq 11$ 時，在 $-s$ 為模 p 的二次剩餘下，質數 p 有二種：一是 x^2+sy^2 型的質數 p ：由於 $x^2+sy^2=(x+y\sqrt{si})(x-y\sqrt{si})$，所以此質數 p 為兩個非相伴元的不可約相乘，型如 $p=(x+y\sqrt{si})(x-y\sqrt{si})$，其中 x,y 為整數，稱此質數 p 為**第 II_s 類質數**。二是二次型 $ax^2+bxy+cy^2$ 的質數 p ，底下要推導 p 為 $\left(\frac{x'+y'\sqrt{si}}{2}\right)\left(\frac{x'-y'\sqrt{si}}{2}\right)$ 型的質數，其中 x',y' 為奇數，稱此質數 p 為**第 IV_s 類質數**。

【引理 3】(奇質數 p 為引理 2 中提到的二次型性質，Aleksander Skenderi [2])

給定 $s=11,19,43,67,163$，若奇質數 p 為**引理 2** 中提到的二次型，則

p 為 $\left(\frac{x'+y'\sqrt{si}}{2}\right)\left(\frac{x'-y'\sqrt{si}}{2}\right)$ 型的質數，其中 x',y' 為奇數。

【證明】(i)當 $s=11$ 時，由**引理 2** 可知 p 為二次型 $3x^2+2xy+4y^2$ 的質數，其中 x,y 為奇數。

因為 $4p=4(3x^2+2xy+4y^2)=11x^2+(x+4y)^2$，令 $x'=x+4y, y'=x$，則

$(x')^2+11(y')^2=4p$，即 $\left(\frac{x'}{2}\right)^2+11\left(\frac{y'}{2}\right)^2=p$，故 p 為 $\left(\frac{x'+y'\sqrt{si}}{2}\right)\left(\frac{x'-y'\sqrt{si}}{2}\right)$ 型的質數。

底下要證明 x',y' 為奇數。

因為 $p\equiv 1\pmod 2$ 且 $p=3x^2+2xy+4y^2\equiv x^2\pmod 2$，所以 $x^2\equiv 1\pmod 2$，故 x 為奇數。

又 $x'=x+4y, y'=x$，因此， x',y' 為奇數。

(ii)仿照(i)可證明，當 $s=19,43,67,163$ 時，由**引理 2** 可知 p 為二次型 $4x^2+2xy+ty^2$ 的質數，其中 $t=5,11,17,41$。因為 $4p=4(4x^2+2xy+ty^2)=(4x+y)^2+sy^2$ ，

令 $x'=4x+y, y'=y$ ，則 $(x')^2+s(y')^2=4p$ ，即 $\left(\frac{x'}{2}\right)^2+s\left(\frac{y'}{2}\right)^2=p$ ，故 p 為 $\left(\frac{x'+y'\sqrt{si}}{2}\right)\left(\frac{x'-y'\sqrt{si}}{2}\right)$ 型的質數。

底下要證明 x', y' 為奇數。

因為 $p\equiv 1 \pmod 2$ 且 $p=4x^2+2xy+ty^2\equiv y^2 \pmod 2$ ，所以 $y^2\equiv 1 \pmod 2$ ，故 y 為奇數。

又 $x'=4x+y, y'=y$ ，因此， x', y' 為奇數。 ■

前面提到第 IV_s $(s\geq 11)$ 類奇質數 p 為 $\left(\frac{x'+y'\sqrt{si}}{2}\right)\left(\frac{x'-y'\sqrt{si}}{2}\right)$ 型的質數，其中 x', y' 為奇數。發現 $2=\left(\frac{1+\sqrt{7i}}{2}\right)\left(\frac{1-\sqrt{7i}}{2}\right)$ ，即在虛二次體 $\mathbb{Q}[\sqrt{-7}]$ 的整數環中存在第 IV_7 類偶質數 2 ，底下就來證明。

【性質 2】(在虛二次體 $\mathbb{Q}[\sqrt{-7}]$ 的整數環中第 IV_7 類的質數)

設 p 為在虛二次體 $\mathbb{Q}[\sqrt{-7}]$ 的整數環中第 IV_7 類質數，則 $p=2$ 。

【證明】由**引理 2** 可知在虛二次體 $\mathbb{Q}[\sqrt{-7}]$ 的整數環中不存在第 IV_7 類的奇質數。

底下要證明在虛二次體 $\mathbb{Q}[\sqrt{-7}]$ 的整數環中是否存在第 IV_7 類的偶質數 2 。

令 $p=\left(\frac{x'+y'\sqrt{7i}}{2}\right)\left(\frac{x'-y'\sqrt{7i}}{2}\right)$ ，其中 x', y' 為整數，則 $(x')^2+7(y')^2=4p$ 。

(i)當 x', y' 為偶數時， $\left(\frac{x'+y'\sqrt{7i}}{2}\right)\left(\frac{x'-y'\sqrt{7i}}{2}\right)\in\mathbb{Q}[\sqrt{-7}]$ ，所以 p 不是第 IV_7 類質數。

(ii)當 x' 為偶數及 y' 為奇數時，因為 $(x')^2\equiv 0,4 \pmod 8$ 且 $(y')^2\equiv 1 \pmod 8$ ，所以 $(x')^2+7(y')^2\equiv 3,7 \pmod 8$ ，但 $4p\equiv 0,4 \pmod 8$ ，故此種情況不合。

(iii)當 x' 為奇數及 y' 為偶數時，因為 $(x')^2\equiv 1 \pmod 8$ 且 $(y')^2\equiv 0,4 \pmod 8$ ，所以

$(x')^2+7(y')^2\equiv 1,5 \pmod 8$ ，但 $4p\equiv 0,4 \pmod 8$ ，故此種情況不合。

(iv)當 x', y' 為奇數時，因為 $(x')^2,(y')^2\equiv 1 \pmod 8$ ，所以

$4p=(x')^2+7(y')^2\equiv 1+7\equiv 0 \pmod 8$ ，推得 $p\equiv 0 \pmod 2$ ，但 p 為質數，因此， $p=2$ 。

■

綜合前面的探討：質數 p 在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的分解性可區分成二種：當 $s=1,2,3$ 時，分解性分成三類，而當 $s\geq 7$ 時，分解性分成四類，參見**引理 4**。

【引理 4】(p 在虛二次體 $\mathbb{Q}[\sqrt{-s}]\,(s\geq 7)$ 的整數環中的分解性，Aleksander Skenderi [2])

設 p 為質數，質數 p 則在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中有四種情形：

(i)**第 I_s 類質數 p** ： $s=-(\sqrt{si})^2$ 。

(ii)**第 II_s 類質數 p** ：存在兩個非相伴元的不可約元相乘：型如 $p=(x+y\sqrt{si})(x-y\sqrt{si})$ ，其中 x, y 為整數。

(iii)**第 III_s 類質數 p** ： p 為在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中不可分解。

(iv)**第 IV_s 類質數 p** ：存在兩個非相伴元的不可約相乘：型如 $p=\left(\frac{x'+y'\sqrt{si}}{2}\right)\left(\frac{x'-y'\sqrt{si}}{2}\right)$ ，其中 x', y' 為奇數。

三、計數圓及橢圓 $\Omega_s: x^2+sy^2=m\,(s=1,2,3)$ 上格子點個數

第二章已探討 p 在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的分解性分類有二種：三類($s=1,2,3$)及四類($s\geq 7$)，為了區分每一類質數，除了當 $s=1$ 時第 I_s 類質數為 2 之外，其餘黑格納數時第 I_s 類質數為 s 、以 p 代表第 II_s 類質數、以 r 代表第 III_s 類質數及以 q 代表第 IV_s 類質數，由以上分類可將 m 的不可約元分解分成三種：對於非負整數 $\lambda, \alpha_j, \beta_k$ 及偶數 γ_ℓ ，

(i)當 $s=1$ 時， m 的不可約元分解為 $2^\lambda\times\prod_{j=1}^{\nu}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$ 。

(ii)當 $s=2,3$ 時， m 的不可約元分解為 $s^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$ 。

(iii)當 $s\neq 1,2,3$ 時， m 的不可約元分解為 $s^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{k=1}^{n}q_k^{\beta_k}$ 。

若選定代表元 $1+i$ (或 $\sqrt{si}$), $p_j^{'}=a_j+b_ji$, $p_j^{''}=a_j-b_ji$, $q_k^{'}=\frac{a_k^{'}+b_k^{'}\sqrt{si}}{2}$, $q_k^{''}=\frac{a_k^{'}-b_k^{'}\sqrt{si}}{2}$

($1\le j\le v$ 、 a_j,b_j 為正整數且 $1\le k\le n$ 、 $a_k^{'},b_k^{'}$ 為正奇數) 後，可得到橢圓 $\Omega_s:x^2+sy^2=m$ 中 m 的唯一表示法，分成三種：

(i)當 $s=1$ 時， m 的唯一表示法為

$$(-i)^{\lambda}\times(1+i)^{2\lambda}\times\prod_{j=1}^{v}\left(p_j^{'}p_j^{''}\right)^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$$ ，其中 $(-i)^{\lambda}$ 為可逆元素。 (5)

(ii)當 $s=2,3$ 時， m 的唯一表示法為

$$(-1)^{\lambda}\times(\sqrt{si})^{2\lambda}\times\prod_{j=1}^{v}\left(p_j^{'}p_j^{''}\right)^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$$ ，其中 $(-1)^{\lambda}$ 為可逆元素。 (6)

(iii)當 $s\neq 1,2,3$ 時， m 的唯一表示法為

$$(-1)^{\lambda}\times(\sqrt{si})^{2\lambda}\times\prod_{j=1}^{v}\left(p_j^{'}p_j^{''}\right)^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{k=1}^{n}\left(q_k^{'}q_k^{''}\right)^{\beta_k}$$ ，其中 $(-1)^{\lambda}$ 為可逆元素。 (7)

因為 $x^2+sy^2=(x+y\sqrt{si})(x-y\sqrt{si})$ ，所以可由 m 的唯一表示法推導 $x+y\sqrt{si}$ 與 $x-y\sqrt{si}$ 可能的唯一表示法，又 $x+y\sqrt{si}$ 的選擇對應橢圓 Ω_s 上的整數解，因此， $x+y\sqrt{si}$ 可能的唯一表示法選擇個數相當於橢圓 Ω_s 上的格子點個數。值得一提，取 γ_ℓ 為偶數的原因是 r_ℓ 為在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中不可分解，若要考慮橢圓 Ω_s 上存在格子點，僅能將 $r_\ell^{\gamma_\ell}$ 平均分配給 $x+y\sqrt{si}$ 與 $x-y\sqrt{si}$ ，故 γ_ℓ 為奇數時，橢圓 Ω_s 上不存在格子點。這章探討 $s=1,2,3$ 的情況。

(一)計數圓 $\Omega_1:x^2+y^2=m$ 上的格子點個數

底下要利用唯一表示法來計數圓 $\Omega_1:x^2+y^2=m$ 上的格子點個數，舉例說明：

例如：計數圓 $\Omega_1:x^2+y^2=2^3\times5^5\times7^2$ 上的格子點個數。

【解法】因為 $2=(1+i)(1-i)=-i(1+i)^2$ 為第 I_1 類質數、 $5=(1+2i)(1-2i)$ 為第 II_1 類質數及 7 為第

III_1類質數，當選擇代表元$1+i, p'=1+2i, p''=1-2i$時，$2^3\times5^5\times7^2$的唯一表示法為

$$(-i)^3(1+i)^6(p')^5(p'')^5\times7^2=i(1+i)^6(p')^5(p'')^5\times7^2$$，其中i為可逆元素。

因為$x^2+y^2=(x+yi)(x-yi)$，由$i(1+i)^6(p')^5(p'')^5\times7^2$推導出$x+yi$可能的唯一表示法選擇為$u(1+i)^3\times\left[(p')^t\times(p'')^{5-t}\right]\times7$，其中$t=0,1,2,3,4,5$，並且可逆元素$u$為$\pm1,\pm i$，所以$t$值選擇共有$5+1$個且可逆元素$u$選擇有4個，故$x+yi$可能的唯一表示法選擇個數為$4\times6=24$，因此，圓$\Omega_1:x^2+y^2=2^3\times5^5\times7^2$上格子點個數為24。 □

定理 1 的結果在參考文獻[5]中 **Corollary 4** 已經證明，同樣是利用唯一分解定理來作證明，此文獻中 **Corollary 4** 告訴我們：對於橢圓$\Omega_s:x^2+sy^2=m$，當質數s為2或$s\equiv1\pmod4$型的質數時，計數橢圓上的格子點個數可以以連乘積形式來表示，但考慮質數s為$s\equiv3\pmod4$型的質數時，卻沒有明確說明。本作品探討s為黑格納數，除了文獻已探討的$s=1,2,3$的情況外，其餘均為$s\equiv3\pmod4$的情況，在此條件下的s是否橢圓$\Omega_s:x^2+sy^2=m$上的格子點個數均能以連乘積形式來表示呢？本作品即將給予解答。底下**定理 1** 的證明雖是已知證明，卻可以提供推廣$s\geq3$時，計數$x^2+sy^2=m$上的格子點個數的證明想法。

【定理 1】(計數圓$\Omega_1:x^2+y^2=m$上的格子點個數，J.Cilleruelo and A.C´ordoba[5])

設圓$\Omega_1:x^2+y^2=2^\lambda\times\prod_{j=1}^{\nu}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$，其中2、$p_j$、$r_\ell$分別為第$I_1$、$II_1$、$III_1$類的質數，

並且λ,α_j為非負整數及γ_ℓ為偶數，則圓Ω_1上的格子點個數為$4\prod_{j=1}^{\nu}(\alpha_j+1)$。

【證明】$2^\lambda\times\prod_{j=1}^{\nu}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$的唯一表示法為(5)式，考慮由

$(-i)^\lambda\times(1+i)^{2\lambda}\times\prod_{j=1}^{\nu}\left(p_j'p_j''\right)^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$推導$x+yi$可能的唯一表示法選擇，因為

$(1+i)^{2\lambda},\prod_{j=1}^{\nu}\left(p_j'p_j''\right)^{\alpha_j},\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\in\mathbb{Z}[i]$，但$x^2+y^2=(x+yi)(x-yi)$，並且$x+yi,x-yi$為共軛複

數，所以第 I_1 類質數及第 III_1 類質數皆採平均分配給 $x+yi$ 與 $x-yi$ ，選擇僅有1個，而考慮第 II_1 類質數 p_j 時，$\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\in\square[i]$ 若且唯若 $h_j=0,1,2,3,\cdots,\alpha_j$ ，推得 $x+yi$ 可能的唯一表示法選擇為 $u(1+i)^{\lambda}\times\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\times\prod_{\ell=1}^{\kappa}r_{\ell}^{\frac{\gamma_\ell}{2}}$ ，並且可逆元素 u 為 $\pm1,\pm i$ ，所以 h_j 值選擇共有 $\prod_{j=1}^{v}\left(\alpha_j+1\right)$ 個，且 u 選擇有 4 個，故 $x+yi$ 可能的唯一表示法選擇個數為 $4\prod_{j=1}^{v}\left(\alpha_j+1\right)$ ，因此，圓 Ω_1 上格子點個數為 $4\prod_{j=1}^{v}\left(\alpha_j+1\right)$ 。 ■

(二)計數橢圓 $\Omega_2:x^2+2y^2=m$ 上的格子點個數

同樣利用**唯一表示法**來計數橢圓 $\Omega_2:x^2+2y^2=m$ 上的格子點個數。

【定理 2】(計數橢圓 Ω_2 上的格子點個數，J.Cilleruelo and A.C´ordoba[5])

設橢圓 $\Omega_2:x^2+2y^2=2^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_{\ell}^{\gamma_\ell}$ ，其中 2 、 p_j 、 r_ℓ 分別為第 I_2 、 II_2 、 III_2 類的質數，並且 λ,α_j 為非負整數及 γ_ℓ 為偶數，則橢圓 Ω_2 上格子點個數為 $2\prod_{j=1}^{v}\left(\alpha_j+1\right)$ 。

【證明】仿照**定理 1** 來證明，由(6)式可得 $x+y\sqrt{2}i$ 可能的唯一表示法選擇為

$$u(\sqrt{2}i)^{\lambda}\times\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\times\prod_{\ell=1}^{\kappa}r_{\ell}^{\frac{\gamma_\ell}{2}}\text{ ，其中 }h_j=0,1,2,\cdots,\alpha_j\ (1\le j\le v)\text{ 。}$$

注意第 I_2 類質數及第 III_2 類質數採平均分配給 $x+y\sqrt{2}i$ 與 $x-y\sqrt{2}i$ ，所以選擇僅有1個，而第 II_2 類質數 p_j 時，$\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\in\square[\sqrt{-2}]$ 若且唯若 $h_j=0,1,2,3,\cdots,\alpha_j$ ，推得 h_j 值選擇共有 $\prod_{j=1}^{v}\left(\alpha_j+1\right)$ 個且可逆元素 u 選擇有 2 個($u=\pm1$)，故 $x+y\sqrt{2}i$ 可能的唯一表示法選擇個數為 $2\prod_{j=1}^{v}\left(\alpha_j+1\right)$ ，因此，橢圓 Ω_2 上格子點個數為 $2\prod_{j=1}^{v}\left(\alpha_j+1\right)$ 。 ■

(三)計數橢圓$\Omega_3 : x^2+3y^2=m$上的格子點個數

同樣利用唯一表示法來計數橢圓$\Omega_3 : x^2+3y^2=m$上的格子點個數。

【定理 3】(計數橢圓Ω_3上的格子點個數)

設橢圓$\Omega_3 : x^2+3y^2=3^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$，其中3、$p_j$、$r_\ell$分別為第$I_3$、$II_3$、$III_3$類的質數，並且$\lambda,\alpha_j$為非負整數及$\gamma_\ell$為偶數，則(i)當$r_\ell\neq 2\ (1\le\ell\le\kappa)$時，橢圓$\Omega_3$上格子點個數為$2\prod_{j=1}^{v}(\alpha_j+1)$。(ii)當$r_1=2$時，橢圓$\Omega_3$上格子點個數為$6\prod_{j=1}^{v}(\alpha_j+1)$。

【證明】仿照**定理 1**來證明，由(7)式可得$x+y\sqrt{3}i$可能的唯一表示法選擇為

$$u(\sqrt{3}i)^{\lambda}\times\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\times\prod_{\ell=1}^{\kappa}r_\ell^{\frac{\gamma_\ell}{2}}\ ，其中\ h_j=0,1,2,\cdots,\alpha_j\ (1\le j\le v)。$$

注意第I_3類質數及第III_3類質數採平均分配給$x+y\sqrt{3}i$與$x-y\sqrt{3}i$，所以選擇僅有1個，而第II_3類質數p_j時，$\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\in\mathbb{Z}[\sqrt{-3}]$若且唯若$h_j=0,1,2,3,\cdots,\alpha_j$，又$h_j$值選擇共有$\prod_{j=1}^{v}(\alpha_j+1)$個，且可逆元素$u$選擇有兩種情況，令其選擇有$\chi$個，所以$x+y\sqrt{3}i$可能的唯一表示法選擇個數為$\chi\prod_{j=1}^{v}(\alpha_j+1)$。

由**先備定理 3**可知在$\mathbb{Z}[\sqrt{-3}]$的整數環中的可逆元素為$\pm1,\frac{\pm1\pm\sqrt{3}i}{2}$等6個。注意2為第$III_3$類的質數，當$r_1=2$時，因為$r_1=2$乘以$\frac{\pm1\pm\sqrt{3}i}{2}$使得在$\mathbb{Z}[\sqrt{-3}]$中，此時$\chi=6$，故(i)當$r_\ell\neq 2\ (1\le\ell\le\kappa)$時，可逆元素的選擇為$\chi=2$，因此，橢圓$\Omega_3$上格子點個數為$2\prod_{j=1}^{v}(\alpha_j+1)$。(ii)當$r_1=2$時，可逆元素的選擇為$\chi=6$，因此，橢圓$\Omega_3$上格子點個數為$6\prod_{j=1}^{v}(\alpha_j+1)$。 ■

【註】J.Cilleruelo and A.C´ordoba [5]有提到**定理 3** 中 $r_\ell = 2$ 的結果：$6\prod_{j=1}^{v}(\alpha_j+1)$，僅寫出式子並未詳細說明，而 $r_\ell \neq 2$ 的情況沒有寫出具體式子，這兩種情況在**定理 3** 都給予討論並且證明。

四、計數橢圓 $\Omega_7 : x^2+7y^2=m$ 上格子點個數

由**性質 2** 可知在 $s=7$ 中的第 IV_7 類質數僅為 2，其餘 $s=11,19,43,67,163$ 中的第 IV_s 類質數不僅只有一個質數且皆為奇質數。本作品由第 IV_s 類質數為奇質數或偶質數分成二章來探討，這章探討 $s=7$ 的情況，第五章探討 $s=11,19,43,67,163$ 的情況。在計數上困難點是在第 IV_7 類質數 2，所以先探討第 IV_7 類質數 2 的性質，參見**引理 5~7**，再利用**引理 5~7** 來協助計數橢圓 $\Omega_7 : x^2+7y^2=m$ 上的格子點個數。

令 $2=q'q''$，則 $q'=\frac{1+\sqrt{7}i}{2}$ 且 $q''=\frac{1-\sqrt{7}i}{2}$。先觀察 $(q')^1=\frac{1+\sqrt{7}i}{2}$、$(q')^2=\frac{-3+\sqrt{7}i}{2}$、$(q')^3=\frac{-5-\sqrt{7}i}{2}$、$(q')^4=\frac{1-3\sqrt{7}i}{2}$、$(q')^5=\frac{11-\sqrt{7}i}{2}$、$(q')^6=\frac{9+5\sqrt{7}i}{2}$、…等等，可猜測對於所有正整數 β，$(q')^\beta$ 均為 $\left(\frac{a'+b'\sqrt{7}i}{2}\right)$ 型的複數，其中 a',b' 為奇數。

令 $(q')^\beta=\left(\frac{1+\sqrt{7}i}{2}\right)^\beta=\frac{a_\beta+b_\beta\sqrt{7}i}{2}$，其中 β 為正整數且 a_β,b_β 為實數，則可觀察到三個性質：

(i)**數列** $\{a_\beta\}$ **滿足** $a_1=1,a_2=-3,a_\beta=a_{\beta-1}-2a_{\beta-2}\ (\beta\geq 3)$ **的數列**。

(ii)**數列** $\{b_\beta\}$ **滿足** $b_1=1,b_2=1,b_\beta=b_{\beta-1}-2b_{\beta-2}\ (\beta\geq 3)$ **的數列**。

(iii) a_β,b_β **模 4 同餘，即餘數皆為 1 或 3**。

底下就來證明上述(i)、(ii)及(iii)。

【引理 5】($\{a_\beta\},\{b_\beta\}$ **為遞迴數列且** a_β,b_β **的同餘性質**)

設 $q'=\frac{1+\sqrt{7}i}{2}$ ，令 $(q')^{\beta}=\frac{a_\beta+b_\beta\sqrt{7}i}{2}$ ，其中 β 為正整數且 a_β,b_β 為實數，則

(i)數列 $\{a_\beta\}$ 滿足 $a_1=1,a_2=-3,a_\beta=a_{\beta-1}-2a_{\beta-2}\ (\beta\geq 3)$ 的數列。

(ii)數列 $\{b_\beta\}$ 滿足 $b_1=1,b_2=1,b_\beta=b_{\beta-1}-2b_{\beta-2}\ (\beta\geq 3)$ 的數列。(iii) a_β,b_β 為奇數且模 4 同餘。

【證明】當 $\beta=1$ 時，$(q')^1=\frac{1+\sqrt{7}i}{2}$ ，所以 $a_1=b_1=1$ 。

當 $\beta=2$ 時，$(q')^2=\frac{-3+\sqrt{7}i}{2}$ ，所以 $a_2=-3,b_2=1$ 。

對於所有正整數 k ，令 $(q')^k=\frac{a_k+b_k\sqrt{7}i}{2}$ ，其中 a_k,b_k 為整數，則

$(q')^k=(q')^{k-1}(q')^1=\left(\frac{a_{k-1}+b_{k-1}\sqrt{7}i}{2}\right)\left(\frac{1+\sqrt{7}i}{2}\right)=\frac{(a_{k-1}-7b_{k-1})+(a_{k-1}+b_{k-1})\sqrt{7}i}{4}$ ，推得

$2a_k=a_{k-1}-7b_{k-1}\cdots$① 且 $2b_k=a_{k-1}+b_{k-1}\cdots$② ，解①②的聯立方程組可得

(i) ①式移項可知 $7b_{k-1}=a_{k-1}-2a_k$ ，得到 $b_{k-1}=\frac{a_{k-1}-2a_k}{7}$ ，可得 $b_k=\frac{a_k-2a_{k+1}}{7}$ 。

代入②式得到 $2\left(\frac{a_k-2a_{k+1}}{7}\right)=a_{k-1}+\left(\frac{a_{k-1}-2a_k}{7}\right)$ ，化簡得到 $a_{k+1}=a_k-2a_{k-1}$ 。

(ii) ②式移項可知 $a_{k-1}=2b_k-b_{k-1}$ ，可得 $a_k=2b_{k+1}-b_k$ 。

代入①式得到 $2(2b_{k+1}-b_k)=(2b_k-b_{k-1})-7b_{k-1}$ ，化簡得到 $b_{k+1}=b_k-2b_{k-1}$ 。

因此，數列 $\{a_\beta\}$ 滿足 $a_1=1,a_2=-3,a_\beta=a_{\beta-1}-2a_{\beta-2}\ (\beta\geq 3)$ 的數列。

數列 $\{b_\beta\}$ 滿足 $b_1=1,b_2=1,b_\beta=b_{\beta-1}-2b_{\beta-2}\ (\beta\geq 3)$ 的數列。

(iii)由(i)及(ii)可知 $a_1=1,a_2=-3,a_\beta=a_{\beta-1}-2a_{\beta-2}$ 且 $b_1=1,b_2=1,b_\beta=b_{\beta-1}-2b_{\beta-2}\ (\beta\geq 3)$ 。

因為初始條件 a_1,a_2,b_1,b_2 皆為奇數，所以代入遞迴關係後得到每一項必為奇數，即 a_β 及 b_β 必為奇數。底下利用**數學歸納法**證明 a_β,b_β 模 4 同餘。

當 $\beta=1$ 時，因為 $(q')^1=\frac{1+\sqrt{7}i}{2}$ ，所以 $a_1\equiv b_1\ (\text{mod } 4)$ ，故 a_1,b_1 模 4 同餘。

設 $\beta\leq k$ 時 a_β,b_β 模 4 同餘，得到 $a_k\equiv b_k\ (\text{mod } 4)$ 且 $a_{k-1}\equiv b_{k-1}\ (\text{mod } 4)$ 。

則 $\beta = k+1$ 時，由(i)及(ii)的遞迴關係可知 $a_{k+1} \equiv a_k - 2a_{k-1} \equiv b_k - 2b_{k-1} \equiv b_{k+1} \pmod 4$ 。

所以 a_{k+1}, b_{k+1} 模 4 同餘。

因此，由**數學歸納法**可得對於正整數 β ， a_β, b_β 模 4 同餘。 ■

由**引理 5** 可知 $(q')^\beta = \dfrac{a_\beta + b_\beta\sqrt{7}i}{2}$ ，其中 a_β, b_β 模 4 同餘，進一步要探討給定非負整數 $t = 0,1,2,\cdots,\beta$ ， t 為何值時使得 $(q')^t (q'')^{\beta-t} \in \mathbb{Z}[\sqrt{-7}]$ 呢？

【引理 6】($(q')^t \times (q'')^{\beta-t} \in \mathbb{Z}[\sqrt{-7}]$ 的充要條件)

設 $q' = \dfrac{1+\sqrt{7}i}{2}$ 且 $q'' = \dfrac{1-\sqrt{7}i}{2}$ ，則(i)對於所有正整數 β ， $(q')^\beta$ 與 $(q'')^\beta \notin \mathbb{Z}[\sqrt{-7}]$ 。

(ii)給定非負整數 $t = 0,1,2,\cdots,\beta$ ， $(q')^t \times (q'')^{\beta-t} \in \mathbb{Z}[\sqrt{-7}]$ 若且唯若 $t = 1,2,3,\cdots,\beta-1$ 。

【證明】(i)由**引理 5** 可知對於所有正整數 β ， $(q')^\beta$ 為 $\left(\dfrac{a_\beta + b_\beta\sqrt{7}i}{2}\right)$ 型的複數，其中 a_β, b_β 為奇數且模 4 同餘，推得 $(q')^\beta \notin \mathbb{Z}[\sqrt{-7}]$ 。

又 $q'' = \overline{q'}$ ，所以 $(q'')^\beta = \left(\overline{q'}\right)^\beta = \overline{(q')^\beta} = \dfrac{\overline{a_\beta + b_\beta\sqrt{7}i}}{2} = \dfrac{a_\beta - b_\beta\sqrt{7}i}{2}$ ，故 $(q'')^\beta \notin \mathbb{Z}[\sqrt{-7}]$ 。

(ii)由於 q', q'' 在(i)中有相同性質，不失一般性令 $t \le \beta - t$ ， $(q')^t (q'')^{\beta-t}$ 可拆解為 $(q'q'')^t (q'')^{\beta-2t}$ 。又 $q'q'' = 2$ 且由**引理 5** 及(i)可知 $(q'')^{\beta-2t}$ 為 $\left(\dfrac{a''+b''\sqrt{7}i}{2}\right)$ 型的複數，其中 a'', b'' 為奇數，所以 $(q'q'')^t (q'')^{\beta-2t} = 2^t \times \left(\dfrac{a''+b''\sqrt{7}i}{2}\right) = 2^{t-1}\left(a''+b''\sqrt{7}i\right)$ ，又 $0 < t < \beta$ ，推得 $t - 1 \ge 0$ ，故 $(q')^t (q'')^{\beta-t} \in \mathbb{Z}[\sqrt{-7}]$ 。因此，上述(i)與(ii)討論可知給定非負整數 $t = 0,1,2,\cdots,\beta$ ， $(q')^t \times (q'')^{\beta-t} \in \mathbb{Z}[\sqrt{-7}]$ 若且唯若 $t = 1,2,3,\cdots,\beta-1$ 。 ■

注意底下**性質 3** 的結果對黑格納數 s 均成立，在此證明後，提供後面章節證明使用。

【性質 3】($p'=a+b\sqrt{si},\ p''=a-b\sqrt{si}$ 中 a,b 的性質)

設 p 為奇數且 $p=p'p''$，若 $p'=a+b\sqrt{si}$ 且 $p''=a-b\sqrt{si}$，則 a,b 模 2 不同餘。

【證明】因為 $p=p'p''=(a+b\sqrt{si})(a-b\sqrt{si})=a^2+sb^2$，又奇數 p 模 2 餘 1，所以

$a^2+sb^2\equiv 1\pmod 2$，又 $s\equiv 1\pmod 2$，推得 $a^2+sb^2\equiv 1\equiv a^2+b^2\equiv a+b\pmod 2$，因此，$a,b$ 模 2 不同餘。 ■

【引理 7】($\prod_{j=1}^{v}\left(p_j'\right)^{h_j}\times\left(p_j''\right)^{\alpha_j-h_j}\times(q')^t\times(q'')^{\beta-t}\in\mathbb{Q}[\sqrt{-7}]$ 的充要條件)

設 p_j 為奇質數且 $p_j=p_j'p_j''$，若 $p_j'=a_j+b_j\sqrt{7i}$、$p_j''=a_j-b_j\sqrt{7i}$ 且 $q'=\frac{1+\sqrt{7i}}{2}$、$q''=\frac{1-\sqrt{7i}}{2}$，其中 $1\le j\le v$ 且 a_j,b_j 為模 2 不同餘，則給定 $h_j=0,1,2,\cdots,\alpha_j$ 且 $t=0,1,2,\cdots,\beta$，

$\prod_{j=1}^{v}\left(p_j'\right)^{h_j}\times\left(p_j''\right)^{\alpha_j-h_j}\times(q')^t\times(q'')^{\beta-t}\in\mathbb{Q}[\sqrt{-7}]$ 若且唯若 $t=1,2,3,\cdots,\beta-1$。

【證明】對於非負整數 $h_j=0,1,2,\cdots,\alpha_j(1\le j\le v)$，令 $\prod_{j=1}^{v}\left(p_j'\right)^{h_j}\times\left(p_j''\right)^{\alpha_j-h_j}=c+d\sqrt{7i}$，則

$\left(c+d\sqrt{7i}\right)\left(c-d\sqrt{7i}\right)=\left[\left(p_j'\right)^{h_j}\times\left(p_j''\right)^{\alpha_j-h_j}\right]\times\left[\left(p_j''\right)^{h_j}\times\left(p_j'\right)^{\alpha_j-h_j}\right]=\left(p_j'p_j''\right)^{\alpha_j}=p_j^{\alpha_j}$ 為奇數。

故由**性質 3** 可知 c,d 為模 2 不同餘。

底下分兩種情況討論來證明：

$\left(c+d\sqrt{7i}\right)\left[(q')^t\times(q'')^{\beta-t}\right]\in\mathbb{Q}[\sqrt{-7}]$ 若且唯若 $h_j=0,1,2,\cdots,\alpha_j$ 且 $t=1,2,3,\cdots,\beta-1$。

(i)當 $t=1,2,3,\cdots,\beta-1$ 時，由**引理 6** 可知 $(q')^t\times(q'')^{\beta-t}\in\mathbb{Q}[\sqrt{-7}]$，又 $c+d\sqrt{7i}\in\mathbb{Q}[\sqrt{-7}]$，所以 $\left(c+d\sqrt{7i}\right)\left[(q')^t\times(q'')^{\beta-t}\right]\in\mathbb{Q}[\sqrt{-7}]$。

(ii)當 $t\ne 1,2,3,\cdots,\beta-1$ 時，$t=0$ 或 β，即 $(q')^t\times(q'')^{\beta-t}$ 為 $(q'')^\beta$ 或 $(q')^\beta$。

由**引理 5** 可知 $(q')^\beta$ 與 $(q'')^\beta\notin\mathbb{Q}[\sqrt{-7}]$，並且若 $(q')^\beta$ 為 $\left(\frac{a_\beta+b_\beta\sqrt{7i}}{2}\right)$ 型的複數，其中 a_β,b_β 為奇數，則 $(q'')^\beta$ 為 $\left(\frac{a_\beta-b_\beta\sqrt{7i}}{2}\right)$ 型的複數。

當 $t=0$ 時，$\left(c+d\sqrt{7}i\right)\left[\left(q'\right)^t\times\left(q''\right)^{\beta-t}\right]=\left(c+d\sqrt{7}i\right)\left(q''\right)^{\beta}=\left(c+d\sqrt{7}i\right)\left(\frac{a_\beta-b_\beta\sqrt{7}i}{2}\right)$

$=\frac{(a_\beta c+7b_\beta d)+(a_\beta d-b_\beta c)\sqrt{7}i}{2}$ 。

又 c,d 為模 2 不同餘且 a_β,b_β 為奇數，所以

$a_\beta c+7b_\beta d\equiv c+d\equiv 1\pmod 2$ 且 $a_\beta d-b_\beta c\equiv d-c\equiv 1\pmod 2$ ，故

$\left(c+d\sqrt{7}i\right)\left[\left(q'\right)^t\times\left(q''\right)^{\beta-t}\right]\notin\square[\sqrt{-7}]$ 。同理可證當 $t=\beta$ 時，

$\left(c+d\sqrt{7}i\right)\left[\left(q'\right)^t\times\left(q''\right)^{\beta-t}\right]=\left(c+d\sqrt{7}i\right)\left(q'\right)^{\beta}=\left(c+d\sqrt{7}i\right)\left(\frac{a_\beta-b_\beta\sqrt{7}i}{2}\right)\notin\square[\sqrt{-7}]$ 。

因此，給定 $h_j=0,1,2,\cdots,\alpha_j\ (1\le j\le v)$ 且 $t=0,1,2,\cdots,\beta$ ，

$\prod_{j=1}^{v}\left(p_j'\right)^{h_j}\times\left(p_j''\right)^{\alpha_j-h_j}\times\left(q'\right)^t\times\left(q''\right)^{\beta-t}\in\square[\sqrt{-s}]$ 若且唯若 $t=1,2,3,\cdots,\beta-1$ 。 ■

底下利用**唯一表示法**來計數橢圓 $\Omega_7:x^2+7y^2=7^\lambda\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times 2^\beta$ 上格子點個數，分成兩種： $\beta=0$ 或 $\beta\ne 0$ 來討論。

【定理 4】(計數橢圓 $\Omega_7:x^2+7y^2=7^\lambda\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times 2^\beta$ 上的格子點個數)

設橢圓 $\Omega_7:x^2+7y^2=7^\lambda\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times 2^\beta$ ，其中 7 、 $p_j\ (1\le j\le v)$ 、 $r_\ell\ (1\le\ell\le\kappa)$ 、 2 分別為第 I_7 、 II_7 、 III_7 、 IV_7 類的質數，並且 λ,α_j,β 為非負整數及 γ_ℓ 為偶數，則

(i)當 $\beta=0$ 時，橢圓 Ω_7 上格子點個數為 $2\prod_{j=1}^{v}\left(\alpha_j+1\right)$ 。

(ii)當 $\beta\ne 0$ 時，橢圓 Ω_7 上格子點個數為 $2(\beta-1)\prod_{j=1}^{v}\left(\alpha_j+1\right)$ 。

【證明】 $7^\lambda\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times 2^\beta$ 的唯一表示法為(7)式，考慮由

$u(\sqrt{7}i)^{2\lambda}\times\prod_{j=1}^{v}\left(p_j'p_j''\right)^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times(q'q'')^\beta$ 推導 $x+y\sqrt{7}i$ 可能的唯一表示法選擇，因為

$(\sqrt{7}i)^{2\lambda},\prod_{j=1}^{v}\left(p_j'p_j''\right)^{\alpha_j},\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\in\square[i]$ ，但 $x^2+7y^2=(x+y\sqrt{7}i)(x-y\sqrt{7}i)$ ，並且

$x+y\sqrt{7}i$ 與 $x-y\sqrt{7}i$ 為共軛複數，所以第 I_7 類質數及第 III_7 類質數皆採平均分配給 $x+y\sqrt{7}i$ 與 $x-y\sqrt{7}i$。又由**引理 7** 可知 $\prod_{j=1}^{v}\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\times(q')^t\times(q'')^{\beta-t}\in\square[\sqrt{-s}]$ 若且唯若 $t=1,2,3,\cdots,\beta-1$，故 $x+y\sqrt{7}i$ 可能的唯一表示法選擇為

$$u(\sqrt{7}i)^{\lambda}\times\prod_{j=1}^{v}\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\times\prod_{\ell=1}^{\kappa}r_{\ell}^{\frac{\gamma_{\ell}}{2}}\times(q')^t\times(q'')^{\beta-t}\ ,$$

其中 $h_j=0,1,2,\cdots,\alpha_j\ (1\le j\le v)$ 且 $t=1,2,3,\cdots,\beta-1$，推得平均分配選擇僅有1個、h_j 值選擇共有 $\prod_{j=1}^{v}\left(\alpha_j+1\right)$ 個及 t 值選擇共有 $\beta-1$ 個，並且可逆元素 u 選擇有 2 個，故 $x+y\sqrt{7}i$ 可能的唯一表示法選擇個數為 $2(\beta-1)\prod_{j=1}^{v}\left(\alpha_j+1\right)$。因此，(i)當 $\beta=0$ 時，橢圓 Ω_7 上格子點個數為 $2\prod_{j=1}^{v}\left(\alpha_j+1\right)$。(ii)當 $\beta\neq0$ 時，橢圓 Ω_7 上格子點個數為 $2(\beta-1)\prod_{j=1}^{v}\left(\alpha_j+1\right)$。 ■

五、計數橢圓 $\Omega_s:x^2+sy^2=m\ (s\ge11)$ 上格子點個數

前二章是利用唯一表示法來計數圓或橢圓 $\Omega_s:x^2+sy^2=m\ (s=1,2,3,7)$ 上格子點個數，這章要探討 $s=11,19,43,67,163$ 的情況，注意到這五個數滿足 $s\equiv3\ (\mathrm{mod}\ 8)$ 的同餘性質，發現計數上呈現相同規律，底下橢圓 $\Omega_s:x^2+sy^2=m$ 中 s 是指 $11,19,43,67,163$。在計數上困難點仍是在第 IV_s 類質數，所以先探討第 IV_s 類質數 $q_k\ (1\le k\le n)$ 的性質，參見**引理 8~12**，再利用**引理 8~12** 來協助計數橢圓 $\Omega_s:x^2+sy^2=m$ 上的格子點個數。

(一)第 IV_s 類質數 q_k 的性質

令 $q_k=q_k^{'}q_k^{''}$ 且 $q_k^{'}=\frac{a_k+b_k\sqrt{s}i}{2},q_k^{''}=\frac{a_k-b_k\sqrt{s}i}{2}$，其中 $1\le k\le n$ 且 a_k,b_k 為奇數，底下要探討給定非負整數 $t_k=0,1,2,\cdots,\beta_k$，$\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}$ 有哪些類型的複數呢？先觀察 $n=2$ 中 $s=11$ 的情況，取 $q_1=23=q_1^{'}q_1^{''}=\frac{9+\sqrt{11}i}{2}\times\frac{9-\sqrt{11}i}{2}$ 且 $q_2=31=q_2^{'}q_2^{''}=\frac{5+3\sqrt{11}i}{2}\times\frac{5-3\sqrt{11}i}{2}$，

考慮 $\beta_1=1,\beta_2=2$ ，$\prod_{k=1}^{2}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}$ 有底下六種可能情形，可分成三種類型的複數：

(i) $q_1^{'}\left(q_2^{''}\right)^2=-42-43\sqrt{11}i$ 及 $q_1^{''}\left(q_2^{'}\right)^2=-42+43\sqrt{11}i$ 為 $\left(a+b\sqrt{si}\right)$ 型的複數，其中 a,b 模 2 不同餘。(ii) $q_1^{'}q_2^{'}q_2^{''}=\frac{279}{2}+\frac{31\sqrt{11}i}{2}$ 及 $q_1^{'}\left(q_2^{'}\right)^2=-\frac{249}{2}+\frac{49\sqrt{11}i}{2}$ 為 $\left(\frac{c+d\sqrt{si}}{2}\right)$ 型的複數，其中 c,d 模 4 同餘。(iii) $q_1^{''}q_2^{'}q_2^{''}=\frac{279}{2}-\frac{31\sqrt{11}i}{2}$ 及 $q_1^{''}\left(q_2^{''}\right)^2=-\frac{249}{2}-\frac{49\sqrt{11}i}{2}$ 為 $\left(\frac{c+d\sqrt{si}}{2}\right)$ 型的複數，其中 c,d 模 4 不同餘。上述例子可猜測：給定正整數 n 及非負整數 $t_k=0,1,2,\cdots,\beta_k$ ，$\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}$ 可分為三種類型，記作 W_I 、W_{II} 及 W_{III} ，**定義為**

$W_I=\left\{w\middle|w=a+b\sqrt{si}\text{ ,其中}a,b\text{模}2\text{不同餘}\right\}$ 、$W_{II}=\left\{w\middle|w=\frac{c+d\sqrt{si}}{2}\text{ ,其中奇數}c,d\text{模}4\text{同餘}\right\}$ 、$W_{III}=\left\{w\middle|w=\frac{c+d\sqrt{si}}{2}\text{ ,其中奇數}c,d\text{模}4\text{不同餘}\right\}$ 。底下就來證明上述三種類型的複數兩兩相乘也為三種類型的其中一類。

【引理 8】($w_Iw_I^{'}$ 、w_Iw_{II} 、w_Iw_{III} 、$w_{II}w_{II}^{'}$ 、$w_{II}w_{III}$ 及 $w_{III}w_{III}^{'}$ 的性質)

給定 $s=11,19,43,67,163$ ，設 $w_I,w_I^{'}\in W_I$ 、$w_{II},w_{II}^{'}\in W_{II}$ 且 $w_{III},w_{III}^{'}\in W_{III}$ ，則

(i) $w_Iw_I^{'}$ 及 $w_{II}w_{III}$ 為 $\left(a'+b'\sqrt{si}\right)$ 型的複數，其中 a',b' 模 2 不同餘，即在 W_I 中。

(ii) $w_{II}w_{II}^{'}$ 及 w_Iw_{III} 為 $\left(\frac{e'+f'\sqrt{si}}{2}\right)$ 型的複數，其中奇數 e',f' 模 4 不同餘，即在 W_{III} 中。

(iii) w_Iw_{II} 及 $w_{III}w_{III}^{'}$ 為 $\left(\frac{c'+d'\sqrt{si}}{2}\right)$ 型的複數，其中奇數 c',d' 模 4 同餘，即在 W_{II} 中。

【證明】(i)①令 $w_I=a_1+b_1\sqrt{si}\in W_I$ 且 $w_I^{'}=a_2+b_2\sqrt{si}\in W_I$ ，則 a_1,b_1 與 a_2,b_2 模 2 不同餘，且

$w_Iw_I^{'}=(a_1+b_1\sqrt{si})(a_2+b_2\sqrt{si})=(a_1a_2-sb_1b_2)+(a_1b_2+a_2b_1)\sqrt{si}$ 。

令 $(a_1a_2-sb_1b_2)+(a_1b_2+a_2b_1)\sqrt{si}=a'+b'\sqrt{si}$ ，則

$$\left(a'+b'\sqrt{si}\right)\left(a'-b'\sqrt{si}\right)=\left[(a_1a_2-sb_1b_2)+(a_1b_2+a_2b_1)\sqrt{si}\right]\times\left[(a_1a_2-sb_1b_2)-(a_1b_2+a_2b_1)\sqrt{si}\right]$$

$$=(a_1a_2-sb_1b_2)^2+s(a_1b_2+a_2b_1)^2 \text{ 為奇數。}$$

由**性質 3** 可知 a',b' 為模 2 不同餘，故 $w_I w_I^{'}$ 在 W_I 中。

②令 $w_{II}=\frac{c+d\sqrt{si}}{2}\in W_{II}$ 且 $w_{III}=\frac{e+f\sqrt{si}}{2}\in W_{III}$ ，則 $d\equiv c \pmod 4$ 、 $f\equiv -e \pmod 4$ 且

$\left(\frac{c+d\sqrt{si}}{2}\right)\left(\frac{e+f\sqrt{si}}{2}\right)=\frac{(ce-sdf)+(cf+de)\sqrt{si}}{4}$ 。

令 $c=4t_1+d$ 及 $e=4t_2-f$ ，其中 d,f 為奇數及 t_1,t_2 為整數，因為 $s\equiv 3 \pmod 8$ ，所以

$ce-sdf=(4t_1+d)(4t_2-f)-sdf\equiv -4(t_1f-t_2d+df)\equiv 4(t_1f-t_2d+df) \pmod 8$ 且

$cf+de=(4t_1+d)f+d(4t_2-f)\equiv 4(t_1f+t_2d) \pmod 8$ 。又 $d,f\equiv 1 \pmod 2$ ，所以

$t_1f-t_2d+df\equiv t_1f+t_2d+1 \pmod 2$ ，故 t_1f-t_2d+df,t_1f+t_2d 模 2 不同餘且 $4\mid ce-sdf$ 且

$4\mid cf+de$ ，因此， $w_{II}w_{III}$ 為 $\left(a'+b'\sqrt{si}\right)$ 型的複數，即在 W_I 中。

(ii)①令 $w_{II}=\frac{c_1+d_1\sqrt{si}}{2}\in W_{II}$ 且 $w_{II}^{'}=\frac{c_2+d_2\sqrt{si}}{2}\in W_{II}$ ，則 $d_1\equiv c_1 \pmod 4$ 、 $d_2\equiv c_2 \pmod 4$

且 $w_{II}w_{II}^{'}=\left(\frac{c_1+d_1\sqrt{si}}{2}\right)\left(\frac{c_2+d_2\sqrt{si}}{2}\right)=\frac{(c_1c_2-sd_1d_2)+(c_1d_2+c_2d_1)\sqrt{si}}{4}$ 。

又 $s\equiv 3 \pmod 4$ 及 c_1,c_2 為奇數，推得 $c_1c_2-sd_1d_2\equiv c_1c_2-3c_1c_2\equiv -2c_1c_2\equiv 2 \pmod 4$ 且

$c_1d_2+c_2d_1\equiv c_1c_2+c_2c_1\equiv 2c_1c_2\equiv 2 \pmod 4$ ，故 $w_{II}w_{II}^{'}$ 為 $\left(\frac{e'+f'\sqrt{si}}{2}\right)$ 型的複數。

令 $c_1=4t_1+d_1$ 及 $c_2=4t_2+d_2$ ，其中 d_1,d_2 為奇數、 t_1,t_2 為整數，則

$e'=\frac{c_1c_2-sd_1d_2}{2}=\frac{(4t_1+d_1)(4t_2+d_2)-3d_1d_2}{2}\equiv 2(t_1d_2+t_2d_1)-d_1d_2 \pmod 4$ ，並且

$f'=\frac{c_1d_2+c_2d_1}{2}\equiv\frac{(4t_1+d_1)d_2+(4t_2+d_2)d_1}{2}\equiv 2(t_1d_2+t_2d_1)+d_1d_2 \pmod 4$ 。

又 $e'\equiv (-2)(t_1d_2+t_2d_1)-d_1d_2\equiv -\left[2(t_1d_2+t_2d_1)+d_1d_2\right]\equiv -f' \pmod 4$ ，所以 e',f' 模 4 不同

餘且e', f'為奇數，因此，$w_{II}w_{II}^{'}$為$\left(\frac{e'+f'\sqrt{si}}{2}\right)$型的複數，即在$W_{III}$中。

②令$w_I=a+b\sqrt{si}\in W_I$、$w_{III}=\frac{e+f\sqrt{si}}{2}\in W_{III}$，則$a,b$模2不同餘、$e, f\equiv 1\pmod 2$，並且$w_Iw_{III}=\left(a+b\sqrt{si}\right)\left(\frac{e+f\sqrt{si}}{2}\right)=\frac{(ae-sbf)+(af+be)\sqrt{si}}{2}$。又$s\equiv 1\pmod 2$，推得

$ae-sbf\equiv a-3b\equiv 1\pmod 2$且$af+be\equiv a+b\equiv 1\pmod 2$，故$w_Iw_{III}$為$\left(\frac{e''+f''\sqrt{si}}{2}\right)$型的複數。因為$s\equiv -1\pmod 4$且$f\equiv -e\pmod 4$，所以

$e''=ae-sbf\equiv ae+b(-e)\equiv e(a-b)\pmod 4$、$f''=af+be\equiv a(-e)+be\equiv -e(a-b)\pmod 4$。又$a-b$為奇數，故$e''\equiv -f''\pmod 4$且$e'', f''$為奇數，即$e'', f''$模4不同餘，因此，$w_Iw_{III}$為$\left(\frac{e''+f''\sqrt{si}}{2}\right)$型的複數，即在$W_{III}$中。

(iii)①令$w_I=a+b\sqrt{si}\in W_I$、$w_{II}=\frac{c+d\sqrt{si}}{2}\in W_{II}$，則$a,b$模2不同餘、$c,d\equiv 1\pmod 2$且$w_Iw_{II}=\left(a+b\sqrt{si}\right)\left(\frac{c+d\sqrt{si}}{2}\right)=\frac{(ac-sbd)+(ad+bc)\sqrt{si}}{2}$。

又$s\equiv 1\pmod 2$，所以$ac-sbd\equiv a-b\equiv 1\pmod 2$且$ad+bc\equiv a+b\equiv 1\pmod 2$，故$w_Iw_{II}$為$\left(\frac{c'+d'\sqrt{si}}{2}\right)$型的複數。因為$s\equiv -1\pmod 4$且$d\equiv c\pmod 4$，所以

$c'=ac-sbd\equiv ac+bc\equiv c(a+b)\pmod 4$、$d'=ad+bc\equiv ac+bc\equiv c(a+b)\pmod 4$，故$c', d'$模4同餘且$c', d'$為奇數，因此，$w_Iw_{II}$為$\left(\frac{c'+d'\sqrt{si}}{2}\right)$型的複數，即在$W_{II}$中。

②令$w_{III}=\frac{e_1+f_1\sqrt{si}}{2}\in W_{III}$且$w_{III}^{'}=\frac{e_2+f_2\sqrt{si}}{2}\in W_{III}$，則$f_1\equiv -e_1\pmod 4$、$f_2\equiv -e_2\pmod 4$且$w_{III}w_{III}^{'}=\left(\frac{e_1+f_1\sqrt{si}}{2}\right)\left(\frac{e_2+f_2\sqrt{si}}{2}\right)=\frac{(e_1e_2-sf_1f_2)+(e_1f_2+e_2f_1)\sqrt{si}}{4}$。

又$s\equiv 3\pmod 4$，所以$e_1e_2-sf_1f_2\equiv e_1e_2-3(-e_1)(-e_2)\equiv -2e_1e_2\equiv 2\pmod 4$且

$e_1 f_2 + e_2 f_1 \equiv e_1(-e_2) + e_2(-e_1) \equiv -2e_1e_2 \equiv 2 \pmod 4$ ，故 $w_{III} w_{III}^{'}$ 為 $\left(\frac{c'' + d''\sqrt{si}}{2}\right)$ 型的複數。

令 $e_1 = 4t_1 - f_1$ 及 $e_2 = 4t_2 - f_2$ ，其中 f_1, f_2 為奇數、 t_1, t_2 為整數，則

$$\begin{aligned} c'' &= \frac{e_1e_2 - sf_1f_2}{2} = \frac{(4t_1 - f_1)(4t_2 - f_2) - sf_1f_2}{2} \\ &= 8t_1t_2 - 2(f_1t_2 + f_2t_1) - \left(\frac{s-1}{2}\right) f_1f_2 \ (\because 2 \mid s-1 \text{ 且 } \frac{s-1}{2} \text{為奇數}) \\ &\equiv -2(f_1t_2 + f_2t_1) - f_1f_2 \pmod 4 \end{aligned}$$

並且 $d'' = \frac{(4t_1 - f_1) f_2 + (4t_2 - f_2) f_1}{2} = 8t_1t_2 + 2(f_1t_2 + f_2t_1) - f_1f_2 \equiv 2(f_1t_2 + f_2t_1) - f_1f_2 \pmod 4$ 。

又 $c'' \equiv -2(f_1t_2 + f_2t_1) - f_1f_2 \equiv 2(f_1t_2 + f_2t_1) - f_1f_2 \equiv d'' \pmod 4$ ，所以 c'', d'' 模 4 同餘且 c'', d'' 為奇數，因此， $w_{III} w_{III}^{'}$ 為 $\left(\frac{c'' + d''\sqrt{si}}{2}\right)$ 型的複數，即在 W_{II} 中。 ■

【引理 9】 (n 個在 W_{II} 中的元素相乘在 W_I 、 W_{II} 、 W_{III} 中性質)

設 $w_j \in W_{II}$ ，其中 $1 \le j \le n$ ，則(i)當 $n \equiv 0 \pmod 3$ 時， $\prod_{j=1}^{n} w_j \in W_I$ 。

(ii)當 $n \equiv 1 \pmod 3$ 時， $\prod_{j=1}^{n} w_j \in W_{II}$ 。(iii)當 $n \equiv 2 \pmod 3$ 時， $\prod_{j=1}^{n} w_j \in W_{III}$ 。

【證明】 對於 $w_1, w_2, w_3 \in W_{II}$ ，由**引理 8** 可知 $w_1w_2 \in W_{III}$ ，當 w_1w_2 再乘以 w_3 時，由**引理 7** 可知 $w_1w_2w_3 \in W_I$ ，即任三個在 W_{II} 中的元素相乘在 W_I 中。

(i)當 $n \equiv 0 \pmod 3$ 時，存在正整數 λ 使得 $n = 3\lambda$ ，即三個在 W_{II} 中的元素相乘視為一組，共有 λ 組。又任三個在 W_{II} 中的元素相乘在 W_I 中，並且 λ 個在 W_I 中的元素相乘在 W_I 中，故 $\prod_{j=1}^{n} w_j \in W_I$ 。

(ii)當 $n \equiv 1 \pmod 3$ 時，存在正整數 λ 使得 $n = 3\lambda + 1$ ，即 $\prod_{j=1}^{n} w_j = \left(\prod_{j=1}^{3\lambda} w_j\right) \times w_{3\lambda+1}$ 。

由(i)可知 $\prod_{j=1}^{3\lambda} w_j \in W_I$ ，再由**引理 8** 可知 $\prod_{j=1}^{3\lambda} w_j$ 再乘以一個在 W_{II} 中的元素 $w_{3\lambda+1}$ 在 W_{II} 中，

故$\prod_{j=1}^{n} w_j \in W_{II}$。

(iii)當$n \equiv 2 \pmod 3$時，存在正整數λ使得$n = 3\lambda + 2$，即$\prod_{j=1}^{n} w_j = \left(\prod_{j=1}^{3\lambda+1} w_j\right) \times w_{3\lambda+2}$。

由(ii)可知$\prod_{j=1}^{3\lambda+1} w_j \in W_{II}$，再由**引理 8** 可知$\prod_{j=1}^{3\lambda+1} w_j$再乘以一個在$W_{II}$中的元素$w_{3\lambda+2}$在$W_{III}$中，故$\prod_{j=1}^{n} w_j \in W_{III}$。 ■

底下**引理 10** 要探討$\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k} \times \left(q_k^{''}\right)^{\beta_k - t_k} \in W_I$、$W_{II}$、$W_{III}$的充要條件，由於$q_k^{'}$與$q_k^{''}$可互換，令$q_k^{'} = \frac{a_k + b_k\sqrt{si}}{2} \in W_{II}$及$q_k^{''} = \frac{a_k - b_k\sqrt{si}}{2} \in W_{III}$。

【引理 10】($\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k} \times \left(q_k^{''}\right)^{\beta_k - t_k} \in W_I$、$W_{II}$、$W_{III}$**的充要條件**)

給定$s = 11, 19, 43, 67, 163$，設$q_k^{'} = \frac{a_k + b_k\sqrt{si}}{2}$及$q_k^{''} = \frac{a_k - b_k\sqrt{si}}{2}$，其中$1 \le k \le n$且奇數$a_k, b_k$為模4同餘，則給定非負整數$t_k = 0, 1, 2, \cdots, \beta_k \ (1 \le k \le n)$，

(i)$\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k} \times \left(q_k^{''}\right)^{\beta_k - t_k} \in W_I$若且唯若$\sum_{k=1}^{n}\left(2\beta_k - t_k\right) \equiv 0 \pmod 3$。

(ii)$\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k} \times \left(q_k^{''}\right)^{\beta_k - t_k} \in W_{II}$若且唯若$\sum_{k=1}^{n}\left(2\beta_k - t_k\right) \equiv 1 \pmod 3$。

(iii)$\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k} \times \left(q_k^{''}\right)^{\beta_k - t_k} \in W_{III}$若且唯若$\sum_{k=1}^{n}\left(2\beta_k - t_k\right) \equiv 2 \pmod 3$。

【證明】底下要探討$\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k} \times \left(q_k^{''}\right)^{\beta_k - t_k}$在$W_I$、$W_{II}$、$W_{III}$中哪一類，即要探討$\sum_{k=1}^{n} t_k$個在$W_{II}$中的元素相乘與$\sum_{k=1}^{n}\left(\beta_k - t_k\right)$個在$W_{III}$中的元素相乘在$W_I$、$W_{II}$、$W_{III}$中哪一類。

由**引理 8** 可知$\beta_k - t_k$個在W_{III}中的元素相乘在W_I、W_{II}、W_{III}中哪一類相當於$2\left(\beta_k - t_k\right)$個在$W_{II}$中的元素相乘在$W_I$、$W_{II}$、$W_{III}$中哪一類，所以底下要探討

$\sum_{k=1}^{n} t_k + \sum_{k=1}^{n} 2\left(\beta_k - t_k\right) = \sum_{k=1}^{n}\left(2\beta_k - t_k\right)$個在$W_{II}$中的元素相乘在$W_I$、$W_{II}$、$W_{III}$中哪一類。

(i)當$\sum_{k=1}^{n}\left(2\beta_k - t_k\right) \equiv 0 \pmod 3$時，由**引理 9** 可知$\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k} \times \left(q_k^{''}\right)^{\beta_k - t_k} \in W_I$。

(ii)當 $\sum_{k=1}^{n}(2\beta_k - t_k) \equiv 1 \pmod 3$ 時，由**引理 9** 可知 $\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k} \times \left(q_k^{''}\right)^{\beta_k - t_k} \in W_{II}$ 。

(iii)當 $\sum_{k=1}^{n}(2\beta_k - t_k) \equiv 2 \pmod 3$ 時，由**引理 9** 可知 $\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k} \times \left(q_k^{''}\right)^{\beta_k - t_k} \in W_{III}$ 。 ■

底下要探討數組 $(t_1, t_2, t_3, \cdots, t_n)$ 中滿足 $\sum_{k=1}^{n}(2\beta_k - t_k) \equiv 0,1,2 \pmod 3$ 的個數，令 $T_0(n)$ 、$T_1(n)$ 、$T_2(n)$ 為數組 $(t_1, t_2, t_3, \cdots, t_n)$ 中滿足 $\sum_{k=1}^{n}(2\beta_k - t_k) \equiv 0,1,2 \pmod 3$ 的個數，先觀察 $n=2$ 中 $s=11$ 的情況：由 $\prod_{k=1}^{2}(\beta_k + 1) \equiv 1,2,0 \pmod 3$ 區分成三種，分別取 $\beta_1 = \beta_2 = 6$ 、 $\beta_1 = 6, \beta_2 = 7$ 、、 $\beta_1 = 6, \beta_2 = 8$ 為例，發現得到

當 $\prod_{k=1}^{2}(\beta_k + 1) \equiv 1 \pmod 3$ 時， $T_0(2) = 17 = \dfrac{\prod_{k=1}^{2}(\beta_k + 1) + 2}{3}$ 、 $T_1(2) = T_2(2) = 16 = \dfrac{\prod_{k=1}^{2}(\beta_k + 1) - 1}{3}$ 。

當 $\prod_{k=1}^{2}(\beta_k + 1) \equiv 2 \pmod 3$ 時， $T_0(2) = 18 = \dfrac{\prod_{k=1}^{2}(\beta_k + 1) - 2}{3}$ 、 $T_1(2) = T_2(2) = 19 = \dfrac{\prod_{k=1}^{2}(\beta_k + 1) + 1}{3}$ 。

當 $\prod_{k=1}^{2}(\beta_k + 1) \equiv 0 \pmod 3$ 時， $T_0(2) = T_1(2) = T_2(2) = 21 = \dfrac{\prod_{k=1}^{2}(\beta_k + 1)}{3}$ 。

由上述數據可猜測對於所有正整數 n ， $T_0(n)$ 、 $T_1(n)$ 、 $T_2(n)$ 的值，結果參見**引理 10**，底下就來證明。

【引理 11】(數組 $(t_1, t_2, t_3, \cdots, t_n)$ 中滿足 $\sum_{k=1}^{n}(\beta_k - 2t_k) \equiv 0,1,2 \pmod 3$ 的個數)

給定非負整數 $t_k = 0,1,2,\cdots,\beta_k \ (1 \le k \le n)$ ，設 $T_0(n)$ 、 $T_1(n)$ 、 $T_2(n)$ 分別為數組 $(t_1, t_2, t_3, \cdots, t_n)$ 中滿足 $\sum_{k=1}^{n}(2\beta_k - t_k) \equiv 0,1,2 \pmod 3$ 的個數，則

(i)當 $\prod_{k=1}^{n}(\beta_k + 1) \equiv 1 \pmod 3$ 時， $T_0(n) = \dfrac{\prod_{k=1}^{n}(\beta_k + 1) + 2}{3}$ 、 $T_1(n) = T_2(n) = \dfrac{\prod_{k=1}^{n}(\beta_k + 1) - 1}{3}$ 。

(ii)當 $\prod_{k=1}^{n}(\beta_k + 1) \equiv 2 \pmod 3$ 時， $T_0(n) = \dfrac{\prod_{k=1}^{n}(\beta_k + 1) - 2}{3}$ 、 $T_1(n) = T_2(n) = \dfrac{\prod_{k=1}^{n}(\beta_k + 1) + 1}{3}$ 。

(iii)當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 0 \pmod 3$ 時，$T_0(n)=T_1(n)=T_2(n)=\dfrac{\prod_{k=1}^{n}(\beta_k+1)}{3}$ 。

【證明】底下是由數學歸納法來證明 $T_0(n)$ 、$T_1(n)$ 、$T_2(n)$ 的值。

當 $n=1$ 時，令 $\beta_1\equiv r \pmod 3$ 且 $t_1\equiv r' \pmod 3$ ，其中 $r,r'=0,1,2$ ，所以

①當 $2\beta_1-t_1\equiv 2r-r'\equiv 0 \pmod 3$ 時，$r=r'=0$ 或 $r=1,r'=2$ 或 $r=2,r'=1$ ，所以

當 $\beta_1+1\equiv 1 \pmod 3$ 時，$t_1=0,3,6,\cdots,\beta_1$ ，所以 $T_0(1)=\dfrac{\beta_1+3}{3}$ ，可寫成 $\dfrac{(\beta_1+1)+2}{3}$ 。

當 $\beta_1+1\equiv 2 \pmod 3$ 時，$t_1=2,5,8,\cdots,\beta_1-2$ ，所以 $T_0(1)=\dfrac{\beta_1-1}{3}$ ，可寫成 $\dfrac{(\beta_1+1)-2}{3}$ 。

當 $\beta_1+1\equiv 0 \pmod 3$ 時，$t_1=1,4,7,\cdots,\beta_1-1$ ，所以 $T_0(1)=\dfrac{\beta_1+1}{3}$ 。

②當 $2\beta_1-t_1\equiv 2r-r'\equiv 1 \pmod 3$ 時，$r=0,r'=2$ 或 $r=1,r'=1$ 或 $r=2,r'=0$ ，所以

當 $\beta_1+1\equiv 1 \pmod 3$ 時，$t_1=2,5,8,\cdots,\beta_1-1$ ，所以 $T_1(1)=\dfrac{\beta_1}{3}$ ，可寫成 $\dfrac{(\beta_1+1)-1}{3}$ 。

當 $\beta_1+1\equiv 2 \pmod 3$ 時，$t_1=1,4,7,\cdots,\beta_1$ ，所以 $T_1(1)=\dfrac{\beta_1+2}{3}$ ，可寫成 $\dfrac{(\beta_1+1)+1}{3}$ 。

當 $\beta_1+1\equiv 0 \pmod 3$ 時，$t_1=0,3,6,\cdots,\beta_1-2$ ，所以 $T_1(1)=\dfrac{\beta_1+1}{3}$ 。

③當 $2\beta_1-t_1\equiv 2r-r'\equiv 2 \pmod 3$ 時，$r=0,r'=1$ 或 $r=1,r'=0$ 或 $r=2,r'=2$ ，所以

當 $\beta_1+1\equiv 1 \pmod 3$ 時，$t_1=1,4,7,\cdots,\beta_1-2$ ，所以 $T_2(1)=\dfrac{\beta_1}{3}$ ，可寫成 $\dfrac{(\beta_1+1)-1}{3}$ 。

當 $\beta_1+1\equiv 2 \pmod 3$ 時，$t_1=0,3,6,\cdots,\beta_1-1$ ，所以 $T_2(1)=\dfrac{\beta_1+2}{3}$ ，可寫成 $\dfrac{(\beta_1+1)+1}{3}$ 。

當 $\beta_1+1\equiv 0 \pmod 3$ 時，$t_1=2,5,8,\cdots,\beta_1$ ，所以 $T_2(1)=\dfrac{\beta_1+1}{3}$ 。

設 $n=h$ 時成立，即

當 $\prod_{k=1}^{h}(\beta_k+1)\equiv 1 \pmod 3$ 時，$T_0(h)=\dfrac{\prod_{k=1}^{h}(\beta_k+1)+2}{3}$ 、$T_1(h)=T_2(h)=\dfrac{\prod_{k=1}^{h}(\beta_k+1)-1}{3}$ 。

當 $\prod_{k=1}^{h}(\beta_k+1)\equiv 2 \pmod 3$ 時，$T_0(h)=\dfrac{\prod_{k=1}^{h}(\beta_k+1)-2}{3}$ 、$T_1(h)=T_2(h)=\dfrac{\prod_{k=1}^{h}(\beta_k+1)+1}{3}$ 。

當 $\prod_{k=1}^{h}(\beta_k+1)\equiv 0 \pmod 3$ 時，$T_0(h)=T_1(h)=T_2(h)=\dfrac{\prod_{k=1}^{h}(\beta_k+1)}{3}$ 。

則 $n=h+1$ 時，因為 $\sum_{k=1}^{h+1}(2\beta_k-t_k)\equiv\sum_{k=1}^{h}(2\beta_k-t_k)+(2\beta_{h+1}-t_{h+1}) \pmod 3$ ，

令 $\sum_{k=1}^{h}(2\beta_k-t_k)\equiv r'' \pmod 3$ 且 $2\beta_{h+1}-t_{h+1}\equiv r''' \pmod 3$ ，其中 $r'',r'''=0,1,2$ ，則

當 $\sum_{k=1}^{h+1}(2\beta_k-t_k)\equiv 0 \pmod 3$ 時，推得 $r''=r'''=0$ 或 $r''=1,r'''=2$ 或 $r''=2,r'''=1$ ，所以

$$T_0(h+1)=\underbrace{T_0(h)T_0(1)}_{r''=r'''=0}+\underbrace{T_1(h)T_2(1)}_{r''=1,r'''=2}+\underbrace{T_2(h)T_1(1)}_{r''=2,r'''=1} \text{ 。} \tag{8}$$

底下由 $\prod_{k=1}^{h+1}(\beta_k+1)$ 模3分成三種情況討論：

(I)當 $\prod_{k=1}^{h+1}(\beta_k+1)\equiv 1 \pmod 3$ 時，因為 $\prod_{k=1}^{h+1}(\beta_k+1)\equiv\prod_{k=1}^{h}(\beta_k+1)\times(\beta_{h+1}+1)$ ，所以 $\prod_{k=1}^{h}(\beta_k+1)$ 及 $(\beta_{h+1}+1)$ 模3的餘數可能選擇有二種情況，底下分別討論：

①當 $\prod_{k=1}^{h}(\beta_k+1)\equiv\beta_{h+1}+1\equiv 1 \pmod 3$ 時，(8)式可得到

$$T_0(h+1)=\frac{\prod_{k=1}^{h}(\beta_k+1)+2}{3}\times\frac{(\beta_{h+1}+1)+2}{3}+\frac{\prod_{k=1}^{h}(\beta_k+1)-1}{3}\times\frac{(\beta_{h+1}+1)-1}{3}$$
$$+\frac{\prod_{k=1}^{h}(\beta_k+1)-1}{3}\times\frac{(\beta_{h+1}+1)-1}{3}=\frac{\prod_{k=1}^{h}(\beta_k+1)\times(\beta_{h+1}+1)+2}{3}=\frac{\prod_{k=1}^{h+1}(\beta_k+1)+2}{3} \text{ 。}$$

②當 $\prod_{k=1}^{h}(\beta_k+1)\equiv\beta_{h+1}+1\equiv 2 \pmod 3$ 時，(8)式可得到

$$T_0(h+1)=\frac{\prod_{k=1}^{h}(\beta_k+1)-2}{3}\times\frac{(\beta_{h+1}+1)-2}{3}+\frac{\prod_{k=1}^{h}(\beta_k+1)+1}{3}\times\frac{(\beta_{h+1}+1)+1}{3}$$
$$+\frac{\prod_{k=1}^{h}(\beta_k+1)+1}{3}\times\frac{(\beta_{h+1}+1)+1}{3}=\frac{\prod_{k=1}^{h}(\beta_k+1)\times(\beta_{h+1}+1)+2}{3}=\frac{\prod_{k=1}^{h+1}(\beta_k+1)+2}{3}$$

所以 $n=h+1$ 時亦成立，故得證。

(II)當 $\prod_{k=1}^{h+1}(\beta_k+1)\equiv 2 \pmod 3$ 時，因為 $\prod_{k=1}^{h+1}(\beta_k+1)\equiv\prod_{k=1}^{h}(\beta_k+1)\times(\beta_{h+1}+1)$ ，所以 $\prod_{k=1}^{h}(\beta_k+1)$ 及 $(\beta_{h+1}+1)$ 模3的餘數可能選擇有二種情況，底下分別討論：

①當 $\prod_{k=1}^{h}(\beta_k+1)\equiv 1 \pmod 3,\ \beta_{h+1}+1\equiv 2 \pmod 3$ 時，(8)式可得到

$$T_0(h+1)=\frac{\prod_{k=1}^{h}(\beta_k+1)+2}{3}\times\frac{(\beta_{h+1}+1)-2}{3}+\frac{\prod_{k=1}^{h}(\beta_k+1)-1}{3}\times\frac{(\beta_{h+1}+1)+1}{3}$$
$$+\frac{\prod_{k=1}^{h}(\beta_k+1)-1}{3}\times\frac{(\beta_{h+1}+1)+1}{3}=\frac{\prod_{k=1}^{h}(\beta_k+1)\times(\beta_{h+1}+1)-2}{3}=\frac{\prod_{k=1}^{h+1}(\beta_k+1)-2}{3}$$。

②當$\prod_{k=1}^{h}(\beta_k+1)\equiv 2\pmod 3$, $\beta_{h+1}+1\equiv 1\pmod 3$時，(8)式可得到

$$T_0(h+1)=\frac{\prod_{k=1}^{h}(\beta_k+1)-2}{3}\times\frac{(\beta_{h+1}+1)+2}{3}+\frac{\prod_{k=1}^{h}(\beta_k+1)+1}{3}\times\frac{(\beta_{h+1}+1)-1}{3}$$
$$+\frac{\prod_{k=1}^{h}(\beta_k+1)+1}{3}\times\frac{(\beta_{h+1}+1)-1}{3}=\frac{\prod_{k=1}^{h}(\beta_k+1)\times(\beta_{h+1}+1)-2}{3}=\frac{\prod_{k=1}^{h+1}(\beta_k+1)-2}{3}$$。

所以$n=h+1$時亦成立，故得證。

(III)當$\prod_{k=1}^{h+1}(\beta_k+1)\equiv 0\pmod 3$時，因為$\prod_{k=1}^{h+1}(\beta_k+1)\equiv\prod_{k=1}^{h}(\beta_k+1)\times(\beta_{h+1}+1)$，所以$\prod_{k=1}^{h}(\beta_k+1)$及$(\beta_{h+1}+1)$模3的餘數可能選擇有五種情況，底下分別討論：

①當$\prod_{k=1}^{h}(\beta_k+1)\equiv 0\pmod 3$, $\beta_{h+1}+1\equiv 0\pmod 3$時，(8)式可得到

$$T_0(h+1)=\frac{\prod_{k=1}^{h}(\beta_k+1)}{3}\times\frac{(\beta_{h+1}+1)}{3}+\frac{\prod_{k=1}^{h}(\beta_k+1)}{3}\times\frac{(\beta_{h+1}+1)}{3}$$
$$+\frac{\prod_{k=1}^{h}(\beta_k+1)}{3}\times\frac{(\beta_{h+1}+1)}{3}=\frac{\prod_{k=1}^{h}(\beta_k+1)\times(\beta_{h+1}+1)}{3}=\frac{\prod_{k=1}^{h+1}(\beta_k+1)}{3}$$。

②當$\prod_{k=1}^{h}(\beta_k+1)\equiv 0\pmod 3$, $\beta_{h+1}+1\equiv 1\pmod 3$時，(8)式可得到

$$T_0(h+1)=\frac{\prod_{k=1}^{h}(\beta_k+1)}{3}\times\frac{(\beta_{h+1}+1)+2}{3}+\frac{\prod_{k=1}^{h}(\beta_k+1)}{3}\times\frac{(\beta_{h+1}+1)-1}{3}$$
$$+\frac{\prod_{k=1}^{h}(\beta_k+1)}{3}\times\frac{(\beta_{h+1}+1)-1}{3}=\frac{\prod_{k=1}^{h}(\beta_k+1)\times(\beta_{h+1}+1)}{3}=\frac{\prod_{k=1}^{h+1}(\beta_k+1)}{3}$$。

③當$\prod_{k=1}^{h}(\beta_k+1)\equiv 0\pmod 3$, $\beta_{h+1}+1\equiv 2\pmod 3$時，(8)式可得到

$$T_0(h+1)=\frac{\prod_{k=1}^{h}(\beta_k+1)}{3}\times\frac{(\beta_{h+1}+1)-2}{3}+\frac{\prod_{k=1}^{h}(\beta_k+1)}{3}\times\frac{(\beta_{h+1}+1)+1}{3}$$
$$+\frac{\prod_{k=1}^{h}(\beta_k+1)}{3}\times\frac{(\beta_{h+1}+1)+1}{3}=\frac{\prod_{k=1}^{h}(\beta_k+1)\times(\beta_{h+1}+1)}{3}=\frac{\prod_{k=1}^{h+1}(\beta_k+1)}{3}$$

。

仿照②或③的證明得到當 $\prod_{k=1}^{h}(\beta_k+1)\equiv 1 \pmod 3,\ \beta_{h+1}+1\equiv 0 \pmod 3$ 及

$\prod_{k=1}^{h}(\beta_k+1)\equiv 2 \pmod 3,\ \beta_{h+1}+1\equiv 0 \pmod 3$ 等二種情況，推得 $T_0(h+1)=\frac{\prod_{k=1}^{h+1}(\beta_k+1)}{3}$ 。

所以 $n=h+1$ 時亦成立，故得證。

仿照上面數學歸納法來證明 $T_1(n)$ 及 $T_2(n)$ 的情況。 ■

【引理 12】 ($\prod_{j=1}^{v}\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\times\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\in\mathbb{Z}[\sqrt{-s}]$ **的充要條件)**

給定 $s=11,19,43,67,163$ ，設 p_j 為奇質數且 $p_j=p_j^{'}p_j^{''}$ ，若 $p_j^{'}=a_j+b_j\sqrt{si}$ 、 $p_j^{''}=a_j-b_j\sqrt{si}$ 、

$q_k^{'}=\frac{a_k+b_k\sqrt{si}}{2}$ 及 $q_k^{''}=\frac{a_k-b_k\sqrt{si}}{2}$ ，其中 $1\le j\le v$ 、 $1\le k\le n$ 、 a_j,b_j 為模 2 不同餘且 a_k,b_k 為

奇數，則對於非負整數 $h_j=0,1,2,\cdots,\alpha_j$ 、正整數 n 且非負整數 $t_k=0,1,2,\cdots,\beta_k$ ，

$\prod_{j=1}^{v}\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\times\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\in\mathbb{Z}[\sqrt{-s}]$ 若且唯若 $\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\in\mathbb{Z}[\sqrt{-s}]$ 。

【證明】 令 $\prod_{j=1}^{v}\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}=c+d\sqrt{si}\in\mathbb{Z}[\sqrt{-s}]$ ，其中 $1\le j\le v$ 且 $h_j=0,1,2,\cdots,\alpha_j$ ，則

仿照**性質 3** 的證明可得 c,d 為模 2 不同餘，再由**引理 7** 可知滿足

$\prod_{j=1}^{v}\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\times\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{'}\right)^{1-t_k}\in\mathbb{Z}[\sqrt{-s}]$ 僅有型如 $w_I w_I^{'}\in\mathbb{Z}[\sqrt{-s}]$ 的一種選擇，即

$\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{'}\right)^{1-t_k}\in\mathbb{Z}[\sqrt{-s}]$ ，故得證。 ■

(二)計數橢圓 $\Omega_s : x^2+sy^2=m$ 上格子點個數

底下計數橢圓 $\Omega_s : x^2+sy^2=s^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{k=1}^{n}q_k^{\beta_k}$ 上格子點個數，分成兩種：$r_\ell\neq 2\,(1\le\ell\le\kappa)$ 或 $r_1=2$ 來討論。

【定理 5】(計數橢圓 $\Omega_s : x^2+sy^2=s^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{k=1}^{n}q_k^{\beta_k}$ $(r_\ell\neq 2)$ 上格子點個數)

給定 $s=11,19,43,67,163$，設橢圓 $\Omega_s : x^2+sy^2=s^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{k=1}^{n}q_k^{\beta_k}$，其中 s、$p_j\,(1\le j\le v)$、$r_\ell\,(1\le\ell\le\kappa)$、$q_k\,(1\le k\le n)$ 分別為第 I_s、II_s、III_s、IV_s 類的質數，並且 λ,α_j,β_k 為非負整數、γ_ℓ 為偶數，若 $r_\ell\neq 2\,(1\le\ell\le\kappa)$，則

(i)當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 1\pmod 3$ 時，橢圓 Ω_s 上格子點個數為 $\dfrac{2\prod_{k=1}^{n}(\beta_k+1)+4}{3}\left[\prod_{j=1}^{v}(\alpha_j+1)\right]$。

(ii)當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 2\pmod 3$ 時，橢圓 Ω_s 上格子點個數為 $\dfrac{2\prod_{k=1}^{n}(\beta_k+1)-4}{3}\left[\prod_{j=1}^{v}(\alpha_j+1)\right]$。

(iii)當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 0\pmod 3$ 時，橢圓 Ω_s 上格子點個數為 $\dfrac{2\prod_{k=1}^{n}(\beta_k+1)}{3}\left[\prod_{j=1}^{v}(\alpha_j+1)\right]$。

【證明】 $s^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{k=1}^{n}q_k^{\beta_k}$ 的唯一表示法為(7)式，考慮由

$u\times(\sqrt{s}i)^{2\lambda}\times\prod_{j=1}^{v}\left(p_j^{'}p_j^{''}\right)^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{k=1}^{n}\left(q_k^{'}q_k^{''}\right)^{\beta_k}$ 推導 $x+y\sqrt{s}i$ 可能的唯一表示法選擇。

因為 $x^2+sy^2=(x+y\sqrt{s}i)(x-y\sqrt{s}i)$ 且 $x+y\sqrt{s}i$ 與 $x-y\sqrt{s}i$ 為共軛複數，所以 $(\sqrt{s}i)^{2\lambda}$ 是採平均分配給 $x+y\sqrt{s}i$ 與 $x-y\sqrt{s}i$，此時 $\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$ 也採平均分配給 $x+y\sqrt{s}i$ 與 $x-y\sqrt{s}i$。故 $x+y\sqrt{s}i$ 可能的唯一表示法選擇為

$$u(\sqrt{s}i)^{\lambda}\times\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\times\prod_{\ell=1}^{\kappa}r_\ell^{\frac{\gamma_\ell}{2}}\times\prod_{k=1}^{n}\left[\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\right]。$$

當 $r_\ell \neq 2\,(1\le \ell \le \kappa)$ 時，$\prod_{\ell=1}^{\kappa} r_\ell^{\frac{\gamma_\ell}{2}}$ 為奇數，所以當 $\prod_{\ell=1}^{\kappa} r_\ell^{\frac{\gamma_\ell}{2}}$ 與

$(\sqrt{si})^{\lambda}\times\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\times\prod_{k=1}^{n}\left[\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\right]$ 相乘時是否在 $\square[\sqrt{-s}]$ 中不受 $\prod_{\ell=1}^{\kappa} r_\ell^{\frac{\gamma_\ell}{2}}$ 所

影響，即若 $(\sqrt{si})^{\lambda}\times\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\times\prod_{\ell=1}^{\kappa} r_\ell^{\frac{\gamma_\ell}{2}}\times\prod_{k=1}^{n}\left[\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\right]\in\square[\sqrt{-s}]$，

則只考慮 $\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\times\prod_{k=1}^{n}\left[\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\right]\in\square[\sqrt{-s}]$。

由**引理 12** 可知當考慮 $\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\times\prod_{k=1}^{n}\left[\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\right]\in\square[\sqrt{-s}]$ 時，僅有

$\prod_{j=1}^{v}\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\in\square[\sqrt{-s}]$ 且 $\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\in\square[\sqrt{-s}]$ 的情況，即在計數上是考

慮上述兩者各自計數。又由**引理 11** 可知數組 $(t_1,t_2,t_3,\cdots,t_n)$ 中滿足

$\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\in\square[\sqrt{-s}]$ 的個數為 $T_0(n)$，其中

當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 1\pmod 3$ 時，$T_0(n)=\dfrac{\prod_{k=1}^{n}(\beta_k+1)+2}{3}$。

當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 2\pmod 3$ 時，$T_0(n)=\dfrac{\prod_{k=1}^{n}(\beta_k+1)-2}{3}$。

當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 0\pmod 3$ 時，$T_0(n)=\dfrac{\prod_{k=1}^{n}(\beta_k+1)}{3}$。

所以數組 $(h_1,h_2,h_3,\cdots,h_v)$ 及 $(t_1,t_2,t_3,\cdots,t_n)$ 中滿足

$\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\times\prod_{k=1}^{n}\left[\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\right]\in\square[\sqrt{-s}]$ 的個數為 $T_0(n)\left[\prod_{j=1}^{v}(\alpha_j+1)\right]$。

又 $(\sqrt{si})^{2\lambda}$ 與 $\prod_{\ell=1}^{\kappa} r_\ell^{\gamma_\ell}$ 均採平均分配，所以選擇僅有1個，並且可逆元素 u 選擇有 2 個，故

$x+y\sqrt{si}$ 可能的唯一表示法選擇個數為橢圓 Ω_s 上格子點個數，因此，

(i)當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 1 \pmod 3$ 時，橢圓 Ω_s 上格子點個數為 $\frac{2\prod_{k=1}^{n}(\beta_k+1)+4}{3}\left[\prod_{j=1}^{v}(\alpha_j+1)\right]$。

(ii)當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 2 \pmod 3$ 時，橢圓 Ω_s 上格子點個數為 $\frac{2\prod_{k=1}^{n}(\beta_k+1)-4}{3}\left[\prod_{j=1}^{v}(\alpha_j+1)\right]$。

(iii)當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 0 \pmod 3$ 時，橢圓 Ω_s 上格子點個數為 $\frac{2\prod_{k=1}^{n}(\beta_k+1)}{3}\left[\prod_{j=1}^{v}(\alpha_j+1)\right]$。 ■

【定理 6】(計數橢圓 $\Omega_s: x^2+sy^2=s^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{k=1}^{n}q_k^{\beta_k}$ $(r_1=2)$ 上格子點個數)

給定 $s=11,19,43,67,163$，設橢圓 $\Omega_s: x^2+sy^2=s^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{k=1}^{n}q_k^{\beta_k}$，其中 s、$p_j\ (1\le j\le v)$、$r_\ell\ (1\le \ell\le \kappa)$、$q_k\ (1\le k\le n)$ 分別為第 I_s、II_s、III_s、IV_s 類的質數，並且 λ,α_j,β_k 為非負整數、γ_ℓ 為偶數，若 $r_1=2$，則

橢圓 Ω_s 上格子點個數為 $2\prod_{j=1}^{v}(\alpha_j+1)\prod_{k=1}^{n}(\beta_k+1)$。

【證明】 $s^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{k=1}^{n}q_k^{\beta_k}$ 的唯一表示法為(7)式，仿照**定理 5** 可知 $x+y\sqrt{si}$ 可能的唯一表示法選擇為 $u(\sqrt{si})^{\lambda}\times\prod_{j=1}^{v}\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\times r_1^{\frac{\gamma_1}{2}}\times\prod_{\ell=2}^{\kappa}r_\ell^{\frac{\gamma_\ell}{2}}\times\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}$。

當 $r_1=2$ 時，對於非負整數 β_k 且 $t_k=0,1,2,\cdots,\beta_k\ (1\le k\le n)$，

令 $\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{'}\right)^{\beta_k-t_k}=\frac{a'+b'\sqrt{si}}{2}$，其中 a',b' 為整數，則 a',b' 的奇偶性有四種，不論哪一種均使得 $r_1^{\frac{\gamma_1}{2}}\times\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{'}\right)^{\beta_k-t_k}\in\mathbb{Z}[\sqrt{-s}]$，推得 $t_k=0,1,2,3,\cdots,\beta_k$，所以數組

$(h_1,h_2,h_3,\cdots,h_v)$ 及 $(t_1,t_2,t_3,\cdots,t_n)$ 中滿足

$\prod_{j=1}^{v}\left[\left(p_j^{'}\right)^{h_j}\times\left(p_j^{''}\right)^{\alpha_j-h_j}\right]\times r_1^{\frac{\gamma_1}{2}}\times\prod_{k=1}^{n}\left[\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\right]\in\square[\sqrt{-s}]$ 的個數為 $\prod_{j=1}^{v}\left(\alpha_j+1\right)\prod_{k=1}^{n}\left(\beta_k+1\right)$

。再考慮 $r_\ell\neq 2\ (2\le\ell\le\kappa)$ 的情況，計數上採平均分配，選擇僅有1個，並且可逆元素 u 選擇有 2 個，故 $x+y\sqrt{si}$ 可能的唯一表示法選擇個數為 $2\prod_{j=1}^{v}\left(\alpha_j+1\right)\prod_{k=1}^{n}\left(\beta_k+1\right)$。因此，橢圓 Ω_s 上格子點個數為 $2\prod_{j=1}^{v}\left(\alpha_j+1\right)\prod_{k=1}^{n}\left(\beta_k+1\right)$。 ■

肆、研究結果

在作品中，主要探討圓及橢圓 $\Omega_s:x^2+sy^2=m$ 上的格子點個數(s 為黑格納數)，在計數上困難點在第 IV_s 類質數 q 的探討，可由質數 q 存在與否作分類，分成二類： $s=1,2,3$ 及 $s=7,11,19,43,67,163$。前者沒有第 IV_s 類質數 q ，計數上比較單純；後者有第 IV_s 類質數 q ，造成計數較為困難。底下是我們探討圓及橢圓 Ω_s 上的格子點個數的結果：

一、設圓 $\Omega_1:x^2+y^2=2^\lambda\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$ ，則圓 Ω_1 上的格子點個數為 $4\prod_{j=1}^{v}\left(\alpha_j+1\right)$。

二、設橢圓 $\Omega_2:x^2+2y^2=2^\lambda\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$ ，則橢圓 Ω_2 上格子點個數為 $2\prod_{j=1}^{v}\left(\alpha_j+1\right)$。

三、設橢圓 $\Omega_3:x^2+3y^2=3^\lambda\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$ ，則(i)當 $r_\ell\neq 2\ (1\le\ell\le\kappa)$ 時，橢圓 Ω_3 上格子點個數為 $2\prod_{j=1}^{v}\left(\alpha_j+1\right)$。(ii)當 $r_1=2$ 時，橢圓 Ω_3 上格子點個數為 $6\prod_{j=1}^{v}\left(\alpha_j+1\right)$。

四、設橢圓 $\Omega_7:x^2+7y^2=7^\lambda\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times 2^\beta$ ，則(i)當 $\beta=0$ 時，橢圓 Ω_7 上格子點個數為 $2\prod_{j=1}^{v}\left(\alpha_j+1\right)$。(ii)當 $\beta\neq 0$ 時，橢圓 Ω_7 上格子點個數為 $2(\beta-1)\prod_{j=1}^{v}\left(\alpha_j+1\right)$。

五、給定 $s=11,19,43,67,163$ ，設橢圓 $\Omega_s: x^2+sy^2=s^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{k=1}^{n}q_k^{\beta_k}$ ，則

(i)若 $r_\ell\neq 2\ (1\le\ell\le\kappa)$ ，則

當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 1\pmod 3$ 時，橢圓 Ω_s 上格子點個數為 $\frac{2\prod_{k=1}^{n}(\beta_k+1)+4}{3}\left[\prod_{j=1}^{v}(\alpha_j+1)\right]$。

當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 2\pmod 3$ 時，橢圓 Ω_s 上格子點個數為 $\frac{2\prod_{k=1}^{n}(\beta_k+1)-4}{3}\left[\prod_{j=1}^{v}(\alpha_j+1)\right]$。

當 $\prod_{k=1}^{n}(\beta_k+1)\equiv 0\pmod 3$ 時，橢圓 Ω_s 上格子點個數為 $\frac{2\prod_{k=1}^{n}(\beta_k+1)}{3}\left[\prod_{j=1}^{v}(\alpha_j+1)\right]$。

(ii)若 $r_1=2$ ，則橢圓 Ω_s 上格子點個數為 $2\prod_{j=1}^{v}(\alpha_j+1)\prod_{k=1}^{n}(\beta_k+1)$。

伍、結論及未來展望

一、本作品主要探討圓及橢圓 $\Omega_s: x^2+sy^2=m$ 上的格子點個數，首先遇到問題是 m 中的質因數有哪些質數會影響格子點個數呢？我們對於不同黑格納數 s ，探討出質數 p 在虛二次體 $\mathbb{Q}[\sqrt{-s}]$ 的整數環中的分解性，再由分解性分類決定 m 的不可約元分解。當選定代表元後，即可決定 m 的唯一表示法，接著進一步推導出 $x+y\sqrt{si}, x-y\sqrt{si}$ 可能的唯一表示法，就可以計數圓及橢圓上的格子點個數，本作品推導出 s 為所有黑格納數情況的計數公式。

二、值得一提的是由**引理 8** 可知三種類型的複數 W_I 、W_{II} 及 W_{III} 任選兩兩相乘也為三種類型的其中一類，將其關係整理成表 1。注意到整數模3加法群 $\mathbb{Z}_3$ ，定義在 $\mathbb{Z}_3$ 上二元運算加法為 $\bar{a}+\bar{b}=\overline{a+b}$ ，二元運算加法整理成表 2。有趣地，當表 1 中 W_I 換成0 、W_{II} 換成1、W_{III} 換成2時，表 1 與表 2 就相同，這表示我們可以從 W_I 、W_{II} 及 W_{III} 的分類訂出一個交換群與 $(\mathbb{Z}_3,+)$ 同構。

表 1：W_I 、W_{II} 及W_{III} 相乘的分類

×	W_I	W_{II}	W_{III}
W_I	W_I	W_{II}	W_{III}
W_{II}	W_{II}	W_{III}	W_I
W_{III}	W_{III}	W_I	W_{II}

表 2：整數模3加法群$\square_3$

+	0	1	2
0	0	1	2
1	1	2	0
2	2	0	1

三、我們推導黑格納數情況的計數，若不是取黑格納數，在計數上有何不同呢？以橢圓 $x^2+5y^2=p$ 為例：虛二次體$\square[\sqrt{-5}]$的整數環不為唯一分解整環，為了瞭解質數 p 的性質，所以查閱 David A. Cox[3]，書中提到

$$p\equiv 1,3,7,9 \pmod{20} \Leftrightarrow \left(\frac{-5}{p}\right)=1 \Leftrightarrow p=x^2+5y^2 \text{ or } 2x^2+2xy+3y^2 \text{ 。}$$

由數據中觀察質數 p 的同餘性可分成四類：定義第 I_5 類質數 p 為5 、第 II_5 類質數 p 為 $p\equiv 1,9 \pmod{20}$ 的質數、第 III_5 類質數 p 為 $p=2$ 或 $p\equiv 11,13,17,19 \pmod{20}$ 的質數、第V_5 類質數 p 為 $p\equiv 3,7 \pmod{20}$ 的質數。若根據上述同餘性來觀察計數橢圓上格子點個數，令橢圓$\Omega_5: x^2+5y^2=5^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}\times\prod_{\eta=1}^{o}h_\mu^{\zeta_\eta}$ ，其中5 、 $p_j\ (1\le j\le v)$ 、 $r_\ell\ \ (1\le \ell\le \kappa)$ 、 $h_\eta\ (1\le \eta\le o)$ 分別為第 I_5 、 II_5 、 III_5 、V_5 類的質數，那麼與黑格納數時在計數上有何不同呢？從數據顯示當不考慮第V_5 類的質數時，計數上與黑格納數情況中只有第 I_s 、 II_s 、 III_s 類的質數是相同的。進一步探討第V_5 類質數h ，因為$\left(\frac{-5}{h}\right)=1$，所以仿照**引理 3** 的證明可得$h$ 可表為$\left(\frac{x'+y'\sqrt{5}i}{2}\right)\left(x'-y'\sqrt{5}i\right)$型的質數，其中 x',y' 為奇數，從數據顯示此類質數在計數上與黑格納數情況中第 IV_s 類的質數是不同的。於是我們提出三個猜測：

(一)設橢圓$\Omega_5: x^2+5y^2=5^{\lambda}\times\prod_{j=1}^{v}p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa}r_\ell^{\gamma_\ell}$ ，其中5 、 p_j 、 r_ℓ 分別為第 I_5 、 II_5 、 III_5 類的質數，並且 λ,α_j 為非負整數及 γ_ℓ 為偶數，則(i)當 γ_ℓ 為奇數時，橢圓Ω_5 上格子點個數為0 。

(ii)當 γ_ℓ 為偶數時，橢圓Ω_5 上格子點個數為$2\prod_{j=1}^{v}\left(\alpha_j+1\right)$ 。

(二)設橢圓 $\Omega_5 : x^2+5y^2=\prod_{\eta=1}^{o} h_\eta^{\chi_\eta}$ ，其中 h_η $(1\le\eta\le o)$ 為第 V_5 類的質數，若 $\sum_{\eta=1}^{o}\chi_\eta$ 為奇數，則橢圓 Ω_5 上格子點個數為 0 。

(三)給定橢圓 $\Omega_5 : x^2+5y^2=5^\lambda\times\prod_{j=1}^{v} p_j^{\alpha_j}\times\prod_{\ell=1}^{\kappa} r_\ell^{\gamma_\ell}\times\prod_{\eta=1}^{o} h_\eta^{\chi_\eta}$ ，其中 5 、 p_j 、 r_ℓ 、 h_η 分別為第 I_5 、 II_5 、 III_5 、 V_5 類的質數，並且 λ,α_j 為非負整數及 $\gamma_\ell,\sum_{\eta=1}^{o}\chi_\eta$ 為偶數，則橢圓 Ω_5 上格子點個數為 $2\prod_{j=1}^{v}(\alpha_j+1)\prod_{j=1}^{o}(\chi_\eta+1)$ 。

本作品在論證上是利用黑格納數 s 有唯一分解環性質，於是虛二次體的整數環中任一非零元素的分解有唯一表示法，並且以此性質來計數。我們好奇若 s 所對應到的環不是唯一分解如 $s=5$ 時的情況，此時格子點個數要如何計算呢？另外探討黑格納數 $s(\ge 11)$ 時，可以訂出一個乘法交換群與 $\square_3$ 同構，那麼 s 不為黑格納數時，是否可訂出一個乘法交換群呢？那和哪一個交換群同構呢？相信要解決以上問題必須再學習背後的數學理論，這是更令人期待的，未來努力去突破，解開謎題。

四、**先備定理 4** 中(i)的證明提出一個演算法(參見 p8 中的**註 1**)，此演算法可以檢查 $x^2+sy^2=p$ 有整數解的存在性，我們嘗試推廣證明 $s=2,3,7$ ，當 $s=2,3$ 時，演算法規律較單純，但證明到 $s=7$ 時，演算法仍有規律，但無法證明此規律，未來將重新檢視演算法中的規律並且證明。值得一提的是數據顯示在 $s\ge 7$ 均有此演算法，此演算法可求得 $x^2+sy^2=p$ 或 $x^2+sy^2=4p$ 的整數解。

五、本作品致力於探討圓及橢圓上的格子點個數之連乘積表達式，困難點是探討第 IV_s 類質數 q 時，在論證上也是花了一些功夫，學習到很多的數論論證技巧，也因此使得格子點個數連乘積表達式有了豐富的結果。值得一提的是**引理 10** 中探討 $\prod_{k=1}^{n}\left(q_k^{'}\right)^{t_k}\times\left(q_k^{''}\right)^{\beta_k-t_k}\in W_I$ 相當於探討 $\sum_{k=1}^{n}\left(2\beta_k-t_k\right)\equiv 0\pmod 3$ ，此同餘觀點使得由繁化簡成功論證格子點個數，令我們驚喜不已，不僅僅學習到此論證的技巧，也使我們不禁讚嘆數學證明真奇妙！

陸、參考文獻資料

[1] 游森棚 (2019)。圓上的格子點。**科學月刊 5 月**。**591**(3)。

[2] Aleksander Skenderi (2018).Quadratic forms, reciprocity laws, and primes of the form x^2+ny^2.
chrome-extension://efaidnbmnnnibpcajpcglclefindmkaj/https://math.uchicago.edu/~may/REU2018/REUPapers/Skenderi.pdf

[3] David A. Cox (1989).*Primes of the Form* x^2+ny^2 ：*Fermat, Class Field Theory, and Complex Multiplication, Second Edition*. John Wiley & Sons, Inc.

[4] David M. Burton (2002).*Elementary Number Theory (Sixth Edition)*.Published by McGraw-Hill, a business unit of The McGraw-Hill Companies, Inc.

[5] J.Cilleruelo and A.C´ordoba (1994).Lattice Points on Ellipses. *Duke Mathematical Journal*,76(3).

[6] Henri Cohen (1993).A *Course in Computational Algebraic Number Theory*.springer.

[7] Joseph J. Rotman (1996). A First Course in Abstract Algebra. Prentice Hall, Inc.

[8] Stark, H. M. (1967). A Complete Determination of the Complex Quadratic Fields of Class Number One.Michigan Math. J. 14, 1-27.

[9] 二次體及虛二次體□[$\sqrt{-d}$]的整數環：維基百科 https://pse.is/4jmm2b

[10] 代數整數環：百度百科 https://pse.is/4hcy9d

[11] 可逆元素：維基百科 https://pse.is/4hz9ml

[12] 高斯整數：維基百科 https://pse.is/4et7q9

[13] 費馬平方和定理：維基百科 https://pse.is/4hvlnt

[14] 黑格納數：維基百科 https://pse.is/4k9udj

【評語】010019

作者擬探討整係數橢圓的個子點數，透過將問題轉換成二次整環內的唯一分解性的探討，作者可以清楚的呈現格子點數量(二次整環為唯一分解環的情況)，整體而言解得乾淨俐落，完整度高。若是能夠對非唯一分解環也有相當的討論會更完善。