2025年臺灣國際科學展覽會
優勝作品專輯

作品編號　010018

參展科別　數學

作品名稱　廣義佩爾方程式的一些探討

得獎獎項　四等獎

就讀學校　裕德學校財團法人新北市裕德高級中等學校
指導教師　譚國強
作者姓名　張耕宇

關鍵詞　廣義佩爾方程式、因數倍數、正整數解

作者簡介

我是張耕宇，就讀於裕德高中數理資優班二年級。在國中時，受班導啟發，以及對數學的熱愛，開始了數學專題研究。在譚老師指導下，我已研究廣義佩爾方程式4年，經常利用午休還有社團活動等課餘時間討論，並取得多項進展。

平時我也喜歡觀看數學影片，並拍攝教學影片分享有趣的數學知識，教學相長，與大家共同探索數學的奧妙。

2025 年臺灣國際科學展覽會

研究報告

區別：

科別：數學科

作品名稱：廣義佩爾方程式的一些探討

關鍵詞：廣義佩爾方程式、因數倍數、正整數解

編號：

（編號由國立臺灣科學教育館統一填列）

目錄

摘要

這是一份將近持續四年的研究，而這一年佩爾質數的出現，讓我們的討論「突飛猛進」。

佩爾方程式是形如 $x^2 - my^2 = 1$ 的方程式，其中 k 不為完全平方數之正整數。我們定義廣義佩爾方程式是形如 $x^2 - my^2 = n$ 的方程式。在過去的研究中，我們主要從 $x^2 - ky^2 = p$ $(k, p$ 皆為互質的奇質數$)$ 的正整數解開始研究，接著延伸到 $x^2 - ky^2 = 2^m p_1^{n_1} p_2^{n_2} \cdots p_j^{n_j}$ ，進而得到了解的唯一分解性質。而本次的研究，延續之前的工作，對佩爾質數展開了討論。利用蜈蚣兿，我們成功地發現了一些佩爾質數，猜測出一些可能的結果並證明；同時我們對佩爾質數的生成結構做了相當程度的了解。作為結束，設法利用分析的方法解決的之前的問題，以及對方程式的不可約解，是否存在較低次方根解，給出了必要條件。

Abstract

The Pell equation is a type of equation in the form $x^2 - my^2 = 1$, where m is a positive integer that is not a perfect square. We define the generalized Pell equation as an equation in the form $x^2 - my^2 = n$. In previous research, we primarily began by studying the integer solutions of $x^2 - ky^2 = p$ (where both k and p are distinct odd prime numbers), and then extended the equation to $x^2 - ky^2 = 2^m p_1^{n_1} p_2^{n_2} \cdots p_j^{n_j}$, from which we derived the unique factorization properties of the solutions (see Reference [8]). In this research, we continue the unfinished work from before, specifically focusing on the discussion of Pell primes. Using the centipede method, we successfully discovered some Pell primes, and from these, we conjectured and then proved certain possible results. At the same time, we gained a significant understanding of the generation structure of Pell primes. In conclusion, we addressed problems raised in previous research by analytical methods and provided necessary conditions regarding whether there exist lower-order roots for the irreducible solutions of the generalized Pell equation.

1. 前言

研究動機

在之前的研究中，我們證明了對於數個相異的奇質數 p_1 、⋯ 、p_m 與 k，若對於任意的正整數 $i = 1$ 、⋯ 、m， $x^2 - ky^2 = p_i^{n_i}$、皆有正整數解，則 $x^2 - ky^2 = p_1^{n_1}p_2^{n_2}\cdots p_m^{n_m}$ 的解，均可表示成 $x^2 - ky^2 = p_i^{n_i}$ 解之乘積（見參考資料**【5】【定理 3.2】**）。

得到這結果後，我們思考著另一個問題：「假設p_1 和 p_2 為相異奇質數，且 $x^2 - ky^2 = p_1$ 及 $x^2 - ky^2 = p_2$ 都沒有正整數解時，$x^2 - ky^2 = p_1p_2$ 是否會有正整數解？」起先，我們遍尋不著有解的例子，卻也無法得出在該情況下無解的證明；然而，一組反例的出現，否定了我們認為無解的猜想。（$x^2 - 37y^2 = 3$ 、$x^2 - 37y^2 = 7$ 皆無正整數解，但是 $x^2 - 37y^2 = 21$ 卻有正整數解）。

這意外的發現，其實跟我們之前研究的蜈蚣彘（見參考資料**【8】【四、蜈蚣彘】**）有非常大的關係，也因為如此，霎時間我們得到了更多的數據，也因此展開了我們對這類的方程式的研究。

研究目的

1. 延伸之前蜈蚣彘的技巧，對廣義佩爾方程式逕行更多分解，並探究佩爾質數是否也有唯一分解性質。
2. 從已知的佩爾質數，來產生新的佩爾質數，並且對佩爾質數相互作用進行探討。
3. 了解二維與三維佩爾地毯的『形狀』以及形成的方式與種類。
4. 解決過去研究中有關 Shoes 函數的問題，並針對不可約解分布的問題進行了解。

2. 研究方法或過程

1. 基本的定義和結果

在開始討論之前，我們需要先行給出在之前研究中所用到的定義，以及這次研究中我們會引用到之前的結果；而定義的相關說明以及結果的證明，可詳見相對應的參考資料，故在此並不贅述。

首先，我們必須先強調的是，**以下討論的方程式均有正整數解。**

【定義 2.1.1】（廣義佩爾方程式）

對於任意的正整數 m，以及一個非零的整數 n，當

（1） $n=1$ 時，方程式 $x^2-my^2=1$ 被稱為一個佩爾方程式；

（2） $n\neq 1$ 時，方程式 $x^2-my^2=n$ 被稱為一個廣義的佩爾方程式。

若 m 不為完全平方數時，佩爾方程式 $x^2-my^2=1$ 都一定會有無限多組的正整數解（見參考資料【1】）；事實上，

【定理 2.1.1】（佩爾方程式的解；見參考資料【1】）

對於任意的佩爾方程式 $x^2-my^2=1$，若 $\sqrt{m}\notin\mathbb{Z}$，則存在一個正整數數對 (x_1,y_1)，使得下列敘述成立：

（1） $x_1^2-my_1^2=1$；

（2） 對於任意的正整數 n，若正整數數對 (x_n,y_n) 滿足 $x_n+y_n\sqrt{m}=\left(x_1+y_1\sqrt{m}\right)^n$，則數對 (x_n,y_n) 會是佩爾方程式 $x^2-my^2=1$ 的一組正整數解，即 $x_n^2-my_n^2=1$；

（3） 若數對 (u,v) 會是佩爾方程式 $x^2-my^2=1$ 的一組正整數解，則存在一個正整數 n，使得 $(u,v)=(x_n,y_n)$。

然而，對於任意的廣義佩爾方程式 $x^2-my^2=n$ 卻不一定有正整數解。比如說，利用同餘的技巧，很容易可以知道廣義佩爾方程式 $x^2-3y^2=2$ 不會有任何的正整數解。因此，我們必須先強調，

以下所討論的廣義佩爾方程式均有正整數解。

在【定理 2.1.1】(2)中將一個整數數對數對 (x,y) 看成 $x+y\sqrt{m}$，這樣的定義除了是良好的(well-defined)以外，更是我們在研究廣義佩爾方程式時最常見的手法。其優點除了將 (x,y) 看成 $x+y\sqrt{m}$ 時可以進行基本的四則運算外，一些相當有用且直接可以利用計算而證明的技巧，更是常被我們利用：

【定理 2.1.2】

（1） 若整數數對 (u,v) 是廣義佩爾方程式 $x^2-my^2=n$ 的一個整數解，則數對 $(u,-v)$ 也會是該方程式的一組解，且 $\left(u+v\sqrt{m}\right)\left(u-v\sqrt{m}\right)=n$。

（2） 設整數數對 (u,v) 和 (s,t) 分別為廣義佩爾方程式 $x^2-my^2=\alpha$ 與 $x^2-my^2=\beta$

的解，則 $(u+v\sqrt{m})(s+t\sqrt{m})=(us+mvt)+(ut+sv)\sqrt{m}$ 會是 $x^2-my^2=\alpha\beta$ 的的一組整數解；意即 $(us+mvt)^2-m(ut+sv)^2=\alpha\beta$。

為了方便起見，當我們說

（1） (正)整數數對 (u,v) 是廣義佩爾方程式 $x^2-my^2=n$ 的一個解時，係指 (u,v) 是該方程式的一組(正)整數解。

（2） $u+v\sqrt{m}$ 是廣義佩爾方程式 $x^2-my^2=n$ 的一個解時，所表示的意思是指數對 (u,v) 是廣義佩爾方程式 $x^2-my^2=n$ 的一個解。（所以是整數解）

在【定理 2.1.2】(1) 中，考慮 $u+v\sqrt{m}$ 所相對應的另一個解 $u-v\sqrt{m}$ 的技巧，也被我們經常性的使用，因此為了方便起見，我們有下面的定義（**見參考資料【3】;【性質 3.1】**）

【定義 2.1.2】（解的共軛）

設 $\omega=u+v\sqrt{m}$，其中 (u,v) 是一個整數數對。則 ω 的共軛（記做 $\bar{\omega}$），被定義為

$$\bar{\omega}=u-v\sqrt{m}$$

同樣可以利用計算直接證明下列結果（**見參考資料【3】;【性質 3.1】**）

【定理 2.1.2】

設 $\alpha=\alpha_1+\alpha_2\sqrt{m}$ 以及 $\beta=\beta_1+\beta_2\sqrt{m}$ ，其中 (α_1,α_2) 以及 (β_1,β_2) 均為整數數對，則有

$$\overline{\alpha\cdot\beta}=\bar{\alpha}\cdot\bar{\beta}$$

最後，也是為了討論的便利性，我們定義（**見參考資料【7】;【定義一】**）

【定義 2.1.3】（σ 的定義）

設正整數 m 不為完全平方數。則佩爾方程式 $x^2-my^2=1$ 的第一個正整數解，均以符號 $\sigma_m=\alpha_m+\beta_m\sqrt{m}$ 表示；若在討論時 m 並不會有混淆的情況發生，則將 σ_m 簡寫成 $\sigma=\alpha+\beta\sqrt{k}$。

2. 過去的研究結果

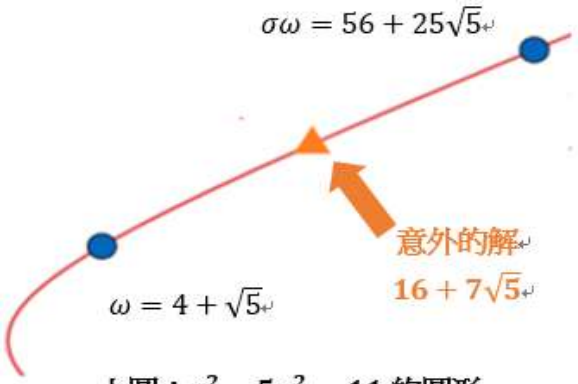
在這一章節中，我們將簡述過去所得到的一些結果，而這些結果大部分都是來自於**參考資料【7】【8】**；這也表示在這兩年的研究裡，我們得到了相當大的進展，進而對接下來的研究有一定的影響。

一開始的問題：解的長度 $l(m,n)$

我們有興趣的問題是，來自於廣義佩爾方程式正整數解的一個現象，以下用例子來說明：考慮佩爾方程式與廣義佩爾方程式 $x^2-5y^2=1$ 與 $x^2-5y^2=11$，這個兩個方程式的第一個正整數解分別為 $\sigma=9+4\sqrt{5}$ 以及 $\omega=4+\sqrt{5}$，則根據【定理 2.1.1】與【定理 2.1.2】，我們很容易可以發現對於任意的正整數 n，$\sigma^n\omega$ 都會是 $x^2-5y^2=11$的一個正整數解。因此，我們**猜測 $x^2-5y^2=11$ 的所有正整數解就應該是**

$$\omega、\sigma\omega、\sigma^2\omega、\sigma^3\omega、\cdots、、\sigma^n\omega、\cdots$$

然而，在 $\omega=4+\sqrt{5}$ 和 $\sigma\omega=56+25\sqrt{5}$ 之間，還另外有一個『意外的』解 $\sigma\bar{\omega}=16+7\sqrt{5}$；而事實上，$x^2-5y^2=11$ 在 ω 和 $\sigma\omega$ 之間也就只有這三個解（見下圖）。



上圖：$x^2-5y^2=11$ 的圖形

我們不禁想問，對於一個給定的廣義佩爾方程式 $x^2-my^2=n$，若 ω 是該方程式的第一個正整數解，那麼從 ω 到 $\sigma\omega$，一共會有多少方程式 $x^2-my^2=n$ 的解。而在當時為了方便起見，我們給出了下面的定義：

【定義 2.2.1】（解的長度 $l(m,n)$）

設廣義佩爾方程式 $x^2-my^2=n$ 的第 t 個正整數解是 ω_t。若 $\omega_s=\sigma\cdot\omega_1$，則我們稱

(1) 方程式 $x^2-My^2=n$ 解的長度是 s，且記為 $l(M,n)=s$。

(2) 若 n 是完全平方數，則 $\omega_0=\sqrt{n}<\omega_2<\cdots<\omega_{s-1}=\sigma\cdot\sqrt{n}$ 稱為該方程式第一段的解。

(3) 若 n 不是完全平方數，則 $\omega_1<\omega_2<\cdots<\omega_s=\sigma\cdot\omega_1$ 稱為該方程式第一段的解。

討論 $l(m,n)$ 是有意義的；如果我們了解了廣義佩爾方程式 $x^2-my^2=n$ 所有的正整數解，那麼我們就了解了該方程式的所有整數解；若我們能掌握 $l(m,n)$，那只要找出 ω 到 $\sigma\omega$ 之間所有的正整數解，也就等同於掌握了方程式 $x^2-my^2=n$ 所有的整數解（**見參考資料【5】；定理 3.3(2)**）。

$$\boldsymbol{l(k,p^n)=n+2}$$

因此，在過去的研究中，我們致力於了解 $l(m,n)$。首先，由於**【定理 2.1.2】**（2）說明廣義佩爾方程式的解相乘後，會得到另外一個廣義佩爾方程式的解，這給了我們以下的想法：若我們將方程式 $x^2-my^2=n$ 中的 n 做質因數分解 $p_1^{n_1}p_2^{n_2}\cdots p_j^{n_j}$，則掌握了每個 $x^2-my^2=p_i^{n_i}$ 的解，就可以創造出 $x^2-my^2=n$ 的解。我們猜測 $x^2-my^2=n$ 的解，皆可以利用 $x^2-my^2=p_i^{n_i}$ 的解產生，而且 $l(m,n)$ 或許會和每個 $l(m,p_i^{n_i})$ 有一定的關聯性。

因此，我們當時的研究，就全部轉至討論 $x^2-my^2=p^n$ 的解以及 $l(m,p^n)$。後來，我們發現當 m 也被限制成另一個與 p 互質的質數 k 時，我們會得到一些不錯的結果。

首先，我們藉由**參考資料【3】**可以知道，對於兩個相異的奇質數 k 和 p，會有

$$l(k,p)=3$$

利用蜈蚣分解（**見參考資料【7】**），可以說明對於任意非負整數 n，解的長度

$$l(k,p^n)=n+2$$

（**見參考資料【7】【8】**）。事實上，我們掌握了所有的正整數解：若 $x^2-ky^2=p$ 的第一個正整數解是 ω，我們可以知道方程式 $x^2-ky^2=p^n$ 的正整數解必形如

$$\sigma^s p^t \omega^{n-2t} \text{ 或 } \sigma^u p^v \bar{\omega}^{n-2v}$$

其中 $0\le t,v\le\left[\frac{n}{2}\right]$（**見參考資料【8】**）。也就是說，了解了第一個正整數解，事實上就是了解了所有的整數解。

唯一分解性質

接著，如前面所述，當我們能夠掌握某些廣義佩爾方程式 $x^2-ky^2=p_i^{n_i}\ (i=1,\cdots,t)$ 的所有正整數解，再利用**【定理 2.1.2】**（2）便可產生廣義佩爾方程式 $x^2-ky^2=p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t}$ 的解；事實上，廣義佩爾方程式 $x^2-ky^2=p_1^{n_1}p_2^{n_2}\cdots p_t^{n_t}$ 的所有正整數解，也可以寫成廣義佩爾方程式 $x^2-ky^2=p_i^{n_i}\ (i=1,\cdots,t)$ 正整數解的乘積，我們稱這性質為『唯一分解性質』。由於後面一開始的發想，是源於蜈蚣分解以及唯一分解性質，我們在此將分解性質敘述如下，詳細證明可見**參考資料【8】**：

【唯一分解性質】

設正整數 P 的標準分解式為 $p_1^{n_1}\ p_2^{n_2}\cdots\ p_j^{n_j}$ 。若對於任意的 $i=1,\cdots,j$，方程式 $x^2-ky^2=p_i$ 都有不可約解（其中 p_i 和 k互質），則 $x^2-ky^2=P$ 的任何一個正整數解，可以被唯一分解為

$$\sigma^n p_1^{m_1}\ p_2^{m_2}\cdots\ p_j^{m_j}\omega_1\omega_2\cdots\omega_j$$

其中 m_i 為任意非負整數，且對於所有的 i， $0\le 2m_i\le n_i$，且 ω_i 是 $x^2-ky^2=p_i^{n_i-2m_i}$ 在第一段中的不可約解。

在分解性質的敘述中，不可約解的定義如下：

【定義 2.2.2】（不可約解）

對於一個給定的廣義佩爾方程式 $x^2-my^2=n$，一個解 $\omega=u+v\sqrt{m}$ 被稱為不可約，如果 u 和 v 為互質的兩數。

所以，根據，對於廣義佩爾方程式解的長度，我們會有

【定理 2.2.1】

設整數 P 的標準分解式為 $p_1^{n_1}\ p_2^{n_2}\cdots\ p_j^{n_j}$ 。若對於任意的 $i=1,\cdots,j$，方程式 $x^2-ky^2=p_i$ 都有不可約解（其中 p_i 和 k互質），則

$$l(k,P)=\left(l\left(k,p_1^{n_1}\right)-1\right)\cdot\left(l\left(k,p_2^{n_2}\right)-1\right)\cdot\cdots\cdot\left(l\left(k,p_j^{n_j}\right)-1\right)+1$$

關於**【定理 2.2.1】**的證明，可詳**見參考資料【7】【定理2.6】**。

蜈蚣分解

我們先從蜈蚣分解開始：假設 k 和 p 分別為相異的兩個奇質數，且設 ω_1 是 $x^2-ky^2=p$ 有不可約解，則對於任意的正整數 n， ω_1^n 會是 $x^2-ky^2=p^n$ 的一個不可約解（見**【定理 7.1.1】**）。有趣的地方是，我們可以從 $x^2-ky^2=p^{2n}$，分解出其他方程式的不可約解。

假設 (x,y) 是方程式 $x^2-ky^2=p^{2n}$，則會得到

$$(x-p^n)(x+p^n)=x^2-p^{2n}=ky^2$$

若令 $d=\gcd(x-p^n,x+p^n)$ ，則 d 有可能為

1 、2 、p 、p^2 、p^3 、$\cdots$ 、p^n 、$2p$ 、$2p^2$ 、$2p^3$ 、$\cdots$ 、$2p^{n-1}$ 或 $2p^n$ 。

根據 d 的請況，我們可以做以下四種分類

(1) $d=1$；k 可以整除 $x-p^n$ 或 $x+p^n$。因此，我們可將 y 寫成兩個互質整數的乘積 y_1y_2，則會有

$$\begin{cases} x+p^n=y_1^2 \\ x-p^n=ky_2^2 \end{cases} \quad 或 \quad \begin{cases} x+p^n=ky_1^2 \\ x-p^n=y_2^2 \end{cases}$$

將上面兩式相減，就可以得到 $x^2-ky^2=2p^n$ 的一個不可約解 $y_1+y_2\sqrt{k}$（或是 $x^2-ky^2=-2p^n$ 的一個解 $y_2+y_1\sqrt{k}$）。

(2) $d=2$；同樣的，k 可以整除 $x-p^n$ 或 $x+p^n$，而且 y 是偶數。因此我們可將 y 寫成 $2^m\,y_1y_2$，其中 y_1 和 y_2 為兩個互質奇整數，且 m 為一正整數，與上述情況相同，我們會有以下兩種情況

$$\begin{cases} x+p^n=2^ay_1^2 \\ x-p^n=k2^by_2^2 \end{cases} \quad 或 \quad \begin{cases} x+p^n=k2^ay_1^2 \\ x-p^n=2^by_2^2 \end{cases}$$

其中 $2m=a+b$；將上面兩式相減，就可以得到 $2^ay_1^2-k2^by_2^2=2p^n$ 或 $2^by_2^2-k2^ay_1^2=-2p^n$ 兩式；化簡後後可以得到

$$2^{a-1}y_1^2-k2^{b-1}y_2^2=p^n \text{ 或 } 2^{b-1}y_2^2-2^{a-1}ky_1^2=-p^n$$

因為 $d=2$，$a-1$ 與 $b-1$ 兩數中必定只有一個是 0，而另一個數會是偶數。根據以上討論，我們將方程式 $x^2-ky^2=p^{2n}$ 的解分解出了方程式 $x^2-ky^2=\pm p^n$ 的不可約解。

(3) $d=p^s$，$s=1,2,\cdots,n$；由於 p^s 可以整除 $x-p^n$ 和 $x+p^n$，故可得 p^s 是 x 的因數。設 $x=2^rtd=2^rtp^s$（其中 $r\geq 1$ 且奇數 t 與 p 互質）並將其代入方程式 $x^2-ky^2=p^{2n}$ 中，我們可得 $2^{2r}t^2p^{2s}-ky^2=p^{2n}$，故 p^s 是 y 的因數。現假設 $y=wp^s$（w 為奇數）且將 $x+y\sqrt{k}=2^rtp^s+wp^s\sqrt{k}$ 代入 $x^2-ky^2=p^{2n}$ 中，則可得 $(2^rt)^2-w^2=p^{2(n-s)}$；由於 2^rt 與 p 互質， $2^rt+u\sqrt{k}$ 是方程式 $x^2-ky^2=p^{2(n-s)}$ 的一個不可約解。

(4) $d=2p^s$，$s=1,2,\cdots,n$；同樣的，從 d 可以整除 $x-p^n$ 和 $x+p^n$，可推得 $d\mid 2x$，因此 $p^s\mid x$。故情況等同於 $d=p^s$，$s=1,2,\cdots,n$。

我們以下表來整理上述四個情況的分解：

$x^2-ky^2=p^{2n}$ 的任一個解 (x,y)					(x,y) 分解成 (u,v)				
可約性	情況	d	奇偶性	型態	可約性	奇偶性	型態	所對應的方程式	備註
不可約	(1)	1	(偶,奇)	$\left(\frac{y_1^2+ky_2^2}{2},y_1y_2\right)$	不可約	(奇,奇)	(y_1,y_2)	$x^2-ky^2=2p^n$	k 整除 $x-p^n$
								$x^2-ky^2=-2p^n$	k 整除 $x+p^n$
	(2)	2	(奇,偶)	$\left(y_1+2^{b-1}ky_2,2^{\frac{b+1}{2}}y_1y_2\right)$	不可約	(奇,偶)	$\left(y_1,2^{\frac{b-1}{2}}y_2\right)$	$x^2-ky^2=p^n$	k 整除 $x-p^n$
				$\left(2^{a-1}y_1+ky_2,2^{\frac{a+1}{2}}y_1y_2\right)$	不可約	(偶,奇)	$\left(2^{\frac{a-1}{2}}y_1,y_2\right)$		
				$\left(ky_1+2^{b-1}y_2,2^{\frac{b+1}{2}}y_1y_2\right)$	不可約	(偶,奇)	$\left(2^{\frac{b-1}{2}}y_2,y_1\right)$	$x^2-ky^2=-p^n$	k 整除 $x+p^n$
				$\left(k2^{a-1}y_1+y_2,2^{\frac{a+1}{2}}y_1y_2\right)$	不可約	(奇,偶)	$\left(y_2,2^{\frac{a-1}{2}}y_1\right)$		
可約	(3)	p^s	(偶,奇)	(p^s2^rt,p^sw)	不可約	(偶,奇)	$(2^rt,w)$	$x^2-ky^2=p^{2(n-s)}$	x 是偶數
	(4)	$2p^s$	(奇,偶)	(p^st,p^s2^rw)	不可約	(奇,偶)	$(t,2^rw)$		x 是奇數

根據以上的表格，我們可以知道一個 $x^2-ky^2=p^{2n}$ 的不可約解，可以分解成另一個廣義佩爾方程式的解，而 $x^2-ky^2=p^{2n}$ 的可約解，可以看成 $x^2-ky^2=p^{2(n-s)}$ 的一個不可約解乘上 p^s 所得；我們利用下圖來表示上述的分解

$$\begin{array}{ccccc} & & A & & \\ & & \uparrow & & \\ p^{2n-2} & \xleftarrow{\times\frac{1}{p}} & p^{2n} & \xleftarrow{\times\frac{1}{p}} & p^{2n+2} \\ & & \downarrow & & \\ & & B & & \end{array}$$

圖中的 p^*、A 以及 B 分別代表廣義佩爾方程式 $x^2-ky^2=p^*$、$x^2-ky^2=A$ 以及 $x^2-ky^2=B$ 的所有解。水平方向的箭頭（稱為蜈蚣的身體） $p^{*-2}\xleftarrow{\times\frac{1}{p}}p^*$ 代表將 $x^2-ky^2=p^*$ 中的可約解除以 p 之後，得到 $x^2-ky^2=p^{*-2}$ 中的一個解；垂直方向的箭頭（稱為蜈蚣的腳）代表將 $x^2-ky^2=p^*$ 中的不可約解，利用上表的分解後，得到 $x^2-ky^2=A$ 或 B中的一個不可約解。

總結以上的內容，以 k 和 p 作為分類依據**(見參考資料【7】)**，我們歸納出以下**五種型態的分解，**而這些分解便稱為**蜈蚣分解**：

(1) 當 $k\equiv 1\ (mod\ 4)$ 時，

$$\begin{array}{ccccccccccccc} & & p & & p^2 & & p^3 & & & & p^{2n} & & p^{n+1} \\ & & \uparrow & & \uparrow & & \uparrow & & & & \uparrow & & \uparrow \\ 1 & \xleftarrow{\times\frac{1}{p}} & p^2 & \xleftarrow{\times\frac{1}{p}} & p^4 & \xleftarrow{\times\frac{1}{p}} & p^6 & \xleftarrow{\times\frac{1}{p}} & \cdots & \xleftarrow{\times\frac{1}{p}} & p^{2n} & \xleftarrow{\times\frac{1}{p}} & p^{2n+2} & \xleftarrow{\times\frac{1}{p}} & \cdots \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\ -1 & & -p & & -p^2 & & -p^3 & & & & -p^n & & -p^{n+1} & & \end{array}$$

(2) 當 $k\equiv 3\ (mod\ 8)$ 且 $p\equiv 1\ (mod\ 4)$ 時，

$$\begin{array}{ccccccccccccc} & & p & & p^2 & & p^3 & & & & p^{n-1} & & p^n \\ & & \uparrow & & \uparrow & & \uparrow & & & & \uparrow & & \uparrow \\ 1 & \xleftarrow{\times\frac{1}{p}} & p^2 & \xleftarrow{\times\frac{1}{p}} & p^4 & \xleftarrow{\times\frac{1}{p}} & p^6 & \xleftarrow{\times\frac{1}{p}} & \cdots & \xleftarrow{\times\frac{1}{p}} & p^{2n-2} & \xleftarrow{\times\frac{1}{p}} & p^{2n} & \xleftarrow{\times\frac{1}{p}} & \cdots \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\ -2 & & -2p & & -2p^2 & & -2p^3 & & & & -2p^{n-1} & & -2p^n & & \end{array}$$

(3) 當 $k\equiv 3\ (mod\ 8)$ 且 $p\equiv 3\ (mod\ 4)$ 時，

$$\begin{array}{ccccccccccccc} & & -p & & p^2 & & -p^3 & & & & -p^{2n-1} & & p^{2n} \\ & & \uparrow & & \uparrow & & \uparrow & & & & \uparrow & & \uparrow \\ 1 & \xleftarrow{\times\frac{1}{p}} & p^2 & \xleftarrow{\times\frac{1}{p}} & p^4 & \xleftarrow{\times\frac{1}{p}} & p^6 & \xleftarrow{\times\frac{1}{p}} & \cdots & \xleftarrow{\times\frac{1}{p}} & p^{4n-2} & \xleftarrow{\times\frac{1}{p}} & p^{4n} & \xleftarrow{\times\frac{1}{p}} & \cdots \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\ -2 & & 2p & & -2p^2 & & 2p^3 & & & & 2p^{2n-1} & & -2p^{2n} & & \end{array}$$

(4) 當 $k\equiv 7\ (mod\ 8)$ 且 $p\equiv 1\ (mod\ 4)$ 時，

$$\begin{array}{ccccccccccccc} & & p & & p^2 & & p^3 & & & & p^{n-1} & & p^n \\ & & \uparrow & & \uparrow & & \uparrow & & & & \uparrow & & \uparrow \\ 1 & \xleftarrow{\times\frac{1}{p}} & p^2 & \xleftarrow{\times\frac{1}{p}} & p^4 & \xleftarrow{\times\frac{1}{p}} & p^6 & \xleftarrow{\times\frac{1}{p}} & \cdots & \xleftarrow{\times\frac{1}{p}} & p^{2n-2} & \xleftarrow{\times\frac{1}{p}} & p^{2n} & \xleftarrow{\times\frac{1}{p}} & \cdots \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & & \\ 2 & & 2p & & 2p^2 & & 2p^3 & & & & 2p^{n-1} & & 2p^n & & \end{array}$$

(5) 當 $k \equiv 7\ (mod\ 8)$ 且 $p \equiv 3\ (mod\ 4)$ 時，

$$\begin{array}{ccccccccccccc} & & -p & & p^2 & & -p^3 & & & & -p^{2n-1} & & p^{2n} & \\ & \overset{\times\frac{1}{p}}{\longleftarrow} & \uparrow & \overset{\times\frac{1}{p}}{\longleftarrow} & \uparrow & \overset{\times\frac{1}{p}}{\longleftarrow} & \uparrow & \overset{\times\frac{1}{p}}{\longleftarrow} \cdots \overset{\times\frac{1}{p}}{\longleftarrow} & & \uparrow & \overset{\times\frac{1}{p}}{\longleftarrow} & \uparrow & \overset{\times\frac{1}{p}}{\longleftarrow} \cdots \\ 1 & & p^2 & & p^4 & & p^6 & & & & p^{4n-2} & & p^{4n} & \\ \downarrow & & \downarrow & & \downarrow & & \downarrow & & & & \downarrow & & \downarrow & \\ 2 & & -2p & & 2p^2 & & -2p^3 & & & & -2p^{2n-1} & & 2p^{2n} & \end{array}$$

有關蜈蚣分解更多的性質，可詳**見參考資料【7】**，在此便不加以贅述。

蜈蚣彘

最後，關於我們這次的工作，蜈蚣彘扮演著相當重要的角色，所以接下來我們以介紹蜈蚣彘以及與其相關的結果，作為這一章節的結束。首先我們先給出蜈蚣彘的定義：

【定義 2.2.3】（蜈蚣彘）

令 k 和 p 為相異的奇質數，並假設廣義佩爾方程式 $x^2 - ky^2 = p$ 並沒有正整數解。若對於某一個大於 1 正整數 n，廣義佩爾方程式 $x^2 - ky^2 = p^n$ 有不可約的正整數解，則我們說質數 p 有 k −蜈蚣彘現象；若沒有混淆的的情況下，我們就簡稱質數 p 有蜈蚣彘現象。

舉例來說，當 $k = 37$ 、79 、101 時，以下表格呈現的是「當 p 無解時，p^3有解」的情況，也就是有質數 p 有 k −蜈蚣彘現象：

k	37	79	101
p	3,7,11,41,47,53,71,73,83	5,13,89,97,101	5,13,17,19,23,31,47,71,79

假設 p 有蜈蚣彘現象，則在蜈蚣分解中，只有特定的冪次有不可約解可以分出腳。從數據中可以發現（**見參考資料【8】**），腳出現的位置看似是有規律性的；以 $x^2 - 37y^2 = 3^n$ 為例，其蜈蚣分解如下圖所示：

$$\begin{array}{ccccccccccc} & & & & 3^3 & & & & 3^6 & & \\ & & & & \uparrow & & & & \uparrow & & \\ 3^0 & \longleftarrow & 3^2 & \longleftarrow & 3^4 & \longleftarrow & 3^6 & \longleftarrow & 3^8 & \longleftarrow & 3^{10} & \longleftarrow & 3^{12} & \longleftarrow \cdots \longleftarrow \\ & & & & \downarrow & & & & \downarrow & & \\ & & & & -3^3 & & & & -3^6 & & \end{array}$$

從圖中所示，看起來蜈蚣的腳皆出現於指數都是 3 的倍數時，這個規律性其實是可以證明的，但首先要解決的問題是，在 $x^2 - ky^2 = p$ 無解的情況下，對於任意正整數 n，$l(k, p^n)$ 之值為何？在上述例子中，$x^2 - 37y^2 = 3^3$ 時是第一個出現不可約解的方程式，3次方為最小的冪次使得方程式有不可約解。於是為了之後方便討論，我們給出以下的定義：

【定義 2.2.4】

設質數 p 有 k −蜈蚣彘現象。對於某個正整數 m ，如果 $x^2-ky^2=p^m$有不可約解，且對於所有正整數 $n<m$，$x^2-ky^2=p^n$ 都沒有不可約解，則 m 被稱為是廣義佩爾方程式 $x^2-ky^2=p^*$ 的「最低次方解」。

有關我們在蜈蚣彘現象的探討，可以詳見**參考資料【8】**，以下我們就 $l(k,p^n)$ 提出相關的結果，以及呈現有蜈蚣彘現象的蜈蚣分解（以下均假設質數 p 有 k −蜈蚣彘現象，且正整數 m 是廣義佩爾方程式 $x^2-ky^2=p^*$ 的最低次方解）:

【定理 2.2.2】

只有 $x^2-ky^2=p^{mn}$才會有不可約解，其中 n 為任意正整數。

【定理 2.2.3】

則對於任意正整數 n，會有 $l(k,p^{mn})=\begin{cases} n+2, \text{ 當 } m \text{ 為奇數} \\ 2n+2, \text{ 當 } m \text{ 為偶數} \end{cases}$

【定理 2.2.4】

對於任意正整數 t，會有

(1) 當 m 是偶數時 $l(k,p^t)=\begin{cases} 2\left[\frac{t}{m}\right]+2 & \text{當 } t \text{ 為偶數} \\ 0, & \text{當 } t \text{為奇數} \end{cases}$

(2) 當 m 是奇數時 $l(k,p^t)=\begin{cases} \left[\frac{t}{m}\right]+2, & \text{當 } t-m\left[\frac{t}{m}\right] \text{ 為偶數} \\ \left[\frac{t}{m}\right]+1, & \text{當 } t-m\left[\frac{t}{m}\right] \text{ 為奇數} \end{cases}$

關於以上三個定理的證明，可詳**見參考資料【8】【定理4.4】、【定理4.5】**以及**【定理4.6】**。

根據以上定理，我們整理出蜈蚣彘的分解形態必定如下:

當 $k\equiv 1 \pmod 4$ 時，m 必為奇數，其分解如下

$$\begin{array}{ccccccccccccccccc} & & & & & & p^m & & & & & & p^{2m} & & & & \\ & & & & & & \uparrow & & & & & & \uparrow & & & & \\ 1 & \xleftarrow{\times\frac{1}{p}} & p^2 & \xleftarrow{\times\frac{1}{p}} & \cdots & \xleftarrow{\times\frac{1}{p}} & p^{2m} & \xleftarrow{\times\frac{1}{p}} & p^{2m+2} & \xleftarrow{\times\frac{1}{p}} & p^{2m+4} & \cdots & p^{4m} & \xleftarrow{\times\frac{1}{p}} & p^{4m+2} & \xleftarrow{\times\frac{1}{p}} & p^{4m+4} \cdots \\ \downarrow & & & & & & \downarrow & & & & & & \downarrow & & & & \\ -1 & & & & & & -p^m & & & & & & -p^{2m} & & & & \end{array}$$

當 $k\equiv 3 \pmod 4$，m 為奇數時，其分解如下

$$\begin{array}{ccccccccccccccc} & & & & & & p^m & & & & \pm p^{2m} & & & & \\ & & & & & & \uparrow & & & & \uparrow & & & & \\ 1 & \xleftarrow{\times\frac{1}{p}} & p^2 & \xleftarrow{\times\frac{1}{p}} & \cdots & \xleftarrow{\times\frac{1}{p}} & p^{2m} & \xleftarrow{\times\frac{1}{p}} & p^{2m+2} & \xleftarrow{\times\frac{1}{p}} & p^{2m+4} & \cdots & \xleftarrow{\times\frac{1}{p}} & p^{4m} & \xleftarrow{\times\frac{1}{p}} & p^{4m+2} & \xleftarrow{\times\frac{1}{p}} & p^{4m+4} \\ \downarrow & & & & & & \downarrow & & & & & & & \downarrow & & & & \\ \pm 2 & & & & & & \pm 2p^m & & & & & & & \pm 2p^{2m} & & & & \end{array}$$

當 $k \equiv 3 \pmod 4$，且 $m = 2n$ 為偶數時，其分解如下

$$\begin{array}{ccccccccccccccc} & & & & & & -p^n & & & & -p^{2n} & & & & \\ & & & & & & \uparrow & & & & \uparrow & & & & \\ 1 & \xleftarrow{\times\frac{1}{p}} & p^2 & \xleftarrow{\times\frac{1}{p}} & \cdots & \xleftarrow{\times\frac{1}{p}} & p^{2n} & \xleftarrow{\times\frac{1}{p}} & p^{2n+2} & \xleftarrow{\times\frac{1}{p}} & p^{2n+4} & \cdots & \xleftarrow{\times\frac{1}{p}} & p^{4n} & \xleftarrow{\times\frac{1}{p}} & p^{4n+2} & \xleftarrow{\times\frac{1}{p}} & p^{4n+4} \\ \downarrow & & & & & & \downarrow & & & & & & & \downarrow & & & & \\ \pm 2 & & & & & & \pm 2p^n & & & & & & & \pm 2p^{2n} & & & & \end{array}$$

$l(k, 2^n)$

在之前的研究我們證明了 $l(k, 2^n)$ 會根據 k 給 8 除的餘數而有非常不同的結果。首先，我們討論了當 $k \equiv 3 \pmod 4$ 時， $l(k, 2^n)$ 的值會是多少：

【定理 2.2.5】

當 $k \equiv 3 \pmod 8$ 時， $l(k, 2^n) = \begin{cases} 0, & n\text{為奇數} \\ 2, & n\text{為偶數} \end{cases}$

當 $k \equiv 7 \pmod 8$ 時，$l(k, 2^n) = 2$。

相較於 $k \equiv 3 \pmod 4$，$k \equiv 1 \pmod 4$ 的情況複雜了許多，先從 $k \equiv 1 \pmod 8$ 開始：

【定理 2.2.6】

設 m 是 $x^2 - ky^2 = 2^n$ 的最低次方解

則當 $k \equiv 1 \pmod 8$ 時，$l\left(k, 2^{m+(m-2)(n-1)}\right) = n + 2$

若不可將次方表示為 $m + (m-2)(n-1)$ 這種形式時，

$$l(k, 2^t) = \begin{cases} \left[\frac{t-2}{m-2}\right] + 1 \ (\text{當} t - m - (m-2)\left[\frac{t-m}{m-2}\right] \text{為奇數}) \\ \left[\frac{t-2}{m-2}\right] + 2 \ (\text{當} t - m - (m-2)\left[\frac{t-m}{m-2}\right] \text{為偶數}) \end{cases}$$

到了 $k \equiv 5 \pmod 8$ ，利用同於可以了解 $x^2 - ky^2 = 4$ 以外的方程式，然而 $x^2 - ky^2 = 4$ 的長度會隨著 k 的不同而變化，可能是 2 或 4，我們有發現一個方法來判斷 $l(k, 4)$ 的值，取決於 $\sqrt[3]{8\sigma}$ 是否為正整數來求得：

【定理 2.2.7】

當 $k \equiv 5 \ (mod\ 8)$ 時，若 $x^2 - ky^2 = 4$ 有不可約解，則 $l(k, 4) = 4$；再假設 ω 為第一個不可約解，則 $\omega = \sqrt[3]{8\sigma}$。

3. 研究結果與討論

1.研究內容簡述

接下來，我們就開始說明我們這一年的研究成果。首先，我們將蜈蚣分解的技巧延伸，得到對不可約解分解的結果，這個結果對後面的研究，扮演著著決定性的角色。同時間，我們也給出了唯一分解性質的推廣結果。

接下來，我們著眼於『佩爾質數』討論；在之前的研究中，我們只能大概給出佩爾質數的輪廓，而在討論中這個定義卻不是那麼方便。至此，我們轉念到廣義佩爾方程式解的分解，給出了佩爾不可約的定義，進而完整刻畫出佩爾質數的定義。

然而，在研究的初期，佩爾質數只是一個抽象的定義，我們手邊尚無任何的實際例子，直到利用蜈蚣堯來產生佩爾質數，才使得佩爾質數不再是一個虛無的假設。由於目前手邊的佩爾質數均由蜈蚣堯相乘所產生，一些相關的不可約生成問題和不可約解的結構想法，便隨著蜈蚣堯產生。我們試著處理這些問題以及將想法具體化，也得到了一些不錯的結果。

我們整理了在這段研究過程中，一些相當有趣的結果。首先，我們將在之前作品中所提出的一個問題，再次提出討論，並利用了連續將問題作一處理；另外，我們還對廣義佩爾方程式的不可約解是否有較低次方根，給出了必要條件。

2. 蜈蚣分解的延伸

在蜈蚣分解的技巧中，我們利用了平方差公式將一個不可約解分解出更多的不可約解；當時，我們僅侷限於 $x^2-ky^2=p^{2n}$ 這種型態的廣義佩爾方程式（其中 k 和 p 為相異的奇質數）。然而，我們若將 p 為奇質數改為和 k 互質的奇數，也會得到類似的結果；然而分解的過程卻較質數的情況複雜的更多：

【定理 3.2.1】

假設 k 是一個奇質數且 $A>0$ 為一個與 k 互質的奇數。若 $x^2-ky^2=A^2$ 有不可約解，則 $x^2-ky^2=A$ 或 $x^2-ky^2=-A$ 亦有不可約解。

【證明】

假設 $\omega = u + \sqrt{k}v$ 是 $x^2 - ky^2 = A^2$ 一個不可約解，則有

$$kv^2 = u^2 - A^2 = (u + A)(u - A)$$

接著，我們針對 $\gcd(u + A, u - A)$ 來個別討論：

【第一種情況】若 $\gcd(u + A, u - A) = 1$

則 v 必定是奇數，且可將其寫成兩個互質整數 v_+ 與 v_- 的乘積，其中滿足下列其中之一的條件

（1） $u + A = v_+^2$ 且 $u - A = kv_-^2$

（2） $u + A = kv_+^2$ 且 $u - A = v_-^2$

將上面條件中的兩式相減，則 $\lambda_+ = v_+ + \sqrt{k}v_-$ (或 $\lambda_- = v_- + \sqrt{k}v_+$) 會是 $x^2 - ky^2 = 2A$ (或 $x^2 - ky^2 = -2A$) 的一個不可約解；特別要注意的是，這情況只會在 $k \equiv 3 \bmod 4$ 發生。

由於 $k \equiv 3 \bmod 4$，我們令 $x^2 - ky^2 = 2$（ $k \equiv 7 \bmod 8$）或 $x^2 - ky^2 = -2$（$k \equiv 3 \bmod 8$）的第一個不可約正整數解為 τ。

由於

$$\lambda_\pm^2 = v_\pm^2 + kv_\mp^2 + 2\sqrt{k}v_+v_- = 2\omega \Longrightarrow \frac{1}{2}\lambda_\pm^2 = \omega$$

當 τ 是 $x^2 - ky^2 = 2$ 的解，我們會有

$$\omega = \frac{1}{2}\lambda_\pm^2 = \omega = 2 \cdot \frac{\lambda_\pm^2}{4} = \left(\frac{\tau\lambda_\pm}{2}\right)\left(\frac{\bar{\tau}\lambda_\pm}{2}\right) ;$$

特別要注意的，$\frac{\tau\lambda_\pm}{2}$ 與 $\frac{\bar{\tau}\lambda_\pm}{2}$ 會是 $x^2 - ky^2 = \pm A$ 的不可約解；

若 τ 是 $x^2 - ky^2 = -2$ 的解，我們會有

$$\omega = \frac{1}{2}\lambda_\pm^2 = \omega = (-2) \cdot \frac{\lambda_\pm^2}{-4} = \left(\frac{\tau\lambda_\pm}{2}\right)\left(\frac{\bar{\tau}\lambda_\pm}{-2}\right)$$

同樣的，$\frac{\tau\lambda_\pm}{2}$ 與 $\frac{\bar{\tau}\lambda_\pm}{-2}$ 會是 $x^2 - ky^2 = \mp A$ 的不可約(整數)解。

因此，當 $\gcd(u + A, u - A) = 1$ 時，$x^2 - ky^2 = A$ 或 $x^2 - ky^2 = -A$ 會有不可約解。

【第二種情況】若 $\gcd(u + A, u - A) > 1$

現假設 p 是 $\gcd(u + A, u - A)$ 的一個質因數，那麼 p 必定整除 $2A$，故 p 等於

2 或是 A 的質因數。但是後者如果成立，p 也是 u 的質因數；又因為 A 與 k 互質，p 必定整除 v，這與 ω 不可約矛盾，故 p 只能等於 2。在這個情況下，v 必可表示成 $2^t \cdot v_+ \cdot v_-$，其中 $t \geq 1$ 且v_+ 與 v_-為兩個互質奇數，且滿足以下其中之一的關係：

（1） $\begin{cases} u - A = k \cdot 2v_-^2 \\ u + A = 2^{2t-1}v_+^2 \end{cases}$　　（2） $\begin{cases} u - A = 2v_-^2 \\ u + A = k \cdot 2^{2t-1}v_+^2 \end{cases}$

（3） $\begin{cases} u - A = k \cdot 2^{2t-1}v_-^2 \\ u + A = 2v_+^2 \end{cases}$　　（4） $\begin{cases} u - A = 2^{2t-1}v_-^2 \\ u + A = 2kv_+^2 \end{cases}$

將上面的四個關係中的上下兩式相減，會得到

（1） $(2^{t-1}v_+)^2 - kv_-^2 = A$　　（2） $v_-^2 - k(2^{t-1}v_+)^2 = -A$

（3） $v_+^2 - k(2^{t-1}v_-)^2 = A$　　（4） $(2^{t-1}v_-)^2 - kv_+^2 = -A$

這表示當 $\gcd(u + A, u - A) = 2$ 時，$x^2 - ky^2 = A$ 或 $x^2 - ky^2 = -A$ 也會有不可約解；若令上面四式中的任一不可約解為 λ，則 λ^2 等於

（1） $(2^{2t-2}v_+^2 + kv_-^2) + k \cdot 2^t v_+ v_-$　　（2） $(v_-^2 + 2^{2t-2}v_+^2) + k \cdot 2^t v_+ v_-$

（3） $(v_+^2 + k2^{2t-2}v_-^2) + k \cdot 2^t v_+ v_-$　　（4） $(2^{2t-2}v_-^2 + kv_+^2) + k \cdot 2^t v_+ v_-$

無論上面哪一種情況，均表示了 ω 等於 λ^2。■

【定理 3.2.1】有許多值得討論的部分，以下的**【備註 3.2.1】**到**【備註 3.2.1】**，就是我們對於該定理有更多的了解：

【備註 3.2.1】

我們在**【第一種情況】**中提到，當 τ 是 $x^2 - ky^2 = 2\ (-2)$的不可約解時，$\frac{\tau\lambda_\pm}{2}$ 與 $\frac{\bar{\tau}\lambda_\pm}{2}$ 以及 $\frac{\tau\lambda_\pm}{2}$ 與 $\frac{\bar{\tau}\lambda_\pm}{-2}$ 分別會是$x^2 - ky^2 = \pm A$ 的不可約解。以下對其不可約性作一補充說明：

根據 τ 與 $\lambda_\pm$ 的不可約性，我們可以假設 $\tau = \alpha + \beta\sqrt{k}$ 以及 $\lambda_\pm = \lambda_1 + \lambda_2\sqrt{k}$，其中 α, β, λ_1 與 λ_2 均為奇數，且 $\gcd(\alpha, \beta) = \gcd(\lambda_1, \lambda_2) = 1$。根據計算

$$\tau \cdot \lambda_\pm = (\alpha\lambda_1 + k\beta\lambda_2) + \sqrt{k}(\alpha\lambda_2 + \beta\lambda_1)$$

我們必須說明 $\gcd(\alpha\lambda_1 + k\beta\lambda_2, \alpha\lambda_2 + \beta\lambda_1) = 2$。現假設 p 是 $\gcd(\alpha\lambda_1 + k\beta\lambda_2, \alpha\lambda_2 + \beta\lambda_1)$ 的

一個質因數，由於

$$\pm 2\lambda_1 = \lambda_1(\alpha^2 - k\beta^2) = \alpha(\alpha\lambda_1 + k\beta\lambda_2) - k\beta(\alpha\lambda_2 + \beta\lambda_1)$$

以及

$$\pm 2\lambda_2 = \lambda_2(\alpha^2 - k\beta^2) = \alpha(\alpha\lambda_2 + \beta\lambda_1) - \beta(\alpha\lambda_1 + k\beta\lambda_2)$$

因此 p 是 $\gcd(2\lambda_1, 2\lambda_2) = 2 \cdot \gcd(\lambda_1, \lambda_2) = 2 \cdot 1 = 2$ 的一個質因數；這就證明了

$$\gcd(\alpha\lambda_1 + k\beta\lambda_2, \alpha\lambda_2 + \beta\lambda_1) = 2$$

也因此 $\frac{\tau\lambda_\pm}{2}$ 為不可約；同樣的，若考慮

$$\bar{\tau} \cdot \lambda_\pm = (\alpha\lambda_1 - k\beta\lambda_2) + \sqrt{k}(\alpha\lambda_2 - \beta\lambda_1)$$

則會有：

$$\pm 2\lambda_1 = \lambda_1(\alpha^2 - k\beta^2) = \alpha(\alpha\lambda_1 - k\beta\lambda_2) + k\beta(\alpha\lambda_2 - \beta\lambda_1)$$

以及

$$\pm 2\lambda_2 = \lambda_2(\alpha^2 - k\beta^2) = \alpha(\alpha\lambda_2 - \beta\lambda_1) + \beta(\alpha\lambda_1 - k\beta\lambda_2)$$

故 $\frac{\bar{\tau}\lambda_\pm}{\pm 2}$ 亦為不可約。

【備註 3.2.2】

【第一種情況】的分解過程可以解讀成

$$x^2 - ky^2 = A^2 \xrightarrow{\text{step1}} x^2 - ky^2 = \pm 2A \xrightarrow{\text{step2}} x^2 - ky^2 = \pm A$$

其中 step1 是從 $u \pm A$ 分裂出 $x^2 - ky^2 = \pm 2A$ 的解 $\lambda_\pm$；而在 step2 中，我們將 $\lambda_\pm$ 乘上 τ 或 $\bar{\tau}$ 後再除以 2 或 -2。由於

$$\frac{\tau\lambda_+}{2} = \begin{cases} \frac{\lambda_+}{\bar{\tau}}, & \tau \cdot \bar{\tau} = 2 \\ -\frac{\lambda_+}{\bar{\tau}}, & \tau \cdot \bar{\tau} = -2 \end{cases}$$

以及 $-\frac{\lambda_+}{\bar{\tau}}$ 是不可約解若且惟若 $\frac{\lambda_+}{\bar{\tau}}$ 也是不可約解，因此我們可以將 step2 直接看成計算 $\lambda_\pm$ 與 τ 或 $\bar{\tau}$ 的比值，也就是說

$$x^2 - ky^2 = A^2 \xrightarrow{\text{split } u^2 - A^2} x^2 - ky^2 = \pm 2A \xrightarrow{\times\frac{1}{\tau}\left(\text{或}\frac{1}{\bar{\tau}}\right)} x^2 - ky^2 = \pm A$$

我們把以上論述整理成下表：

$k \equiv 3 \pmod 4$ 且 u 是偶數		
$split\ u^2 - A^2$	$k \equiv 7 \pmod 8$ $(\tau \cdot \bar{\tau} = 2)$	$k \equiv 3 \pmod 8$ $(\tau \cdot \bar{\tau} = -2)$
$\begin{cases} u + A = v_+^2 \\ u - A = kv_-^2 \end{cases}$	$\frac{\tau\lambda_+}{2}$ 與 $\frac{\bar{\tau}\lambda_+}{2}(x^2 - ky^2 = A)$	$\frac{\tau\lambda_+}{2}$ 與 $\frac{\bar{\tau}\lambda_+}{-2}(x^2 - ky^2 = -A)$
$\begin{cases} u + A = kv_+^2 \\ u - A = v_-^2 \end{cases}$	$\frac{\tau\lambda_-}{2}$ 與 $\frac{\bar{\tau}\lambda_-}{2}(x^2 - ky^2 = -A)$	$\frac{\tau\lambda_-}{2}$ 與 $\frac{\bar{\tau}\lambda_-}{-2}(x^2 - ky^2 = A)$

【備註 3.2.3】

另一個值得注意得地方，在的表格中所呈現的是 $x^2 - ky^2 = \pm A$ 的是兩個不可約解，如果我們考慮分解後這兩個因子的比值，則利用 $\tau = \sqrt{2\sigma}$ ，我們會發現這比值恆為 σ：

$$\underbrace{\frac{\frac{\tau\lambda_\pm}{2}}{\frac{\bar{\tau}\lambda_\pm}{2}} = \frac{\tau}{\bar{\tau}} = \frac{\tau^2}{2} = \sigma}_{k\equiv 7 \pmod 8} \text{ 以及 } \underbrace{\frac{\frac{\tau\lambda_\pm}{\pm 2}}{\frac{\bar{\tau}\lambda_\pm}{\mp 2}} = -\frac{\tau}{\bar{\tau}} = -\frac{\tau^2}{-2} = \sigma}_{k\equiv 3 \pmod 8}$$

因此這個條件下的 ω 可以看成 $\sigma\lambda \cdot \lambda$；更進一步的解釋，$\omega$ 可由 $x^2 - ky^2 = \pm A$ 的不可約解 λ 平方後，再乘上 σ 得來。由於這情況只會發生在 $k \equiv 3 \pmod 4$，這也充分反應佩爾方程式在 k 這樣的條件下，σ 無法表示完全平方的情況。為了後面研究的方便，我們將**【定理 3.2.1】**中的分解情況以下面表格呈現：假設 $\omega = u + \sqrt{k}v$ 是 $x^2 - ky^2 = A^2$ 一個不可約解，則 ω 可分解成以下的分解情況

	$k \equiv 1 \pmod 4$	$k \equiv 3 \pmod 4$	
		v 為偶數	v 為奇數
$x^2 - ky^2 = A$	有不可約解 λ	只有一個有不可約解 λ	
$x^2 - ky^2 = -A$	有不可約解 $\sqrt{\sigma}\lambda$		
ω 的分解	λ^2 或 $\left(\sqrt{\sigma}\lambda\right)^2 = \sigma\lambda^2$	λ^2	$\sigma\lambda^2$

【備註 3.2.4】

在**【定理 3.2.1】**中的 A 被要求是一個奇數，倘若我們放寬條件，讓**【定理 3.2.1】**中的 A 是一個正整數，**【定理 3.2.1】**的結果是否依然會成立呢？答案是否定的，以下就是一個反例：$x^2 - 37y^2 = 22^2$ 有不可約解 $59 + 9\sqrt{37}$ 以及 $311 + 51\sqrt{37}$；然而，利用 Legendre symbol

$\left(\frac{22}{37}\right) = -1$ ，或是考慮將方程式 $x^2 - 37y^2 = \pm 22$ 在同餘 4 時，所得到的方程式為 $x^2 - y^2 \equiv 2 \pmod 4$的情況下，我們都可以得到 $x^2 - 37y^2 = \pm 22$ 並無整數解的結論，也因此 $59 + 9\sqrt{37}$ 和 $311 + 51\sqrt{37}$ 並不會有**【定理 3.2.1】**的結果。

根據【備註 3.2.4】，在以下我們的討論中，若我們會引用【定理 3.2.1】，那麼對於 A 的限制就會要求是一個正奇數。

根據**【定理3.2.1】**可知，若 Legendre symbol $\left(\frac{A}{k}\right) = 1$，則 $x^2 - ky^2 = A$ 有不可約解的充分必要條件為 $x^2 - ky^2 = A^2$ 有不可約解，因此便有了以下**【推論 3.2.1】**的結果；仿效之前學長的技巧，我們可以將**【推論 3.2.1】**再更一般化：

【推論 3.2.1】

設 k 是一個奇質數，而 A 為一個與 k 互質的奇數，以及 $\left(\frac{A}{k}\right) = 1$，則對於任意的非負整數 n，$x^2 - ky^2 = A^{2^n}$ 有不可約解，若且為若存在一個非負整數 m，使得 $x^2 - ky^2 = A^{2^m}$ 有不可約解。

【推論 3.2.2】

假設對於任意的正整數 n，$x^2 - ky^2 = A^n$ 有不可約解，若且為若存在一個非負整數 m，使得 $x^2 - ky^2 = A^{2^m}$ 有不可約解。

要注意的是在上面**【推論 3.2.2】**的條件中，『存在一個非負整數 m，使得 $x^2 - ky^2 = A^{2^m}$ 有不可約解』不能弱化成『存在一個非負整數 m，使得 $x^2 - ky^2 = A^m$ 有不可約解』。一個顯而易見的反例便是蜈蚣兔的存在，以及其不可約解出現的規律性。

接下來，我們從一個較簡單的結果**【定理 3.2.2】**開始：

【定理 3.2.2】

假設 k 是一個奇質數且 $A_i, i = 1, \cdots, n$ 均為兩兩互質的奇數。若對於任意的正整數 i ，k 與 A_i 皆互質且 $x^2 - ky^2 = A_i$均有不可約解 ω_i，那麼 $\omega_1\omega_2 \cdots \omega_n$ 會是方程式 $x^2 - ky^2 = A_1A_2 \cdots A_n$ 的不可約解。

【證明】

根據之前的結果（**見參考資料【5】;【定理 3. 2】**），$\omega_1\omega_2 \cdots \omega_n$ 會是方程式 $x^2 - ky^2 = A_1A_2 \cdots A_n$ 的一個解，因此我們只需要說明該解的不可約性即可。

設 $\omega_1 = u_1 + v_1\sqrt{k}$ 與 $\omega_2 = u_2 + v_2\sqrt{k}$分別為 $x^2 - ky^2 = A_1$ 以及 $x^2 - ky^2 = A_2$ 的一個不可約解，因此 $\omega_1\omega_2 = (u_1u_2 + kv_1v_2) + \sqrt{k}(u_1v_2 + u_2v_1)$。

若質數 p 是 $u_1u_2 + kv_1v_2$ 與 $u_1v_2 + u_2v_1$ 的公因數，那麼該質數必定整除某一個 A_i，在此我們不訪假設 p 整除 A_1。由於 A_1 和 A_2 互質，根據下面的計算

$$u_2(u_1v_2 + u_2v_1) - v_2(u_1u_2 + kv_1v_2) = v_1(u_2^2 - kv_2^2) = v_1A_2$$

我們可以知道 p 整除 v_1。因此，p 必定整除 $A_1 + kv_1^2 = u_1^2$；然而，這與 ω_1為 $x^2 - ky^2 = A_1$ 的一個不可約解矛盾；再利用數學歸納法，故得證。■

若根據**【定理 3.2.2】**可知， $x^2 - ky^2 = A_i$ 均有不可約解 ω_i，則 $\omega_1\omega_2 \cdots \omega_n$ 會是方程式 $x^2 - ky^2 = A$ 的不可約，其中 $A = A_1 \times A_2 \times \cdots \times A_n$。但是，隨意給定一個$x^2 - ky^2 = A$ 均有不可約解 ω，ω 未必是某個 ω_i 的倍數。

然而，利用**【定理 3.2.1】**的結果，我們可以說明 ω 和 ω_i 的關係：

【定理 3.2.3】

假設 k 是一個奇質數且 A_i 為相異奇數，其中 $i = 1, \cdots, n$。若

（1） 對於任意且相異的 $i, j, k \in \{1,2, \cdots, n\}$，$(k, A_i) = \left(A_j, A_k\right) = 1$

（2） $x^2 - ky^2 = A_i$ 以及 $x^2 - ky^2 = A$ 均有不可約解，其中 $A = A_1 \times A_2 \times \cdots \times A_n$。

那麼對於 $x^2 - ky^2 = A$ 任意的一個不可約解，都可以分解成兩個不可約解的乘積。

【證明】

首先，我們先假設 $\omega_i = u_i + \sqrt{k}v_i$ 以及 $\omega = u + \sqrt{k}v$ 分別是$x^2 - ky^2 = A_i$ 與 $x^2 -$

$ky^2 = A$ 的某一個不可約解，其中 $A = A_1 \times A_2 \times \cdots \times A_n$。考慮

$$\begin{cases} u_1^2 - kv_1^2 = A_1 \\ u^2 - kv^2 = A_1 \cdot A_2 A_3 \cdots A_n \end{cases}$$

分別將上式和下式乘上 v^2 以及 v_1^2 後相減，會有

$$(u_1 v + u v_1)(u_1 v - u v_1) = A_1(v^2 - A_2 A_3 \cdots A_n v_1^2)$$

要注意的是，A_1 僅只是一個奇數，不一定是 $uv_1 + u_1 v$ 或 $uv_1 - u_1 v$ 的因數。

我們先說明 $\gcd(A_1, uv_1 + u_1 v,\ uv_1 - u_1 v) = 1$；假設不是，則存在一個奇質數 p 整除 $\gcd(A_1, uv_1 + u_1 v,\ uv_1 - u_1 v)$。由於 p 會整除 $(uv_1 + u_1 v) - (uv_1 - u_1 v) = 2u_1 v$，因此 p 會是 u_1 或是 v 的一個因數；若 p 整除 v，又 p 整除 A_1，p 一定可以整除 $u^2 = A - kv^2$，這將與 ω 的不可約性矛盾；故 p 只會是 u_1 的一個因數。在此條件底下，p 必定會整除 $u_1^2 - A_1 = kv_1^2$。由於$(k, A_1) = 1$，p 只會是 v_1 的一個因數，這也與 ω_1 的不可約性矛盾。這也就說明了 $\gcd(A_1, uv_1 + u_1 v,\ uv_1 - u_1 v) = 1$。

根據上面的論述，我們可以假設 $A_1 = A_{1+}A_{1-}$，其中 $A_{1+}(= A_{1+}(\omega, \omega_1))$和 $A_{1-}(=\ A_{1-}(\omega, \omega_1))$ 分別為 $uv_1 + u_1 v$ 和 $uv_1 - u_1\, v$ 的因子，因此 $\frac{\omega\omega_1}{A_{1+}}$ 和 $\frac{\omega\overline{\omega_1}}{A_{1-}}$ 分別為

$$x^2 - ky^2 = A_{1-}^2 A_2 A_3 \ldots A_n \text{ 與 } x^2 - ky^2 = A_{1+}^2 A_2 A_3 \ldots A_n$$

這兩個方程式的解。

我們現在要說明這兩個解的不可約性：假設質數 p 可以整除 $\frac{\omega\omega_1}{A_{1+}}$ ，則 p 可整除 $\omega\omega_1$ 以及 A_{1-} 或$A_2 A_3 \ldots A_n$ 其中一者。然而，若 p 可整除 $\omega\omega_1$以及 A_{1-} ，這會與 A_{1+} 的選擇矛盾，故我們可以斷言 p 只可整除 $\omega\omega_1$以及 $A_2 A_3 \ldots A_n$。

根據下列式子

$$p \cdot \frac{u_1 v + u v_1}{p \cdot A_{1+}}(u_1 v - u v_1) = \frac{u_1 v + u v_1}{A_{1+}}(u_1 v - u v_1) = A_{1-}(v^2 - A_2 A_3 \cdots A_n v_1^2)$$

故 p 必可整除 v ；又 p 整除 $u_1 v + u v_1$，因此 p 可以整除 u 或 v_1 其中一者；若 p 整除 u，則與 ω 的不可約性矛盾，故 p 必整除 v_1。最後，因為 p 可整除 $\omega\omega_1 = (uu_1 + kvv_1) + \sqrt{k}(uv_1 + u_1 v)$，$p$ 會是 uu_1 的因數，所以 p 可整除 u_1；這亦與 ω_1的不可約性矛盾，因此我們證明了 $\frac{\omega\omega_1}{A_{1+}}$ 的不可約性；利用類似的論述，也可以得到 $\frac{\omega\overline{\omega_1}}{A_{1-}}$ 也是一個不可約解。為了方便接下來

的討論，我們用以下的符號代表上述討論中的不可約解 $\frac{\omega\omega_1}{A_{1+}}$ 和 $\frac{\omega\overline{\omega_1}}{A_{1-}}$ ：

$$+(\omega,\omega_1)=\frac{\omega\omega_1}{A_{1+}} \text{ 和 } -(\omega,\omega_1)=\frac{\omega\overline{\omega_1}}{A_{1-}}$$

接著，我們分別來到方程式 $x^2-ky^2=A_{1-}^2A_2A_3\dots A_n$ 與 $x^2-ky^2=A_{1+}^2A_2A_3\dots A_n$，這兩個方程式同時都有不可約解 $+(\omega,\omega_1)$ 以及 $-(\omega,\omega_1)$。我們將 $x^2-ky^2=A_2$ 的 解 $\omega_2=u_2+\sqrt{k}v_2$ 作用到這兩個方程式，那麼我們會得到以下四個方程式的以及他們的解：

$$+(+(\omega,\omega_1),\omega_2)\cdot\overline{+(+(\omega,\omega_1),\omega_2)}=A_{1-}(\omega,\omega_1)^2A_{2-}(+(\omega,\omega_1),\omega_2)^2A_3A_4\dots A_n$$

$$-(+(\omega,\omega_1),\omega_2)\cdot\overline{-(+(\omega,\omega_1),\omega_2)}=A_{1-}(\omega,\omega_1)^2A_{2+}(+(\omega,\omega_1),\omega_2)^2A_3A_4\dots A_n$$

$$+(-(\omega,\omega_1),\omega_2)\cdot\overline{+(-(\omega,\omega_1),\omega_2)}=A_{1+}(\omega,\omega_1)^2A_{2-}(-(\omega,\omega_1),\omega_2)^2A_3A_4\dots A_n$$

$$-(-(\omega,\omega_1),\omega_2)\cdot\overline{-(-(\omega,\omega_1),\omega_2)}=A_{1+}(\omega,\omega_1)^2A_{2+}(-(\omega,\omega_1),\omega_2)^2A_3A_4\dots A_n$$

其中

$$+(+(\omega,\omega_1),\omega_2)=\frac{\frac{\omega\omega_1}{A_{1+}}\omega_2}{A_{2+}(+(\omega,\omega_1),\omega_2)}=\frac{\omega\omega_1\omega_2}{A_{1+}(\omega,\omega_1)A_{2+}(+(\omega,\omega_1),\omega_2)}\qquad(1)$$

$$-(+(\omega,\omega_1),\omega_2)=\frac{\frac{\omega\omega_1}{A_{1+}}\overline{\omega_2}}{A_{2-}(+(\omega,\omega_1),\omega_2)}=\frac{\omega\omega_1\overline{\omega_2}}{A_{1+}(\omega,\omega_1)A_{2-}(+(\omega,\omega_1),\omega_2)}\qquad(2)$$

$$+(-(\omega,\omega_1),\omega_2)=\frac{\frac{\omega\overline{\omega_1}}{A_{1-}}\omega_2}{A_{2+}(-(\omega,\omega_1),\omega_2)}=\frac{\omega\overline{\omega_1}\omega_2}{A_{1-}(\omega,\omega_1)A_{2+}(-(\omega,\omega_1),\omega_2)}\qquad(3)$$

$$-(-(\omega,\omega_1),\omega_2)=\frac{\frac{\omega\overline{\omega_1}}{A_{1-}}\overline{\omega_2}}{A_{2-}(-(\omega,\omega_1),\omega_2)}=\frac{\omega\overline{\omega_1\omega_2}}{A_{1-}(\omega,\omega_1)A_{2-}(-(\omega,\omega_1),\omega_2)}\qquad(4)$$

要特別注意的是，這些解都是不可約解；另外，如果我們將 ω_1 和 ω_2 的次序改變，那麼我們會有（為了接下來說明需要起見，我們也在$(1')(2')(3')(4')$下方，列出$(1)(2)(3)(4)$四式

$$+(+(\omega,\omega_2),\omega_1)=\frac{\frac{\omega\omega_2}{A_{2+}}\omega_1}{A_{1+}(+(\omega,\omega_2),\omega_1)}=\frac{\omega\omega_2\omega_1}{A_{2+}(\omega,\omega_2)A_{1+}(+(\omega,\omega_2),\omega_1)}\qquad(1')$$

$$+(+(\omega,\omega_1),\omega_2)=\frac{\frac{\omega\omega_1}{A_{1+}}\omega_2}{A_{2+}(+(\omega,\omega_1),\omega_2)}=\frac{\omega\omega_1\omega_2}{A_{1+}(\omega,\omega_1)A_{2+}(+(\omega,\omega_1),\omega_2)}\qquad(1)$$

$$+(-(\omega,\omega_2),\omega_1)=\frac{\frac{\omega\overline{\omega_2}}{A_{2-}}\omega_1}{A_{1+}(-(\omega,\omega_2),\omega_1)}=\frac{\omega\overline{\omega_2}\omega_1}{A_{2-}(\omega,\omega_2)A_{1+}(-(\omega,\omega_2),\omega_1)}\qquad(2')$$

$$-(+(\omega,\omega_1),\omega_2)=\frac{\frac{\omega\omega_1}{A_{1+}}\overline{\omega_2}}{A_{2-}(+(\omega,\omega_1),\omega_2)}=\frac{\omega\omega_1\overline{\omega_2}}{A_{1+}(\omega,\omega_1)A_{2-}(+(\omega,\omega_1),\omega_2)}\qquad(2)$$

$$-(+(\omega,\omega_2),\omega_1)=\frac{\frac{\omega\omega_2}{A_{2+}}\overline{\omega_1}}{A_{1-}(+(\omega,\omega_2),\omega_1)}=\frac{\omega\omega_2\overline{\omega_1}}{A_{2+}(\omega,\omega_2)A_{1-}(+(\omega,\omega_2),\omega_1)}\qquad(3')$$

$$+(-(\omega,\omega_1),\omega_2)=\frac{\frac{\omega\overline{\omega_1}}{A_{1-}}\omega_2}{A_{2+}(-(\omega,\omega_1),\omega_2)}=\frac{\omega\overline{\omega_1}\omega_2}{A_{1-}(\omega,\omega_1)A_{2+}(-(\omega,\omega_1),\omega_2)}\qquad(3)$$

$$-(-(\omega,\omega_2),\omega_1)=\frac{\frac{\omega\overline{\omega_2}}{A_{2-}}\overline{\omega_1}}{A_{1-}(-(\omega,\omega_2),\omega_1)}=\frac{\omega\overline{\omega_2\omega_1}}{A_{2-}(\omega,\omega_2)A_{1-}(-(\omega,\omega_2),\omega_1)}\qquad(4')$$

$$-(-(\omega,\omega_1),\omega_2)=\frac{\frac{\omega\overline{\omega_1}}{A_{1-}}\overline{\omega_2}}{A_{2-}(-(\omega,\omega_1),\omega_2)}=\frac{\omega\overline{\omega_1\omega_2}}{A_{1-}(\omega,\omega_1)A_{2-}(-(\omega,\omega_1),\omega_2)}\qquad(4)$$

從 (1) 和 (1′) 我們注意到 $+(+(\omega,\omega_1),\omega_2)$ 和 $+(+(\omega,\omega_2),\omega_1)$ 都是不可約，也就是將 $\omega\omega_1\omega_2=\omega\omega_2\omega_1=x+\sqrt{k}y$ ，同時除去 x 和 y 的最大公因數後得到，所以我們會有

$$+(+(\omega,\omega_1),\omega_2)=+(+(\omega,\omega_2),\omega_1)$$

以及

$$A_{1+}(\omega,\omega_1)A_{2+}(+(\omega,\omega_1),\omega_2)=A_{2+}(\omega,\omega_2)A_{1+}(+(\omega,\omega_2),\omega_1)$$

由於 A_1 和 A_2 互質，我們會有

$$A_{1+}(\omega,\omega_1)=A_{1+}(+(\omega,\omega_2),\omega_1)\text{ 以及 }A_{2+}(\omega,\omega_2)=A_{2+}(+(\omega,\omega_1),\omega_2)$$

對於其他的不可約解 (2)(3)(4) 以及(2′)(3′)(4′)，我們也會有

$$-(+(\omega,\omega_1),\omega_2)=+(-(\omega,\omega_2),\omega_1)$$

$$+(-(\omega,\omega_1),\omega_2)=-(+(\omega,\omega_2),\omega_1)$$

$$-(-(\omega,\omega_1),\omega_2)=-(-(\omega,\omega_2),\omega_1)$$

以及

$$A_{1+}(\omega,\omega_1)A_{2-}(+(\omega,\omega_1),\omega_2)=A_{2-}(\omega,\omega_2)A_{1+}(-(\omega,\omega_2),\omega_1)$$

$$A_{1-}(\omega,\omega_1)A_{2+}(-(\omega,\omega_1),\omega_2)=A_{2+}(\omega,\omega_2)A_{1-}(+(\omega,\omega_2),\omega_1)$$

$$A_{1-}(\omega,\omega_1)A_{2-}(-(\omega,\omega_1),\omega_2)=A_{2-}(\omega,\omega_2)A_{1-}(-(\omega,\omega_2),\omega_1)$$

再次利用 A_1 和 A_2 互質的假設，最後會得到以下結論

$$A_{1+}(\omega,\omega_1)=A_{1+}(+(\omega,\omega_2),\omega_1)=A_{1+}(-(\omega,\omega_2),\omega_1)$$

$$A_{1-}(\omega,\omega_1)=A_{1-}(+(\omega,\omega_2),\omega_1)=A_{1-}(-(\omega,\omega_2),\omega_1)$$

$$A_{2+}(\omega,\omega_2)=A_{2+}(+(\omega,\omega_1),\omega_2)=A_{2+}(-(\omega,\omega_1),\omega_2)$$

$$A_{2-}(\omega,\omega_2)=A_{2-}(+(\omega,\omega_1),\omega_2)=A_{2-}(-(\omega,\omega_1),\omega_2)$$

因此不可約解 (1)(2)(3)(4) 可改寫為

$$+(+(\omega,\omega_1),\omega_2)=+(+(\omega,\omega_2),\omega_1)=\frac{\omega\omega_1\omega_2}{A_{1+}(\omega,\omega_1)A_{2+}(\omega,\omega_2)} \qquad (1")$$

$$-(+(\omega,\omega_1),\omega_2)=+(-(\omega,\omega_2),\omega_1)=\frac{\omega\omega_1\overline{\omega_2}}{A_{1+}(\omega,\omega_1)A_{2-}(\omega,\omega_2)} \qquad (2")$$

$$+(-(\omega,\omega_1),\omega_2)=-(+(\omega,\omega_2),\omega_1)=\frac{\omega\overline{\omega_1}\omega_2}{A_{1-}(\omega,\omega_1)A_{2+}(\omega,\omega_2)} \qquad (3")$$

$$-(-(\omega,\omega_1),\omega_2)=-(-(\omega,\omega_2),\omega_1)=\frac{\omega\overline{\omega_1\omega_2}}{A_{1-}(\omega,\omega_1)A_{2-}(\omega,\omega_2)} \qquad (4")$$

且由不可約解 (1)(2)(3)(4)所得到的方程式可改寫為

$$x^2-ky^2=A_{1-}(\omega,\omega_1)^2A_{2-}(\omega,\omega_2)^2A_3A_4\dots A_n$$

$$x^2-ky^2=A_{1-}(\omega,\omega_1)^2A_{2+}(\omega,\omega_2)^2A_3A_4\dots A_n$$

$$x^2-ky^2=A_{1+}(\omega,\omega_1)^2A_{2-}(\omega,\omega_2)^2A_3A_4\dots A_n$$

$$x^2-ky^2=A_{1+}(\omega,\omega_1)^2A_{2+}(\omega,\omega_2)^2A_3A_4\dots A_n$$

至此，我們整理一下以上的結果：首先，利用 ω_1 和 ω_2，我們將方程式依次分解成兩個和四個方程式

$$A_1A_2\cdot A_n\xrightarrow{\omega_1\text{ 分解}}\begin{cases}A_{1+}^2A_2A_3\dots A_n\xrightarrow{\omega_2\text{ 分解}}\begin{cases}A_{1+}^2A_{2+}^2A_3\dots A_n\\A_{1+}^2A_{2-}^2A_3\dots A_n\end{cases}\\A_{1-}^2A_2A_3\dots A_n\xrightarrow{\omega_2\text{ 分解}}\begin{cases}A_{1-}^2A_{2+}^2A_3\dots A_n\\A_{1-}^2A_{2-}^2A_3\dots A_n\end{cases}\end{cases}$$

同時間，ω_1 和 ω_2 也將依次 ω 分解成上述兩個和四個方程式的解

$$\omega\xrightarrow{\omega_1\text{ 分解}}\begin{cases}+(\omega,\omega_1)=\dfrac{\omega\omega_1}{A_{1+}}\xrightarrow{\omega_2\text{ 分解}}\begin{cases}+(+(\omega,\omega_1),\omega_2)=\dfrac{\omega\omega_1\omega_2}{A_{1+}(\omega,\omega_1)A_{2+}(\omega,\omega_2)}\\-(+(\omega,\omega_1),\omega_2)=\dfrac{\omega\omega_1\overline{\omega_2}}{A_{1+}(\omega,\omega_1)A_{2-}(\omega,\omega_2)}\end{cases}\\-(\omega,\omega_1)=\dfrac{\omega\overline{\omega_1}}{A_{1-}}\xrightarrow{\omega_2\text{ 分解}}\begin{cases}+(-(\omega,\omega_1),\omega_2)=\dfrac{\omega\overline{\omega_1}\omega_2}{A_{1-}(\omega,\omega_1)A_{2+}(\omega,\omega_2)}\\-(-(\omega,\omega_1),\omega_2)=\dfrac{\omega\overline{\omega_1\omega_2}}{A_{1-}(\omega,\omega_1)A_{2-}(\omega,\omega_2)}\end{cases}\end{cases}$$

此外，ω_1 和 ω_2 在進行分解時的次序並不重要：

$$+(+(\omega,\omega_1),\omega_2)=+(+(\omega,\omega_2),\omega_1) \qquad -(+(\omega,\omega_1),\omega_2)=+(-(\omega,\omega_2),\omega_1)$$

$$+(-(\omega,\omega_1),\omega_2)=-(+(\omega,\omega_2),\omega_1) \qquad -(-(\omega,\omega_1),\omega_2)=-(-(\omega,\omega_2),\omega_1)$$

因此，依 ω_3、ω_4、…、ω_n 的順序重複以上的分解動作，我們會到 2^n 個廣義佩爾方程式

$$x^2-ky^2=A_{1a_1}^2(\omega,\omega_1)A_{2a_2}^2(\omega,\omega_2)\dots A_{na_n}^2(\omega,\omega_n)$$

以及該方程式的某一個不可約解

$$a_n(a_{n-1}(a_{n-2}(\cdots a_2(a_1(\omega,\omega_1),\omega_2)\cdots,\omega_{n-2}),\omega_{n-1}),\omega_n)=\frac{\omega\cdot\prod_{i=1}^n a_i(\omega_i)}{\prod_{i=1}^n A_{ia_i}(\omega,\omega_i)}$$

其中 $a_j\in\{+,-\}$，$+(\omega_*)=\omega_*$，以及 $-(\omega_*)=\overline{\omega_*}$。

在這 2^n 組 a_j 中，若固定某一組 $a_1',a_2',\cdots,a_n'$ ，那麼必會有另一組 b_j，使得

$$b_j=\begin{cases}+, & \text{若 } a_j'=-\\ -, & \text{若 } a_j'=+\end{cases}$$

而其相對應的方程式，以及該方程式的一個不可約解分別為

$$x^2-ky^2=A_{1b_1}^2(\omega,\omega_1)A_{2b_2}^2(\omega,\omega_2)\dots A_{nb_n}^2(\omega,\omega_n)$$

$$b_n(b_{n-1}(b_{n-2}(\cdots b_2(b_1(\omega,\omega_1),\omega_2)\cdots,\omega_{n-2}),\omega_{n-1}),\omega_n)=\frac{\omega\cdot\prod_{i=1}^n b_i(\omega_i)}{\prod_{i=1}^n A_{ib_i}(\omega,\omega_i)}$$

要注意的是，對於任意的 $i\in\{1,2,\cdots,n\}$，會有

$$A_{ib_i}(\omega,\omega_i)\cdot A_{ia_i'}(\omega,\omega_i)=A_i \text{ 以及 } b_i(\omega_i)\cdot a_i'(\omega_i)=A_i$$

根據上面兩式，當我們將與 b_i 和 a_i' 相對應的不可約解相乘時，會得到

$$\begin{aligned}\frac{\omega\cdot\prod_{i=1}^n b_i(\omega_i)}{\prod_{i=1}^n A_{ib_i}(\omega,\omega_i)}\cdot\frac{\omega\cdot\prod_{i=1}^n a_i'(\omega_i)}{\prod_{i=1}^n A_{ia_i'}(\omega,\omega_i)} &=\omega^2\cdot\frac{\prod_{i=1}^n(b_i(\omega_i)\cdot a_i'(\omega_i))}{\prod_{i=1}^n(A_{ib_i}(\omega,\omega_i)\cdot A_{ia_i'}(\omega,\omega_i))}\\ &=\omega^2\cdot\frac{\prod_{i=1}^n A_i}{\prod_{i=1}^n A_i}\\ &=\omega^2\end{aligned}$$

由於 $\frac{\omega\cdot\prod_{i=1}^n b_i(\omega_i)}{\prod_{i=1}^n A_{ib_i}(\omega,\omega_i)}$ 以及 $\frac{\omega\cdot\prod_{i=1}^n a_i'(\omega_i)}{\prod_{i=1}^n A_{ia_i'}(\omega,\omega_i)}$ 分別是方程式

$$x^2-ky^2=\left(A_{1b_1}(\omega,\omega_1)A_{2b_2}(\omega,\omega_2)\cdots A_{nb_n}(\omega,\omega_n)\right)^2$$

以及

$$x^2-ky^2=\left(A_{1a_1'}(\omega,\omega_1)A_{2a_2'}(\omega,\omega_2)\cdots A_{na_n'}(\omega,\omega_n)\right)^2$$

的不可約解，現在根據【**備註 3.2.3**】的表格，我們可以對這兩個解做以下的分解：

【**情況一**】當 $k \equiv 1 \bmod 4$

在這個情況下，$\frac{\omega \cdot \prod_{i=1}^{n} b_i(\omega_i)}{\prod_{i=1}^{n} A_{ib_i}(\omega,\omega_i)}$ 和 $\frac{\omega \cdot \prod_{i=1}^{n} a_i'(\omega_i)}{\prod_{i=1}^{n} A_{ia_i'}(\omega,\omega_i)}$ 可分別表示為 λ_b^2 以及 $\lambda_{a'}^2$，

其中 λ_b 和 λ_a, 分別為方程式

$$x^2 - ky^2 = A_{1b_1}(\omega,\omega_1)A_{2b_2}(\omega,\omega_2)\cdots A_{nb_n}(\omega,\omega_n)$$

以及

$$x^2 - ky^2 = A_{1a_1'}(\omega,\omega_1)A_{2a_2'}(\omega,\omega_2)\cdots A_{na_n'}(\omega,\omega_n)$$

的兩根。綜合以上的討論，我們得到

$$\omega^2 = \frac{\omega \cdot \prod_{i=1}^{n} b_i(\omega_i)}{\prod_{i=1}^{n} A_{ib_i}(\omega,\omega_i)} \cdot \frac{\omega \cdot \prod_{i=1}^{n} a_i'(\omega_i)}{\prod_{i=1}^{n} A_{ia_i'}(\omega,\omega_i)} = \lambda_b^2 \cdot \lambda_{a'}^2 = (\lambda_b \lambda_{a'})^2$$

因此

$$\omega = \lambda_b \lambda_{a'} \text{ 或 } -\lambda_b \lambda_{a'} = \sqrt{\sigma}\lambda_b \cdot \overline{\sqrt{\sigma}}\lambda_{a'}$$

【**情況二**】$k \equiv 3 \bmod 4$

根據表格，我們必須先要了解 $\frac{\omega \cdot \prod_{i=1}^{n} b_i(\omega_i)}{\prod_{i=1}^{n} A_{ib_i}(\omega,\omega_i)}$ 和 $\frac{\omega \cdot \prod_{i=1}^{n} a_i'(\omega_i)}{\prod_{i=1}^{n} A_{ia_i'}(\omega,\omega_i)}$ 兩者 y 座標的奇偶性。我們令 $\omega = u + \sqrt{k}v$ ； $\prod_{i=1}^{n} b_i(\omega_i) = \alpha + \sqrt{k}\beta$ ，根據前述之 $b_i(\omega_i) = \overline{a_i'(\omega_i)}$ 結果，我們會有 $\prod_{i=1}^{n} a_i'(\omega_i) = \overline{\prod_{i=1}^{n} b_i(\omega_i)} = \alpha - \sqrt{k}\beta$ 。因此，我們會有

$$\frac{\omega \cdot \prod_{i=1}^{n} b_i(\omega_i)}{\prod_{i=1}^{n} A_{ib_i}(\omega,\omega_i)} = \frac{(u+\sqrt{k}v)\cdot(\alpha+\sqrt{k}\beta)}{\prod_{i=1}^{n} A_{ib_i}(\omega,\omega_i)}$$

$$= \frac{u\alpha + kv\beta}{\prod_{i=1}^{n} A_{ib_i}(\omega,\omega_i)} + \sqrt{k}\,\frac{v\alpha + u\beta}{\prod_{i=1}^{n} A_{ib_i}(\omega,\omega_i)}$$

以及

$$\frac{\omega \cdot \prod_{i=1}^{n} a_i'(\omega_i)}{\prod_{i=1}^{n} A_{ia_i'}(\omega,\omega_i)} = \frac{(u+\sqrt{k}v)\cdot(\alpha-\sqrt{k}\beta)}{\prod_{i=1}^{n} A_{ia_i'}(\omega,\omega_i)}$$

$$= \frac{u\alpha - kv\beta}{\prod_{i=1}^{n} A_{ia_i'}(\omega,\omega_i)} + \sqrt{k}\,\frac{v\alpha - u\beta}{\prod_{i=1}^{n} A_{ia_i'}(\omega,\omega_i)}$$

由於 $(v\alpha + u\beta) - (v\alpha - u\beta) = 2u\beta$ ，$v\alpha + u\beta$ 和 $v\alpha - u\beta$ 有相同的奇偶性。

又 $\prod_{i=1}^{n} A_{ib_i}(\omega,\omega_i)$ 和 $\prod_{i=1}^{n} A_{ia_i'}(\omega,\omega_i)$ 同為奇數，故我們斷言 $\frac{\omega \cdot \prod_{i=1}^{n} b_i(\omega_i)}{\prod_{i=1}^{n} A_{ib_i}(\omega,\omega_i)}$

和 $\frac{\omega\cdot\prod_{i=1}^{n}a_i'(\omega_i)}{\prod_{i=1}^{n}A_{ia_i'}(\omega,\omega_i)}$ 兩者 y 座標的奇偶性相同。因此 $\frac{\omega\cdot\prod_{i=1}^{n}b_i(\omega_i)}{\prod_{i=1}^{n}A_{ib_i}(\omega,\omega_i)}$ 和 $\frac{\omega\cdot\prod_{i=1}^{n}a_i'(\omega_i)}{\prod_{i=1}^{n}A_{ia_i'}(\omega,\omega_i)}$ 可分別表示為 λ_b^2 以及 $\lambda_{a'}^2$或 $\sigma\lambda_b^2$ 以及 $\sigma\lambda_{a'}^2$，也因此

$$\omega^2=\frac{\omega\cdot\prod_{i=1}^{n}b_i(\omega_i)}{\prod_{i=1}^{n}A_{ib_i}(\omega,\omega_i)}\cdot\frac{\omega\cdot\prod_{i=1}^{n}a_i'(\omega_i)}{\prod_{i=1}^{n}A_{ia_i'}(\omega,\omega_i)}$$

$$=\begin{cases}\lambda_b^2\cdot\lambda_{a'}^2=(\lambda_b\lambda_{a'})^2(y\text{ 座標為偶數})\\ \sigma\lambda_b^2\cdot\sigma\lambda_{a'}^2=(\sigma\lambda_b\lambda_{a'})^2(y\text{ 座標為奇數})\end{cases}$$

故最後可以得到

$$\omega=\pm\lambda_b\lambda_{a'}\text{ 或 }\omega=\pm\sigma\lambda_b\lambda_{a'}$$

故得證。■

【備註 3.2.4】

我們現針對以上的推導作一討論：

1. **【定理 3.2.3】**說明了雖然 $x^2-ky^2=A_i$ 都有不可約解 ω_i，也對於 ω 的分解，一定會有『貢獻』，但不一定有『充分的貢獻』，而這『貢獻』可以用 $A_{i\pm}(\omega,\omega_i)$ 來作一衡量。
2. **【定理 3.2.3】**的證明是逐次利用 ω_i 來對 ω 來進行分解，期間還證明了分解的次序並不會影響結果，即 $\alpha\big(\beta(\omega,\omega_i),\omega_j\big)=\beta\big(\alpha\big(\omega,\omega_j\big),\omega_i\big)$，其中 $\alpha,\beta\in\{+,-\}$。事實上，後來我們發現如果直接用 $\widetilde{\omega_1}\cdot\widetilde{\omega_2}\cdot\cdots\cdot\widetilde{\omega_n}$ 對 ω 來進行分解(其中 $\widetilde{\omega_i}\in\{\omega_i,\overline{\omega_i}\}$)，也會得到同樣的結果；另外，從直接用 $\widetilde{\omega_1}\cdot\widetilde{\omega_2}\cdot\cdots\cdot\widetilde{\omega_n}$ 對 ω 來進行分解的角度來看，$\alpha\big(\beta(\omega,\omega_i),\omega_j\big)=\beta\big(\alpha\big(\omega,\omega_j\big),\omega_i\big)$ 便不證自明。而在**【定理 3.2.3】**會想到逐次利用 ω_i 來對 ω 來進行分解，乃是受到唯一分解性質的證明所發想，也就是在唯一分解性質的證明中，每個質因數逐項逐次去進行分解，而該分解並不會與分解的次序有關這些步驟，就被我們直接引用到**【定理 3.2.3】**的證明中。
3. 我們從唯一分解性質來看**【定理 3.2.3】**；為了方便說明起見，我們先假設 $A_i=p_i^{n_i}$ 是一奇質數的冪次，其中 $i=1,2,3$。再依據**【定理 3.2.3】**的設定，我們假設 ω_i 是 $x^2-ky^2=A_i$ 的一個不可約解，另外設 $\omega=\omega_1\omega_2\omega_3$ 是 $x^2-ky^2=A_1A_2A_3$ 的一個不可約解。我們依序

將 ω_1、ω_2、ω_3 作用到 ω上，並將其分解逐步記錄下來（見**七、附錄**）。從表格中可見，雖然 ω 可分解出 8 個不可約解 E_j，而且

$$\omega = \sqrt{E_j E_{8-j}}, j = 1, \cdots, 8$$

但事實上，就唯一分解性質的角度看來，$\sqrt{E_j E_{8-j}}$ 的呈現等同於將 $\omega_1\omega_2\omega_3$ 分成兩個不同的不可約解的乘積；反過來說，從**【定理 3.2.3】**的觀點來看，唯一分解性質就是在這些分解中的某一種分解，也是為『最細緻』的分解。

綜合上述的推論，我們在想**【定理 3.2.3】**的分解是否也含有可能的『唯一分解』；也就是說雖然 ω 的分解有 2^n 種可能，但是否與**【備註 3.2.4】**中的第三點類似，不同的分解僅只是呈現的方式不同，最終總是會有一個「最細緻」的分解呢？這問題可以做為我們日後討論的可能方向。

3. 佩爾質數的重新詮釋

我們在之前就曾提出佩爾質數的概念（**見參考資料【8】**），當時的定義為

我們稱一個數 A 為佩爾質數，如果 $x^2 - ky^2 = A$ 有不可約解，但 A 不能再寫成 $\alpha_1 \cdot \alpha_2 \cdot \cdots \cdot \alpha_n$ ，其中每個 $\alpha_i \neq= \pm 1$ 而且 $x^2 - ky^2 = \alpha_i$ 都有不可約解。

在當時，佩爾質數只是一個概念，除了有蜈蚣齒現象的質數冪次以外，是否還有存在其他形式的佩爾數都還不得而知；另外，在我們使用上面定義來討論佩爾質數可能的性質時，往往必須考慮 α 的所有因數，這當時在我們討論的時候著實給了不小的麻煩；然而利用**【定理 3.2.3】**的啟示，我們可以將佩爾質數的定義，給出等價的敘述，而以下就是重新給出定義的過程。

首先，對於給定的奇質數 k，我們將形如 $a + b\sqrt{k}$的數（其中 a 和 b 均為整數），均稱為<u>二次整數</u>；一個二次整數 $a + b\sqrt{k}$ 被稱為不可約，如果 a 和 b 的公因數只有 ± 1。這裡要特別說明的是，這裡所謂的二次整數的定義與數論中二次整數$(quadratic\ integer)$的定義有些許的不同，我們僅將原來的定義延伸到我們所討論的數字，以便接下來的定義，除此之外，並不會引用到任何有關二次整數$(quadratic\ integer)$的相關性質。

【定義 3.3.1】（佩爾不可約）

對於給定的奇質數 k，一個不可約的二次整數 ω 被稱為佩爾不可約 ，如果將其寫成其他兩個不可約的二次整數的乘積時，則這兩個二次整數至少有一個是 $\pm\sqrt{\sigma}^m$（其中 m 是任意整數）。

在這裡，$\sqrt{\sigma}$ 指的是方程式 $x^2-ky^2=-1$ 的第一個正整數解；而在之前的研究中有指出（**見參考資料【7】**），$x^2-ky^2=-1$ 有正整數解的充分必要條件是 $k\equiv 1 \bmod 4$。

目前，我們手邊有的佩爾不可約二次整數有

1. $\pm\sigma$、$\pm\bar{\sigma}$，其中 σ 是佩爾方程式的第一個正整數解；
2. $\pm\sqrt{\sigma}$、$\pm\overline{\sqrt{\sigma}}$，其中 $\sqrt{\sigma}$ 是廣義佩爾方程式 $x^2-ky^2=-1$ 的第一個正整數解；
3. $\pm\sqrt{2\sigma}$、$\pm\overline{\sqrt{2\sigma}}$，其中 $\sqrt{2\sigma}$ 是廣義佩爾方程式 $x^2-ky^2=\pm 2$ 的第一個正整數解；
4. $\pm\omega$、$\pm\bar{\omega}$，其中 ω 是廣義佩爾方程式 $x^2-ky^2=p^n$ 的第一個正整數解，其中 k 和 p 為兩相異的奇質數，而且 $l(k,p^n)=3$。

比如說，$2+\sqrt{3}$ 和 $9+2\sqrt{7}$ 都是佩爾不可約的二次整數；而 $9+4\sqrt{5}\left(=\left(1+\sqrt{5}\right)^2\right)$ 則不是。事實上，若 ω 是一個佩爾不可約的二次整數，那麼形如 $\sigma^m\omega$ 的二次整數都是佩爾不可約。

在上述四種型態的佩爾不可約二次整數中，前三種的共通點除了和 σ 有關外，就是與其相對應的廣義佩爾方程式長度都是 2，而第四種的佩爾不可約二次整數，方程式的長度都是 3；是否廣義佩爾方程式的長度會和佩爾不可約的二次整數有關係呢？以下是我們的發現：

【定理 3.3.1】

假設 k 是一個奇質數且 ω 為不可約的二次整數。若令 $\omega\cdot\bar{\omega}=A$ 且 $\mathrm{GCD}(k,A)=1$，則我們會有 $l(k,\omega\cdot\bar{\omega})=2 \Leftrightarrow \omega\cdot\bar{\omega}=\pm 1$ 或 ± 2

【證明】

顯然，當 $\omega\cdot\bar{\omega}=\pm 1$ 或 ± 2 時，$l(k,\omega\cdot\bar{\omega})$必定等於 2；假設 $\omega=u+v\sqrt{k}$ 且 $l(k,\omega\cdot\bar{\omega})=2$，我們就以下的兩種情況分別討論：

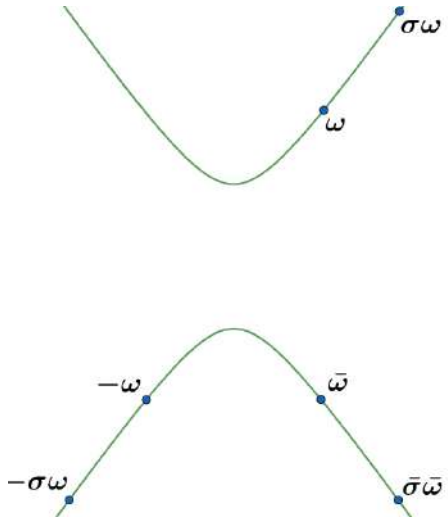
【情況一】$A>0$

在這種況下，二次曲線 $x^2-ky^2=A$ 的圖形是左右開的雙曲線，且 (u,v) 是線上一點。由於 ω 為不可約的二次整數且 $l(k,\omega\cdot\bar{\omega})$必定等於 2，$x^2-ky^2=A$ 的所有解必定都是不可約解。因此，我們不訪假設 ω 是第一個正整數解。在這樣的假設下，$\sigma\bar{\omega}$ 必定等於 ω（見圖），也因此會有

$$\sigma\bar{\omega}=\omega\Longrightarrow\sigma\cdot A=\omega^2$$

若以 $\alpha+\sqrt{k}\beta$ 表示 α，則上式可表示為 $\begin{cases}A\alpha=u^2+kv^2\\A\beta=2uv\end{cases}$。若 (A,u)，則與 ω 為不可約的二次整數互相矛盾。因此，β 必定等於 uv 或 $2uv$，而前者必推得 A 等於 2 ；後為者 1。

【情況二】$A<0$



假設 ω 是第一個在上下對開的雙曲線 $x^2-ky^2=A$ 上的正整數解，則我們會有 $-\sigma\omega<-\omega<\bar{\omega}<\bar{\sigma}\bar{\omega}$；將上式均乘以正數 $\sigma=\alpha+\sqrt{k}\beta$，則會有 $-\sigma\omega<\sigma\bar{\omega}<\bar{\omega}$；這代表 $\sigma\bar{\omega}$ 必定等於 $-\omega$（見左圖）。換句話說，也就是會得到聯立方程式 $\begin{cases}A\alpha=-(u^2+kv^2)\\A\beta=-2uv\end{cases}$。與第一種情況的判斷方式相同，$\beta$ 會等於 $2uv$ 或 uv，而 A 就會分別等於 -1 或-2。■

【備註 3.3.1】

為了方便說明起見，在【**定理 3.3.1**】中我們假設了 $\mathrm{GCD}(k,A)=1$；而事實上，如果 k 是 A 的一個質因數，則 k 亦是 u 的一個質因數。故可從方程式 $u^2-kv^2=A$ ，轉換到另一個方程式 $v^2-kU^2=A'$，其中 $u=kU$ 且 $A=kA'$。由於 ω 為不可約的二次整數，k 與 A' 一定互質；故根據【**定理 3.3.1**】的結論，A 只有可能等於 $\pm k$ 或是 $\pm 2k$。

當 $k\equiv 1 \bmod 4$ 時，$x^2-ky^2=\pm k$ 都會有解，而 $x^2-ky^2=\pm 2k$都無解；當 $k\equiv 3 \bmod 4$ 時，在 $x^2-ky^2=\pm k$ 中，只有$x^2-ky^2=-k$ 有解，其正整數解集合為$\{\sqrt{k}\cdot\sigma^n|\ n\in\mathbb{N}\}$；而對於 $x^2-ky^2=\pm 2k$，當 $k\equiv 3\ (\mathrm{mod}\ 8)$ 時，只有 $x^2-ky^2=2k$ 有解，其正整數解集合為 $\{\sqrt{k}\cdot\sqrt{2\sigma}\cdot\sigma^n|\ n\in\mathbb{N}\}$，當 $k\equiv 7\ (\mathrm{mod}\ 8)$ 時，只有 $x^2-ky^2=-2k$ 有解，其正整數解集合為

$\{\sqrt{k}\cdot\sqrt{2\sigma}\cdot\sigma^n \mid n\in\mathbb{N}\}$

接下來，我們想試著說明，若 ω 為不可約的二次整數，$l(k,\omega\bar{\omega})=3$；首先，很自然的，我們有以下結果：

【定理 3.3.2】

假設 $k>2$ 是一個質數且 ω 為佩爾不可約的二次整數，且 $\omega\cdot\bar{\omega}=A$ 是一個正奇數且 $\gcd(k,A)=1$，則對於方程式 $x^2-ky^2=A$ 任意的不可約解 ω'，我們會有 $\omega'=\sigma^m\omega$ 或是 $\omega'=\sigma^m\bar{\omega}$，其中 m 是一整數。

【證明】

我們假設 $\omega=u+\sqrt{k}v$ 且 $\omega'=s+t\sqrt{v}$，那麼我們會有

$$(ut+vs)(ut-vs)=A(t^2-v^2)$$

由於 A 是正奇數，若質數 $p>2$ 是 $\gcd(A,ut+vs,ut-vs)$ 的一個因數，那 p 也會是 ut 的因數；則無論是 p 整除 u 或者是 t 的，都將與 ω 和 ω' 不可約性矛盾；因此 $\gcd(A,ut+vs,ut-vs)=1$，也就是可將 A 表示成兩互質整數 A_+ 與 A_- 的乘積，使得 A_+ 和 A_- 分別為 $ut+vs$ 與 $ut-vs$ 的因數。特別要注意的是 $\frac{\omega\omega'}{A_+}$ 與 $\frac{\omega\overline{\omega'}}{A_-}$ 分別為方程式 $x^2-ky^2=A_-^2$ 與 $x^2-ky^2=A_+^2$ 的不可約解。利用**【定理 3.2.1】**的結論，我們有以下的結果：

當 $k\equiv 1 \bmod 4$ 時，$\frac{\omega\omega'}{A_+}=\lambda_1^2$ 以及 $\frac{\omega\overline{\omega'}}{A_-}=\lambda_2^2$，也因此會有

$$\omega^2=\left(\frac{\omega\omega'}{A_+}\right)\left(\frac{\omega\overline{\omega'}}{A_-}\right)=\lambda_1^2\lambda_2^2$$

這表示 $\omega=\pm\lambda_1\lambda_2$；又 ω 為佩爾不可約，會有 $\frac{\omega\omega'}{A_+}=\sigma^m$ 或 $\frac{\omega\overline{\omega'}}{A_-}=\sigma^m$。無論是哪一種情況都會有

$$\frac{\omega\omega'}{A_+}=\sigma^m \implies \omega\omega'=\sigma^m A=\sigma^m\omega\bar{\omega} \implies \omega'=\sigma^m\bar{\omega}$$

或是

$$\frac{\omega\overline{\omega'}}{A_-}=\sigma^m \implies \omega\overline{\omega'}=\sigma^m A=\sigma^m\omega\bar{\omega} \implies \omega'=\sigma^m\omega$$

當 $k\equiv 3 \bmod 4$ 時，根據**【備註 3.2.3】**中的表格，我們必須確認 $\omega\omega'$ 和 $\omega\overline{\omega'}$ y 座標的奇

偶性。由於 $ut+vs \equiv ut-vs \bmod 2$，$\frac{\omega\omega'}{A_+}$ 與 $\frac{\omega\overline{\omega'}}{A_-}$ 的奇偶性也一致，這表示

$$\frac{\omega\omega'}{A_+}=\lambda_1^2 \ 、\ \frac{\omega\overline{\omega'}}{A_-}=\lambda_2^2 \implies \omega^2=\lambda_1^2\lambda_2^2 \implies \omega=\pm\lambda_1\lambda_2$$

或是

$$\frac{\omega\omega'}{A_+}=\sigma\lambda_1^2 \ 、\ \frac{\omega\overline{\omega'}}{A_-}=\sigma\lambda_2^2 \Longrightarrow \omega^2=\sigma^2\lambda_1^2\lambda_2^2 \implies \omega=\pm\sigma\lambda_1\lambda_2$$

再次利用佩爾不可約的定義，以及仿效上述當 $k \equiv 1 \bmod 4$ 時的作法，也可以得到相同的結論；故得證。■

【備註 3.3.2】

【定理 3.3.2】說明了當一個佩爾不可約的二次整數在一條雙曲線 Γ 上的時候，所有的不可約解都是佩爾不可約。然而，很遺憾的我們並未得出想要的結論，也就是在**【定理 3.3.2】**的條件下，$l(k,A)$ 的值是否就是 3。事實上，**【定理 3.3.2】**只證明了在 Γ 上的不可約解只有兩類，就是 $[\omega]$ 和 $[\bar{\omega}]$；但是否有更多的可約解，則尚未知曉；這亦作為日後可以討論的方向。

回到佩爾質數的原始定義，假設一個正奇數 A 是一個佩爾質數，而且 ω 是其一個不可約解。倘若 ω 並非佩爾不可約，則 ω 可表示為兩個不可約解的乘積 $\lambda_1\lambda_2$，且 $\lambda_1\overline{\lambda_1}$、$\lambda_2\overline{\lambda_2} \neq \pm1 \vee \pm2$。但是 $A=\omega\bar{\omega}=\lambda_1\overline{\lambda_1}\cdot\lambda_2\overline{\lambda_2}$，這矛盾於 A 是一個佩爾質數；因此 ω 是佩爾不可約。反過來說，若 ω 是佩爾不可約且滿足**【定理 3.3.2】**中的前提假設，可是 $A=\omega\bar{\omega}$ 並非一個佩爾質數，那麼 A 可以寫成 $\alpha_1\cdot\alpha_2\cdot\cdots\cdot\alpha_n$ ，其中每個 $\alpha_i \neq \pm1 \vee \pm2$ 而且 $x^2-ky^2=\alpha_i$ 都有不可約解。根據

【定理 3.2.3】的結論，ω 可以看成數個不可約解的乘積，這也矛盾於 ω 是佩爾不可約的前提假設。

以上的說明，重新詮釋了佩爾質數的定義，而這個定義只需要我們著眼於其不可約解是否有第二種分解型態，免去了一開始我們對原來定義，在討論上的拙劣與可能的不足。故在此，我們重新給出佩爾質數以下的定義：

【定義 3.3.2】（佩爾質數）

假設 k 是一個奇質數且 ω 為佩爾不可約的二次整數，若 $\omega \cdot \bar{\omega} = A$ 是一個正奇數，則 A 稱為一個佩爾質數。

在之前的研究中，佩爾質數只是一個概念，是否有存在有別於上述佩爾不可約的佩爾質數，當時還是一個問題。幾經嘗試，我們總算從蜈蚣彘中『提煉』出了佩爾質數。而產生佩爾質數的方式很簡單，假設奇質數均有蜈蚣彘現象，那麼有可能就是一個佩爾質數；以下就是我們蒐集到，由蜈蚣彘生成出來的佩爾質數：

【例子 3.3.1】（佩爾質數）

首先是第一個例子，$k = 79$ 且 $p = 5$、13 以及 101。在這個情況底下，質數 p 有 79 −蜈蚣彘現象，而且最低次方解均為 3。在下表中表示，當 $p = 5, 13$ 以及 101 時，這三數兩兩相乘的結果，均會是一個佩爾質數。（見右表）

79	5	13	101
5		65	505
13			1313
101			

401	5	7	11	29	41	43	47
5				145	205		235
7			77			301	
11						473	
29					1189		1363
41							1927
43							

接著是 $k = 401$ 且 $p = 5$、7、11、29、41、43 以及 47。這些質數均有 401 −蜈蚣彘現象，最低次方解為 5。與上面的例子不同，任意兩個質數相乘不一定會有解；在右表中顯示，若將這些質數分成 $p = 5$、29、41、47 以及 $p = 7$、11、43 這兩群，則這兩群內的任意相異質數相乘，都會是佩爾質數；但是從這兩群中任意挑選一個質數相乘，得到的卻是一個無解的廣義佩爾方程式。

隨著佩爾質數的出現，一個困擾著我們許久的問題便解決了。對於兩個相異的廣義佩爾方程式 $x^2 - ky^2 = A$ 以及 $x^2 - ky^2 = B$，是否這兩個方程式的可解性，會連動到方程式 $x^2 - ky^2 = AB$ 的可解性呢？我們利用下表來說明彼此之間的關係：

A	B	AB	說明或例子
有解	有解	有解	見參考資料【5】【定理 3.2】
有解	無解	有解	$x^2-79y^2=65$ 有解 $x^2-79y^2=101$ 無解，$x^2-79y^2=65\cdot 101$ 有解
		無解	$x^2-5y^2=11$ 有解而 $x^2-5y^2=2$ 無解，但 $x^2-5y^2=11\cdot 2$ 無解
無解	無解	有解	$x^2-79y^2=101$，$x^2-79y^2=5$ 皆無解，但 $x^2-79y^2=505$ 有解
		無解	$x^2-401y^2=5$ 、$x^2-401y^2=7$ 以及 $x^2-401y^2=5\cdot 7$ 均無解

值得注意的是，在 $k=79$ 和 401時，我們取的都是在**【例子 3.3.1】**的方程式，其中 65、$65\cdot 101$ 以及 505 都是佩爾質數。

目前，我們能產生的佩爾質數都是來自於蜈蚣彘，是否還有其他於蜈蚣彘無關的廣義佩爾質數依然是不得而知。另外，從**【例子 3.3.1】**我們發現，並非所有的蜈蚣彘現象的質數相乘，就可以得到佩爾質數；再者，將相乘可得佩爾質數的這數集合起來，似乎有一定的封閉性。因此，接下來我們就從這裡開始對佩爾質數的研究。

4. 產生新的佩爾質數

為了說明方便，以下我們固定一個奇質數 k，且規定任意不同的奇質數 p、q 以及 r ，皆與 k相異。另外，為了敘述簡潔，對於一個正整數 A，我們會說方程式 A 有解的意思，是指方程式 $x^2-ky^2=A$ 有不可約解。延續前面對佩爾質數的討論，我們先給出以下引理：

【引理 3.4.1】

設 p 和 q 為相異奇質數，若在 p、q 以及 pq 中任意兩者有解，那麼第三者也會有解。（若改成 $-p$ 和 $-q$，結論同樣成立）

【證明】

我們只須證明當方程式 p 以及 pq 有解時，q 也會有解。假設 $\omega_p=u_p+\sqrt{k}v_p$ 以及$\omega_{pq}=u_{pq}+\sqrt{k}v_{pq}$分別為方程式 p 和 pq 的一個不可約解。則有

$$(u_{pq}v_p+u_pv_{pq})(u_{pq}v_p-u_pv_{pq})=p(qv_p^2-v_{pq}^2)$$

p 必整除 $u_{pq}v_p \pm u_p v_{pq}$ 其中一者，也因此 $\frac{\omega_{pq}\omega_p}{p}$ 和 $\frac{\omega_{pq}\overline{\omega_p}}{p}$ 必有一個是 $x^2 - ky^2 = q$ 的不可約解。故得證。■

【備註 3.4.2】

在**【引理 3.4.1】**中 p 和 q 為相異質數的限制是必須的，例如方程式 $x^2 - 79y^2 = 65$ 與 $x^2 - 79y^2 = 65 \cdot 101$ 都有解，但是 $x^2 - 79y^2 = 101$無解。

利用**【引理 3.4.1】**，我們可以得到以下**【定理 3.4.1】**的結論：

【定理 3.4.1】

假設 pq 與 qr 皆為佩爾質數，則 pr 亦為佩爾質數。

【證明】

假設 $\omega_{pq} = u_{pq} + \sqrt{k}v_{pq}$ 和 $\omega_{qr} = u_{qr} + \sqrt{k}v_{qr}$ 分別是 $x^2 - ky^2 = pq$ 和 $x^2 - ky^2 = qr$ 的不可解。由於

$$(u_{pq}v_{qr} + u_{qr}v_{pq})(u_{pq}v_{qr} - u_{qr}v_{pq}) = q(v_{qr}^2 - v_{pq}^2)$$

q 必整除 $u_{pq}v_{qr} \pm u_{qr}v_{pq}$ 其中一者，也因此 $\frac{\omega_{pq}\omega_{qr}}{q}$ 和 $\frac{\omega_{pq}\overline{\omega_{qr}}}{q}$ 必有一個是 $x^2 - ky^2 = pr$ 的不可約解。若 pr 不是佩爾質數，那麼存在一個方程式 pr 的解 ω，使得 ω 可以寫成方程式 $\pm p$ 和 $\pm r$ 的解的乘積；那麼根據**【引理 3.4.1】**的結果，方程式 $\pm q$ 也會有解，但這會和 pq 是佩爾質數的假設矛盾；因此 pr 是一個佩爾質數。故得證。■

【備註 3.4.2】

【定理 3.4.1】徹底反應了**【例子 3.3.1】**中的第二個現象，說明如下：若我們給定一個奇質數 $p \neq k$，其中該質數所對應的方程式 $\pm p$ 均無解。我們定義

$$\Omega_p = \left\{ r\text{是一個質數} \mid r = p \text{ 或 } pr \text{ 是一個佩爾質數} \right\}$$

那麼根據【**定理 3.4.1**】，在 Ω_p 內的任兩個相異的質數相乘，都會是一個佩爾質數；此外，對於任意的兩個異於 k 的奇質數 p 與 q 且方程式 $\pm p$ 和 $\pm q$ 均無解，那麼 $\Omega_p \cap \Omega_q \neq \phi$ 或是 $\Omega_p = \Omega_q$。這便說明了在【**例子 3.3.1**】中的第二個現象中，$\Omega_5 = \Omega_{29} = \Omega_{41} = \Omega_{47}$ 以及 $\Omega_7 = \Omega_{11} = \Omega_{43}$ ，而且這兩個集合並不會有交集。

我們想利用 Ω_p 產生新的佩爾質數，其中任取三個質數相乘就是其中一個想法。會這樣構思是因為在前面的一段例證中，我們發現了$x^2 - 79y^2 = 5 \cdot 13 \cdot 101$ 是有解的廣義佩爾方程式，而且 5 、13 、101 都是 Ω_5 中的元素。很直接的聯想到，在集合 Ω_p 中的元素是否任取三個質數相乘，都會是新的佩爾質數呢？

這答案是否定的，一個最直接的反例便是方程式 $x^2 - 401y^2 = 7 \cdot 11 \cdot 43$ 無解，但 7 、11 、43 都是 Ω_7 中的元素。然而，在集合 Ω_p 中如何取三個質數相乘後會產生新的佩爾質數，我們迄今尚未有一個定論。不過很顯然的，若 p_1 、p_2 、p_3 都是 Ω_p 中的相異元素，且使得方程式 $p_1p_2p_3$ 有解，那麼 $p_1p_2p_3$ 一定是一個佩爾質數，而且

$$l(k, p_1p_2p_3) = 3$$

事實上，上述的現象與蜈蚣質有極大的關係：

【定理 3.4.2】

若對於任意的 $p_1, p_2, p_3 \in \Omega_p$ ， $l(k, p_1p_2p_3) > 0$，則 $l(k, p_i^3) = 3$。

【證明】

設 ω_{12} 和 ω_{123} 分別為 $x^2 - ky^2 = p_1p_2$ 與 $x^2 - ky^2 = p_1p_2p_3$ 的不可約解，則必存在一個正整數 A 使得 $\frac{\omega_{12}\omega_{123}}{A}$ 是 $x^2 - ky^2 = \frac{p_1^2p_2^2p_3}{A}$ 的一個整數解，其中 $A = 1$ 、p_1 、p_2 或 p_1p_2。若 $A = 1$ 或 p_1p_2，則 $\frac{\omega_{12}\overline{\omega_{123}}}{p_1p_2}$ 或 $\frac{\omega_{12}\omega_{123}}{p_1p_2}$ 會是 $x^2 - ky^2 = p_3$ 的一個解，這與該方程式無解相互矛盾。因此 $x^2 - ky^2 = p_1^2p_3$ 與 $x^2 - ky^2 = p_2^2p_3$ 均有不可約解。

但以第一個方程式來說，若 ω 是其一不可解，那麼與前面論述相同， $\frac{\omega_{13}\overline{\omega}}{p_3}$ 或 $\frac{\omega_{13}\omega}{p_3}$

必是 $x^2-ky^2=p_1^3$ 的一個解；又 $x^2-ky^2=p_1$ 無解，因此$x^2-ky^2=p_1^3$ 必是一個蜈蚣堯。故得證。■

另外，我們還發現了另一個相當有趣的現象；雖然在 $k=401$ 的情況下，我們有這 Ω_5 和 Ω_7 這兩個集合（可能還有更多），而且無論在這兩個集合中的那一個，於其中任取三個質數相乘都是無解的。但是隨意在 Ω_5 或 Ω_7 挑選兩個質數，並且在另一者中挑選一個質數，三者相乘後的方程式都會有解（也因此是佩爾質數）。比如說 $x^2-401y^2=(7\cdot 11)\cdot 5$ 以及 $x^2-401y^2=(5\cdot 29)\cdot 7$ 都會有解。我們就現有的兩個同類項進行計算，發現當 p_j 和 p_k 都在同一個等價類時，$p_ip_jp_k$ 都是一個佩爾質數。下表列出佩爾方程式 $x^2-401y^2=p_i\cdot(p_j\times p_k)$ 的一個不可約解 $u+v\sqrt{k}$：

	5	u	v	29	u	v	41	u	v	47	u	v
7×11	385	321	16	2233	93	4	3157	69	2	3619	190	9
7×43	1505	89	4	8729	1285	64	12341	229	10	14147	2066	103
11×43	2365	63	2	13717	379	18	19393	2487	124	22231	300	13

$p_i\in\Omega_5;\ p_j,p_k\in\Omega_7$

	7	u	v	11	u	v	43	u	v
5×29	1015	68	3	1595	742	37	6235	234	11
5×41	1435	542	27	2255	148	7	8815	96	1
5×47	1645	57	2	2585	563	28	10105	491	24
29×41	8323	202	9	13079	152	5	51127	1876	93
29×47	9541	1565	78	14993	343	16	58609	255	4
41×47	13489	417	20	21197	151	2	82861	1431	70

$p_i\in\Omega_7;\ p_j,p_k\in\Omega_5$

表格中灰底的數字都是佩爾質數；我們想問在 [7] 和 [5] 若還有其他的元素，是否用同樣方法創造出來的數字依然是佩爾質數？答案是肯定的：

【定理 3.4.3】

設 $a_i\in\Omega_{p_i}$，其中 $i=1,2,3$。若 $a_1a_2a_3$ 是一個佩爾質數，則對於任意的 $p\in\Omega_{p_i}$，pa_2a_3 也是一個佩爾質數。

【證明】

設 $\omega_{123}=u_{123}+v_{123}\sqrt{k}$ 是 $x^2-ky^2=a_1a_2a_3$ 的一個解，且 $\omega_p=u_p+v_p\sqrt{k}$ 是 $x^2-ky^2=pa_1$ 的一個解。同樣的，我們考慮

$$(u_{123}v_p-u_pv_{123})(u_{123}v_p+u_pv_{123})=a_1(a_2a_3v_p^2-pv_{123}^2)$$

那麼 $\frac{\omega_{123}\omega_p}{a_1}$ 與 $\frac{\omega_{123}\overline{\omega_p}}{a_1}$ 之中，一定有一個是 $x^2-ky^2=pa_2a_3$ 不可約解。故得證。■

到目前為止，我們都在利用集合 Ω_p 中的元素去創造新的佩爾質數。而且目前只能從蜈蚣彘去產生佩爾質數，但是佩爾質數與蜈蚣彘是否有一定的關聯性，我們仍無法確實掌握。然而，是【**定理 3.4.2**】我們目前唯一可以掌握到兩者有關聯的可能；事實上，從過去我們就對蜈蚣彘有了以下的猜想

〔**猜想一**〕對於任意給定的奇質數，有蜈蚣彘現象的質數有無窮多個。

〔**猜想二**〕蜈蚣彘的「最低次方解」都會是質數。

而藉由這次的討論，我們猜測

〔**猜想三**〕對於一個給定的奇質數 $\boldsymbol{k}$，若相異的兩質數 $\boldsymbol{p_1}$ 與 $\boldsymbol{p_2}$ 均有 $\boldsymbol{k}$ −蜈蚣彘現象（假設最低次方解分別為 $\boldsymbol{n_1}$ 和 $\boldsymbol{n_2}$），則存在 $\boldsymbol{1\le\alpha<n_1}$ 以及 $\boldsymbol{1\le\beta<n_2}$，使得是 $\boldsymbol{p_1^{\alpha}p_2^{\beta}}$ 佩爾質數。

然而，我們最一開始的討論，並非是前面的討論，而是我們想知道若對於正整數 $i=1,\cdots,2j$，若都有 $p_i\in\Omega_p$，則方程式 $x^2-ky^2=p_1p_2p_3p_4\cdots p_{2j}$ 其解的長度是多少。而想要瞭解這類方程式解的長度，主要是想探測是否將唯一分解性質中的質數改成佩爾質數時，也會有相同的情況。想法是，如果我們將第一段中的解用一些固定的佩爾質數來產生，並去計算在第一段中的數量，然後與去解的長度去作比較，這樣就可以知道是否有重複的情況發生，進而可以得知是否有唯一分解的情況。

我們從以下的【**定理 3.4.4**】開始：

【**定理 3.4.4**】

假設對於任意的 $i,j=1,\cdots,4,$ 皆有 $p_i\in\Omega_p$，則 $x^2-ky^2=p_1p_2p_3p_4$ 的不可約解均由方程式

$x^2 - ky^2 = p_i p_j$ 的不可約解所生成。

【證明】

假設 ω 、ω_{12} 和 ω_{34} 分別是 $x^2 - ky^2 = p_1p_2p_3p_3$ 、p_1p_2 和 p_3p_4 的不可約解，則可從 $\omega\omega_{12}\omega_{34}$ 以及 $\omega\overline{\omega_{12}\omega_{34}}$ 得到一些佩爾方程式的不可約解（以下表格）

不可約解 \ A	1	p_i	p_ip_j	$p_ip_jp_k$	$p_ip_jp_kp_l$
$\frac{\omega\omega_{12}\omega_{34}}{A}$	$(p_1p_2p_3p_4)^2$	$(p_jp_kp_l)^2$	$p_k^2p_l^2$	p_l^2	1
$\frac{A\omega\overline{\omega_{12}\omega_{34}}}{p_1p_2p_3p_4}$	1	p_i^2	$p_i^2p_j^2$	$(p_ip_jp_k)^2$	$(p_1p_2p_3p_4)^2$

由於對稱性的關係，我們會分別討論前三情況：

【情況一】$A = 1$

在這個情況下，$\frac{\omega\overline{\omega_{12}\omega_{34}}}{p_1p_2p_3p_4}$ 等同於 σ^*，也因此會有

$$\omega\overline{\omega_{12}\omega_{34}} = \sigma^* p_1p_2p_3p_4 = \sigma^*\omega_{12}\omega_{34}\cdot\overline{\omega_{12}\omega_{34}} \Rightarrow \omega = \sigma^*\omega_{12}\omega_{34}$$

因此，ω 可由 ω_{12} 和 ω_{34} 所生成。

【情況二】$A = p_i$

在這個情況下，$x^2 - ky^2 = p_i^2$ 會有一個不可約解 $\frac{\omega\overline{\omega_{12}\omega_{34}}}{p_jp_kp_l}$ ；然而根據之前的定理，方程式$x^2 - ky^2 = p_i$ 或 $x^2 - ky^2 = -p_i$ 至少會有一個不可約解。若是 $x^2 - ky^2 = \pm p_i$ 有不可解，則因為 $p_i \sim p_j$，對於任意的 $n = 1,\cdots,4$，$x^2 - ky^2 = \pm p_n$ 都會有不可約解；這與 p_ip_j 是佩爾質數矛盾。

【情況三】$A = p_ip_j$

假設 $\frac{\omega\omega_{12}\omega_{34}}{p_ip_j}$ 以及 $\frac{\omega\overline{\omega_{12}\omega_{34}}}{p_kp_l}$ 分別是 $x^2 - ky^2 = p_k^2p_l^2$ 和 $x^2 - ky^2 = p_k^2p_l^2$ 的一個解。由於 $\omega\omega_{12}\omega_{34}$ 和 $\omega\overline{\omega_{12}\omega_{34}}$ 的 y 座標有相同的奇偶性，根據**【備註 3.2.3】**中的表格，分別會存在一個 $x^2 - ky^2 = p_kp_l$ 和 $x^2 - ky^2 = p_ip_j$ 的不可約 $\widetilde{\omega_{kl}}$ 以及 $\widetilde{\omega_{ij}}$，使得

$$\omega = \frac{p_ip_j\widetilde{\omega_{kl}}^2}{\omega_{12}\omega_{34}} = \frac{p_kp_l\widetilde{\omega_{ij}}^2}{\overline{\omega_{12}\omega_{34}}} \text{ 或 } \omega = \sigma\cdot\frac{p_ip_j\widetilde{\omega_{kl}}^2}{\omega_{12}\omega_{34}} = \sigma\cdot\frac{p_kp_l\widetilde{\omega_{ij}}^2}{\overline{\omega_{12}\omega_{34}}}$$

因此

$$\omega^2 = \frac{p_i p_j \widetilde{\omega_{kl}}^2}{\omega_{12}\omega_{34}} \cdot \frac{p_k p_l \widetilde{\omega_{lJ}}^2}{\overline{\omega_{12}\omega_{34}}} = \widetilde{\omega_{lJ}}^2 \widetilde{\omega_{kl}}^2$$

或

$$\omega^2 = \left(\sigma \cdot \frac{p_i p_j \widetilde{\omega_{kl}}^2}{\omega_{12}\omega_{34}}\right) \cdot \left(\sigma \cdot \frac{p_k p_l \widetilde{\omega_{lJ}}^2}{\overline{\omega_{12}\omega_{34}}}\right) = \sigma^2 \cdot \widetilde{\omega_{lJ}}^2 \widetilde{\omega_{kl}}^2$$

這會表示 $\omega = \pm\widetilde{\omega_{lJ}}\widetilde{\omega_{kl}}$ 或 $\pm\sigma\widetilde{\omega_{lJ}}\widetilde{\omega_{kl}}$ 或；故得證■。

為了方便接下來以及下一章的討論，我們需要以下的定義：

【定義 3.4.1】$L(A,B)$

假設 A 和 B 是兩個正整數，我們定義

1. 假設 λ_1 是 $x^2 - Ay^2 = B$ 的一個不可約解，且 $\lambda_1 < \lambda_2 < \cdots < \lambda_n < \lambda_{n+1} = \sigma\lambda_1$ 依序為該方程式的不可約解，則我們定義

$$L_{irr}(A,B) \coloneqq \begin{cases} n\,, & \text{方程式有不可約解} \\ 0\,, & \text{方程式無可約解} \end{cases}$$

2. 同樣的，若將在 1.中的 λ 不可約解改成可約解，我們同樣可以定義

$$L_{re}(A,B) \coloneqq \begin{cases} n\,, & \text{方程式有可約解} \\ 0\,, & \text{方程式無可約解} \end{cases}$$

3. 承上，我們定義 $L(A,B)$

$$L(A,B) \coloneqq L_{irr}(A,B) + L_{re}(A,B)$$

在過去，學長姐一開始對解的長度的了解 $l(A,B)$，是從任一個解 ω 到 $\sigma\omega$，統計總共有幾個解。但是事實上，由於 ω 和 $\sigma\omega$可以看成同一類，也因此長度應該是 $l(A,B)-1$，也因此等同於 $L(A,B)$；而由於之後不可約解與可約解的產生，$L_{irr}(A,B)$ 和 $L_{re}(A,B)$ 也很自然的定義產生。另外，$L(A,B)$ 的定義會讓在唯一分解定理中，解的長度公式：

$$l\left(k, \prod_{i=1}^{j} p_i^{n_i}\right) = \prod_{i=1}^{j} \left(l\left(k, p_i^{n_i}\right) - 1\right) + 1$$

有著更加簡約的呈現：

$$L\left(k,\prod_{i=1}^{j}p_i^{n_i}\right)=\prod_{i=1}^{j}L\left(k,p_i^{n_i}\right)$$

接著，我們就接著下面的備註開始：

【備註 3.4.3】（佩爾質數並無唯一分解性質）

從上述定理得知方程式 $x^2-ky^2=p_1p_2p_3p_4$ 的解，均從 $x^2-ky^2=p_ip_j$ 所生成，這樣的解共計有 $3\times4=12$ 個組合。也因此，我們會有

$$\boldsymbol{L(k,p_1p_2p_3p_4)=L_{irr}(k,p_1p_2p_3p_4)\leq12}$$

然而，這並非是最好的估計；以 $k=37$ 為例，當 $p=3$、11、41、47 時，方程式 $x^2-ky^2=p$ 均為蜈蚣彘且最小整數解均為 3。現令 $p_1=3$、$p_2=11$、$p_3=41$、$p_4=47$，則 $x^2-ky^2=p_ip_j$ 均為佩爾質數，而根據電腦計算，我們得到 $\boldsymbol{L_{irr}(37,p_1p_2p_3p_4)=L_{irr}(37,63591)=6<12}$。這代表在 12 個組合中，兩兩重複的個數占了一半。

再繼續深究 $\boldsymbol{L_{irr}(k,p_1p_2p_3p_4)}$ 這個問題之前，這個例子著實告訴了我們，在唯一分解性質中，若我們將『質數』的條件改成『佩爾質數』，那麼縱使一個不可約解可以成分解相異的佩爾質數解的乘積，其分解也並非唯一。

接著，我們從上面的定理開始，將證明的過程推演到這個例子，想看看是否可以知道在證明之中，還有哪些地方我們沒有注意到。首先，我們將 $x^2-37y^2=p_1p_2=33$、$x^2-37y^2=p_3p_4=1927$ 以及 $x^2-37y^2=p_1p_2p_3p_4=63591$ 在第一段的解列出來(詳見下表)：

$x^2-ky^2=33$	$x^2-37y^2=1927$	$x^2-37y^2=63591$
$25+4\sqrt{37}$	$170+27\sqrt{37}$	$254+5\sqrt{37}$、$338+37\sqrt{37}$
$49+8\sqrt{37}$	$422+69\sqrt{37}$	$698+107\sqrt{37}$、$3446+565\sqrt{37}$
		$8246+1355\sqrt{37}$、$16322+2683\sqrt{37}$

接著，我們挑選 $\omega_{12}=25+4\sqrt{37}$ 以及 $\omega_{34}=422+69\sqrt{37}$，則 $\omega_{12}\omega_{34}=20762+3413\sqrt{37}$。我們將 $\omega_{12}\omega_{34}$ 依序乘上 $x^2-37y^2=p_1p_2p_3p_4$ 的解，並且判斷其結果是否是 p_i 的倍數，內容

詳見下表：

$x^2-37y^2=63591$ 的解	$\omega_{12}\omega_{34}$	p_1	p_2	p_3	p_4
		3	11	41	47
$\omega_1=254+5\sqrt{37}$	$5904953+970712\sqrt{37}$				
$\omega_2=338+37\sqrt{37}$	$11689953+1921788\sqrt{37}$	×	×		
$\omega_3=698+107\sqrt{37}$	$28003943+4603808\sqrt{37}$		×	×	
$\omega_4=3446+565\sqrt{37}$	$14289461+723491728\sqrt{37}$	×			×
$\omega_5=8246+1355\sqrt{37}$	$342314207+56276108\sqrt{37}$			×	×
$\omega_6=16322+2683\sqrt{37}$	$677689287+111411432\sqrt{37}$	×	×	×	×

若 p_j 可整除 $\omega_i\cdot\omega_{12}\omega_{34}$ ，我們在 p_j 下方的 ω_i 列劃記 ×； 從表中可以知道， $\omega_i\cdot\omega_{12}\omega_{34}$ 以及 $\omega_i\cdot\overline{\omega_{12}\omega_{34}}$ 可被 p_ip_j 整除的個數相同，而根據定理， p_i 必定僅會整除 $\omega_i\cdot\omega_{12}\omega_{34}$ 或 $\omega_i\cdot\overline{\omega_{12}\omega_{34}}$ 其中一者。所以，$\omega_i\cdot\omega_{12}\omega_{34}$ 或 $\omega_i\cdot\overline{\omega_{12}\omega_{34}}$ 一定可分解出 ω_{12}、ω_{13} 或 ω_{14} 其中一者（或者是其共軛），而剩下部分僅為 ω_{23}、ω_{24} 或 ω_{34} 其中一者（或者是其共軛），而 ω_{23}、ω_{24} 或 ω_{34} 亦可以由 ω_{12}、ω_{13} 或 ω_{14} 所產生，因此 $p_1p_2p_3p_4$ 的不可約解，應該可以由 ω_{12}、ω_{13} 以及 ω_{14} 所生成。又因為生成的『原料』從六個減少成了三個，重複的機會也減少了許多；從排列組合的角度來看，也從 12 種可能降到 8 種；根據以上討論，我們可以得到以下的結果：

【定理 3.4.5】

假設對於任意的 $i,j=1,\cdots,4,$ 皆有 $p_i\in\Omega_p$，則

$$\boldsymbol{L(k,p_1p_2p_3p_4)=L_{irr}(k,p_1p_2p_3p_4)=6}$$

【證明】

我們先從 $x^2-ky^2=p_1p_2$ 開始，選定第一個正整數解為 ω_{12}；接著分別從 $x^2-ky^2=p_1p_3$ 的第一個解或是該解的共軛中，選擇一個作為 ω_{13}；而選擇的依據就是 $\omega_{23}:=\frac{\omega_{12}\omega_{13}}{p_1}$ 是 $x^2-ky^2=p_1p_3$ 的一個不可約解；同樣的，ω_{14} 的選取就是依據 $\omega_{24}:=\frac{\omega_{12}\omega_{14}}{p_1}$ 為 $x^2-ky^2=p_1p_3$ 的一個不可約解。而在這樣的設定下， $\frac{\omega_{23}\omega_{24}}{p_2}$ 或 $\frac{\omega_{23}\overline{\omega_{24}}}{p_2}$ 中，只有一者為 x^2

$-ky^2 = p_3p_4$ 的解。事實上，因為

$$\omega_{23}\overline{\omega_{24}} = \frac{\omega_{12}\omega_{13}}{p_1} \cdot \frac{\overline{\omega_{12}\omega_{14}}}{p_1} = \frac{\omega_{12}\overline{\omega_{12}} \cdot \overline{\omega_{14}}\,\omega_{13}}{p_1^2} = \frac{p_2 \cdot \overline{\omega_{14}}\,\omega_{13}}{p_1} = p_2 \cdot \frac{\overline{\omega_{14}}\,\omega_{13}}{p_1}$$

會有一個 p_2因子，故 $\omega_{34} := \dfrac{\omega_{23}\overline{\omega_{24}}}{p_2}$ 必為 $x^2 - ky^2 = p_3p_4$ 的解。

接下來，我們就可以利用 ω_{12}、ω_{13} 以及 ω_{14} 來表示出所有的 $\widetilde{\omega_{ij}} \cdot \widetilde{\omega_{kl}}$。以 $\omega_{12}\omega_{34}$ 為例，我們會有 $\omega_{12} \cdot \omega_{34} = \omega_{12} \cdot \dfrac{\omega_{23}\overline{\omega_{24}}}{p_2} = \omega_{12} \cdot \dfrac{\overline{\omega_{14}}\,\omega_{13}}{p_1} = \dfrac{\omega_{12}\omega_{13}\overline{\omega_{14}}}{p_1}$ 。

我們用以下表格展示將 $\widetilde{\omega_{ij}} \cdot \widetilde{\omega_{kl}}$ 以 ω_{12}、ω_{13} 和 ω_{14} 來表示的結果：

	ω_{12}	$\overline{\omega_{12}}$
ω_{34}	$\dfrac{\omega_{12}\omega_{13}\overline{\omega_{14}}}{p_1}$	$\dfrac{\overline{\omega_{12}}\omega_{13}\overline{\omega_{14}}}{p_1}$
$\overline{\omega_{34}}$	$\dfrac{\omega_{12}\overline{\omega_{13}}\omega_{14}}{p_1}$	$\dfrac{\overline{\omega_{12}\omega_{13}}\,\omega_{14}}{p_1}$

	ω_{13}	$\overline{\omega_{13}}$
ω_{24}	$\dfrac{\omega_{13}\omega_{12}\omega_{14}}{p_1}$	$\dfrac{\overline{\omega_{13}}\omega_{12}\omega_{14}}{p_1}$
$\overline{\omega_{24}}$	$\dfrac{\omega_{13}\overline{\omega_{12}\omega_{14}}}{p_1}$	$\dfrac{\overline{\omega_{13}\omega_{12}\omega_{14}}}{p_1}$

	ω_{14}	$\overline{\omega_{14}}$
ω_{23}	$\dfrac{\omega_{14}\omega_{12}\omega_{13}}{p_1}$	$\dfrac{\overline{\omega_{14}}\omega_{12}\omega_{13}}{p_1}$
$\overline{\omega_{23}}$	$\dfrac{\omega_{14}\overline{\omega_{12}\omega_{13}}}{p_1}$	$\dfrac{\overline{\omega_{14}\omega_{12}\omega_{13}}}{p_1}$

比較表格中的解，我們發現共有六組解是相同的：

$$\omega_{12} \cdot \omega_{34} = \frac{\omega_{12}\omega_{13}\overline{\omega_{14}}}{p_1} = \overline{\omega_{14}} \cdot \omega_{23} \qquad \overline{\omega_{12}} \cdot \omega_{34} = \frac{\overline{\omega_{12}\omega_{13}}\omega_{14}}{p_1} = \omega_{14} \cdot \overline{\omega_{23}}$$

$$\overline{\omega_{12}} \cdot \omega_{34} = \frac{\overline{\omega_{12}}\omega_{13}\overline{\omega_{14}}}{p_1} = \omega_{13} \cdot \overline{\omega_{24}} \qquad \omega_{12} \cdot \overline{\omega_{34}} = \frac{\omega_{12}\overline{\omega_{13}}\omega_{14}}{p_1} = \overline{\omega_{13}} \cdot \omega_{24}$$

$$\omega_{13} \cdot \omega_{24} = \frac{\omega_{13}\omega_{12}\omega_{14}}{p_1} = \omega_{14} \cdot \omega_{23} \qquad \overline{\omega_{13}} \cdot \overline{\omega_{24}} = \frac{\overline{\omega_{12}\omega_{13}\omega_{14}}}{p_1} = \overline{\omega_{14}} \cdot \overline{\omega_{23}}$$

簡而言之，利用 ω_{12}、ω_{13} 以及 ω_{14} ，生成了 $\omega_{12} \cdot \omega_{34}$、$\overline{\omega_{12}} \cdot \omega_{34}$、$\omega_{13} \cdot \omega_{24}$（以及他們的共軛）一共六個解。最後，我們須說明這六個解都是不相同的解；也就是說若 λ_1 和 λ_2 是上述六個解中的相異兩解，則對於任意的整數 n，$\sigma^n\lambda_1$和 λ_2 皆不相等；由於這六個解的分母均為 p_1，我們只要考慮分子比值是否為 σ^n 即可，意即

$$\frac{\widetilde{\omega_{12}} \cdot \widetilde{\omega_{13}} \cdot \widetilde{\omega_{14}}}{\widetilde{\widetilde{\omega_{12}}} \cdot \widetilde{\widetilde{\omega_{13}}} \cdot \widetilde{\widetilde{\omega_{14}}}} = \sigma^n$$

其中 $\widetilde{\omega_{1i}}$和 $\widetilde{\widetilde{\omega_{1i}}}$ 表示 ω_{1i} 或是 $\overline{\omega_{1i}}$。由於在上面的分式中，$\widetilde{\omega_{1i}}$ 和 $\widetilde{\widetilde{\omega_{1i}}}$ 必會相等或是共軛，若

將相等的項約分後，所留下來的分式，其分子和分母必定共軛，故我們可以假設此分式為

$$\frac{\lambda}{\bar{\lambda}} = \sigma^n \text{ 或 } \frac{P_1\lambda'}{P_1\bar{\lambda'}} = \sigma^n$$

其中 λ 和 λ' 皆為不可約解，因此我們可以假設 $\frac{\lambda}{\bar{\lambda}} = \sigma^n$ 其中 $n \neq 0$。因為 $\frac{\lambda}{\bar{\lambda}}$

$= \frac{\lambda^2}{\bar{\lambda}\cdot\lambda}$，若我們假

設 $\lambda = u + v\sqrt{k}$，那麼 p_1、p_2、p_3 和 p_4 中，至少有一個 p_i 會是 $u^2 + kv^2$ 和 $2uv$ 的公因數；由於 p_i 和 k 互質，我們會推得 p_i 會是 u 和 v 的公因數，這便與 λ 的不可約性矛盾；也就是說這六個解均屬於不同類的不可約解。故得證。■

【備註 3.4.4】

在最一開始的定理中，我們假設了所有的佩爾質數都在同一個中 Ω_p；但是僅要求 p_1p_2 和 p_3p_4是佩爾質數，且 $\Omega_{p_1} \neq \Omega_{p_3}$ $(\text{也因此 } \Omega_{p_1} \neq \Omega_{p_4})$ 時，在證明的三個情況中，會有以下結果：

【情況一】 $A = 1$ 有成立的可能，也就是 $\omega = \sigma^*\omega_{12}\omega_{34}$ (以及 $\omega = \sigma^*\overline{\omega_{12}\omega_{34}}$)；

【情況二】 $A = p_i$ 同樣也不會發生。

【情況三】 $A = p_ip_j$，(i,j) 只有可能等於 $(1,2)$ 或 $(3,4)$。

當 $A = p_1p_2$ 時，$\frac{\omega\omega_{12}\omega_{34}}{A} = \frac{\omega\omega_{12}\omega_{34}}{p_1p_2} = \sigma^n\omega_{34}^2$ 或 $\sigma^n\overline{\omega_{34}}^2$；當 $\frac{\omega\omega_{12}\omega_{34}}{p_1p_2} = \sigma^n\omega_{34}^2$ 時，$\omega = \sigma^n\overline{\omega_{12}}\omega_{34}$；若 $\frac{\omega\omega_{12}\omega_{34}}{p_1p_2} = \sigma^n\overline{\omega_{34}}^2$ 時，會有

$$\omega\omega_{34} = \sigma^n\overline{\omega_{34}}^2\overline{\omega_{12}}$$

$$\Longrightarrow \omega\cdot p_3p_4 = \sigma^n\overline{\omega_{34}}^3\overline{\omega_{12}}$$

$$\Longrightarrow \omega\cdot\omega_{12}\cdot p_3p_4 = \sigma^n\overline{\omega_{34}}^3\cdot p_1p_2$$

但這會得到 p_3p_4 整除 $\overline{\omega_{34}}^3$ 如此一個矛盾，因此 $\frac{\omega\omega_{12}\omega_{34}}{p_1p_2}$ 並不會等於 $\sigma^n\overline{\omega_{34}}^2$。

根據上面的討論，我們知道在這樣的假設底下，$x^2 - ky^2 = p_1p_2p_3p_4$ 的解只會由 ω_{12} 和 ω_{34}（以及其共軛）所生成，也因此我們會有

【定理 3.4.6】

假設 $p_2 \in \Omega_{p_1}$且 $p_4 \in \Omega_{p_3}$。若 $\Omega_{p_1} \neq \Omega_{p_3}$，則有

$$L(k, p_1p_2p_3p_4) = L_{irr}(k, p_1p_2p_3p_4) = 4$$

接著，我們有興趣的是，對於任意的正整數 $i, j = 1, \cdots, 2n$ 皆有 $p_i, p_j \in \Omega_p$ 時，$x^2 - ky^2 = p_1p_2 \cdots p_{2n}$ 的不可約解是否會被 ω_{ij} 所生成？也就是說任一個 $x^2 - ky^2 = p_1p_2 \cdots p_{2n}$ 的不可約解 ω，是否存在一個數列 1、2、…、$2n$ 的一個重排 $\{a_i\}_{i=1}^{2n}$，使得 $\omega = \prod_{j=1}^{n} \omega_{a_{2j-1}a_{2j}}$，其中 $\omega_{a_{2j-1}a_{2j}}$ 是 $x^2 - ky^2 = p_{a_{2i-1}}p_{a_{2i}}$ 的一個不可約解。

仿效**【定理 3.4.5】**，我們的確可以建構一組 ω_{ij}，來表示出 $x^2 - ky^2 = p_1p_2 \cdots p_{2n}$ 的一些解，而且僅利用這些 ω_{ij} 所呈現的解，其表示法是唯一的：

【定理 3.4.7】

設 $p_i \in [p_1]$，其中 $i = 1,2, \cdots, 2n, n > 1$。若令 ω_{ij} 是佩爾方程式 $x^2 - ky^2 = p_ip_j$ 的一個正整數解，則

1. $\prod_{i=1}^{n} \widetilde{\omega_{a_{2i-1}a_{2i}}}$ 是 $x^2 - ky^2 = p_1p_2 \cdots p_{2n}$ 的一個不可約解，其中 a_i 是 $\{1,2, \cdots, 2n\}$ 的一個重排，且$\widetilde{\omega_{a_{2i-1}a_{2i}}} = \omega_{a_{2i-1}a_{2i}}$ 或 $\overline{\omega_{a_{2i-1}a_{2i}}}$。
2. 在 $\left(\sqrt{p_1p_2 \cdots p_{2n}}, \sigma \cdot \sqrt{p_1p_2 \cdots p_{2n}}\right)$ 之間由 ω_{ij} 所生成的解共有$2 \times (C_{n-1}^{2n-2} + C_n^{2n-2})$ 個。

【證明】

我們現在考慮等價類 $[p_1]$，並不妨假設 $p_1 < p_2 < \cdots < p_n < p_{n+1} < \cdots < p_{2n}$。由於 p_ip_j 是佩爾質數，$L_{irr}(k, p_ip_j) = 2$，因此只要知道 $x^2 - ky^2 = p_ip_j$ 其中一個不可約解 λ，那麼其他的不可約解必定形如 $\sigma^m\lambda$ 或是 $\sigma^m\bar{\lambda}$，其中 m 為任意整數。接下來，我們先利用一些不可約解，來生成等價類內佩爾質數的不可約解。

首先，我們先選取 $x^2 - ky^2 = p_1p_2$ 的第一個正整數解，並以符號 ω_{12} 表之。現在，對於任意的正整數 $3 \leq i \leq 2n$，我們考慮 $x^2 - ky^2 = p_1p_i$ 的第一個正整數解 λ_{1i}。那麼

$$\frac{\omega_{12}\lambda_{1i}}{p_1} \text{ 和 } \frac{\omega_{12}\overline{\lambda_{1i}}}{p_1}$$

之中，只有一者會是 $x^2 - ky^2 = p_2p_i$ 的一個不可約解，我們將該解記為 ω_{1i}，而 ω_{1i} 與

ω_{12}所生成的解稱為 ω_{2i}，意即 $\omega_{2i}=\dfrac{\omega_{12}\omega_{1i}}{p_1}$ 。

現在固定 $4\le i<2n$，我們考慮 ω_{23} 和 $\omega_{2\,i}$，那麼我們會有

$$\omega_{23}\cdot\omega_{2\,i}=\frac{\omega_{12}\omega_{13}}{p_1}\cdot\frac{\omega_{12}\omega_{1i}}{p_1}\text{ 以及 }\omega_{23}\cdot\overline{\omega_{2\,i}}=\frac{\omega_{12}\omega_{13}}{p_1}\cdot\frac{\overline{\omega_{12}\omega_{1i}}}{p_1}$$

由於

$$\omega_{23}\cdot\overline{\omega_{2\,i}}=\frac{\omega_{12}\omega_{13}}{p_1}\cdot\frac{\overline{\omega_{12}\omega_{1i}}}{p_1}=\frac{p_1p_2\cdot\omega_{13}\cdot\overline{\omega_{1i}}}{p_1^2}=p_2\cdot\frac{\omega_{13}\overline{\omega_{1i}}}{p_1}$$

因此我們定義 $\omega_{3\,i}=\dfrac{\omega_{13}\overline{\omega_{1i}}}{p_1}\left(=\dfrac{\omega_{23}\cdot\overline{\omega_{2\,i}}}{p_2}\right)$。

現在再次固定 $5\le i<2n$，我們考慮 ω_{34} 和 $\omega_{3\,i}$，那麼我們會有

$$\omega_{34}\cdot\overline{\omega_{3\,i}}=\frac{\omega_{13}\overline{\omega_{14}}}{p_1}\cdot\frac{\overline{\omega_{13}}\omega_{1\,i}}{p_1}=\frac{p_1p_3\cdot\overline{\omega_{14}}\cdot\omega_{1\,i}}{p_1^2}=p_3\cdot\frac{\overline{\omega_{14}}\cdot\omega_{1\,i}}{p_1}$$

因此我們定義 $\omega_{4\,i}=\dfrac{\overline{\omega_{14}}\cdot\omega_{1\,i}}{p_1}\left(=\dfrac{\omega_{34}\cdot\overline{\omega_{3\,i}}}{p_3}\right)$

如此迭代下去，對於 $2\le i<j\le 2n$，我們可以定義

$$\omega_{ij}=\begin{cases}\dfrac{\omega_{12}\omega_{1j}}{p_1}, & i=2\\ \dfrac{\omega_{1i}\overline{\omega_{1j}}}{p_1}, & i\text{ 是奇數}>2\\ \dfrac{\overline{\omega_{1i}}\omega_{1j}}{p_1}, & i\text{ 是偶數}>2\end{cases}$$

現在，我們就利用這些創造出來的 ω_{ij}，來生成 $x^2-ky^2=p_1p_2\cdots p_{2n}$ 的解，並且討論這樣的解會有幾個(也就是不重複的生成)。

現在假設 a_i 是 $\{1,2,\cdots,2n\}$ 的一個重排，$\omega=\prod_{i=1}^{n}\omega_{\widetilde{a_{2i-1}a_{2i}}}$ ，且$\omega_{\widetilde{a_{2i-1}a_{2i}}}=\omega_{a_{2i-1}a_{2i}}$ 或 $\overline{\omega_{a_{2i-1}a_{2i}}}$。根據我們設計的 ω_{ij}，我們可以發現 ω 可以表示成

$$\frac{1}{p_1^{n-1}}\cdot\underbrace{\widetilde{\omega_{12}}\cdot\widetilde{\omega_{13}}\cdot\cdots\cdot\widetilde{\omega_{12n}}}_{2n-1\text{ 個}}$$

我們先考慮 $\widetilde{\omega_{12}}=\omega_{12}$ 的情況，那麼 $\omega_{12}\cdot\widetilde{\omega_{13}}\cdot\cdots\cdot\widetilde{\omega_{12n}}$ 會有以下兩種情況：

$$\omega_{12}\cdot\widetilde{\omega_{13}}\cdot\cdots\cdot\widetilde{\omega_{12n}}=\begin{cases}\dfrac{1}{p_1^{n-1}}\cdot\omega_{12}\cdot\underbrace{\left(\omega_{1a_1}\cdot\cdots\cdot\omega_{1a_{n-1}}\right)}_{n-1\text{ 個}}\cdot\underbrace{\overline{\left(\omega_{1a_n}\cdot\cdots\cdot\omega_{1a_{2n-2}}\right)}}_{n-1\text{ 個}}\\ \dfrac{1}{p_1^{n-1}}\cdot(\omega_{12}\cdot\omega_{1i})\cdot\widetilde{\omega_{1J}}\cdot\underbrace{\left(\omega_{1a_1}\cdot\cdots\cdot\omega_{1a_{n-2}}\right)}_{n-2\text{ 個}}\cdot\underbrace{\overline{\left(\omega_{1a_{n-1}}\cdot\cdots\cdot\omega_{1a_{2n-4}}\right)}}_{n-2\text{ 個}}\end{cases}$$

第一種情況是代表 $(a_{2i-1},a_{2i})=(1,2)$ 或 $(2,1)$，第二種情況則是表示任兩個連續的 a_i都不會等於$(1,2)$ 或 $(2,1)$；舉例來說，下面兩種情況分別表示了第一和第二種情況：

$$\omega=\frac{1}{p_1^{n-1}}\cdot\omega_{12}\cdot\prod_{i=2}^{n}\widetilde{\omega_{a_{2i-1}a_{2i}}}\text{ 以及 }\omega=\frac{1}{p_1^{n-1}}\cdot\widetilde{\omega_{13}}\omega_{24}\cdots\prod_{i=1}^{n}\widetilde{\omega_{a_{2i-1}a_{2i}}}$$

若再將第二種情況中的 $\widetilde{\omega_{1J}}$ 分別表示為 ω_{1j} 和 $\overline{\omega_{1J}}$，則 $\omega_{12}\cdot\widetilde{\omega_{13}}\cdot\cdots\cdot\widetilde{\omega_{12n}}$ 會有以下三種呈現方式：

$$\omega_{12}\cdot\widetilde{\omega_{13}}\cdot\cdots\cdot\widetilde{\omega_{12n}}=\begin{cases}\dfrac{1}{p_1^{n-1}}\cdot\omega_{12}\cdot\underbrace{\left(\omega_{1a_1}\cdot\cdots\cdot\omega_{1a_{n-1}}\right)}_{n-1\text{ 個}}\cdot\underbrace{\overline{\left(\omega_{1a_n}\cdot\cdots\cdot\omega_{1a_{2n-2}}\right)}}_{n-1\text{ 個}}\\ \dfrac{1}{p_1^{n-1}}\cdot\omega_{12}\cdot\underbrace{\left(\omega_{1i}\cdot\omega_{1j}\cdot\omega_{1a_1}\cdot\cdots\cdot\omega_{1a_{n-2}}\right)}_{n\text{ 個}}\cdot\underbrace{\overline{\left(\omega_{1a_{n-1}}\cdot\cdots\cdot\omega_{1a_{2n-4}}\right)}}_{n-2\text{ 個}}\\ \dfrac{1}{p_1^{n-1}}\cdot\omega_{12}\cdot\underbrace{\left(\omega_{1i}\cdot\omega_{1a_1}\cdot\cdots\cdot\omega_{1a_{n-2}}\right)}_{n-1\text{ 個}}\cdot\underbrace{\overline{\left(\omega_{1J}\cdot\omega_{1a_{n-1}}\cdot\cdots\cdot\omega_{1a_{2n-4}}\right)}}_{n-1\text{ 個}}\end{cases}$$

同樣舉例說明這兩種情況的發生：當

$$\omega=\frac{1}{p_1^{n-1}}\cdot\widetilde{\omega_{13}}\omega_{24}\cdots\prod_{i=1}^{n}\widetilde{\omega_{a_{2i-1}a_{2i}}}$$

$$=\begin{cases}\dfrac{1}{p_1^{n-1}}\cdot(\omega_{12}\cdot\omega_{14})\cdot\omega_{13}\cdot\underbrace{\left(\omega_{1a_1}\cdot\cdots\cdot\omega_{1a_{n-2}}\right)}_{n-2\text{ 個}}\cdot\underbrace{\overline{\left(\omega_{1a_{n-1}}\cdot\cdots\cdot\omega_{1a_{2n-4}}\right)}}_{n-2\text{ 個}} & \widetilde{\omega_{13}}=\omega_{13}\\ \dfrac{1}{p_1^{n-1}}\cdot(\omega_{12}\cdot\omega_{14})\cdot\overline{\omega_{13}}\cdot\underbrace{\left(\omega_{1a_1}\cdot\cdots\cdot\omega_{1a_{n-2}}\right)}_{n-2\text{ 個}}\cdot\underbrace{\overline{\left(\omega_{1a_{n-1}}\cdot\cdots\cdot\omega_{1a_{2n-4}}\right)}}_{n-2\text{ 個}} & \widetilde{\omega_{13}}=\overline{\omega_{13}}\end{cases}$$

$$=\begin{cases}\dfrac{1}{p_1^{n-1}}\cdot\omega_{12}\underbrace{\left(\omega_{14}\cdot\omega_{13}\cdot\omega_{1a_1}\cdot\cdots\cdot\omega_{1a_{n-2}}\right)}_{n\text{ 個}}\cdot\underbrace{\overline{\left(\omega_{1a_{n-1}}\cdot\cdots\cdot\omega_{1a_{2n-4}}\right)}}_{n-2\text{ 個}} & \widetilde{\omega_{13}}=\omega_{13}\\ \dfrac{1}{p_1^{n-1}}\cdot\omega_{12}\cdot\underbrace{\left(\omega_{14}\cdot\omega_{1a_1}\cdot\cdots\cdot\omega_{1a_{n-2}}\right)}_{n-1\text{ 個}}\cdot\underbrace{\overline{\left(\omega_{13}\omega_{1a_{n-1}}\cdot\cdots\cdot\omega_{1a_{2n-4}}\right)}}_{n-1\text{ 個}} & \widetilde{\omega_{13}}=\overline{\omega_{13}}\end{cases}$$

然而，第一種和第三種都是相同的，所以可能會產生的情況會有 C_{n-1}^{2n-2}（第一種表示）與

C_n^{2n-2}（第二種表示），再將 ω_{12} 的共軛納入，則共有 $2\times(C_{n-1}^{2n-2}+C_n^{2n-2})$ 種情況；接著我們要試著說明，這些情況都不會重複；假設 $A=\sigma^n B$，其中 A 和 B 是兩種情況的某一種。兩邊相互約分後，我們可以假設該示被化簡為 $C=\sigma^n\bar{C}$ 也因此 $C^2=\sigma^n p_1^{2m}p_{a_1}\cdots p_{a_m}$。若 $m\neq 0$，則 p_{a_1} 可以整除 C，也因此 $p_{a_1}^2$ 可以整除 $C\cdot\bar{C}$，矛盾；因此 $C^2=\sigma^n$，這只有當 $C=1$ 才有可能；故得證。■

【備註 3.4.5】

關於**【定理 3.4.7】**，雖然是仿效**【定理 3.4.5】**所得到，但是並無如**【定理 3.4.4】**般的結果，來支持 ω_{ij} 可以製成所有的不可約解。舉例來說，雖然我們可以將**【定理 3.4.4】**的方法，延伸到方程式 $x^2-ky^2=p_1p_2\cdots p_6$，也就是任選一個 $x^2-ky^2=p_1p_2\cdots p_6$ 的解 ω，並與方程式 $x^2-ky^2=p_{2t-1}p_{2t}$ 的一固定解 ω_t 相乘（其中 $t=1,2,3$），但是這有可能得到方程式 $x^2-ky^2=(p_1p_2p_3)^2$ 和 $x^2-ky^2=(p_4p_5p_6)^2$ 的兩個不可約解

$$\frac{\omega\omega_{12}\omega_{34}\omega_{56}}{p_4p_5p_6}\text{ 以及 }\frac{\omega\overline{\omega_{12}\omega_{34}\omega_{56}}}{p_1p_2p_3}$$

而這兩個不可約解，至多只能反映 ω 可以表示成方程式 $x^2-ky^2=\pm p_1p_2p_3$ 與 $x^2-ky^2=\pm p_4p_5p_6$ 兩解的乘積，但這並無法說明 ω 可以以 ω_t 表示。

在**【備註 3.4.5】**中，我們再次預見當 $p_2,p_3\in\Omega_{p_1}$ 時，可以創造出新的佩爾質數 $p_1p_2p_3$。而事實上，也的確有這樣的例子，例如當 $k=37$ 時，$11,41\in\Omega_3$，而方程式

$$x^2-37y^2=3\times 11\times 41=1353$$

會有不可約解 $61+8\sqrt{37}$ 以及 $901+148\sqrt{37}$，也因此是一個佩爾質數。

然而，並非在同一個 Ω_p 中的任三個相異質數相乘，就會得到佩爾質數；也就是說在同一個 Ω_p 中的任三個相異質數相乘，有可能會無解。例如之前所提到的，當 k 等於 401 時，$5,29,41,47\in\Omega_5$ 以及 $7,11,43\in\Omega_7$。然而

$$x^2-37y^2=5\times 29\times 41=5945$$

以及

$$x^2-37y^2=7\times 11\times 43=3311$$

卻是無解。

然而，我們從這些例子中，發現了一些有趣的情況：

1. 首先，同樣考慮當 $k = 401$ ， $5,29,41,47 \in \Omega_5$ 以及 $7,11,43 \in \Omega_7$ 時，以下的兩個方程式

$$x^2 - 401 = 5 \times 29 \times 7 = 1015$$

以及

$$x^2 - 401 = 11 \times 43 \times 47 = 22231$$

均是有解的方程式。根據**【定理 3.4.3】**，這意味著在 Ω_5 與 Ω_7 中分別挑選兩個相異以及一個質數（或者相反）後相乘，都會是佩爾質數。

2. 再者，方程式

$$x^2 - 401 = (5 \times 29 \times 7) \times (11 \times 43 \times 47)$$

會有一個不可約解

$$\omega = \left(68 + 3\sqrt{401}\right) \cdot \left(300 + 13\sqrt{401}\right) = 36039 + 1784\sqrt{401}$$

其中 $68 + 3\sqrt{401}$ 和 $300 + 13\sqrt{401}$ 分別是方程式$x^2 - 401 = 1015\ (= 5 \times 7 \times 29)$與 $x^2 - 401 = 22231(= 11 \times 43 \times 47)$ 的解。

雖然 ω 無法寫成 $\omega_{a_1a_2} \cdot \omega_{a_3a_4} \cdot \omega_{a_5a_6}$，然而，若我們將 $x^2 - 401 = 77\ (= 7 \times 11)$ 的一個解 $\omega_{77} = \ 41 + 2\sqrt{401}$ 作用於 ω，那麼我們會有

$$\begin{aligned} \omega \cdot \omega_{77} &= \left(36039 + 1784\sqrt{401}\right) \\ &\qquad \cdot \left(41 + 2\sqrt{401}\right) \\ &= 2908367 + 145222\sqrt{401} \\ &= 77\left(3771 + 1886\sqrt{401}\right) \\ &= 77 \cdot \omega_{5\times29\times43\times47} \end{aligned}$$

因此，$\omega = \overline{\omega_{77}} \cdot \omega_{5\times29\times43\times47}$；也就是說 ω 可以分解成 ω_{77} 和 $\omega_{5\times29\times43\times47}$ 這兩個佩爾質數的乘積。我們同樣試著將其他的 $\omega_{i\times j} = (u_{i\times j} + v_{i\times j}\sqrt{401})$ 作用到 ω 上：（見下表）

i	j	$u_{i\times j}$	$v_{i\times j}$	36039	1784	GCD
7	43	201	10	14397679	718974	1
11	43	83	4	5852773	292228	43
5	29	81	4	5780695	288660	5
5	47	62	3	4380570	218725	5
29	47	42	1	2229022	110967	47

根據上表，我們發現

$$\omega \cdot \omega_{7\times 43(=301)} = \left(36039 + 1784\sqrt{401}\right) \cdot \left(201 + 10\sqrt{401}\right) = 14397679 + 718974\sqrt{401}$$

且有 $\mathrm{GCD}(14397679,718974) = 1$，因此我們斷言

$$\omega \cdot \overline{\omega_{301}} = 301 \cdot \omega_{5\times 11\times 29\times 47}$$

也因此會有：

$$\omega = \omega_{301} \cdot \omega_{5\times 11\times 29\times 47} = \left(201 + 10\sqrt{401}\right) \cdot \left(299 + 6\sqrt{401}\right)$$

這意味我們再次將 ω 再次寫成兩種不同的兩個佩爾質數的乘積：

$$\omega = \omega_{301} \cdot \omega_{5\times 11\times 29\times 47} = \omega_{5\times 29\times 7} \times \omega_{11\times 43\times 47}$$

【備註 3.4.】

做為結束這一章節的討論，總結以上所述，我們有以下的結論以及提問：

1. 再次找到了將一個不可約解 ω，可以將其寫成兩種以上，不同的佩爾質數的乘積：

$$\omega = \omega_{5\times 7\times 29} \cdot \omega_{11\times 43\times 47} = \overline{\omega_{7\times 11}} \cdot \omega_{5\times 29\times 43\times 47} = \omega_{7\times 43} \cdot \omega_{5\times 11\times 29\times 47}$$

2. 當 $j > 4$時，考慮廣義佩爾方程式 $x^2 - ky^2 = p_1 p_2 \cdots p_j$ 的任一解 ω ，可以找到多少個 $\{1,2,\cdots,j\}$ 的重排 $\{a_n\}$ 且滿足

   (1) $p_1 p_2 \cdots p_j = \left(p_{a_1} p_{a_2} \cdots p_{a_m}\right)\left(p_{a_{m+1}} p_{a_{m+2}} \cdots p_{a_{m+n}}\right) \cdots \left(p_{a_{m+t+1}} p_{a_{m+t+2}} \cdots p_{a_j}\right)$

   (2) $p_{a_1} p_{a_2} \cdots p_{a_m}$ 、$p_{a_{m+1}} p_{a_{m+2}} \cdots p_{a_{m+n}}$ 、$\cdots$ 、$p_{a_{m+t+1}} p_{a_{m+t+2}} \cdots p_{a_j}$ 都是佩爾質數

   (3) $\omega = \omega_{p_{a_1} p_{a_2} \cdots p_{a_m}} \cdot \omega_{p_{a_{m+1}} p_{a_{m+2}} \cdots p_{a_{m+n}}} \cdot \cdots \cdot \omega_{p_{a_{m+t+1}} p_{a_{m+t+2}} \cdots p_{a_j}}$ 其中每個 ω_* 都是佩爾質數。

3. 雖然佩爾質數並沒有唯一分解性質，是否在某些條件下具有唯一分解的性質？

5. 在佩爾地毯上爬行的蜈蚣

在這一個章節裡面，我們著眼於有蜈蚣兗現象的質數，因此若沒有特別說明，以下均假設一個給定的奇質數 k，$p > 0$ 皆為蜈蚣兗，且擁有相同的最低次方解 n。我們先從**【定理 3.5.1】**開始：

【定理 3.5.1】

假設佩爾方程式 $x^2-ky^2=p_1^{\alpha}p_2^{\beta}$ 與 $x^2-ky^2=p_1^{\gamma}p_2^{\delta}$ 分別有不可約解，則下列其中之一個情況必定發生

(1) 佩爾方程式 $x^2-ky^2=p_1^{|\alpha-\gamma|}p_2^{\beta}$ 與 $x^2-ky^2=p_1^{\alpha}p_2^{|\beta-\delta|}$ 均有不可約解。

(2) 佩爾方程式 $x^2-ky^2=p_1^{|\alpha-\gamma|}p_2^{|\beta-\delta|}$ 與 $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{\beta+\delta}$ 均有不可約解。

【證明】

令 $m=\min\{\alpha,\gamma\}$ 以及 $n=\min\{\beta,\delta\}$，且假設 $\omega_{\alpha\beta}=u_{\alpha\beta}+v_{\alpha\beta}\sqrt{k}$ 與 $\omega_{\gamma\delta}=u_{\gamma\delta}+v_{\gamma\delta}\sqrt{k}$ 分別為佩爾方程式 $x^2-ky^2=p_1^{\alpha}p_2^{\beta}$ 與 $x^2-ky^2=p_1^{\gamma}p_2^{\delta}$ 的一個不可約解。則我們會有

$$(u_{\alpha\beta}v_{\gamma\delta}-v_{\alpha\beta}u_{\gamma\delta})(u_{\alpha\beta}v_{\gamma\delta}+v_{\alpha\beta}u_{\gamma\delta})=p_1^{m}p_2^{n}\left(p_1^{\alpha-m}p_2^{\beta-n}v_{\gamma\delta}^2-p_1^{\gamma-m}p_2^{\delta-n}v_{\alpha\beta}^2\right)$$

我們先說明 $\mathrm{GCD}\left(p_1p_2,u_{\alpha\beta}v_{\gamma\delta}-v_{\alpha\beta}u_{\gamma\delta},u_{\alpha\beta}v_{\gamma\delta}-v_{\alpha\beta}u_{\gamma\delta}\right)=1$：若 p_i 是 $u_{\alpha\beta}v_{\gamma\delta}-v_{\alpha\beta}u_{\gamma\delta}$ 和 $u_{\alpha\beta}v_{\gamma\delta}+v_{\alpha\beta}u_{\gamma\delta}$ 的公因數，那麼 p_i 是會整除 $2u_{\alpha\beta}v_{\gamma\delta}$，也因此整除 $u_{\alpha\beta}$ 或 $v_{\gamma\delta}$ 其中之一；又因為 $(k,p_i)=1$，$kv_{\alpha\beta}^2=p_1^{\alpha}p_2^{\beta}-u_{\alpha\beta}^2$ 以及 $u_{\gamma\delta}^2=kv_{\gamma\delta}^2+p_1^{\gamma}p_2^{\delta}$，因此會推得 $\omega_{\alpha\beta}$ 或 $\omega_{\gamma\delta}$ 是可約解這樣的一個矛盾。故此，我們會有

(1) p_1^m 是 $u_{\alpha\beta}v_{\gamma\delta}-v_{\alpha\beta}u_{\gamma\delta}$ 的因數，且 p_2^n 是 $u_{\alpha\beta}v_{\gamma\delta}+v_{\alpha\beta}u_{\gamma\delta}$ 的因數。

(2) p_1^m 是 $u_{\alpha\beta}v_{\gamma\delta}+v_{\alpha\beta}u_{\gamma\delta}$ 的因數，且 p_2^n 是 $u_{\alpha\beta}v_{\gamma\delta}-v_{\alpha\beta}u_{\gamma\delta}$ 的因數。

(3) $p_1^mp_2^n$ 是 $u_{\alpha\beta}v_{\gamma\delta}-v_{\alpha\beta}u_{\gamma\delta}$ 的因數。

(4) $p_1^mp_2^n$ 是 $u_{\alpha\beta}v_{\gamma\delta}+v_{\alpha\beta}u_{\gamma\delta}$ 的因數。

由於

$$\omega_{\alpha\beta}\omega_{\gamma\delta}=\left(u_{\alpha\beta}u_{\gamma\delta}+kv_{\gamma\delta}v_{\alpha\beta}\right)+\sqrt{k}(u_{\alpha\beta}v_{\gamma\delta}+v_{\alpha\beta}u_{\gamma\delta})$$

$$\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}=\left(u_{\alpha\beta}u_{\gamma\delta}-kv_{\gamma\delta}v_{\alpha\beta}\right)+\sqrt{k}(u_{\alpha\beta}v_{\gamma\delta}-v_{\alpha\beta}u_{\gamma\delta})$$

均為方程式 $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{\beta+\delta}$ 的一個解，根據上面四種情況，我們將會得到

(1) $\dfrac{\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}}{p_1^m}$ 是 $x^2-ky^2=p_1^{|\alpha-m|}p_2^{\beta+\delta}$ 的解，且 $\dfrac{\omega_{\alpha\beta}\omega_{\gamma\delta}}{p_2^n}$ 是 $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{|\beta-\delta|}$ 的解

(2) $\dfrac{\omega_{\alpha\beta}\omega_{\gamma\delta}}{p_1^m}$ 是 $x^2-ky^2=p_1^{|\alpha-m|}p_2^{\beta+\delta}$ 的解，且 $\dfrac{\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}}{p_2^n}$ 是 $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{|\beta-\delta|}$ 的解

(3) $\dfrac{\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}}{p_1^mp_2^n}$ 是 $x^2-ky^2=p_1^{|\alpha-m|}p_2^{|\beta-\delta|}$ 的解，且 $\omega_{\alpha\beta}\omega_{\gamma\delta}$ 是 $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{\beta+\delta}$ 的解

(4) $\frac{\omega_{\alpha\beta}\omega_{\gamma\delta}}{p_1^m p_2^n}$ 是 $x^2-ky^2=p_1^{|\alpha-m|}p_2^{|\beta-\delta|}$ 的解，且 $\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}$ 是 $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{\beta+\delta}$ 的解

接著，我們要說明這些都是不可約解：首先，我們注意到

$$\frac{(u_{\alpha\beta}v_{\gamma\delta}-v_{\alpha\beta}u_{\gamma\delta})(u_{\alpha\beta}v_{\gamma\delta}+v_{\alpha\beta}u_{\gamma\delta})}{p_1^m p_2^n}=p_1^{\alpha-m}p_2^{\beta-n}v_{\gamma\delta}^2-p_1^{\gamma-m}p_2^{\delta-n}v_{\alpha\beta}^2$$

而我們將利用這個式子來說明解的不可約解；

在(1)的情況下，如果是 $\frac{\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}}{p_1^m}$ 可約解，那麼 p_1 是唯一可以整除該解的質數，也因此 p_1 可整除$p_1^{\alpha-m}p_2^{\beta-n}v_{\gamma\delta}^2-p_1^{\gamma-m}p_2^{\delta-n}v_{\alpha\beta}^2$。若 $\alpha>\gamma$，p_1 可整除 $p_1^{\alpha-m}p_2^{\beta-n}v_{\gamma\delta}^2-p_2^{\delta-n}v_{\alpha\beta}^2$，由於 $(p_1,p_2)=1$，p_1 會是 $v_{\alpha\beta}$ 的因數；然而，這會導致與 $\omega_{\alpha\beta}$ 是不可約解的矛盾，這便說明了該解的不可約性；如果 $\alpha=\gamma$，該解所對應到的方程式便為 $x^2-ky^2=p_2^{\beta+\delta}$，但如此一來，該解不可能會有任何整數因子，這同時說明了解的不可約性。至於在(1)情況的另一個解，以及在情況(2)中解的不可約性證明與上述類似，便不再贅述；因此我們說明了在前兩個狀況中的解，均是不可約解。

現在來到(3)的情況；同樣的只有 p_1 和 p_2 才可能整除$\frac{\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}}{p_1^m p_2^n}$。若 $\alpha>\gamma$，p_1 將會整除 $v_{\alpha\beta}$；若 $\beta>\delta$，p_2 也將會整除 $v_{\alpha\beta}$；以上的情況都會和 ω_1 和 ω_2 是不可約解矛盾；若 $\alpha=\gamma$ 且 $\beta=\delta$，那麼該解所對應到的方程式便為 $x^2-ky^2=1$，也就是說 $\frac{\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}}{p_1^m p_2^n}=\sigma^t$。這也就是說無論 $(\alpha-\gamma)(\beta-\delta)$ 之值為何，該解必定為一個不可約解；至於在情況(3)中的另一個解 $\omega_{\alpha\beta}\omega_{\gamma\delta}$，由於$u_{\alpha\beta}v_{\gamma\delta}+v_{\alpha\beta}u_{\gamma\delta}$ 與 p_1 和 p_2 互值，該解必不可約；最後，由於情況(4)中解不可約性的證明與情況(3)相同，我們說明了無論在那種情況下，所產生的解均為不可約。故得證。■

【備註 3.5.1】

對於以上的**【定理 3.5.1】**，我們有以下的觀點：

(1) 首先，兩個不可約解的乘積，雖然不一定不可約，但是經過去除公因數部分後，可能出現的不可約型態必定是上述的情況之一。

(2) 要特別注意的，每個狀況確實反映了 $\omega_{\alpha\beta}$、$\overline{\omega_{\alpha\beta}}$ 與 $\omega_{\gamma\delta}$、$\overline{\omega_{\gamma\delta}}$ 彼此相乘的型態。

(3) 從指數的角度來看，p_1 和 p_2 可能出現的指數分別為 $|\alpha-\gamma|$、$\alpha+\gamma$ 與 $|\beta-\delta|$、$\beta+\delta$，而單一從 p_1 或 p_2 的角度來看，指數『向前』或『向後』都會有不可約解。

我們將【**定理 3.5.1**】的結果整理如下表，以便後面討論：

	$u_{\alpha\beta}v_{\gamma\delta}-v_{\alpha\beta}u_{\gamma\delta}$ 的因數	$u_{\alpha\beta}v_{\gamma\delta}+v_{\alpha\beta}u_{\gamma\delta}$ 的因數	$\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}$ 解與方程式	$\omega_{\alpha\beta}\omega_{\gamma\delta}$ 解與方程式
(1)	p_1	p_2	$\frac{\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}}{p_1^m}$ $x^2-ky^2=p_1^{\lvert\alpha-m\rvert}p_2^{\beta+\delta}$	$\frac{\omega_{\alpha\beta}\omega_{\gamma\delta}}{p_2^n}$ $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{\lvert\beta-n\rvert}$
(2)	p_2	p_1	$\frac{\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}}{p_2^n}$ $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{\lvert\beta-n\rvert}$	$\frac{\omega_{\alpha\beta}\omega_{\gamma\delta}}{p_1^m}$ $x^2-ky^2=p_1^{\lvert\alpha-m\rvert}p_2^{\beta+\delta}$
(3)	p_1p_2	1	$\frac{\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}}{p_1^mp_2^n}$ $x^2-ky^2=p_1^{\lvert\alpha-m\rvert}p_2^{\lvert\beta-n\rvert}$	$\omega_{\alpha\beta}\omega_{\gamma\delta}$ $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{\beta+\delta}$
(4)	1	p_1p_2	$\overline{\omega_{\alpha\beta}}\omega_{\gamma\delta}$ $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{\beta+\delta}$	$\frac{\omega_{\alpha\beta}\omega_{\gamma\delta}}{p_1^mp_2^n}$ $x^2-ky^2=p_1^{\lvert\alpha-m\rvert}p_2^{\lvert\beta-n\rvert}$

【**定理 3.5.1**】會在一開始就在這章節出現出現，是因為我們還發現當 p_1p_2 是一個佩爾質數時，且在最低次方解 $n=3$ 的情況下，利用程式計算的結果，$x^2-ky^2=p_1^2p_2$、$x^2-ky^2=p_1p_2^2$、$x^2-ky^2=p_1^2p_2^2$，也會有正整數解。因此，我們便根據以上所觀測到的這個現象，開始了我們的研究，而【**定理 3.5.1**】便是我們主要使用的工具。

現在回到蜈蚣兗的情況，我們先考慮兩個有蜈蚣兗現象的質數；也就是對於某個正整數 $n>1$，$L_{irr}(k,p_1^n)=L_{irr}(k,p_2^n)=3$。首先，若將【**定理 3.5.1**】中的 (γ,δ) 改為 $(n,0)$ 或是 $(0,n)$，則我們有下面的結果：

【定理 3.5.2】

設 $\omega_1=u_1+v_1\sqrt{k}$ 是方程式 $x^2-ky^2=p_1^n$ 的一個不可約解。若 α 和 β 均是任意正整數，且

$\omega_\alpha = u_\alpha + v_\alpha\sqrt{k}$ 是 $x^2 - ky^2 = p_1^\alpha p_2^\beta$ 的一個不可約解，則

$$\frac{\omega_\alpha \omega_1}{p_1^{\min\{\alpha,n\}}} \text{ 或 } \frac{\omega_\alpha \overline{\omega_1}}{p_1^{\min\{\alpha,n\}}}$$

會是 $x^2 - ky^2 = p_1^{|\alpha-n|} p_2^\beta$ 的一個不可約解；同樣的，若 $\omega_2 = u_2 + v_2\sqrt{k}$ 是方程式 $x^2 - ky^2 = p_2^n$ 的一個不可約解，則

$$\frac{\omega_\alpha \omega_2}{p_2^{\min\{\beta,n\}}} \text{ 或 } \frac{\omega_\alpha \overline{\omega_2}}{p_2^{\min\{\beta,n\}}}$$

會是 $x^2 - ky^2 = p_1^\alpha p_2^{|\beta-n|}$的一個不可約解。

【備註 3.5.1】不可約解的前進與後退

關於以上的定理，我們發現了更多的結果。在上述定理中，下列其中之一個數對

$$\left(\frac{\omega_\alpha \overline{\omega_1}}{p_1^{\min\{\alpha,n\}}}, \omega_\alpha \omega_1\right) \text{、} \left(\frac{\omega_\alpha \omega_1}{p_1^{\min\{\alpha,n\}}}, \omega_\alpha \overline{\omega_1}\right)$$

必定是不可約數對。如果就 $\alpha < n$ 和 $\alpha \geq n$ 再細分，就會有

$$\frac{\omega_\alpha \overline{\omega_1}}{p_1^{\min\{\alpha,n\}}} = \begin{cases} \dfrac{\omega_\alpha \overline{\omega_1}}{p_1^\alpha} = \dfrac{(\overline{\omega_\alpha} \cdot \omega_\alpha) \cdot \overline{\omega_1}}{\overline{\omega_\alpha} \cdot p_1^\alpha} = p_2^\beta \cdot \dfrac{\overline{\omega_1}}{\overline{\omega_\alpha}}, & \alpha < n \\ \dfrac{\omega_\alpha \overline{\omega_1}}{p_1^n} = \dfrac{\omega_\alpha \cdot (\overline{\omega_1} \cdot \omega_1)}{p_1^n \cdot \omega_1} = \dfrac{\omega_\alpha}{\omega_1}, & \alpha \geq n \end{cases}$$

以及

$$\frac{\omega_\alpha \omega_1}{p_1^{\min\{\alpha,n\}}} = \begin{cases} \dfrac{\omega_\alpha \omega_1}{p_1^\alpha} = \dfrac{(\overline{\omega_\alpha} \cdot \omega_\alpha) \cdot \omega_1}{\overline{\omega_\alpha} \cdot p_1^\alpha} = p_2^\beta \cdot \dfrac{\omega_1}{\overline{\omega_\alpha}}, & \alpha < n \\ \dfrac{\omega_\alpha \omega_1}{p_1^n} = \dfrac{\omega_\alpha \cdot (\omega_1 \cdot \overline{\omega_1})}{p_1^n \cdot \overline{\omega_1}} = \dfrac{\omega_\alpha}{\overline{\omega_1}}, & \alpha \geq n \end{cases}$$

也因此不可約解數對就可以改寫成

$$\left(\frac{\omega_\alpha \overline{\omega_1}}{p_1^{\min\{\alpha,n\}}}, \omega_\alpha \omega_1\right) = \begin{cases} \left(p_2^\beta \cdot \dfrac{\overline{\omega_1}}{\overline{\omega_\alpha}}, \omega_\alpha \omega_1\right), & \alpha < n \\ \left(\dfrac{\omega_\alpha}{\omega_1}, \omega_\alpha \omega_1\right), & \alpha \geq n \end{cases}$$

以及

$$\left(\frac{\omega_\alpha\omega_1}{p_1^{\min\{\alpha,n\}}},\omega_\alpha\overline{\omega_1}\right)=\begin{cases}\left(p_2^\beta\cdot\dfrac{\omega_1}{\overline{\omega_\alpha}},\omega_\alpha\overline{\omega_1}\right), & \alpha<n\\ \left(\dfrac{\omega_\alpha}{\overline{\omega_1}},\omega_\alpha\overline{\omega_1}\right), & \alpha\geq n\end{cases}$$

【備註 3.5.2】

在上面的證明，我們是先降 x 座標 (除以 $\widetilde{\omega_1}$)，再降 y 座標(除以 $\widetilde{\omega_2}$)，但其實這個步驟並沒有限制先後順序，不管誰先誰後，最後都會得到 $\omega_{\alpha\beta}=\widetilde{\omega_1}^{q_\alpha}\cdot\widetilde{\omega_2}^{q_\beta}\cdot\omega_{\alpha'\beta'}$。但至於甚麼時候是除以 ω_1 或是 $\overline{\omega_1}$，我們就不得而知了。

蜈蚣彘的指數 n 可以讓 p_1 的指數 α 前進和後退，這一概念引起了我們對 $\boldsymbol{\omega_\alpha}$ 分解的注意。當 $\alpha\geq n$ 時，假設 $\dfrac{\omega_\alpha\overline{\omega_1}}{p_1^{min\{\alpha,n\}}}$ 是一個不可約解；在這樣的情況下，ω_α 可以寫成 $\dfrac{\omega_\alpha\overline{\omega_1}}{p_1^n}$和 ω_1 兩個不可約解的乘積。我們繼續假設 $\alpha-n$ 仍大於等於 n。

我們持續對 $\dfrac{\omega_\alpha\overline{\omega_1}}{p_1^n}$ 進行相同的分解步驟，則根據 ω_α 的不可約性，$\dfrac{\omega_\alpha\overline{\omega_1}}{p_1^n}$ 只能寫成 $\omega'\cdot\omega_1$，其中 ω' 是方程式$x^2-ky^2=p_1^{\alpha-n}p_2^\beta$ 的不可約解，也因此我們會有

$$\omega_\alpha=\frac{\omega_\alpha\overline{\omega_1}}{p_1^n}\cdot\omega_1=(\omega'\cdot\omega_1)\cdot\omega_1=\omega'\cdot\omega_1^2$$

若將 α 除以 n 以 $q_\alpha\cdot n+\alpha'$ 表示，其中 $0\leq\alpha'<n$，那麼 ω_α 可以寫成 $\omega_1^{q_\alpha}\cdot\omega_{\alpha'}$， 其中 $\omega_{\alpha'}$ 是方程式$x^2-ky^2=p_1^{\alpha'}p_2^\beta$ 的不可約解；同樣的，當 $\alpha\geq n$ ，若$\dfrac{\omega_\alpha\omega_1}{p_1^{min\{\alpha,n\}}}$ 為不可約時，以上論述一樣成立，也就是說ω_α 可以寫成 $\omega_1^{q_\alpha}\cdot\overline{\omega_{\alpha'}}$， 其中 $\overline{\omega_{\alpha'}}$ 是方程式 $x^2-ky^2=p_1^{\alpha'}p_2^\beta$ 的不可約解。總結以上論述，我們會有：

【定理 3.5.3】

對於正整數 $i=1$ 或 2，設 ω_i 是方程式 $x^2-ky^2=p_i^n$ 的一個不可約解。若 α 和 β 均是任意正整數，且 ω 是 $x^2-ky^2=p_1^\alpha p_2^\beta$ 的一個不可約解，則

$$\omega=\widetilde{\omega_1}^{q_\alpha}\cdot\widetilde{\omega_2}^{q_\beta}\cdot\omega_{\alpha'\beta'}$$

其中 $\alpha = q_\alpha \cdot n + \alpha'$，$\beta = q_\beta \cdot n + \beta'$、$0 \le \alpha'$、$\beta' < n$、$\widetilde{\omega_*} = \omega_*$ 或 $\overline{\omega_*}$ ，以及 $\omega_{\alpha'\beta'}$ 是$x^2 - ky^2 = p_1^{\alpha'} p_2^{\beta'}$ 的一個不可約解。

根據【**定理 3.5.3**】，簡而言之，對於某個正整數 $n > 1$，方程式 $x^2 - ky^2 = p_1^n$ 和 $x^2 - ky^2 = p_2^n$ 皆有蜈蚣螮現象的狀況底下，方程式 $x^2 - ky^2 = p_1^\alpha p_2^\beta$ 的不可約解必定可以被分解成為 $x^2 - ky^2 = p_1^{\alpha'} p_2^{\beta'}$ 的一個不可約解與 $x^2 - ky^2 = p_1^n$ 和$x^2 - ky^2 = p_2^n$ 解的冪次的乘積。

在繼續接下來的討論以前，為了方便起見，我們，給出了以下的三個定義：

【定義 3.5.1】

對於給定的質數 (k, p_1, p_2)，數對 (α, β) 指的是 $x^2 - ky^2 = p_1^\alpha p_2^\beta$ 這個方程式。

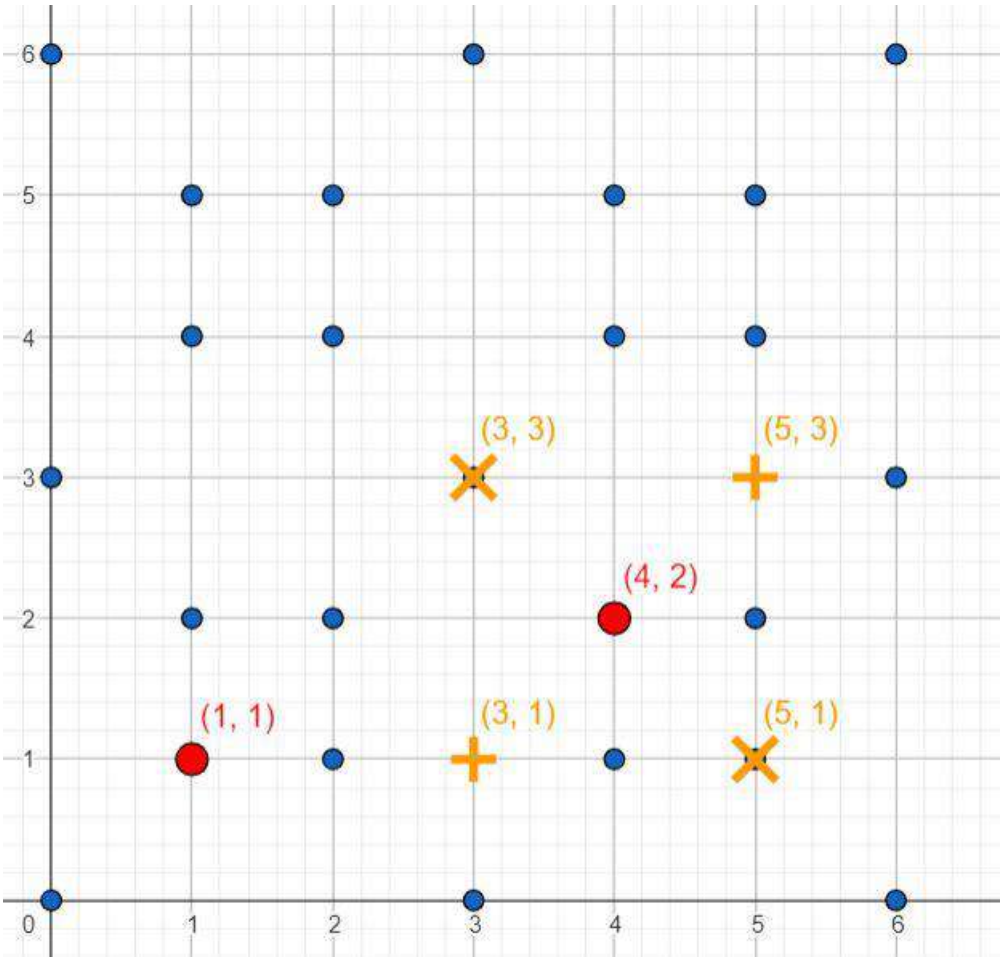
利用以上的定義，我們將【**定理 3.5.1**】以函數方式呈現如下：

【定義 3.5.2】Φ 函數

令以下的 (1)、(2) 以及 (3)、(4) 是泛指出現在【**定理 3.5.1**】的四種情況，則我們定義函數

$$\Phi_{(\gamma,\delta)}(\alpha, \beta) = \begin{cases} (|\alpha - \gamma|, \beta + \delta) \text{ 與 } (\alpha + \gamma, |\beta - \delta|) & \text{當(1)、(2)成立} \\ (|\alpha - \gamma|, |\beta - \delta|) \text{ 與 } (\alpha + \gamma, \beta + \delta) & \text{當(3)、(4)成立} \end{cases}$$

以下利用圖示對函數 $\Phi_{(\gamma,\delta)}(\alpha, \beta)$ 進行說明：



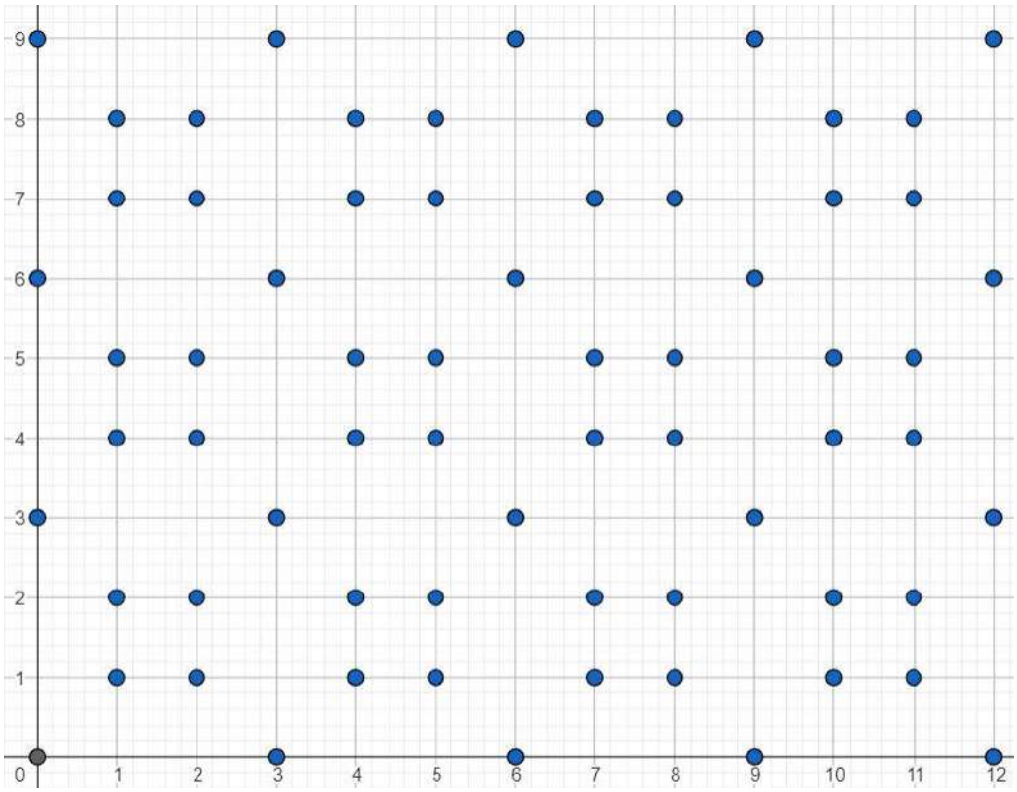
上圖中，紅色圓點代表的是 $(\alpha,\beta)=(1,1)$ 和 $(\gamma,\delta)=(4,2)$，橘色交叉是 $x^2-ky^2=p_1^{|\alpha-\gamma|}p_2^{\beta+\delta}$ 與 $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{|\beta-\delta|}$ 有解的情況，這時我們可以說 $\Phi_{(1,1)}(4,2)=(3,3)$ 與 $(5,1)$；而橘色加號是 $x^2-ky^2=p_1^{|\alpha-\gamma|}p_2^{|\beta-\delta|}$ 與 $x^2-ky^2=p_1^{\alpha+\gamma}p_2^{\beta+\delta}$ 有解的情況，這時我們可以說 $\Phi_{(1,1)}(4,2)=(3,1)$ 與 $(5,3)$

同樣利用**【定義 3.5.1】**，我們可以將所有形如 $x^2-ky^2=p_1^Xp_2^Y$ 且有不可約解廣義佩爾方程式圖像化，我們就將其稱為佩爾地毯：

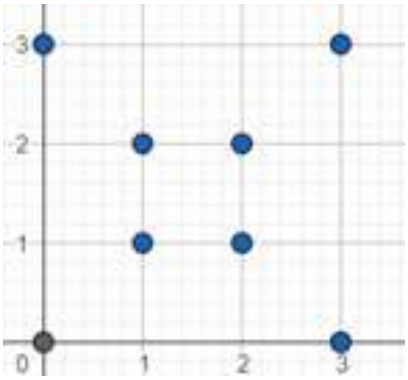
【定義 3.5.3】佩爾地毯

對於所有非負整數 X,Y，由所有有不可約解的廣義佩爾方程式 (X,Y) 所構成的集合稱為佩爾地毯。

以$x^2-37y^2=3^X7^Y$為例，下圖就是該類型方程式所對應到的佩爾地毯：



在上圖，藍色的點代表的是有不可約解的方程式，我們可以發現整個地毯似乎存在著相同的結構。也就是說，從圖形上來看，地毯可以利用下圖拼貼出來：



利用**【定理 3.5.3】**，我們可以將佩爾地毯上的任一點$(\alpha,\beta)=(nq_\alpha+\alpha',nq_\beta+\beta')$對應到$[0,n]\times[0,n]$中的一個整數數對$(\alpha',\beta')$；反過來，若固定$[0,n]\times[0,n]$中的一個整數數對$(\alpha',\beta')$，對於任意的非負整數數對$(q_\alpha,q_\beta)$，方程式$(\alpha,\beta)=(nq_\alpha+\alpha',nq_\beta+\beta')$都會是一個有不可約解的方程式，那麼我們就可以利用在$[0,n]\times[0,n]$中有不可約解的數對(α',β')，『複製貼上』進而產生出整張佩爾地圖。事實上，以下的**【定理 3.5.1】**，不僅僅證明了對於任

意的非負整數數對 (q_α, q_β)，$(\alpha,\beta)=(nq_\alpha+\alpha', nq_\beta+\beta')$ 都會是一個有不可約解的方程式以外，還證明了 $L_{irr}\left(k, p_1^{nq_\alpha+\alpha'}p_2^{nq_\beta+\beta'}\right)=L_{irr}(k,p_1^{\alpha'}p_2^{\beta'})$。

【定理 3.5.4】

$x^2-ky^2=p_1^\alpha p_2^\beta$ 的不可約解與 $x^2-ky^2=p_1^{\alpha+n}p_2^\beta$ 的不可約解是一一對應的。

【證明】

利用**【推論 3.5.1】**的結果

$$\left(\frac{\omega_\alpha\overline{\omega_1}}{p_1^{\min\{\alpha,n\}}},\omega_\alpha\omega_1\right)=\begin{cases}\left(p_2^\beta\cdot\dfrac{\overline{\omega_1}}{\overline{\omega_\alpha}},\omega_\alpha\omega_1\right), & \alpha<n\\ \left(\dfrac{\omega_\alpha}{\omega_1},\omega_\alpha\omega_1\right), & \alpha\geq n\end{cases}$$

若我們從 $(\alpha+n,\beta)$ 中任意挑選一個不可約解 ω_α，那麼存在一個 $\widetilde{\omega_1}\in\{\omega_1,\overline{\omega_1}\}$，使得

$$\frac{\omega_\alpha\cdot\widetilde{\omega_1}}{p_1^{\min\{\alpha,n+\alpha\}}}=\frac{\omega_\alpha}{\widetilde{\overline{\omega_1}}}$$

是 (α,β) 中的一個不可約解，因此我們可以在 $(\alpha+n,\beta)$ 和 (α,β) 之間的不可約解定義一個函數

$$\omega_\alpha\longrightarrow\frac{\omega_\alpha}{\widetilde{\overline{\omega_1}}}$$

相反的，在**【定理 3.5.1】**的證明中，對於在 (α,β) 中任意一個不可約解 ω_α，存在一個 $\widehat{\omega_1}\in\{\omega_1,\overline{\omega_1}\}$，使得 $\omega_\alpha\cdot\widehat{\omega_1}$是 $(\alpha+n,\beta)$ 的一個不可約解。如此我們可以在 (α,β) 和 $(\alpha+n,\beta)$ 之間的不可約解定義一個函數

$$\omega_\alpha\longrightarrow\ \omega_\alpha\cdot\widehat{\omega_1}$$

很顯然的 $\widetilde{\omega_1}=\widehat{\omega_1}$，也因此 $(\alpha+n,\beta)$ 和 (α,β) 之間不可約解是一一對應的。故得證。■

利用**【定理 3.5.4】**對於$(\alpha+n,\beta)$ 不可約解的探討，我們可以將 $(nq_\alpha+\alpha', nq_\beta+\beta')$ 縮編到方程式(α',β') 的不可約解的討論，其中 (α',β') 是在 $[0,n]\times[0,n]$ 中的一個整數數對。同樣的，為了接下來的討論能夠方便起見，我們有以下的定義：

【定義 3.5.3】基本區域

設 k、p_1 和 p_2 是三個相異的奇質數，且對於某個正奇數 n，會有 $L_{irr}(k,p_1^n)=L_{irr}(k,p_2^n)=2$。以下集合被稱為佩爾方程式 $x^2-ky^2=p_1^n$ 與 $x^2-ky^2=p_2^n$ 的基本區域：

$$F(k,p_1,p_2,n):=\{\,(s,t)\in[1,n-1]\times[1,n-1]\mid L_{irr}(k,p_1^sp_2^t)>0\,\}$$

【備註 3.5.3】

由於我們現在討論的內容是以蜈蚣兿為背景，以下就目前我們因為電腦技術上的有限，提出所受到的限制：

1. 過去曾證明蜈蚣兿的最小整數解必為奇數，而當時找到的例子，其最小整數解亦恰好是質數。然而，隨著質數 k 的增大，蜈蚣兿的尋找相當不易；事實上目前找到有蜈蚣兿現象的佩爾質數並不是很多，而且最小正整數解至多到 5。
2. 承上，對於一個固定的質數 k，所產生的最小正整數解是否為一定值或是有限集合也不得而知。
3. 同樣的，有蜈蚣兿現象的質數 k 或是固定後有蜈蚣兿現象的質數 p 是否有限也尚未明確。

因此，我們以下的討論只先討論兩個有相同最小正整數解均相同的蜈蚣兿；而根據這樣的設定，我們便將基本區域，考慮為在 $[1,n-1]\times[1,n-1]$ 中的子集合。另外，為了方便之後的討論，除了我們先前以數對 (α,β) 表示義佩爾方程式 $x^2-ky^2=p_1^\alpha p_2^\beta$ 以外，以下的符 $L_{irr}\big(k,(\alpha,\beta)\big)$、$L_{re}\big(k,(\alpha,\beta)\big)$以及 $L\big(k,(\alpha,\beta)\big)$，分別表示 $L_{irr}\left(k,p_1^\alpha p_2^\beta\right)$、$L_{re}\left(k,p_1^\alpha p_2^\beta\right)$ 以及 $L(k,p_1^\alpha p_2^\beta)$。

根據之前的定理，我們應該對每個在基本區域中，每一個不可約解的方程式進行討論；以下就是有關這些方程式的一些結果。首先是在基本區域中，每個方程式其不可約解的結構：

【定理 3.5.5】

假設 $(\alpha,\beta)\in F(k,p_1,p_2,n)$ ，則

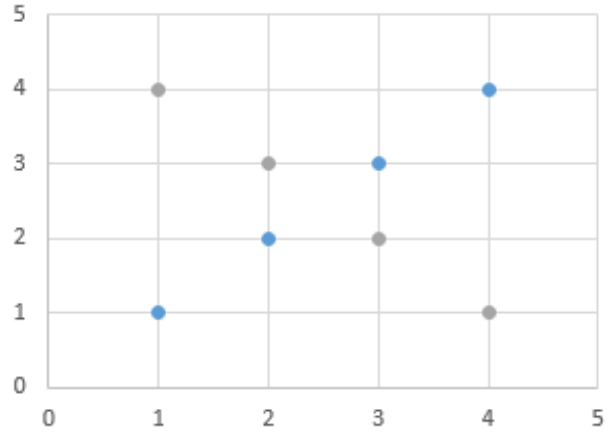
$$L_{irr}(k,(\alpha,\beta))=2$$

【證明】

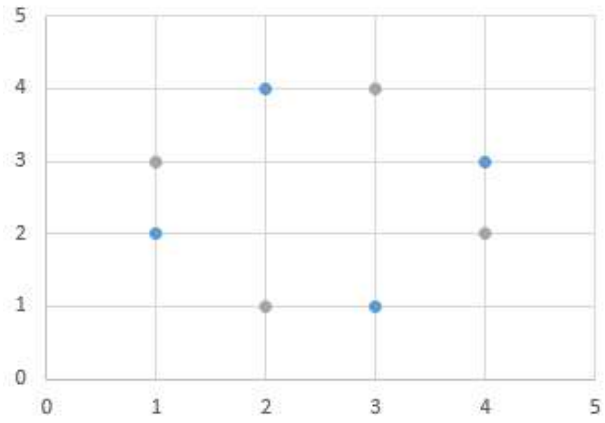
令 $\omega=u+v\sqrt{k}$ 與 $\omega'=u'+v'\sqrt{k}$ 是方程式 $x^2-ky^2=p_1^{\alpha}p_2^{\beta}$ 兩個相異的不可約解，則根據之前的定理可知，這兩個不可約解可衍生出 $(|\alpha-\alpha|,\beta+\beta)=(0,2\beta)$ 或 $(|\alpha-\alpha|,|\beta-\beta|)=(0,0)$ 的不可約解，前者 $(0,2\beta)$ 有不可約解的充要條件為 n 可整除 2β。由於 $(\alpha,\beta)\in F(k,p_1,p_2,n)$，$0<2\beta<2n$，因此 $2\beta=n$，但 n 為一奇數，故只有後者成立，也因此 $\omega'=\sigma^m\omega$ 或 $\omega'=\sigma^m\bar{\omega}$ ；故得證。■

對於**【定理 3.5.5】**，換句話說，在 $[1,n-1]\times[1,n-1]$ 之內有不可約解的方程式 (s,t)，其不可約解必形如 $\sigma^m\omega_{st}$ 或 $\sigma^n\overline{\omega_{st}}$，其中為 ω_{st} 是第一個正整數解，且 m 與 n 是任意整數。另外，若在**【定理 3.5.5】**中的 p_1 和 p_2 的最小整數解不同，結論依然成立。

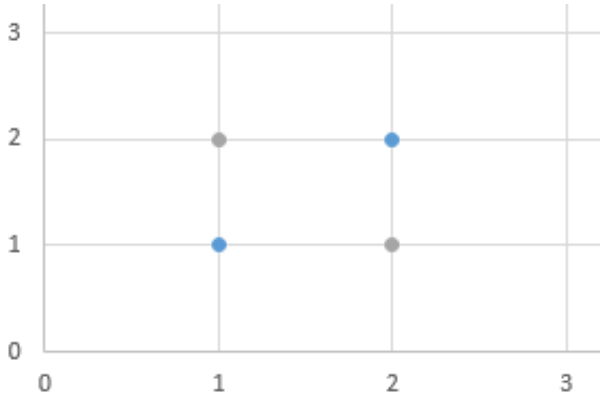
接下來，我們想要對 $F(k,p_1,p_2,n)$ 的『形狀』進行討論。下面是一些 $F(k,p_1,p_2,n)$ 的圖示：



$F(401,577,587,5)$



$F(401,5,7,5)$



$$F(37,3,7,3)$$

這裡舉了最低次方解 $n=5$ 和 $n=3$ 的蜈蚣兔，我們發現

- 最低次方解 $n=3$ 的佩爾地毯，剛好只有一種形狀
- 最低次方解 $n=5$ 的佩爾地毯，剛好只有兩種形狀
- 我們發現 $F(k,p_1,p_2,n)$ 似乎是一個線對稱圖形對稱軸可能會是水平線（$y=1.5$；$y=2.5$）、垂直線（$x=1.5$；$x=2.5$）以及 $45°$ 線（$x=y$），對方程式來說就是

$$x^2-ky^2=p_1^{\alpha}p_2^{\beta} \text{ 有不可約解} \Longrightarrow \begin{cases} x^2-ky^2=p_1^{\alpha}p_2^{n-\beta} \text{ 有不可約解 (對稱於水平線)} \\ x^2-ky^2=p_1^{n-\alpha}p_2^{\beta} \text{ 有不可約解 (對稱於垂直線)} \\ x^2-ky^2=p_1^{\beta}p_2^{\alpha} \quad \text{有不可約解 (對稱於 } 45° \text{ 線)} \end{cases}$$

對於水平線與垂直線對稱的現象，我們有以下結果：

【定理 3.5.6】

假設 $(\alpha,\beta)\in F(k,p_1,p_2,n)$ ，則 $(n-\alpha,\beta),(\alpha,n-\beta),(n-\alpha,n-\beta)\in F(k,p_1,p_2,n)$ 。

【證明】

由於 $\Phi_{(n,0)}(\alpha,\beta)=\big((n-\alpha,\beta),(n+\alpha,\beta)\big)$ 或 $\big((n-\alpha,\beta),(\alpha,\beta)\big)$，因此無論哪一種情況，$(n-\alpha,\beta)$ 都會有不可約解；也就是說 $(n-\alpha,\beta)\in F(k,p_1,p_2,n)$；若考慮 $\Phi_{(0,n)}(\alpha,\beta)$，亦可以得到 $(\alpha,n-\beta)\in F(k,p_1,p_2,n)$，證明於前面類似，故省略。■

【備註 3.5.4】

若最小正整數解不同，即 $L_{irr}\big(k,p_1^{n_1}\big)=L_{irr}\big(k,p_2^{n_2}\big)=2$ 且 $n_2>n_1$，則當

$$(\alpha.\beta)\in[1,n_1-1]\times[1,n_2-1] \text{ 且 } L_{irr}\big(k,(\alpha,\beta)\big)>0 \text{ 時}$$

會有

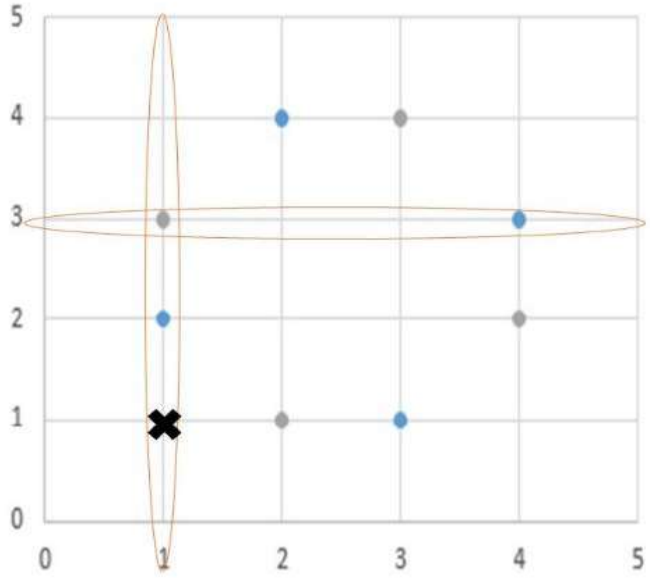
$$L_{irr}(k,(n_1-\alpha,\beta))\cdot L_{irr}\big(k,(\alpha,n_2-\beta)\big)\cdot L_{irr}(k,(n_1-\alpha,n_2-\beta))>0$$

然而，對於 $L_{irr}(k,(\alpha,\beta))>0$ 是否為 $L_{irr}(k,(\beta,\alpha))>0$的充分必要條件，我們目前並未找到證明，而手邊也並無反例否定這猜想。關於這部分，我們後面會在探討。接著，下面的定理表示，在基本區域中的水平線或是垂直線上，一定只會有兩個有不可約解的佩爾方程式。

【定理 3.5.7】

假設 (α,β) 與 (α',β') 為 $F(k,p_1,p_2,n)$ 中兩點，若 $\alpha'=\alpha$，則 $\beta'=\beta$ 或 $\beta'=n-\beta$（同樣的，若 $\beta'=\beta$，則 $\alpha'=\alpha$ 或 $\alpha'=n-\alpha$）。

【證明】



我們利用反證法，假設固定一條鉛垂線，有第三個點也有不可約解，那我們假設該點為 (α,β'')，其中 $\beta''\not\equiv\pm\beta \pmod n$。接著假設該方程式 $x^2-ky^2=p_1^{\alpha}p_2^{\beta''}$ 的解為 $\omega_{\alpha\beta''}=u_{\alpha\beta''}+v_{\alpha\beta''}\sqrt{k}$，那麼 $\Phi_{(\alpha,\beta)}(\alpha,\beta'')=(0,\beta+\beta'')$ 與 $(2\alpha,|\beta-\beta''|)$ 或者 $(0,|\beta-\beta''|)$ 與 $(2\alpha,\beta+\beta'')$。可以發現兩種狀況都會有其中一個指數是 0 的情況，也就是蜈蚣兔，這代表 $\beta+\beta''\equiv 0 \pmod n$ 或 $\beta-\beta''\equiv 0 \pmod n$ 但這兩種情況分別會得到 $\beta''\equiv n-\beta \pmod n$ 或 $\beta''\equiv\beta \pmod n$，與前面假設矛盾，因此不可能有第三個點在一條水平線與垂直線上。故得證。■

由於我們可以利用佩爾方程式 $x^2-ky^2=p_1^sp_2^t$ 的任一不可約解 ω，產生出佩爾方程式 $x^2-ky^2=(p_1^sp_2^t)^u$ 的一個不可約解 ω^u，再利用 $\Phi_{(n,0)}$ 以及 $\Phi_{(0,n)}$ 對 ω^u 的作用，產生出一個在 $F(k,p_1,p_2,n)$ 的佩爾方程式（同樣的，以上的操作對於有著不同最小整數解的情況也成立）。

至此，利用上面的定理與論述，我們漸漸地可以將 $F(k,p_1,p_2,n)$ 的點產生出來。由於 p_1 和 p_2 都具有蜈蚣兿性質，且 $L_{irr}(k,p_i^t)>0$ 若且為若 $t=m_t\cdot n$，其中 $m_t\in\mathbb{N}\cup\{0\}$，我們不禁聯想到是否可以將這『一維』的情況推廣到『二維』，也就是說若 $(t,s)\in F(k,p_1,p_2,n)$

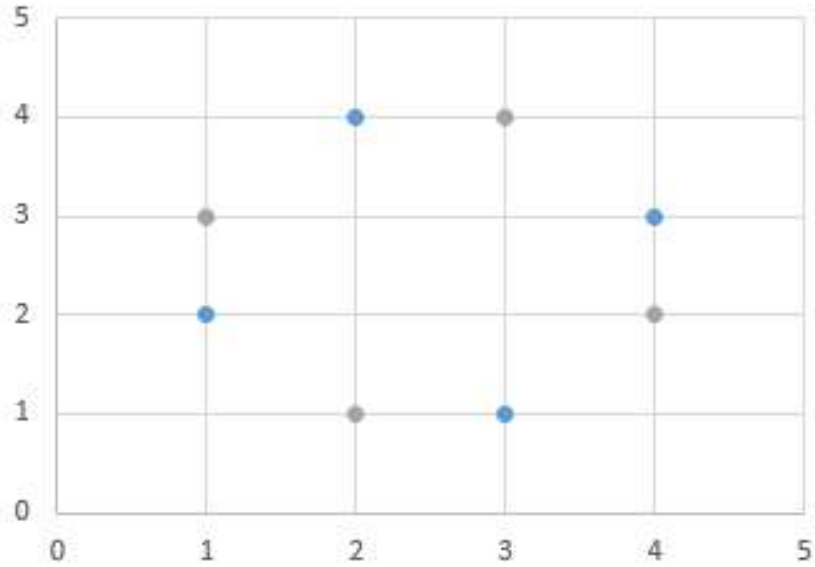
$$L_{irr}(k,p_1^t\cdot p_2^s)>0 \text{ 若且為若 } ([t],[s])=m_t\cdot([\alpha],[\beta])\text{，其中 } m_t\in\mathbb{N}\cup\{0\}$$

然而，$F(401,577,587,5)$ 的圖示否定了我們的猜想。話雖如此，我們依然嘗試著利用『一維』的證明思路，對推『二維』的情況進行探討，最後得到了 $F(k,p_1,p_2,n)$ 的樣子。接下來，為了說明方便，我們定義

$$\alpha=\min\left\{s\,|(s,t)\in F(k,p_1,p_2,n)\right\}\text{ 以及 }\beta=\min\left\{t\,|(s,t)\in F(k,p_1,p_2,n)\right\}$$

也就是說，α 和 β 是 $F(k,p_1,p_2,n)$ 中最小的 x 座標與 y 座標。雖然，$F(k,p_1,p_2,n)$ 不能用某一個點而生成，但我們猜想是否可以由 $F(k,p_1,p_2,n)$ 中的 (α,y) 和 (x,β) 所產生。以 $F(401,5,7,5)$ 為例，該集合中的佩爾方程式有以下八個

$$\left\{(1,2),(2,1),(3,1),(1,3),(4,2),(2,4),(3,4),(4,3)\right\}$$



其中 $(\alpha,y)=(1,2)\ \left(\text{或}(1,3)\right)$ 以及 $(x,\beta)=(2,1)\ \left(\text{或}(3,1)\right)$。則 $F(401,5,7,5)$ 等於

$$\left\{P\big(t(1,2)\big)|\ t=1,2,3,4\right\}=\left\{([1],[2]),([2],[4]),([3],[1]),([4],[3])\right\}$$

與

$$\left\{P\big(t(2,1)\big)|\ t=1,2,3,4\right\}=\left\{([2],[1]),([4],[2]),([1],[3]),([3],[4])\right\}$$

的聯集；也因此 $F(401,5,7,5)$ 便可用 $(1,2)$ 和 $(2,1)$ 所生成。以下，我們便試著證明 $F(k,p_1,p_2,n)$ 可由其中的 (α,y) 和(x,β)所產生。首先，我們需要以下的引理：

【引理 3.5.1】

設 $L_{irr}\big(k,(A,B)\big)>0$ ，則 $A\equiv 0 \bmod n$ 若且為若 $B\equiv 0 \bmod\ n$。

【證明】

假設 $nA'=A$，對於任意的 $m=0,\cdots,A'$，會有

$$L_{irr}\left(k,\Phi_{(n,0)}^{m}(A,B)\right)=L_{irr}(k,(A-mn,B))>0$$

故當 $m=A'$ 時，$L_{irr}(k,(0,B))>0$；這也就是說方程式 $x^2-ky^2=p_2^B$ 會有不可約解，也因此我們就證明了 n 是 B 的因數；反之亦然。故得證。■

接著來到下面的定理：

【定理 3.5.8】

設 $(s,t)\in F(k,p_1,p_2,n)$ 中的一點，則 s 和 t 分別為 α 和 β 的倍數。

【證明】

以下我們只說明 s 是 α 的倍數，至於 t 為 β 的倍數之證明與其相似，故不多加贅述。根據 α 的定義，我們可以假設 $(\alpha,u)\in F(k,p_1,p_2,n)$ 且 $s=\alpha q+r$，其中 $0\le r<\alpha$；接下來，我們要試著證明 $r=0$。將$\Phi_{(\alpha,u)}$ 作用在上 (s,t)，則 $\Phi_{(\alpha,u)}(s,t)=(s-\alpha,b_1)$會是不可約解解數對，其中 $b_1=|u-t|$ 或是 $b_1=u+t$。我們根據以下情況來進行分析：

【情況一】若 $s-\alpha=0$，那麼 $s=\alpha$。

【情況二】當 $s-\alpha\neq 0$ 時，根據引理， b_1 不為 n 的倍數。我們再次將 $\Phi_{(\alpha,u)}$ 作用到 $\Phi_{(\alpha,u)}(s,t)$上，並假設 $\Phi_{(\alpha,u)}^{2}(s,t)=(s-2\alpha,b_2)$。若 $\Phi_{(\alpha,u)}^{2}(s,t)=(s-2\alpha,b_2)$ 滿

足相對應的情況一 $(s-2\alpha=0)$ 時，會有 $s=2\alpha$；若對 $\Phi^2_{(\alpha,u)}(s,t)$ 來說情況一並不滿足，則根據引理， b_2 不為 n 的倍數。再次考慮 $\Phi^3_{(\alpha,u)}(s,t)=(s-3\alpha,b_3)$，並將其與情況一作討論；若情況一並不成立，$b_3$ 必不為 n 的倍數，並且繼續重複上述步驟來討論。倘若對於 $1\le m\le q-1$，s 均與 $m\alpha$ 不同且 b_m 不為 n 的倍數，則考慮 $\Phi^q_{(\alpha,u)}(s,t)=\left(s-\alpha q,b_q\right)=(r,b_q)$。當情況一不成立的時候，此時會有 $0<r<\alpha$ 以及 $L_{irr}\left(k,(r,b_q)\right)>0$。現將 $\Phi^{\left[\frac{b_q}{n}\right]}_{(0,n)}$ 作用到 (r,b_q)，則會有$L_{irr}\left(k,(r,b_q-\left[\frac{b_q}{n}\right]\cdot n)\right)>0$ 也因此 $\left(r,b_q-\left[\frac{b_q}{n}\right]\cdot n\right)\in F(k,p_1,p_2,n)$。但這與的選取 α 有矛盾。因此，我們斷言 s 是 α 的倍數。故得證。■

接著，利用上面的定理，我們會得到接下來的兩個結果，這些結果可以讓我們充分的了解$F(k,p_1,p_2,n)$ 的樣子，以及可能出現的種類。首先是下面的定理：

【定理 3.5.9】

α 和 β 整除 n 。

【證明】

根據前面的定理可知，如果 (α,s) 是 $F(k,p_1,p_2,n)$ 中的一點，那麼 $(n-\alpha,s)$ 也會在 $F(k,p_1,p_2,n)$ 中，因此 α 是 n 的因數；同樣的，如果考慮 $(t,\beta)\in F(k,p_1,p_2,n)$，則點$(t,n-\beta)$ 也在 $F(k,p_1,p_2,n)$中，故 β 也可以整除 n。故得證。■

最後，**【定理 3.5.9】**可推演出以下的結果：

【定理 3.5.10】

$\alpha=\beta$

【證明】

根據上面的定理，我們可以假設 $(\alpha, \beta s)$ 和 $(\alpha t, \beta)$ 是 $F(k, p_1, p_2, n)$ 中最接近原點的兩點，又 α 和 β 均是 n 的因數，故我們可以假設存在兩個正整數 n_α 和 n_β，使得 $n = \alpha n_\alpha = \beta n_\beta$。因此 $P^{-1}([\alpha \cdot n_\beta], [\beta s \cdot n_\beta]) = \left(\alpha n_\beta - \left[\!\left[\frac{\alpha n_\beta}{n}\right]\!\right] \cdot n,\ 0\right)$ 會是一個有不可約解的佩爾方程式，其中 $[\![\ ]\!]$ 為最大整數函數 (***the greatest integer function***)。這表示 n 一定會整除 $\alpha n_\beta - \left[\!\left[\frac{\alpha n_\beta}{n}\right]\!\right] \cdot n$，也因此 $\alpha n_\beta = nl$。又 $n = \beta n_\beta$，所以

$$\alpha n_\beta = nl = \beta n_\beta l \Longrightarrow \alpha = \beta l$$

這便證明了 β 可以整除 α；同樣的利用 $P^{-1}([\alpha t \cdot n_\alpha], [\beta \cdot n_\alpha]) = \left(0, \beta n_\alpha - \left[\!\left[\frac{\beta n_\alpha}{n}\right]\!\right] \cdot n\right)$ 同樣可以證明 α 可以整除 β；故得證。■

根據以上的定理，我們知道在 $F(k, p_1, p_2, n)$ 中的點一定都形如 $(\alpha u, \alpha v)$；又 $\alpha \le \alpha u, \alpha v \le n - 1 < n = \alpha n_\alpha$，我們可以知道 $1 \le u, v < n_\alpha$。也就是說

$$F(k, p_1, p_2, n) = \left\{(\alpha u, \alpha v) \mid 1 \le u, v \le n_\alpha - 1\right\}$$

現在令 $(\alpha, \alpha s) \in F(k, p_1, p_2, n)$，且 $d = \mathrm{GCD}(s, n_\alpha)$，則我們可以假設 $s = dh_s$ 以及 $n_\alpha = dh_\alpha$。在這樣的假設下，$(\alpha h_\alpha, \alpha s h_\alpha)$ 也會有不可約解，然而 $\alpha s h_\alpha = \alpha d h_s h_\alpha = \alpha n_\alpha h_s = n h_s$，因此 n 必定整除 αh_α，又因為 $1 \le h_\alpha \le n_\alpha$，所以 $\alpha h_\alpha \le \alpha n_\alpha = n$。根據這些推論，我們便有 $n_\alpha = h_\alpha$；這代表了 $d = 1$，也就是說 s 和 n_α 互質。

現在，我們想說明 $\boldsymbol{F(k, p_1, p_2, n)}$ 等於

$$\left\{P([\alpha t], [\alpha s t]) \mid t = 1,2,\cdots, n_\alpha - 1\right\} \cup \left\{P([\alpha t], [-\alpha s t]) \mid t = 1,2,\cdots, n_\alpha - 1\right\}$$

顯然，$[\alpha t] = \alpha t$，如此一來我們只須說明 $[\alpha s t] \ne [-\alpha s t]$ 即可。若存在某個小於 n_α 的正整數 t，使得 n 整除 $2\alpha s t$，由於 $n = \alpha n_\alpha$ 且 n 為奇數，n_α 必整除 st。又 s 和 n_α 互質，所以 n_α 一定是 t 的因數，這與正整數 t 小於 n_α 矛盾；故 $P([\alpha t], [\alpha s t]) \ne P^{-1}([\alpha t], [-\alpha s t])$ 皆成立，其中 $1 \le t \le n_\alpha - 1$。

我們將上面的推論寫成下面的定理：

【定理 3.5.11】

在 $F(k,p_1,p_2,n)$ 中，$(\alpha,\alpha s)$ 與 n_α 如上面所定義，則

(1) s 與 n_α 互質。

(2) 對於 $F(k,p_1,p_2,n)$ 中的任一點 $(\alpha u,\alpha v)$，必唯一存在一個正整數 $t=1,2,\cdots,n_\alpha-1$，使得 $(\alpha u,\alpha v)$ 等於 $P^{-1}([\alpha t],[\alpha s t])$ 或 $P^{-1}([\alpha t],[-\alpha s t])$。

我們證明了許多有關佩爾質數的定理，只不過我們都只將範圍侷限在二維的佩爾地毯而已。若我們推廣到三維，並延續上一章節的前提以及定義，則在二維所發現的定理中，在三維的情況中，這些定理是否依然會成立？

首先，在二維的時候，我們利用$\Phi_{(\gamma,\delta)}(\alpha,\beta)$來獲得另外 1 種(或 2 種)分解，這會對應到另外 2 個(或 4 個)方程式的不可約解；那在三維的時候依據$p_1p_2p_3$ 整除 $u_{\alpha\beta}v_{\gamma\delta}-v_{\alpha\beta}u_{\gamma\delta}$ 與 $u_{\alpha\beta}v_{\gamma\delta}+v_{\alpha\beta}u_{\gamma\delta}$ 的情況，我們有四種可能的情況：

$$\Phi_{(\delta,\varepsilon,\zeta)}(\alpha,\beta,\gamma)=(|\alpha-\delta|,\beta+\varepsilon,\gamma+\zeta) \text{ 與 } (\alpha+\delta,|\beta-\varepsilon|,|\gamma-\zeta|)$$

$$\text{或 } (\alpha+\delta,|\beta-\varepsilon|,\gamma+\zeta) \text{ 與 } (|\alpha-\delta|,\beta+\varepsilon,|\gamma-\zeta|)$$

$$\text{或 } (\alpha+\delta,\beta+\varepsilon,|\gamma-\zeta|) \text{ 與 } (|\alpha-\delta|,|\beta-\varepsilon|,\gamma+\zeta)$$

$$\text{或 } (\alpha+\delta,\beta+\varepsilon,\gamma+\zeta) \text{ 與 } (|\alpha-\delta|,|\beta-\varepsilon|,|\gamma-\zeta|)$$

$\Phi_{(\delta,\varepsilon,\zeta)}(\alpha,\beta,\gamma)$特性都跟二維的情況類似，例如說 Φ 依然能夠保持不可約，這證明方法與二維的類似，我們就不多加贅述。跟二維稍微有點不同的是分解可能的情況從 2 種變成 4 種，會變得更加複雜，但我們基本上只會用到以下這三個函數 $\Phi_{(0,0,n)}(\alpha,\beta,\gamma)$、$\Phi_{(0,n,0)}(\alpha,\beta,\gamma)$、$\Phi_{(n,0,0)}(\alpha,\beta,\gamma)$，它們都有個特性，就是它們分解的那 4 種情況的結果都會一模一樣，一定都是 $\Phi_{(0,0,n)}(\alpha,\beta,\gamma)=(\alpha,\beta,n+\gamma)$ 與 $(\alpha,\beta,n-\gamma)$、$\Phi_{(0,n,0)}(\alpha,\beta,\gamma)=(\alpha,n+\beta,\gamma)$ 與 $(\alpha,n-\beta,\gamma)$、以及 $\Phi_{(n,0,0)}(\alpha,\beta,\gamma)=(n+\alpha,\beta,\gamma)$ 與 $(n-\alpha,\beta,\gamma)$，這跟二維的 $\Phi_{(n,0)}(\alpha,\beta)$ 以及 $\Phi_{(0,n)}(\alpha,\beta)$ 有相同的特性。在研究 $\Phi_{(n,0)}$ 和 $\Phi_{(0,n)}$ 的一開始，我們有發現 (α,β) 的解可以由 $(\alpha-sn,\beta-tn)$ 送來，並且兩者的不可約解的個數相等(詳見**【定理 3.5.4】**)，因此我們只須研究佩爾地毯的基本區域即可；在三維的情況下也是如此，只要證明這個定理推廣到三維後依然成立，我們就同樣只需要研究它的基本區域即可 $(1\le\alpha,\beta,\gamma\le n-1)$。

【定理 3.5.12】

若 α,β,γ 三者中至少有一個不小於 n，則 $x^2-ky^2=p_1^{\alpha}p_2^{\beta}p_3^{\gamma}$ 的不可約解可以由 $x^2-ky^2=p_1^{\alpha'}p_2^{\beta'}p_3^{\gamma'}$ 得到，其中 $(1\le\alpha',\beta',\gamma'\le n-1)$，並且兩方程式的不可約解個數相同。

【證明】

三維的證明方式與二維的情況相似。設 $\alpha>n$，並設 $\omega_1=u_1+v_1\sqrt{k}$ 是方程式 $x^2-ky^2=p_1^n$ 的一個不可約解， $\omega_{\alpha\beta\gamma}=u_{\alpha\beta\gamma}+v_{\alpha\beta\gamma}\sqrt{k}$ 是 $x^2-ky^2=p_1^{\alpha}p_2^{\beta}p_3^{\gamma}$ 的一個不可約解，則

$$\frac{\omega_{\alpha\beta\gamma}\omega_1}{p_1}\text{ 或 }\frac{\omega_{\alpha\beta\gamma}\overline{\omega_1}}{p_1}\text{會是 }x^2-ky^2=p_1^{\alpha-n}p_2^{\beta}p_3^{\gamma}\text{的一個不可約解。}$$

$$\omega_{\alpha\beta\gamma}\overline{\omega_1}\text{ 或 }\omega_{\alpha\beta\gamma}\omega_1\text{會是 }x^2-ky^2=p_1^{\alpha+n}p_2^{\beta}p_3^{\gamma}\text{的一個不可約解。}$$

他們是不可約解以及兩方程式的不可約解個數相同的證明方法與二維的情況相似，在此就不加贅述。故得證。■

同樣地，我們也可以根據上面的性質，來得到更完整的結果，可以更了解基本區域以外的點：

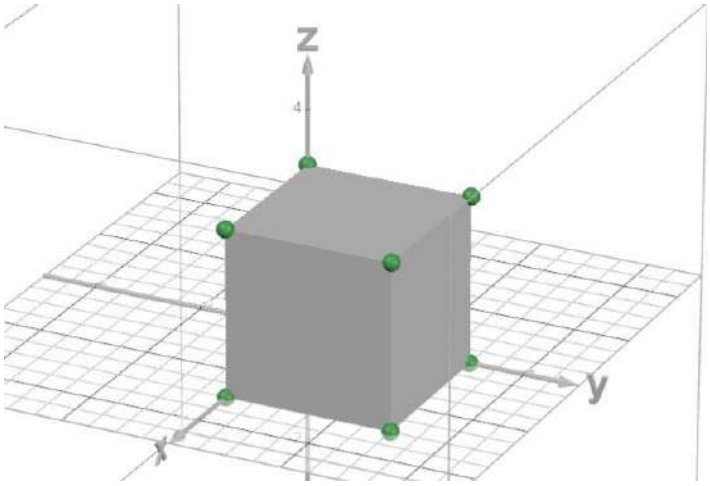
【定理 3.5.13】

設 ω_i 是方程式 $x^2-ky^2=p_i^n$ 的一個不可約解。若 $\alpha,\beta\ge n$，且 $\omega_{\alpha\beta\gamma}$ 是 $x^2-ky^2=p_1^{\alpha}p_2^{\beta}p_3^{\gamma}$ 的一個不可約解，則

$$\omega_{\alpha\beta\gamma}=\widetilde{\omega_1}^{q_\alpha}\cdot\widetilde{\omega_2}^{q_\beta}\cdot\widetilde{\omega_3}^{q_\gamma}\cdot\omega_{\alpha'\beta'\gamma'}$$

其中 $\alpha=q_\alpha\cdot n+\alpha'$，$\beta=q_\beta\cdot n+\beta'$，$\gamma=q_\gamma\cdot n+\gamma'$、$0\le\alpha',\beta',\gamma'<n$、$\widetilde{\omega_*}=\omega_*$ 或 $\overline{\omega_*}$，以及 $\omega_{\alpha'\beta'\gamma'}$ 是 $x^2-ky^2=p_1^{\alpha'}p_2^{\beta'}p_3^{\gamma'}$ 的一個不可約解。

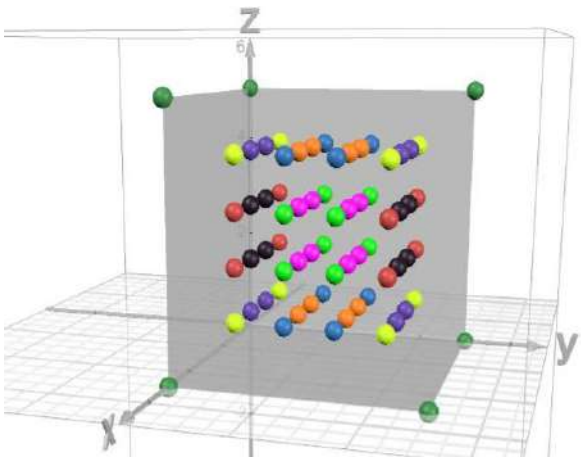
既然基本區域以外的點都可以由基本區域得到，那麼我們就針對基本區域做研究，就可以了解 $x^2-ky^2=p_1^{\alpha}p_2^{\beta}p_3^{\gamma}$ 的所有解了。



這是三維空間中的基本區域(不含邊界)，它是 $n \times n \times n$ 的方塊中有不可約解的點集合。目前我們在上一節了解了 xy 平面、 xz 平面、 yz 平面上佩爾地毯的形狀，若我們將這三個面上的點分別用$\Phi_{(0,0,n)}(x,y,0)$、$\Phi_{(0,n,0)}(x,0,z)$、$\Phi_{(n,0,0)}(0,y,z)$作用，會送到該平面的對面，因此 $x=n$、$y=n$、$z=n$ 平面的形狀我們也了解了。現在我們需要了解的是 $x,y,z \in [1,n-1]$，這個基本區域的形狀，總共包含了 $(n-1)^3$ 個點。以下我們先以 3-次方蜈蚣螺與 5-次方蜈蚣螺作為例子，對它們做研究，我們就先從二維中鉛直線、水平線對稱的這個定理開始做延伸：

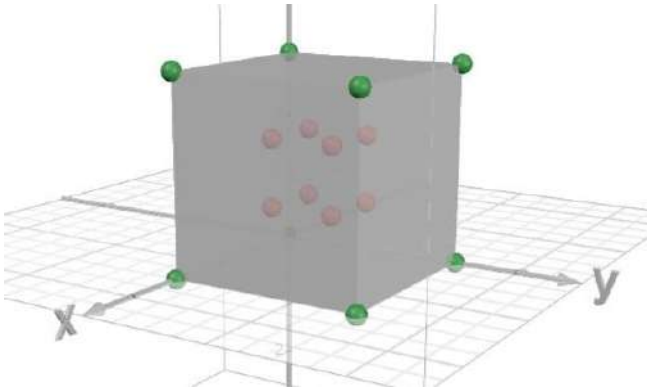
【定理 3.5.14】

假設 $(\alpha,\beta,\gamma) \in F(k,p_1,p_2,p_3,n)$ ，則與該點對稱的另外 7 個點，也會屬於基本區域，也就是說 $(\alpha,\beta,\gamma),(n-\alpha,\beta,\gamma),(\alpha,n-\beta,\gamma),(n-\alpha,n-\beta,\gamma),(\alpha,\beta,n-\gamma),(n-\alpha,\beta,n-\gamma),(\alpha,n-\beta,n-\gamma),(n-\alpha,n-\beta,n-\gamma) \in F(k,p_1,p_2,p_3,n)$ (見下圖相同顏色的點)



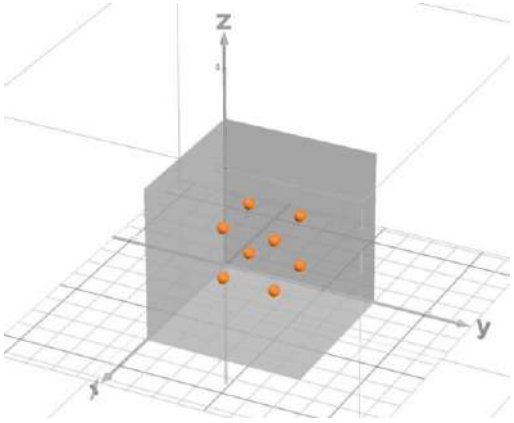
【證明】

由於 $\Phi_{(0,0,n)}(\alpha,\beta,\gamma)=(\alpha,\beta,n+\gamma)$ 與 $(\alpha,\beta,n-\gamma)$、$\Phi_{(0,n,0)}(\alpha,\beta,\gamma)=(\alpha,n+\beta,\gamma)$ 與 $(\alpha,n-\beta,\gamma)$、和 $\Phi_{(n,0,0)}(\alpha,\beta,\gamma)=(n+\alpha,\beta,\gamma)$ 與 $(n-\alpha,\beta,\gamma)$，若某一點有不可約解，那麼經由這三



個函數送到的點在繼續被這些函數作用會後就可以得到以上 8 個點，因此以上這 8 個點會是

互相存在的，了解其中一個點的不可約解就等於了解與他對應的 7 個點的不可約解。那麼我們所需了解的點的數量就從$(n-1)^3$個點，變少為$\frac{(n-1)^3}{8}$個點。故得證。■



我們以 3-次方蜈蚣兿作為例子：我們還不了解的地方從 8 個點變成 1 個點(見左圖)，只要了解其中一個點即可，我們在下個定理會證明 3-次方蜈蚣兿在三維的形狀只有一種。根據我們的前提，我們已知在 3-次方蜈蚣兿時，任意兩個蜈蚣兿相乘會得到佩爾質數，我們會利用我們在二維中已知的形狀來推得三維的形狀。

【定理 3.5.15】

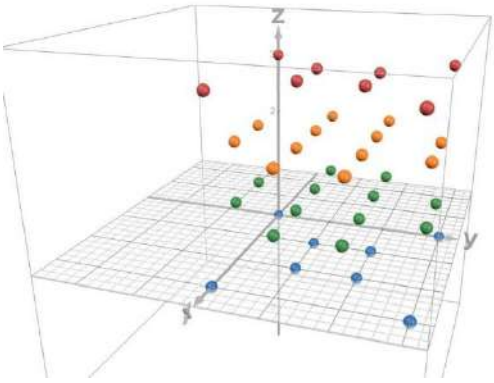
3-次方蜈蚣兿的形狀只有一種：裡面的那 8 個點一定是實心的。

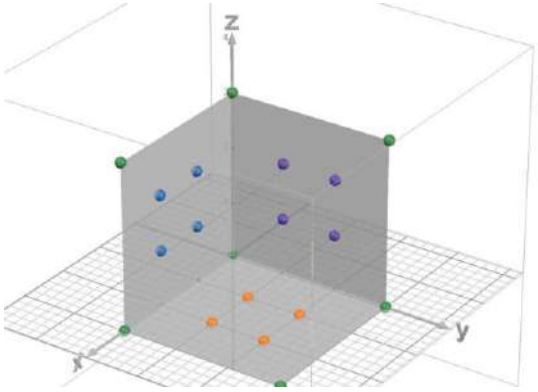
【證明】

我們可以用 $x^2-ky^2=p_1p_2$ 作用在 $x^2-ky^2=p_2p_3$ 上，也就是 $\Phi_{(1,1,0)}(0,1,1)$ 必屬於下列集合：$\{(1,2,1)(1,0,1)\ (1,0,1)(1,2,1)\}$

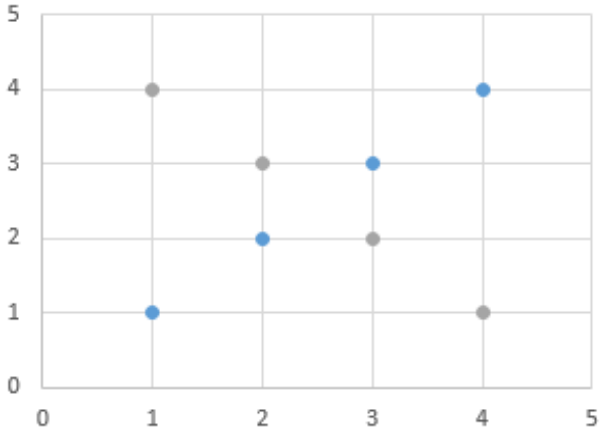
因此 $\Phi_{(1,1,0)}(0,1,1)=(1,2,1)$ 與 $(1,0,1)$

我們確定了 $(1,2,1)$ 有解，這恰好是基本區域中其中一個點，根據**【定理 3.5.14】**我們證明了中間那 8 個點有不可約解。故得證。■

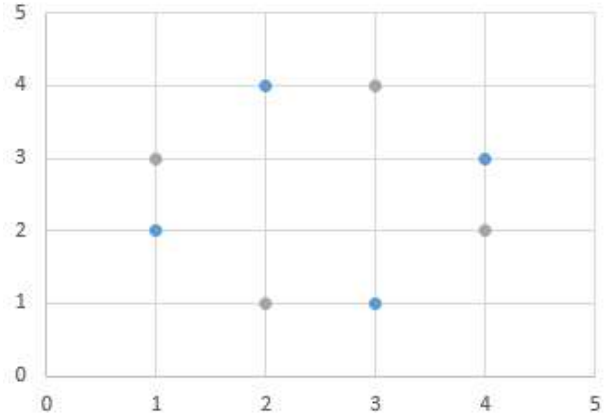




在【定理 3.5.9】～【定理 3.5.13】，我們證明 3-次方蜈蚣彘的地毯只有一種；5-次方蜈蚣彘的地毯只有兩種。那麼拓展到三維，剛剛證明了 3-次方蜈蚣彘也剛好只有一種。證明的過程中，我們發現裡面的點似乎跟 xy 平面、 xz 平面、 yz 平面上佩爾地毯的形狀有關，於是我們研究了面與面之間個關係。接下來，我們就以 5-次方蜈蚣彘兩種不同的佩爾地毯形狀來嘗試。



Type 1



Type 2

我們若選取兩片地毯出來作用，總共有三種選法，分別為Type 1 × Type 1、Type 1 × Type 2 、Type 2 × Type 2，以下就個別請況討論：

Case1 Type 1 × Type 1

選取 $x^2 - ky^2 = p_1p_2$ 和 $x^2 - ky^2 = p_2p_3$ 這兩個 Type 1 的方程式，用**【定理 3.5.15】**中的 $\Phi_{(1,1,0)}(0,1,1) = (1,2,1)$ 與 $(1,0,1)$，可以得到 $x^2 - ky^2 = p_1p_3$ 的不可約解，因此三面都會是Type 1。

Case2 Type 1 × Type 2

選取$x^2 - ky^2 = p_1p_2$ 和 $x^2 - ky^2 = p_2p_3^2$ ，$\Phi_{(1,1,0)}(0,1,2)$ 的四種情況剛剛好都會相同

$$\Phi_{(1,1,0)}(0,1,2) = (1,2,2) \text{ 與 } (1,0,2)$$

我們得到了 $x^2 - ky^2 = p_1p_3^2$ 的不可約解，這只會出現在 Type 2 上，因此我們找出第

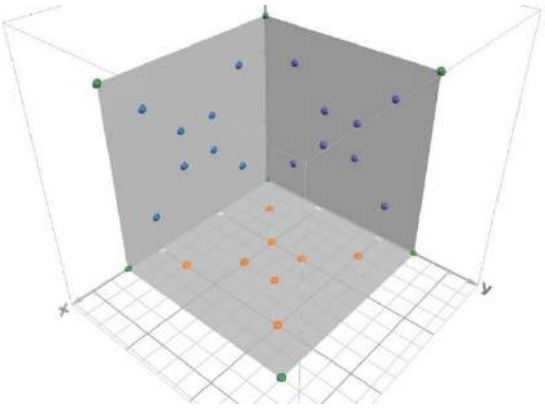
二種三種平面的相對關係了。

Case3 Type 2 × Type 2

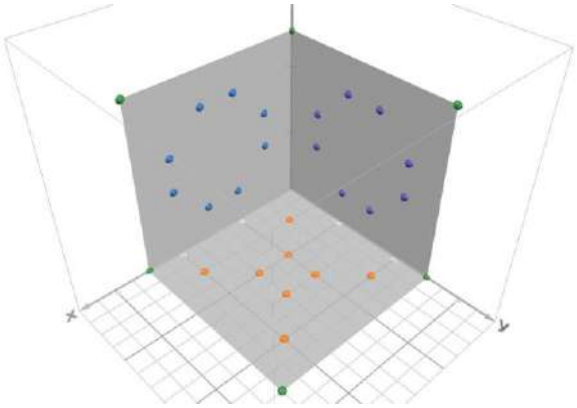
選取$x^2 - ky^2 = p_1^2 p_2$ 和 $x^2 - ky^2 = p_2 p_3^2$，同樣地，四種情況也剛好相同，

$$\Phi_{(2,1,0)}(0,1,2) = (2,2,2) \text{ 與 } (2,0,2)$$

最後我們得出了$x^2 - ky^2 = p_1^2 p_3^2$， Type 2 × Type 2 會得出 Type 1 ，三面的關係與 Case2 相同，最後我們推出 5-次方蜈蚣彘三面的關係只會有 2 種



Type 1 × Type 1 × Type 1



Type 1 × Type 2 × Type 2

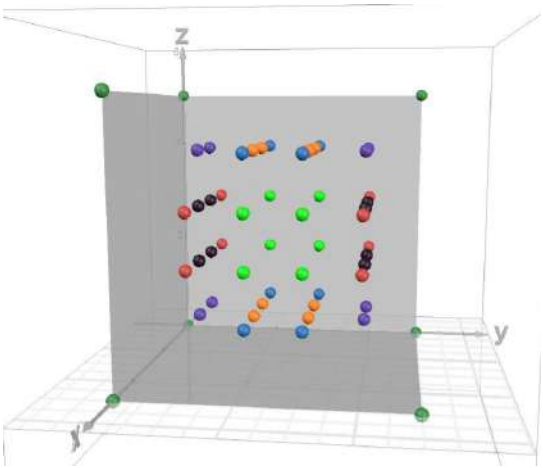
而我們跑了數據研究基本區域的那些點，在 5-次方蜈蚣彘總共有 $(5-1)^3$ 個點，我們需要了解的共有 $\frac{(5-1)^3}{8} = 8$ 個點，也就是**【定理 3.5.14】**中的 8 種顏色。我們只需想盡辦法湊出$(1,1,1), (1,1,2), (1,2,1), (2,1,1), (1,2,2), (2,1,2), (2,2,1), (2,2,2)$

這 8 個點。

【定理 3.5.16】

Type 1 × Type 1 × Type 1 的形狀，$(1,1,1)$ 與 $(2,2,2)$ 無解。

【證明】



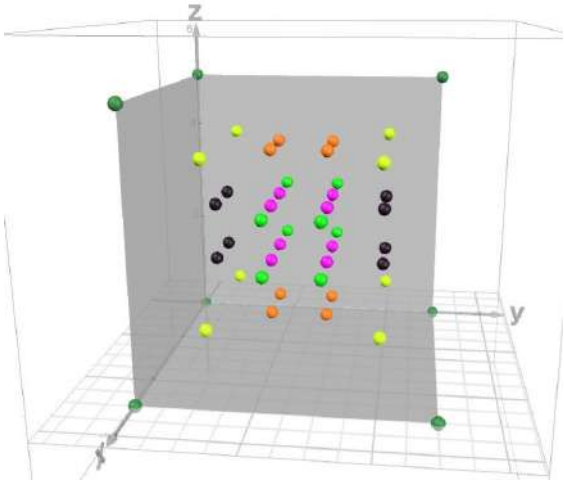
我們可以用$\Phi_{(1,0,1)}(0,1,1) = (1,1,2)$ 與 (1,1,0) 得到 (1,1,2) 的解，同理 (1,2,1), (2,1,1) 也是用同樣的方法得到。接著，用另外兩個點 $\Phi_{(1,0,1)}(0,2,2) = (1,2,1)$ 與 (1,2,3)，因為$\Phi_{(0,0,5)}(1,2,3) = (1,2,2)$ 與 (1,2,8)，所以 (1,2,3) 有解代表 (1,2,2) 也有解，同理(2,1,2), (2,2,1)也有解。

要證明 (1,1,1) 與 (2,2,2) 無解就得利用反證法，首先若(1,1,1) 有不可約解，則 (2,2,2) 有不可約解，再根據上一章的**【定理 3.5.1】**，(2,2,2) 的不可約解可以分解出(1,1,1)的不可約解，兩者方程式的不可約解是相互存在的，因此我們只需證明其中一個矛盾即可。若 (1,1,1) 有不可約解，那麼 $\Phi_{(1,1,0)}(1,1,1) = (0,0,1)$ 與 (2,2,1) 或 (0,2,1) 與 (2,0,1)，前者的 (0,0,1) 不可能有解，後者因為是 Type 1 的佩爾地毯，所以都無解，(1,1,1) 有不可約解會得到矛盾。故得證。■

【定理 3.5.17】

Type 1 × Type 2 × Type 2的形狀，(1,1,2), (1,2,1), (2,1,1) 無解。

【證明】



我們假設兩面關係為 Type 1 的是 p_1, p_2，因此我們有$\Phi_{(1,1,0)}(1,0,2) = (0,1,2)$ 與 (2,1,2)，我們得到了 (2,1,2) ，同樣地 $\Phi_{(1,1,0)}(0,1,2) = (1,0,2)$ 與 (1,2,2)，我們得到了 (1,2,2)；最後 p_2, p_3 的關係為 Type 2 ，$\Phi_{(2,0,1)}(0,,) = (,,)$ 與 (2,2,1) 我們可以得到(1,2,2), (2,2,1)也有不可約解。

接著$\Phi_{(0,1,2)}(1,0,2) = (1,1,0)$ 與 (1,1,4) ，(1,1,4) 有解代表 (1,1,1) 有解。最後$\Phi_{(2,2,0)}(1,0,2) = (1,2,2)$ 與 (3,2,2)，(3,2,2) 有解代表(2,2,2) 有解。故得證。■

6. Shoes 函數的一個問題開始

接下來這一段內容與之前的研究沒有直接的關係。而會在這裡一併提出，是因為在之前的研究裡（見**參考資料【8】**）曾經提到利用解析幾何的方式，得到了一些不錯的結果。因此，主要以代數結構作為研究主要工具的我們，也曾想利用解析幾何的方式，來轉換研究標的，只可惜並未的到較好的結果。

這一段的研究，是學長過去在研究中曾經提問過的問題。當時，學長利用 $x^2-ky^2=p$ 在第一段的不可約解 ω 以及 $\bar{\omega}$，將其 n 次方後產生了 $x^2-ky^2=p^n$ 的不可約解 ω^n 以及 $\bar{\omega}^n$。然而，這兩個解都不一定是 $x^2-ky^2=p^n$ 在第一段的可約解，必須經過 $\bar{\sigma}^i$ 以及 σ^j 來調整到第一段，也就是 $\bar{\sigma}^i\omega^n$ 以及 $\sigma^j\bar{\omega}^n$ 會是在 $x^2-ky^2=p^n$ 第一段的不可約解。然而，當時學長並未完全了解和 i 和 j 與 ω 和 $\bar{\omega}$ 的關係，但顯然 i 和 j 會是 ω 和 $\bar{\omega}$ 與 n 的函數，因此舊稱這兩個函數 $i(\omega,n)$ 和 $j(\bar{\omega},n)$ 為 Shoes 函數。

我們重新檢視這個問題的時候，利用數據來觀察，除了發現一些有趣的現象外，最後引用高三數甲所提到的連續函數的定義，以及有理數的稠密性質，對學長提出的問題得到進一步的進展；而我們認為這研究想法應該被提到，因此安排在這一段落。

證明完廣義佩爾方程式的長度 $l(k,p^n)=n+2$ 之後，我們有個問題尚未解決。在研究廣義佩爾方程式的時，我們對於解的排列方式產生疑惑，舉例來說，我們排列 $x^2-ky^2=p$ 的解時，若該方程式的第一個解定義為 ω，我們發現它的排列方式必定形如

$$\omega<\sigma\bar{\omega}<\sigma\omega \quad (1.1)$$

我們想要了解更高次方時解的排列方式，於是將上式分別乘上 ω 、$\bar{\omega}$，會得到

$$\omega^2<\sigma p<\sigma\omega^2 \text{ 以及 } p<\sigma\bar{\omega}^2<\sigma p$$

上列兩式中的每一項，均為 $x^2-ky^2=p^2$ 的解，但這些解的排列卻出現了兩種情況：

$$p<\sigma\bar{\omega}^2<\omega^2<\sigma p \quad (2.1)$$

或者

$$p<\omega^2<\sigma\bar{\omega}^2<\sigma p \quad (2.2)$$

然而，我們無法確定ω^2 、$\sigma\bar{\omega}^2$究竟是哪個大哪個小，我們一直在想哪一種排列方式才是對的，後來我們藉由例子發現兩種排列方式都有可能發生

(2.1) 的情況： $x^2-5y^2=19^2$ 的解滿足 $\sigma\bar{\omega}^2=(21,4)<\omega^2=(109,48)$

(2.2) 的情況： $x^2-5y^2=139^2$ 的解滿足 $\omega^2=(149,24)<\sigma\bar{\omega}^2=(861,380)$

我們開始困惑，若我們提高冪次，會有幾種排列方式？於是照著這個方法繼續推下去。由於兩種排列方式都有可能發生，因此我們分別進行討論。

首先從 (2.1) 開始，(2.1) 這個不等式分別乘 ω 、$\bar{\omega}$，會得到 $x^2-ky^2=p^3$ 的解

$$p\omega<\sigma p\bar{\omega}<\omega^3<\sigma p\omega \text{ 以及 } p\bar{\omega}<\sigma\bar{\omega}^3<p\omega<\sigma p\bar{\omega}$$

因為是奇數次方，所以 $p^{\frac{3}{2}}$ 不會是一組正整數解，我們在這個步驟還無法確定第一組正整數解會是哪一組，因此我們就先以 $p\omega$ 為首，取其中一段來看。我們從上面的不等式中可以發現 ω^3 和 $\sigma\bar{\omega}^3$ 並沒有在同一段，因此我們再對後者乘上一個 σ ：

$$p\bar{\omega}<\sigma\bar{\omega}^3<p\omega<\sigma p\bar{\omega}<\sigma^2\bar{\omega}^3<\sigma p\omega<\sigma^2 p\bar{\omega}$$

ω^3 與 $\sigma^2\bar{\omega}^3$ 在同一段，所以我們可以得出下列兩組不等式：

$$p\omega<\sigma p\bar{\omega}<\sigma^2\bar{\omega}^3<\omega^3<\sigma p\omega \quad (3.1)$$

$$p\omega<\sigma p\bar{\omega}<\omega^3<\sigma^2\bar{\omega}^3<\sigma p\omega \quad (3.2)$$

為了弄清楚誰是第一個正整數解，我們得乘上 $\bar{\sigma}$ 來調整大小：

$$(3.1)\times\bar{\sigma} \text{ 可得到 } p\bar{\omega}<\sigma\bar{\omega}^3<\bar{\sigma}\omega^3<p\omega<\sigma p\bar{\omega}<\sigma^2\bar{\omega}^3<\omega^3$$

$$(3.2)\times\bar{\sigma} \text{ 可得到 } p\bar{\omega}<\bar{\sigma}\omega^3<\sigma\bar{\omega}^3<p\omega<\sigma p\bar{\omega}<\omega^3<\sigma^2\bar{\omega}^3$$

將注意力集中在<上，可以發現<前後的解剛剛好互為共軛，因此 (3.1) 和 (3.2) 第一個解分別為 $\bar{\sigma}\omega^3$ 以及 $\sigma\bar{\omega}^3$。

接下來輪到 (2.2)，分別乘上 ω 、$\bar{\omega}$ 後可得

$$p\omega<\omega^3<\sigma p\bar{\omega}<\sigma p\omega \text{ 以及 } p\bar{\omega}<p\omega<\sigma\bar{\omega}^3<\sigma p\bar{\omega}$$

引此會有

$$p\omega<\sigma\bar{\omega}^3<\omega^3<\sigma p\bar{\omega}<\sigma p\omega \quad (3.3)$$

$$p\omega<\omega^3<\sigma\bar{\omega}^3<\sigma p\bar{\omega}<\sigma p\omega \quad (3.4)$$

我們依照這個順序往前面寫，將上式乘上 $\bar{\sigma}$ 並合併，就可以得到

$$(3.3)\times\bar{\sigma} \text{ 可得到 } \bar{\omega}^3<\bar{\sigma}\omega^3<p\bar{\omega}<p\omega<\sigma\bar{\omega}^3<\omega^3<\sigma p\bar{\omega}<\sigma p\omega$$

$$(3.4)\times\bar{\sigma} \text{ 可得到 } \bar{\sigma}\omega^3<\bar{\omega}^3<p\bar{\omega}<p\omega<\omega^3<\sigma\bar{\omega}^3<\sigma p\bar{\omega}<\sigma p\omega$$

同樣聚焦在<上，可以確定在這兩種情況下 $p\omega$ 是第一組正整數解。

從 $x^2-ky^2=p$ 的解推到 $x^2-ky^2=p^3$ 的解之後，我們觀察到一個現象，似乎上一個冪次的每一個排列方式都可以再分出兩種情況。於是我們便開始猜測，方程式 $x^2-ky^2=p^n$ 解的排列方式是否可分解出 2^{n-1} ？然而在方程式 $x^2-ky^2=p^4$ 時，可以推測出解的排列方式竟然只有六種：

從 (3.1) 中 推測出解的排列方式分別有以下兩個：

$$p^2<\sigma p\bar{\omega}^2<\sigma^2\bar{\omega}^4<\bar{\sigma}\omega^4<p\omega^2<\sigma p^2 \quad (4.1)$$

$$p^2<\sigma p\bar{\omega}^2<\bar{\sigma}\omega^4<\sigma^2\bar{\omega}^4<p\omega^2<\sigma p^2 \quad (4.2)$$

但從 (3.2) 中 推測出解的排列方式卻只有一個：：

$$p^2<\bar{\sigma}\omega^4<\sigma p\bar{\omega}^2<p\omega^2<\sigma^2\bar{\omega}^4<\sigma p^2 \quad (4.3)$$

這個地方只有推出一種排列方式，我們將步驟仔細地寫下來：

$\sigma p\bar{\omega}^2<p\omega^2<\sigma p^2<\omega^4<\sigma^2 p\bar{\omega}^2<\sigma^2 p\bar{\omega}^2$、$\sigma\bar{\omega}^4<p^2<\sigma p\bar{\omega}^2<p\omega^2<\sigma^2\bar{\omega}^4$

由於共軛後乘 σ 一定會在切點的不同邊，並且是對稱的（見**【定理 3.6.4】2.**），因此 $\bar{\sigma}\omega^4$ 只能填在 p^2 和 $\sigma p\bar{\omega}^2$ 之間：

$$p^2<\bar{\sigma}\omega^4<\sigma p\bar{\omega}^2<p\omega^2<\sigma^2\bar{\omega}^4<\sigma p^2$$

然而，缺少一種分解方式的不只有(3.2)，從 (3.3) 推出來的也只有一種情況：

$$p^2<\sigma\bar{\omega}^4<p\omega^2<\sigma p\bar{\omega}^2<\omega^4<\sigma p^2 \quad (4.4)$$

從 (3.4) 中 推測出解的排列方式會有以下兩個：

$$p^2<p\omega^2<\sigma\bar{\omega}^4<\omega^4<\sigma p\bar{\omega}^2<\sigma p^2 \quad (4.5)$$

$$p^2<p\omega^2<\omega^4<\sigma\bar{\omega}^4<\sigma p\bar{\omega}^2<\sigma p^2 \quad (4.6)$$

對於只出現一種分解狀況的(3.2)和(3.3)，我們嘗試把不等式的順序對調過來，看看究竟是何處會得到矛盾。從正常的(4.3) $p^2<\bar{\sigma}\omega^4<\sigma p\bar{\omega}^2<p\omega^2<\sigma^2\bar{\omega}^4<\sigma p^2$ 開始，若我們將 $\bar{\sigma}\omega^4$ 與 $\sigma^2\bar{\omega}^4$ 對調，變成

$$p^2<\sigma^2\bar{\omega}^4<\sigma p\bar{\omega}^2<p\omega^2<\bar{\sigma}\omega^4<\sigma p^2$$

從 $p^2(=\omega^2\bar{\omega}^2)<\sigma^2\bar{\omega}^4$ 可以看出 $\left(\frac{\omega}{\bar{\omega}}\right)^2<\sigma$，然而從 $\sigma p\bar{\omega}^2<p\omega^2$ 卻得到 $\sigma<\left(\frac{\omega}{\bar{\omega}}\right)^2$，得到矛盾。

在討論完 $x^2-ky^2=p^4$ 解的排列後，我們覺得利用將不等式分別乘 ω 、$\bar{\omega}$ 這個方法，很

難看出一個不等式是否合理，但是，我們從上述討論中猜測，猜測解的排序方式似乎跟 σ 與 $\frac{\omega}{\bar{\omega}}$ 的大小有很大的關聯。於是我們改變了思考方式，轉而了解 σ、$\frac{\omega}{\bar{\omega}}$ 與解的排序方式的關聯。

由於接下來 $\frac{\omega}{\bar{\omega}}$ 會是我們討論的主角，為了方便表示，我們有以下的定義：

【定義 3.6.1】ρ 與 $\sigma_{(m.n)}$

假設 k 是一個給定的奇質數，且 ω 是方程式 $x^2 - ky^2 = A$ 的第一個不可約解，其中 $(k, A) = 1$，則定義

$$\rho = \frac{\omega}{\bar{\omega}}$$

此外，我們從一開始的不等式 (1.1) 依序推導出不等式 (2.1)、(2.2)、(3.1)、(3.2)、(3.3)、(3.4)、(4.1)、(4.2)、(4.3)、(4.4)、(4.5) 以及 (4.6)；我們將會利用這些不等式推得 ρ 冪次和 σ 的不等式，為表明該不等式是出自於上述某一個不等式 (m, n)，我們會在該 σ 和 ρ 冪次的不等式中，於 σ 的足碼處標上 (m, n)。

例如，在不等式 (1.1) 中，由 $\omega < \sigma\bar{\omega} < \sigma\omega$ 可得

$$\rho < \sigma_{(1,1)}$$

而自不等式 (2.1) $(p < \sigma\bar{\omega}^2 < \omega^2 < \sigma p)$ 以及 (2.2) $(p < \omega^2 < \sigma\bar{\omega}^2 < \sigma p)$ 各自會有

$$\sigma_{(2.1)} < \rho^2 \text{ 以及 } \rho^2 < \sigma_{(2.2)}$$

這將 σ 的種類區分成兩塊，分別為 $\rho < \sigma_{(2.1)} < \rho^2$ 與 $\rho^2 < \sigma_{(2.2)}$。

【備注 3.6.1】在(2.1)中，若我們挑選 $p(= \omega\bar{\omega}) < \sigma\bar{\omega}^2$，會得到跟 (1.1) 一樣的結果。這是因為在 (2.1) 中的 $p(= \omega\bar{\omega}) < \sigma\bar{\omega}^2$ 是從 (1.1) $\omega < \sigma\bar{\omega}$ 得出，一定會滿足 (1.1) 的不等式，也就是 $\rho < \sigma_{(1,1)}$。然而在二次方時，ω^2、$\sigma\bar{\omega}^2$ 的大小，將會左右 σ 和 ρ 冪次的大小，所以我們只需要針對新的條件，也就是只需比較 ω^2、$\sigma\bar{\omega}^2$ 的大小，其餘的都只會得到之前就知道大小關係；故因此我們**只需針對最高次方互為共軛的解做比較。**

到了三次方，我們將 (2.1) 的情況拆成 (3.1)、(3.2)，可以先從不等式中看出 σ 的範圍：

(3.1) $\bar{\sigma}\omega^3 < p\omega < \sigma p\bar{\omega} < \sigma^2\bar{\omega}^3 < \omega^3$ 會有 $\rho < \sigma_{(3.1)} < \rho^{\frac{3}{2}}$、

(3.2) $\sigma\bar{\omega}^3 < p\omega < \sigma p\bar{\omega} < \omega^3 < \sigma^2\bar{\omega}^3$會有 $\rho < \rho^{\frac{3}{2}} < \sigma_{(3.2)}$。

就如同剛剛所說的，這兩種情況皆是從(2.1)的情況拆出來的，因此一定也會滿足 $\rho < \sigma_{(3.1)}$、$\sigma_{(3.2)} < \rho^2$ ，只是中間多出了比 $\rho^{\frac{3}{2}}$ 大或小的條件

$$\rho < \sigma_{(3.1)} < \rho^{\frac{3}{2}} < \sigma_{(3.2)} < \rho^2$$

由於中間多出了一個新條件，因此我們會觀察到「拆成兩種情況」這個現象。同樣地，(2.2)的情況可以拆成(3.3)、(3.4) 且 (3.3)、(3.4)都會滿足 $\rho^2 < \sigma$；比較 ω^3 、$\sigma\bar{\omega}^3$，則分別可從不等式(3.3)、(3.4)得到：

$$\sigma_{(3.3)} < \rho^3$$

以及

$$\rho^3 < \sigma_{(3.4)}$$

最後我們總結來看三次方時 σ 們的大小：

$$\rho < \sigma_{(3.1)} < \rho^{\frac{3}{2}} < \sigma_{(3.2)} < \rho^2 < \sigma_{(3.3)} < \rho^3 < \sigma_{(3.4)}$$

接著我們來驗證四次方的排列方式：

從(3.1)推出來的會有：

$$\sigma_{(4.1)} < \rho^{\frac{4}{3}} \text{ 以及 } \rho^{\frac{4}{3}} < \sigma_{(4.2)}$$

從(3.2)推出來的會有：

$$\rho^{\frac{4}{3}} < \sigma_{(4.3)}$$

在(3.2)我們有 $\rho^{\frac{3}{2}} < \sigma_{(3.2)} < \rho^2$，在(4.3)沒有得到更新的條件，依然保持 $\rho^{\frac{3}{2}} < \sigma_{(4.3)} < \rho^2$

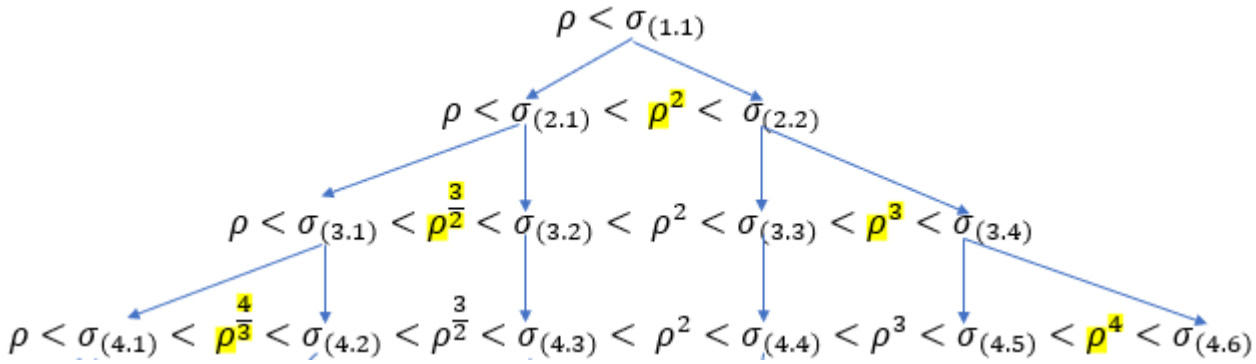
從(3.3)推出來的：

$$\sigma_{(4.4)} < \rho^4$$

從(3.4) 推出來的：

$$\sigma_{(4.5)} < \rho^4 \text{ 以及 } \rho^4 < \sigma_{(4.6)}$$

我們從三次方的排序方式推出四次方的排序方式。我們從一次方到四次方，針對 σ 的大小條件列出來(下面畫螢光筆的部份表示新增的條件)：

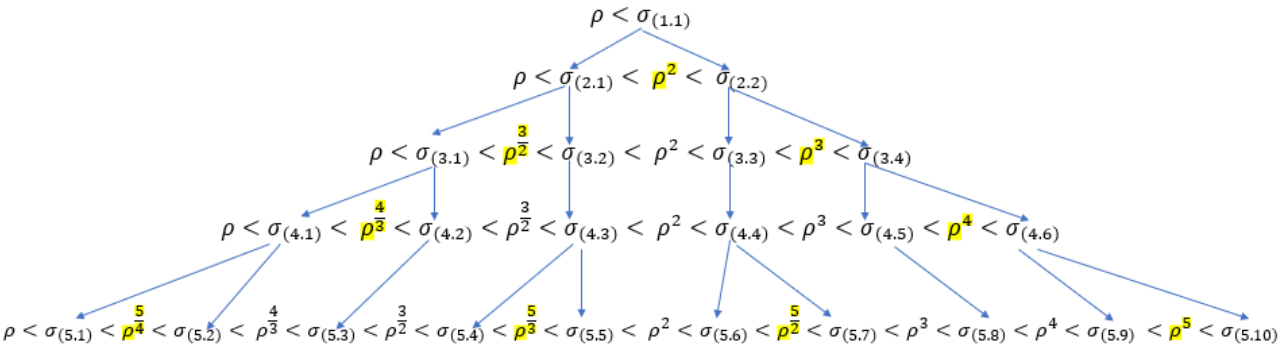


我們仔細觀察新增出來的條件，發現冪次的分子都是該次方：二次方的條件有$\rho^{\frac{2}{2}}$、$\rho^{\frac{2}{1}}$，三次方的條件有$\rho^{\frac{3}{3}}$、$\rho^{\frac{3}{2}}$、$\rho^{\frac{3}{1}}$，四次方的條件有$\rho^{\frac{4}{4}}$、$\rho^{\frac{4}{3}}$、$\rho^{\frac{4}{2}}$、$\rho^{\frac{4}{1}}$。而新增的條件（上圖畫螢光筆的部份）就是分母與分子互質的情況。

【備註 3.6.1】

會有上述這樣的現象，因為我們每往上一個次方，就會針對該次方的 $\bar{\sigma}^i\omega^n$ 與 $\sigma^j\bar{\omega}^n$ 的大小做比較，因此我們就會得到 σ^{i+j}與 ρ^n 的關係，就會多出 $\rho^{\frac{n}{i+j}}$ 這個新條件。

根據以上的觀察，我們預測了五次方的排序方式，應該是新增 $\rho^{\frac{5}{5}}$、$\rho^{\frac{5}{4}}$、$\rho^{\frac{5}{3}}$、$\rho^{\frac{5}{2}}$、$\rho^{\frac{5}{1}}$，所以應該是新增四個（如下圖所示）：



經過驗證，五次方確實有 10 種情況，於是我們開始思考如何 $x^2 - ky^2 = p^n$ 的解會有多少種排列方式。

顯然，不同的方程式的排列是由 ρ 的次方所決定，我們依序將次方的排列寫下：

方程式	ρ 的次方	***Farey sequence*** 的倒數

$x^2-ky^2=p$	1	$\frac{1}{1}$
$x^2-ky^2=p^2$	1、2	$\frac{1}{1}$、$\frac{2}{1}$
$x^2-ky^2=p^3$	1、$\frac{3}{2}$、2、3	$\frac{1}{1}$、$\frac{3}{2}$、$\frac{2}{1}$、$\frac{3}{1}$
$x^2-ky^2=p^4$	1、$\frac{4}{3}$、$\frac{3}{2}$、2、3、4	$\frac{1}{1}$、$\frac{4}{3}$、$\frac{3}{2}$、$\frac{2}{1}$、$\frac{3}{1}$、$\frac{4}{1}$
$x^2-ky^2=p^5$	1、$\frac{5}{4}$、$\frac{4}{3}$、$\frac{3}{2}$、$\frac{5}{3}$、2、$\frac{5}{2}$、3、4、5	$\frac{1}{1}$、$\frac{5}{4}$、$\frac{4}{3}$、$\frac{3}{2}$、$\frac{5}{3}$、$\frac{2}{1}$、$\frac{5}{2}$、$\frac{3}{1}$、$\frac{4}{1}$、$\frac{5}{1}$

對於每個 $x^2-ky^2=p^n$，由於每個 ρ 的次方都是最簡分數，且新增加的次方其分子會是 n，因此在上表中的第三行，我們把原來的分母寫下，便得到了第 n 階$Farey\ sequence$ 的倒數（0 不納入考慮），第 n 階$Farey\ sequence$ 的項數 F_n，恰好等於

$$\sum_{i=1}^{n}\varphi(i)$$

其中 $\varphi(i)$ 是歐拉 φ 函數。

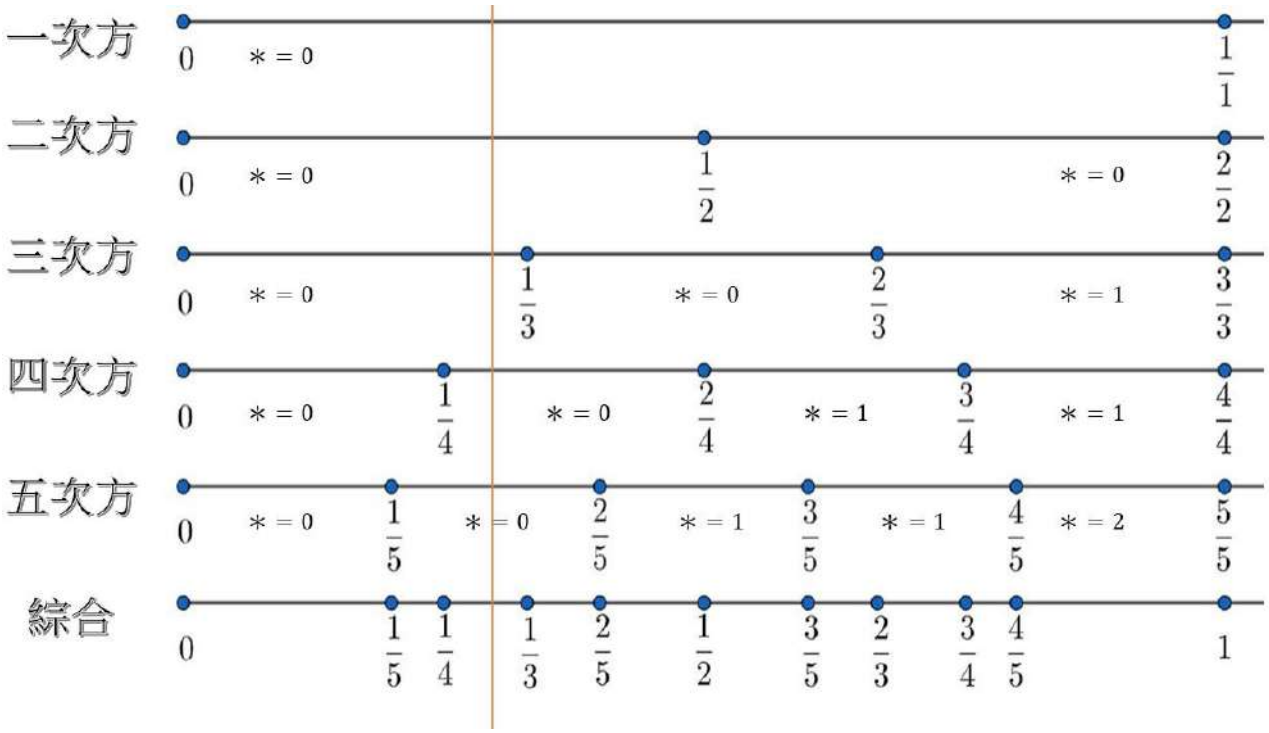
因此我們猜測 $x^2-ky^2=p^n$ 的解的排列方式總數應該為 F_n。這需要證明每一種排列方式都是存在的，這也就是說，對於任意的正整數 n，在第 n 階$Farey\ sequence$ 中任取相鄰兩項 $a<b$，可以找到一個廣義佩爾方程式 $x^2-ky^2=p(n)^n$，其中 $p(n)$ 是一個質數，使得該方程式所對應的到的 ρ 會滿足

$$\rho^{\frac{1}{b}}<\sigma<\rho^{\frac{1}{a}}\ (\text{等價於}\ \sigma^a<\rho<\sigma^b)$$

我們想要問的是，若對每一條次方線，我們都指定一個區間，則是否在一個廣義佩爾方程式 $x^2-ky^2=p$，在其所對應的 n-次方線圖中，σ 都會在指定的區間中。

除了研究排列方式，還對於第一段解的長相感的好奇。已知 σ 會負責將解調整到不同段例如 ω 與 $\sigma\bar{\omega}$ 在第一段，而 $\sigma^3\omega$ 與 $\sigma^4\bar{\omega}$ 就會在第四段。我們假設有一組互為共軛的解為 ω^n 與 $\bar{\omega}^n$，σ^* 可以把解拉回第一段(也就是之前學長提的 shoes 函數)，也就是 $p^n<\bar{\sigma}^*\omega^{2n}$, $\sigma^{*+1}\bar{\omega}^{2n}<\sigma p^n$(見**【定理 3.6.1】**)，我們試圖找方法了解 shoes 函數，最後我們有想出一個方法掌握 shoes 函數的值。

以下簡述我們的方法，再接著給出嚴謹的證明：首先我們要先算出方程式的 ρ 是多少，接著給定 $Farey\ sequence$ 中的兩個項 a, b 使得 $\sigma^a < \rho < \sigma^b$，我們要利用下表來計算出第一段中任一個解的 shoes 函數值：



上圖中的 n −次方線是指在[0,1] 上畫出 $Farey\ sequence$ 分母為 n 的點。若我們在圖上畫一條垂直線，代表在每條 n −次方線上 ρ 所位在的區間。例如：上圖的橘線代表 $\sigma^{\frac{1}{4}} < \rho < \sigma^{\frac{1}{3}}$，在四次方線上會滿足 $\sigma^{\frac{1}{4}} < \rho < \sigma^{\frac{2}{4}}$；五次方線上會滿足 $\sigma^{\frac{1}{5}} < \rho < \sigma^{\frac{2}{5}}$。

接下來，以五次方線的每個線段作為例子，來舉例 $*$ 的求法，基本上就是分區間考慮：

1. 當 $\sigma^{\frac{1}{5}} < \rho$ 時，會得到 $\omega^5 < \sigma\bar{\omega}^5$ ，因此 $* = 0$；
2. 當 $\sigma^{\frac{1}{5}} < \rho < \sigma^{\frac{2}{5}}$ 時，會得到$\omega^5 < \sigma^2\bar{\omega}^5$ 與 $\sigma\bar{\omega}^5 < \omega^5$，由於前者 σ 的冪次相差不是 1，所以不是第一段的解(見**【定理 3.6.1】**)，因此後者才是第一段的解 $* = 0$；
3. 當$\sigma^{\frac{2}{5}} < \rho < \sigma^{\frac{3}{5}}$ 時，會得到 $\omega^5 < \sigma^3\bar{\omega}^5$ ，為了讓 $\bar{\sigma}$ 與 σ 的冪次相差 1，我們將不等式同乘 $\bar{\sigma}$ 以確保那兩個解是落在第一段，推得 $\bar{\sigma}\omega^5 < \sigma^2\bar{\omega}^5$，因此 $* = 1$；
4. 當 $\sigma^{\frac{3}{5}} < \rho < \sigma^{\frac{4}{5}}$ 時，會得到 $\sigma^3\bar{\omega}^5 < \omega^5 \Longrightarrow \sigma^2\bar{\omega}^5 < \bar{\sigma}\omega^5$，因此 $* = 1$；
5. 當$\sigma^{\frac{4}{5}} < \rho < \sigma^{\frac{5}{5}}$時，會得到 $\omega^5 < \sigma^5\bar{\omega}^5 \Longrightarrow \bar{\sigma}^2\omega^5 < \sigma^3\bar{\omega}^5$ 因此 $* = 2$；

利用這個方法，我們可以推出所有的 $*$ (shoes 函數)可能的值。藉由 $n-$次方線可以觀察到

1. 我們只取 $\sigma^{\frac{\text{奇數}}{n}}$ 那一側的不等式，這將在後面的定理做說明(見**【定理 3.6.5】**)。
2. 由左至右 $*$ 的值似乎依序是 $0,0,1,1,2,2,3,3\cdots\left[\frac{n-1}{2}\right]$ 。
3. 當 $\rho < \sigma^{\frac{\text{奇數}}{n}}$ 時，有共軛的比較大；當 $\sigma^{\frac{\text{奇數}}{n}} < \rho$ 時，有共軛的比較小。

接下來，我們就對上述的方法給出證明；此外是否存在一個廣義的佩爾方程式 $x^2 - ky^2 = p$，使得其 ρ 值會包含於給定的區間，我們只得到比較初步的結果，也就是

對於任意的正整數 n，在第 n 階 $Farey\ sequence$ 中任取相鄰兩項 $a < b$，可以找到一個廣義佩爾方程式 $x^2 - ky^2 = A(n)$，其中 $A(n)$ 是一個整數，使得該方程式所對應的到的 ρ 會滿足

$$\rho^{\frac{1}{b}} < \sigma < \rho^{\frac{1}{a}}$$

對於原來問題中的 $p(n)^n$ ，在接下來給出 $A(n)$ 存在的證明中，並沒有任何可以說明 $p(n)^n$ 存在的理由，我們猜測這還是需要回到數論的範疇來討論較為得宜；接下來就是我們證明 $A(n)$ 存在的證明。

【備註 3.6.2】

若 $x^2 - ky^2 = p^n$ 的 k 固定，則 σ 是一個定值，而 ρ 會隨著 p 而改變，因此我們上圖中用 ρ 的次方來比較 σ 這個方法比較不恰當；反倒是用 σ 的次方來比較 ρ 這個方法比較恰當，並且 $Farey\ sequence$ 指的是 0 和 1 之間最簡分數數列，由小至大排列。總上所述，我們將次方改到 σ 上會比較恰當。例如：$\rho^{\frac{3}{2}} < \sigma_{(3.2)} < \rho^2$ 我們將它改成 $\sigma^{\frac{1}{2}} < \rho < \sigma^{\frac{2}{3}}$。這個表示方法將會在**【定理 3.6.9】**用到。

前面的內容都在敘述我們推導的過程，我們藉由例子觀察到許多排列方式的現象，我們

將這些現象給出證明。首先，我們先將之前的一個結果提出：

【定理 3.6.1】

假設 $p^n < \bar{\sigma}^i \omega^{2n},\ \sigma^j \bar{\omega}^{2n} < \sigma p^n$，則 $j = i + 1$。證明(**見參考資料【6】【定理 3.5】**)

其實這個定理不僅限於 $x^2 - ky^2 = p^{2n}$ ，即使 $x^2 - ky^2 = p^n$ 在 n 是奇數時也會成立。而且事實上，不僅限於 ω^n 與 $\bar{\omega}^n$ ，第一段互為共軛的解通通都會滿足上述定理敘述。以下是我們得到的結果：

【定理 3.6.2】

$x^2 - ky^2 = p^n$ 第一段的解會滿足 $p^{\frac{n}{2}} < \bar{\sigma}^* \omega^i \bar{\omega}^{n-i},\ \sigma^{*+1} \omega^{n-i} \bar{\omega}^i < \sigma p^{\frac{n}{2}}$。

更進一步的，$\bar{\sigma}$ 的指數必須滿足以下定理：

【定理 3.6.3】

若 $p^{\frac{n}{2}} < \bar{\sigma}^* \omega^i \bar{\omega}^{n-i},\ \sigma^{*+1} \omega^{n-i} \bar{\omega}^i < \sigma p^{\frac{n}{2}}$ ，且 $i > \frac{n}{2}$ ，則 $* < i - \frac{n}{2}$ 。

【證明】

因為 $p^{\frac{n}{2}} (= \omega^{\frac{n}{2}} \bar{\omega}^{\frac{n}{2}}) < \bar{\sigma}^* \omega^i \bar{\omega}^{n-i}$ 可推得 $\sigma^* < \rho^{i-\frac{n}{2}}$，利用反證法，若 $* \geq i - n$，則 $\sigma < \rho^{\frac{i-\frac{n}{2}}{*}} \leq \rho^1 \Longrightarrow \sigma \bar{\omega} < \omega$ ，與ω 為第一個解的假設前提矛盾。故得證。■

【定理 3.6.4】

ω_t 表示在 $x^2 - ky^2 = p^n$ 第一段中，不能表示為 $\sigma^* p^{\frac{n}{2}}$ 的正整數解。我們將解按照大小順序：若 $p^{\frac{n}{2}} < \omega_1 < \omega_2 < \cdots\cdots < \omega_{m-1} < \omega_m < \sigma p^{\frac{n}{2}}$ ，則：

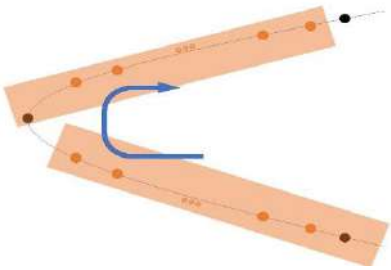
1. m 是偶數，且 $m = 2\lceil n \rceil$，其中 $\lceil n \rceil$ 是 ceiling function。

2. $\omega_m = \sigma\overline{\omega_1}$ 、$\omega_{m-1} = \sigma\overline{\omega_2}$、⋯、$\omega_{\frac{m}{2}+1} = \sigma\overline{\omega_{\frac{m}{2}}}$、⋯、$\omega_t = \sigma\overline{\omega_{m-t+1}}$

3. $\omega_{\frac{m}{2}} < \sqrt{\frac{p^n}{2+2\alpha}}(\alpha+1,\beta) < \omega_{\frac{m}{2}+1}$

【證明】

由於 $p^{\frac{n}{2}}$ 到 ω_m 稱為 $L(k,p^n)$。當 n 是奇數時，$L(k,p^n) = n+1$ 是偶數，這時 $p^{\frac{n}{2}}$ 並非正整數解，所以正整數解是從 ω_1 到 ω_m，$L(k,p^n) = m = n+1$ 是個偶數；當 n 是偶數時，這時 $p^{\frac{n}{2}}$ 是正整數解，所以正整數解是從 $p^{\frac{n}{2}}$ 到 ω_m，$L(k,p^n) = m+1 = n+1$ ，m 是個偶數。故 1.得證。



接著，我們將每個解都取共軛，再乘上 σ 後會得到

$$\sigma p^{\frac{n}{2}} > \sigma\overline{\omega_1} > \sigma\overline{\omega_2} > \cdots\cdots > \sigma\overline{\omega_{m-1}} > \sigma\overline{\omega_m} > p^{\frac{n}{2}}$$

$\sigma\overline{\omega_t}$ 通通都是正整數解，並且都在第一段，所以 2.得證。另外，由於取共軛，再乘上 σ 後會在切點 $\sqrt{\frac{p^n}{2+2\alpha}}(\alpha+1,\beta)$ 的異側(**見參考資料【6】【五、從解析幾何出發】**)，所以 3.得證。■

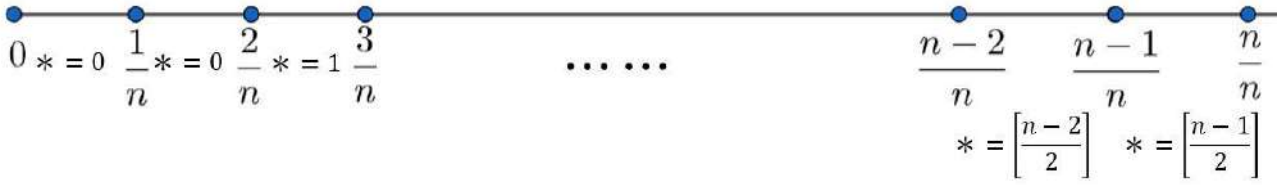
【備註 3.6.3】

在**【定理 3.6.4】**1. 中證明有用到 $L(k,p^n)$ ，若我們放寬質數的限制，改成 $x^2 - ky^2 = A^n$ 是否依然是偶數？我們分 Cases 來討論：當 $L\left(k, A = p_1^{n_1}p_2^{n_2}\cdots p_j^{n_j}\right)$ 是奇數時，利用唯一分解性質，可以知道 $L(k,A) = L\left(k,p_1^{n_1}\right)\cdot L\left(k,p_2^{n_2}\right)\cdot\cdots\cdot L\left(k,p_j^{n_j}\right)$，只有當次方是偶數時，$L\left(k,p_i^{n_i}\right)$ 才會是奇數，所以 A 是完全平方數 $\left(\sqrt{A},0\right)$ 是一個解，那麼由 $\underbrace{A^{\frac{n}{2}} < \omega_1 < \omega_2 < \cdots\cdots < \omega_{m-1} < \omega_m}_{L(k,A)} < \sigma A^{\frac{n}{2}}$ 可以得知 m 是偶數；當 $L(k,A)$ 是偶數時，A 就是完全平方數，同樣會得到 m 是偶數。

【定理 3.6.5】

在 $x^2 - ky^2 = p^n$ 中的 $\bar{\sigma}^*\omega^n$ 與 $\sigma^{*+1}\bar{\omega}^n$， $n-$次方線上，$\sigma^0 < \sigma^{\frac{1}{n}} < \cdots < \sigma^{\frac{n-2}{n}} < \sigma^{\frac{n-1}{n}} <$

ρ^1，由左至右 $*$ 的值依序是 $0,0,1,1,2,2,3,3\cdots\left[\frac{n-1}{2}\right]$。(如下圖所示)



【證明】

我們選取分子為奇數 m 的 $\sigma^{\frac{m}{n}}$，我們可以將 m 表示成 $2*+1$。若我們比較 ρ 與 $\sigma^{\frac{2*+1}{n}}$ 的大小，相當於比較 $\bar{\sigma}^*\omega^n$ 與 $\sigma^{*+1}\bar{\omega}^n$ 的大小，若 $\bar{\sigma}^*\omega^n > \sigma^{*+1}\bar{\omega}^n$，則 $\rho > \sigma^{\frac{2*+1}{n}}$；若 $\bar{\sigma}^*\omega^n < \sigma^{*+1}\bar{\omega}^n$，則 $\rho < \sigma^{\frac{2*+1}{n}}$，因此在 $*$ 的值會在分子為奇數的兩側。■

【備註 3.6.4】

以上**【定理 3.6.1】**到**【定理 3.6.5】**幾乎都沒有用到 $x^2 - ky^2 = p^n$ 中 p 一定要是質數的條件(除前面提過的**【定理 3.6.4】**)，以上定理對 $x^2 - ky^2 = A^n$ 通通都成立。

以上就是說明 $Farey\ sequence$ 與 σ 以及 ρ^n 之間的關係，同時間也闡明了我們想要知道，$x^2 - ky^2 = p^n$ 的解會有多少種排列方式，這問題的確實性。接著，我們便開始對這問題的探討，先從定義一個函數開始：

【定義 3.6.2】$\rho(x)$

設 k 是一個給定的奇質數，函數 $\rho: (\sqrt{k}, \infty) \longrightarrow (1, \infty)$ 定義為

$$\rho(x) = \frac{x + \sqrt{k}}{x - \sqrt{k}}$$

【備註 3.6.5】

函數 $\rho(x)$ 的發想就是源自於之前 ω 和 $\bar{\omega}$ 的比值。假設 $\omega = u + v\sqrt{k}\ (u, v \in \mathbb{Q})$，那麼

$$\rho = \frac{u + v\sqrt{k}}{u - v\sqrt{k}} = \frac{\frac{u}{v} + \sqrt{k}}{\frac{u}{v} - \sqrt{k}} = \rho(x)$$

若我們將上是有理化

$$\rho = \frac{u + v\sqrt{k}}{u - v\sqrt{k}} = \frac{\left(u + v\sqrt{k}\right)^2}{u^2 - v^2 k}$$

我們將分子分母同除 v^2 會有

$$\rho = \frac{\left(\frac{u}{v}\right)^2 + k + 2\left(\frac{u}{v}\right)\sqrt{k}}{\left(\frac{u}{v}\right)^2 - k} = \frac{\left(\frac{u}{v}\right)^2 + k}{\left(\frac{u}{v}\right)^2 - k} + \frac{2\left(\frac{u}{v}\right)}{\left(\frac{u}{v}\right)^2 - k}\sqrt{k}$$

我們令 $x = \frac{u}{v}$ ，並改成 x 的參數式，即可將 $\rho(x)$ 看成座標平面上的一個點：

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

由於 $\sqrt{k}$ 是無理數，這樣的定義是良好的（$well - defined$）。

在【**定義 3.6.2**】中的 $\rho(x)$ 是一個有趣的函數，在備註中的數對 $\left(\frac{x^2+k}{x^2-k}, \frac{2x}{x^2-k}\right)$ 可以看成將 $\rho(x)$ 延伸到 $\mathbb{R}^2$ 上的一個函數；除此之外，我們還有以下的結果：

【定理 3.6.6】

定義函數 $\tilde{\rho}(x) = \left(\frac{x^2+k}{x^2-k}, \frac{2x}{x^2-k}\right)$ ，且定義域為 $\left(\sqrt{k}, \infty\right)$，則對應域為 $x^2 - ky^2 = 1$ 所有在第一象限的解集合。

【證明】

設 $\tilde{\rho}(x) = \left(\rho_1(x), \rho_2(x)\right) = \left(\frac{x^2 + k}{x^2 - k}, \frac{2x}{x^2 - k}\right)$ ，那麼我們有

$$\rho_1^2 - k\rho_2^2 = \frac{(x^2 + k)^2 - 4x^2 k}{(x^2 - k)^2} = 1$$

故 $\tilde{\rho}(x)$ 是 $x^2 - ky^2 = 1$ 在第一象限上的一個點。

現假設 (u, v) 是 $x^2 - ky^2 = 1$ 在第一象限上的一個點。那我們會有以下的方程組

$$\begin{cases}\dfrac{x^2+k}{x^2-k}=u\\ \dfrac{2x}{x^2-k}=v\end{cases}$$

將第二式乘上 $\sqrt{k}$ 後相加可得

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

這樣我們就可以得到

$$x=\frac{u+v\sqrt{k}+1}{u+v\sqrt{k}-1}\cdot\sqrt{k}\in\left(\sqrt{k},\infty\right)$$

故得證。■

由於多項式函數是連續函數，且對於任意的 $x\in\left(\sqrt{k},\infty\right)$，$x^2-k\neq 0$，因此會有

【定理 3.6.7】

$\tilde{\rho}(x)=\left(\rho_1(x),\rho_2(x)\right)=\left(\dfrac{x^2+k}{x^2-k},\dfrac{2x}{x^2-k}\right)$ 是連續函數。

再利用接下來的引理，便可以說明 $\tilde{\rho}(x)$ 會是 $x^2-ky^2=1$ 在第一象限的參數化：

【引理 3.6.1】

設 (u,v) 和 (s,t) 是 $x^2-ky^2=1$第一象限中的兩點，如果 $u>s$，則 $v>t$，反之亦然。

【證明】

由於 (u,v) 和 (s,t) 是 $x^2-ky^2=1$ 第一象限中的兩點，我們有

$$u^2-kv^2=s^2-kt^2\Longrightarrow 0<u^2-s^2=k(v^2-t^2)$$

故得證。■

【備註 3.6.5】

我們在這裡對 $\tilde{\rho}(x)=\left(\rho_1(x),\rho_2(x)\right)=\left(\dfrac{x^2+k}{x^2-k},\dfrac{2x}{x^2-k}\right)$ 討論較多，這是因為這個函數若定

義在 $(\sqrt{k},\infty)$ 上的有理數時，感覺就是將廣義佩爾方程式的 $x^2-ky^2=A$ 上的有理數解 ω_A，所對應的 ρ_A 看成 $x^2-ky^2=1$第一象限中的點；這也是我們一開始思考這個問題時，最一開始著手的想法。雖然之後並未使用這個函數去處理問題，但感覺這也是對廣義佩爾方程式了解的一個工具，故在這強調再三。

接下來，我們就利用 $\rho(x)$ 連續性來得到【**定理 3.6.8**】：

【定理 3.6.8】

對於任意正整數 n，從第 n 階的 $Farey\ sequence$ 中選擇兩個相鄰的有理數 α 和 β(設 $\alpha<\beta$)，一定存在廣義佩爾方程 $x^2-ky^2=A$ 的第一個不可約解 ω，使得

$$\sigma^{\alpha}<\frac{\omega}{\bar{\omega}}<\sigma^{\beta}$$

【證明】

我們只需要找到一個有理數 $r=\frac{u}{v}\in(1,\infty)$，使得 $\rho(r)\in(\sigma^{\alpha},\sigma^{\beta})$，那麼就會有

$$\sigma^{\alpha}<\rho(r)=\frac{\frac{u}{v}+\sqrt{k}}{\frac{u}{v}-\sqrt{k}}=\frac{u+v\sqrt{k}}{u-v\sqrt{k}}<\sigma^{\beta}$$

若令 $A=u^2-kv^2$，那麼根據 r 是最簡分數，$\omega=u+v\sqrt{k}$ 會是 方程式 $x^2-ky^2=A$ 2k7u 的一個不可約解，並且滿足

$$\sigma^{\alpha}<\frac{\omega}{\bar{\omega}}<\sigma^{\beta}$$

這樣就完成了定理證明；由於 $\rho(x)$ 是一個連續函數且值域為 $(1,\infty)$，根據其連續性，在其定義域中必定可找到一個一個開區間 $I\subset(\sqrt{k},\infty)$，使得 $\rho(I)\subset(\sigma^{\alpha},\sigma^{\beta})$。因此，取一有理數 $r\in I$， $\rho(r)\subset(\sigma^{\alpha},\sigma^{\beta})$。

故得證。■

最後，我們為這段研究做一個總結：首先，關於學長之前的問題我們可以利用 ρ 和 σ 的冪次來解決；事實上，這方法並不局限於在方程式 $x^2-ky^2=p$ 中， p 是質數的限制，任意整數都可以。此外，雖然我們尚未確定對於任意正整數 n，從第 n 階的 $Farey\ sequence$ 中選擇兩個相鄰的有理數 α 和 β(設 $\alpha<\beta$)，是否存在一個質數 p，使得

$$\sigma^{\alpha}<\frac{\omega_p}{\overline{\omega_p}}<\sigma^{\beta}$$

其中 ω_p 是 $x^2-ky^2=p$ 的不可約解，但是我們的確找到了無窮多個廣義佩爾方程式 $x^2-ky^2=A$，使得

$$\sigma^{\alpha}<\frac{\omega_A}{\overline{\omega_A}}<\sigma^{\beta}$$

也因此若 $\frac{\omega_A}{\overline{\omega_A}}\in(\alpha_s,\beta_s)$ 其中 α_s 和 β_s 是第 s 階的 $Farey\ sequence$ 中，兩個相鄰的有理數，那麼我們也可以計算出 $i(\omega_A,s)$ 和 $j(\overline{\omega_A},s)$。

7. 三次方根的必要條件

這最後一段的內容不如前面章節長度，但是在寫程式的實用上，提供了一個更便捷的方法；也因此我們決定將這個結果提出來，並做為這次研究的結束。

首先，我們在著眼蜈蚣彘的討論時，一個很自然的想法，卻總是困擾著我們：倘若 ω 是方程式 $x^2-ky^2=p^3$ 的一個解， $\sqrt[3]{\omega}$ 是否是方程式 $x^2-ky^2=p$ 的一個解嗎?

我們就三次方根是正整數解的 ω 開始；令 $\omega=\alpha+\beta\sqrt{k}=\left(u+v\sqrt{k}\right)^3$，那麼 $\omega=u^3+3kuv^2+(kv^3+3u^2v)\sqrt{k}=\alpha+\beta\sqrt{k}$。由於 α、β 皆是已經知道的數，所以我們可以考慮聯立方程式 (1)：

$$\begin{cases}u^3+3kuv^2=\alpha\\kv^3+3u^2v=\beta\end{cases}\quad(1)$$

我們將上下兩式分別除以 u 和 v 後得下式 (2)：

$$\begin{cases}u^2+3kv^2=\dfrac{\alpha}{u}\\kv^2+3u^2=\dfrac{\beta}{v}\end{cases}\quad(2)$$

由於 $u^2-kv^2=p$ 我們可以化簡成 (3)：

$$\begin{cases} u^2+3(u^2-p)=\dfrac{\alpha}{u} \\ kv^2+3(kv^2+p)=\dfrac{\beta}{v} \end{cases} \Rightarrow \begin{cases} 4u^2-3p=\dfrac{\alpha}{u} \\ 4kv^2+3p=\dfrac{\beta}{v} \end{cases} \quad (3)$$

兩式相減後我們會有：

$$4(u^2-kv^2)-6p=\frac{\alpha}{u}-\frac{\beta}{v} \Longrightarrow -2p=\frac{\alpha}{u}-\frac{\beta}{v} \quad (4)$$

從以上的 (2) 式可以知道， u 和 v 分別為 α 和 β 的因數；又從 (4) 式可知，

$$\frac{\alpha}{u}-\frac{\beta}{v}$$

為一負數且是 p 的倍數。將上述內容重新敘述如下：設 u 和 v 分別為 α 和 β 的因數，若

$$\alpha+\beta\sqrt{k}=\left(\frac{\alpha}{u}+\frac{\beta}{v}\sqrt{k}\right)^3$$

則 $-2p=\alpha-\beta$。所以，在實際的應用上，我們可以先把 α 和 β 的因數 α_i 和 β_j 列出後，再確認是否 $\alpha_i-\beta_j$ 等於 $-2p$，再去計算 $\left(\frac{\alpha}{u}+\frac{\beta}{v}\sqrt{k}\right)^3$ 是否等於 $\alpha+\beta\sqrt{k}$。

仔細觀察上式 (1)，(2) 以及 (3)，其操作分別是分組、約分以及化簡，除了 (1) 必須要求是 3 次方以外，其他均和次方無關。因此，我們試著將上述的計算技巧推廣至奇數次方（以利在 (1) 分類時得以均分），便得到了下列的推廣：

【定理 3.7.1】

假設 (α,β) 是方程式 $x^2-ky^2=p^{2n+1}$ 的一個解。若存在正整數使得

$$\alpha+\sqrt{k}\beta=\left(u+\sqrt{k}v\right)^{2n+1}$$

則 $\frac{\alpha}{u}$ 與 $\frac{\beta}{v}$ 皆為整數且 $\frac{\alpha}{u}-\frac{\beta}{v}<0$ 可被 $u^2-kv^2(=p)$ 整除。

【證明】

根據二項式定理

$$\begin{aligned} \alpha+\sqrt{k}\beta &= \left(u+\sqrt{k}v\right)^{2n+1} \\ &= \sum_{j=0}^{2n+1} C_j^{2n+1}u^{2n+1-j}\left(v\sqrt{k}\right)^j \end{aligned}$$

$$= \sum_{j=0}^{n} C_{2j}^{2n+1} u^{2n+1-2j} \left(v\sqrt{k}\right)^{2j} + \sum_{j=0}^{n} C_{2j+1}^{2n+1} u^{2n-2j} \left(v\sqrt{k}\right)^{2j+1}$$

$$= \sum_{j=0}^{n} C_{2j}^{2n+1} u^{2n+1-2j}\, v^{2j} k^{j} + \sum_{j=0}^{n} C_{2j+1}^{2n+1} u^{2n-2j}\, v^{2j+1} k^{2j} \sqrt{k}$$

由於 α、β、u 和 v 都是正整數，我們會有

$$\alpha = \sum_{j=0}^{n} C_{2j}^{2n+1} u^{2n+1-2j}\, v^{2j} k^{j} \Longrightarrow \frac{\alpha}{u} = \sum_{j=0}^{n} C_{2j}^{2n+1} u^{2n-2j}\, v^{2j} k^{j}$$

以及

$$\beta = \sum_{j=0}^{n} C_{2j+1}^{2n+1} u^{2n-2j}\, v^{2j+1} k^{2j} \Longrightarrow \frac{\beta}{v} = \sum_{j=0}^{n} C_{2j+1}^{2n+1} u^{2n-2j}\, v^{2j} k^{j}$$

這便說明了 $\frac{\alpha}{u}$ 與 $\frac{\beta}{v}$ 皆為整數且 $\frac{\alpha}{u} - \frac{\beta}{v}$ 等於

$$\sum_{j=0}^{n} C_{2j}^{2n+1} u^{2n-2j}\, v^{2j} k^{j} - \sum_{j=0}^{n} C_{2j+1}^{2n+1} u^{2n-2j}\, v^{2j} k^{j}$$

接著，我們就從上式開始整理；現令 $2i = 2n - 2j$，那麼對於 $i = n, n-1, \cdots, 1, 0$，會有 $2j = 2n -$

$2i$。因此，$\frac{\alpha}{u} - \frac{\beta}{v}$ 會等於

$$\sum_{j=0}^{n} C_{2j}^{2n+1} u^{2n-2j}\, v^{2j} k^{j} - \sum_{j=0}^{n} C_{2j+1}^{2n+1} u^{2n-2j}\, v^{2j} k^{j}$$

$$= \sum_{i=0}^{n} C_{2i}^{2n+1} u^{2n-2i}\, v^{2i} k^{i} - \sum_{i=0}^{n} C_{2n-2i+1}^{2n+1} u^{2i}\, v^{2n-2i} k^{n-i}$$

$$= \sum_{i=0}^{n} C_{2i}^{2n+1} (u^{2n-2i}\, v^{2i} k^{i} - u^{2i} v^{2n-2i} k^{n-i})$$

我們將上式從「中間」分開：

$$= \sum_{i=0}^{\left[\frac{n}{2}\right]} C_{2i}^{2n+1} (u^{2n-2i}\, v^{2i} k^{i} - u^{2i} v^{2n-2i} k^{n-i}) + \sum_{i=\left[\frac{n}{2}\right]+1}^{n} C_{2i}^{2n+1} (u^{2n-2i}\, v^{2i} k^{i} - u^{2i} v^{2n-2i} k^{n-i})$$

$$= \sum_{i=0}^{\left[\frac{n}{2}\right]} C_{2i}^{2n+1} u^{2i} v^{2i} k^i (u^{2n-4i} - v^{2n-4i} k^{n-2i}) + \sum_{i=\left[\frac{n}{2}\right]+1}^{n} C_{2i}^{2n+1} u^{2n-2i} v^{2n-2i} k^{n-i} (k^{2i-n} v^{4i-2n} - u^{4i-2n})$$

令 $j = n - i$，則上式的第二項 $\sum_{i=\left[\frac{n}{2}\right]+1}^{n} C_{2i}^{2n+1} u^{2n-2i} v^{2n-2i} k^{n-i} \left(k^{2i-n} v^{4i-2n} - u^{4i-2n}\right)$ 會等於

$$\begin{cases} \sum_{j=0}^{\left[\frac{n}{2}\right]-1} C_{2n-2j}^{2n+1} u^{2j} v^{2j} k^j (k^{n-2j} v^{2n-4j} - u^{2n-4j}), \text{當 } n = 2 \cdot \left[\frac{n}{2}\right] \\ \sum_{j=0}^{\left[\frac{n}{2}\right]} C_{2n-2j}^{2n+1} u^{2j} v^{2j} k^j (k^{n-2j} v^{2n-4j} - u^{2n-4j}), \text{當 } n = 2\left[\frac{n}{2}\right] + 1 \end{cases}$$

由於 $n = 2 \cdot \left[\frac{n}{2}\right]$ 時，若令 $j = \left[\frac{n}{2}\right]$ ，則 $k^{n-2j} v^{2n-4j} - u^{2n-4j} = k^0 v^0 - u^0 = 0$，因此，我們可以假設當時 $j = n - i$，會有

$$\sum_{i=\left[\frac{n}{2}\right]+1}^{n} C_{2i}^{2n+1} u^{2n-2i} v^{2n-2i} k^{n-i} \left(k^{2i-n} v^{4i-2n} - u^{4i-2n}\right)$$

$$= \sum_{j=0}^{\left[\frac{n}{2}\right]} C_{2n-2j}^{2n+1} u^{2j} v^{2j} k^j (k^{n-2j} v^{2n-4j} - u^{2n-4j})$$

也因此會得到

$$\frac{\alpha}{u} - \frac{\beta}{v}$$

$$= \sum_{i=0}^{\left[\frac{n}{2}\right]} C_{2i}^{2n+1} u^{2i} v^{2i} k^i (u^{2n-4i} - v^{2n-4i} k^{n-2i}) + \sum_{j=0}^{\left[\frac{n}{2}\right]} C_{2n-2j}^{2n+1} u^{2j} v^{2j} k^j (k^{n-2j} v^{2n-4j} - u^{2n-4j})$$

$$= \sum_{i=0}^{\left[\frac{n}{2}\right]} (C_{2i}^{2n+1} u^{2i} v^{2i} k^i - C_{2n-2i}^{2n+1} u^{2j} v^{2j} k^j)(u^{2n-4i} - v^{2n-4i} k^{n-2i})$$

$$= \sum_{i=0}^{\left[\frac{n}{2}\right]} (C_{2i}^{2n+1} - C_{2n-2i}^{2n+1}) \cdot u^{2i} v^{2i} k^i \cdot \left(u^{2n-4i} - k^{n-2i} v^{2n-4i}\right)$$

我們處理上式中的 $C_{2i}^{2n+1} - C_{2n-2i}^{2n+1}$

$$
\begin{aligned}
C_{2i}^{2n+1} - C_{2n-2i}^{2n+1} &= \frac{(2n+1)!}{(2i)!\,(2(n-i)+1)!} - \frac{(2n+1)!}{(2n-2i)!\,(2i+1)!} \\
&= \frac{(2n+1)!\,\big(2i+1-(2n-2i+1)\big)}{(2i+1)!\,(2(n-i)+1)!} \\
&= \frac{(2n+1)!\,(4i-2n)}{(2i+1)!\,(2(n-i)+1)!} \\
&= C_{2i}^{2n+1} \cdot \frac{4i-2n}{2i+1} \\
&= -2 \cdot C_{2i}^{2n+1} \cdot \frac{n-2i}{2i+1} < 0
\end{aligned}
$$

將其帶入$\frac{\alpha}{u} - \frac{\beta}{v}$，可得

$$
\begin{aligned}
\frac{\alpha}{u} - \frac{\beta}{v} &= -2 \sum_{i=0}^{\left[\frac{n}{2}\right]} C_{2i}^{2n+1} \cdot \frac{n-2i}{2i+1} \cdot u^{2i} v^{2i} k^i \cdot \left(u^{2n-4i} - k^{n-2i} v^{2n-4i}\right) \\
&= -2 \sum_{i=0}^{\left[\frac{n}{2}\right]} C_{2i}^{2n+1} \cdot \frac{n-2i}{2i+1} \cdot u^{2i} v^{2i} k^i \cdot \left(u^{2(n-2i)} - (kv^2)^{n-2i}\right) < 0
\end{aligned}
$$

最後利用乘法公式

$$
u^{2t} - (kv^2)^t = (u^2 - kv^2) \sum_{j=0}^{t-1} u^{2(t-1-j)} k^j v^{2j}
$$

代入上式可得

$$
\begin{aligned}
\frac{\alpha}{u} - \frac{\beta}{v} &= -2 \sum_{i=0}^{\left[\frac{n}{2}\right]} C_{2i}^{2n+1} \cdot \frac{n-2i}{2i+1} \cdot u^{2i} v^{2i} k^i \cdot (u^2 - kv^2) \sum_{j=0}^{n-2i-1} u^{2(n-2i-j)} v^{2j} \\
&= -2(u^2 - kv^2) \sum_{i=0}^{\left[\frac{n}{2}\right]} \sum_{j=0}^{n-2i-1} C_{2i}^{2n+1} \cdot \frac{n-2i}{2i+1} \cdot u^{2i} v^{2i} k^i \cdot u^{2(n-2i-j)} v^{2j}
\end{aligned}
$$

這代表了 $u^2 - kv^2$ 是 $\frac{\alpha}{u} - \frac{\beta}{v}$的一個因數；故得證。■

【備註 3.7.1】

在上述定理中的 u 和 $\frac{\alpha}{u}$ 以及 v 和 $\frac{\alpha}{v}$ ，均分別是 α 和 β 的因數。因此，我們可以先計算 α 和 β 的因數的差（且必須為負數），從中挑選 p 出的倍數後，再將個別除以 α 和 β 的商代入佩爾方程式，即可檢驗 $X^m = \alpha + \sqrt{k}\beta$ 是否有整數解。

4. 結論與應用

在【**蜈蚣分解的延伸**】這一段中，我們將蜈蚣分解的技巧延伸到與 k 互質的奇質數平方 A^2，可以知道若 $x^2-ky^2=A^2$ 有不可約解，則 $x^2-ky^2=A$ 或 $x^2-ky^2=-A$ 亦有不可約解；見【**定理 3.2.1**】。再進一步深究【**定理 3.2.1**】，我們對 $x^2-ky^2=A$ 或 $x^2-ky^2=-A$ 的解，有更進一步的了解（整理至下表）。

$k\equiv 3 \pmod 4$ 且 u 是偶數		
$split\ u^2$ $-A^2$	$k\equiv 7 \pmod 8$ $(\tau\cdot\bar{\tau}=2)$	$k\equiv 3 \pmod 8$ $(\tau\cdot\bar{\tau}=-2)$
$\begin{cases} u+A=v_+^2 \\ u-A=kv_-^2 \end{cases}$	$\frac{\tau\lambda_+}{2}$ 與 $\frac{\bar{\tau}\lambda_+}{2}(x^2-ky^2=A)$	$\frac{\tau\lambda_+}{2}$ 與 $\frac{\bar{\tau}\lambda_+}{-2}(x^2-ky^2=-A)$
$\begin{cases} u+A=kv_+^2 \\ u-A=v_-^2 \end{cases}$	$\frac{\tau\lambda_-}{2}$ 與 $\frac{\bar{\tau}\lambda_-}{2}(x^2-ky^2=-A)$	$\frac{\tau\lambda_-}{2}$ 與 $\frac{\bar{\tau}\lambda_-}{-2}(x^2-ky^2=A)$

見【**備註 3.2.2**】

	$k\equiv 1 \pmod 4$	$k\equiv 3 \pmod 4$	
		v 為偶數	v 為奇數
$x^2-ky^2=A$	有不可約解 λ	只有一個有不可約解 λ	
$x^2-ky^2=-A$	有不可約解 $\sqrt{\sigma}\lambda$		
ω 的分解	λ^2 或 $\left(\sqrt{\sigma}\lambda\right)^2$	λ^2	$\sigma\lambda^2$

見【**備註 3.2.3**】

以【**定理 3.2.1**】的結果為基礎，我們可以進一步將 $x^2-ky^2=A$ 任意的一個不可約解，分解成兩個不可約解的乘積；見【**定理 3.2.3**】。從【**定理 3.2.3**】的證明中，我們可以了解到不可約解彼此影響的程度，可以用函數 $A_{i\pm}(\omega,\omega_i)$ 來形容；見【**備註 3.2.4**】。

由於在之前的作品中，我們曾提到佩爾質數的概念；見**參考資料**【8】。在【**佩爾質數的重新詮釋**】這一章節中，我們對佩爾質數給出了較簡便的定義；見【**定義 3.3.2**】。利用蜈蚣彘，我們產生了一些佩爾質數(見【**例子 3.3.1**】)，而這些佩爾質數的生成方式著實令我們意料之外。隨著這些例子的出現，不但讓佩爾質數的定義實質化，更解決了從以前就一直困擾著我們的問題；也就是對於兩個相異的廣義佩爾方程式 $x^2-ky^2=A$ 以及 $x^2-ky^2=B$ ，是否這

兩個方程式的可解性，會連動到方程式 $x^2-ky^2=AB$ 的可解性（見下表）

A	B	AB	說明或例子
有解	有解	有解	見參考資料【5】【定理 3.2】
有解	無解	有解	$x^2-79y^2=65$有解$x^2-79y^2=101$無解，$x^2-79y^2=65\cdot 101$有解
		無解	$x^2-5y^2=11$ 有解而$x^2-5y^2=2$ 無解，但 $x^2-5y^2=11\cdot 2$ 無解
無解	無解	有解	$x^2-79y^2=101$，$x^2-79y^2=5$ 皆無解，但 $x^2-79y^2=505$ 有解
		無解	$x^2-401y^2=5$ 、$x^2-401y^2=7$ 以及 $x^2-401y^2=5\cdot 7$ 均無解

隨著佩爾質數的出現方式，我們想徹底研究那些無解，但相乘後會是有解的質數；會有這樣的發想，也是因為從**【例子 3.3.1】**的發現。接著，我們試著去分割這些質數：對於給定一個奇質數 $p\neq k$，其中該質數所對應的方程式 $\pm p$ 均無解。我們定義

$$\Omega_p=\left\{ r\text{是一個質數}\mid r=p\text{ 或 }pr\text{ 是一個佩爾質數}\right\}$$

那麼對於相異的質數 p 與 q，會有 $\Omega_p\cap\Omega_q\neq\phi$ 或是 $\Omega_p=\Omega_q$。再根據**【定理 3.4.1】**，在 Ω_p 內的任兩個相異的質數相乘，都會是一個佩爾質數；這也就指出了在每一個相異的 Ω_p 中，兩兩相乘都可產生更多的佩爾質數。

然而，進展到在 Ω_p 中任取三個質數相乘，情況卻不一；有時候會有解（則必是佩爾質數），但有時候卻無解，對於這混亂的現象，我們迄今尚未有一個定論；見**【備註 3.4.2】**。

我們隨後考慮在 Ω_p 中任取四個質數相乘，從這裡我們便了解了**佩爾質數並無唯一分解性質**；見**【備註 3.4.3】**。此外，我們也得到 $L(k,p_1p_2p_3p_4)=L_{irr}(k,p_1p_2p_3p_4)$ 的值；見**【定理 3.4.5】**以及**【定理 3.4.6】**。更進一步的，我們再利用**【定理 3.4.5】**的方法，對於廣義的佩爾方程式 $x^2-ky^2=p_1p_2\cdots p_{2n}$，找出了一些不可約解的生成元；見**【定理 3.4.7】**。最後，我們在**【備註 3.4.5】**中發現了一些有趣的例子，並且再次提供了佩爾質數並沒有唯一分解性的例

子。

在【在佩爾地毯上爬行的蜈蚣】一節中，我們著眼於由兩個擁有蜈蚣彘現象質數的冪次乘積，所相對應到的廣義佩爾方程式。一開始的【定理 3.5.1】提供了極為重要的技巧，利用這個技巧在兩個擁有蜈蚣彘現象質數冪次乘積上，並且將有不可約解的佩爾方程式和坐標平面上的格子點做一對應（我們將其稱為佩爾地毯【定義 3.5.2】）可以發現這些點所構成的圖形宛如地毯的拼貼般的重複出現，利用【定理 3.5.2】到【定理 3.5.4】，我們確定了這些格子點的確會如拼貼般的重複出現，因此我們確定了基本區域的存在（見【定義 3.5.3】）。同樣引【定理 3.5.1】，我們只須了解基本區域內的廣義佩爾方程式，那就可以了解整個佩爾地毯以及地毯上所對應的方程式；因此自【定理 3.5.5】到【定理 3.5.11】，我們都在幾本區域上做討論，並對基本區域的形狀以及生成，有了一定程度的了解；其中最至關緊要的，還是蜈蚣彘的最低次方解是否為質數，以及佩爾地毯的生成因子$(\alpha, \alpha s)$（【定理 3.5.11】見）將會決定整個地毯的樣貌；前者一直是我們無法攻克的問題，而後者中的α將會與低次方有關，事實上會是最低次方解的因數。

接下來，我們試著考慮三維的佩爾地毯，也就是研究由三個具有蜈蚣彘現象的質數，所對應，呈現在三維空間的佩爾地毯。與二維的的地毯不同，雖然有些二維技巧和方法可以繼承到三維的研究上，但是複雜度相較於二維卻多了許多。在此，我們雖然有了一些結果（見【定理 3.5.12】到【定理 3.5.17】），但仍不如二維的討論般，對地毯的組成和形狀了解且清楚。

接著來到【Shoes 函數的一個問題開始】。

Shoes 函數$i(\omega, n)$ 和 $j(\bar{\omega}, n)$是用來衡量當一個不可約解ω^n(或是$\bar{\omega}^n$)要回到第一段時，需要利用多少的σ或是$\bar{\sigma}$來做調整，也就是說 Shoes 函數$i(\omega, n)$ 和 $j(\bar{\omega}, n)$會使得$\bar{\sigma}^{i(\omega,n)}\omega^n$以及 $\sigma^{j(\bar{\omega},n)}\bar{\omega}^n$會是在$x^2 - ky^2 = p^n$第一段的不可約解。

在這一章裡，我們致力於了解 Shoes 函數。首先，我們利用數據和計算先去觀察，發現了ω和$\bar{\omega}$的比值（我們稱為ρ）與σ的冪次有關：

$$\sigma^a < \rho < \sigma^b$$

而σ的冪次似乎就是$Farey\ Sequence$數列。為了，利用【定理 3.6.1】到【定理 3.6.5】，我們驗證了這個猜測，同時間也解決了之前學長對這個函數的一些困擾。為了瞭解解 Shoes 函數，我們定義了ρ函數（見【定義 3.6.2】），並且對ρ函數做了一些探討(見【備註 3.6.5】)，

而相當特別我們也認為或許未來可以當作研究的一個方向，就是將 ρ 函數做延伸到對應域為 $x^2 - ky^2 = 1$ 的函數 $\tilde{\rho}(x)$，而 $\tilde{\rho}(x)$ 將會是$x^2 - ky^2 = 1$ 在第一象限的參數化。

在最後，我們利用 $\rho(x)$ 連續性來得到【**定理 3.6.8**】的結果，也就是是否存在廣義佩爾方程式的不可約，使其解的分布會出現在指定區間的問題。

【**三次方根的必要條件**】是這次報告的最後一段的內容，雖結果不如前面章節多，但是在寫程式的實用上，提供了一個更便捷的方法；也因此我們決定將這個結果提出來，並做為這次研究的結束。

這源自於如何判斷一個不可約解，是否存在正整數解的三次方根的方法；然而我們發現其中的證明手法，可以推廣到奇次方根是否有正整數解的問題上。證明過程雖較為冗長，但結果的確也如我們所預期的，與之前的判斷三次方根的正整數解類似（見【**定理 3.7.1**】）。

5. 一些未解決的問題與猜想

在研究過程中，我們也碰到了一些無法證明的問題，我們將這些問題寫下，也期望之後的研究，對這些問題可以突破，並能從之發現更多有關佩爾方程式的現象與結果。

有關蜈蚣彘

【**問題一**】 首先，我們發現了「蜈蚣彘 × 蜈蚣彘」可能會得到佩爾質數。不僅如此，我們還發現若 $x^2 - ky^2 = p_1^3$ 和 $x^2 - ky^2 = p_2^3$ 均為蜈蚣彘，且這兩個方程式的不可約解分別 ω_1和 ω_2 ，那麼 $x^2 - ky^2 = p_1 p_2$ 的不可約解為

$$\omega_{12} = \sqrt[3]{\sigma\omega_1\overline{\omega_2}} \text{ 或} \sqrt[3]{\sigma\overline{\omega_1}\omega_2}$$

令人驚訝的是， $\sigma\omega_1\overline{\omega_2}$ 或 $\sigma\overline{\omega_1}\omega_2$ 開三次方根的結果都是整數。對於以上現象是否可以在其他有著相同前提的蜈蚣彘成立，或是有反例說明這只是特例，對我們來說仍是個謎。

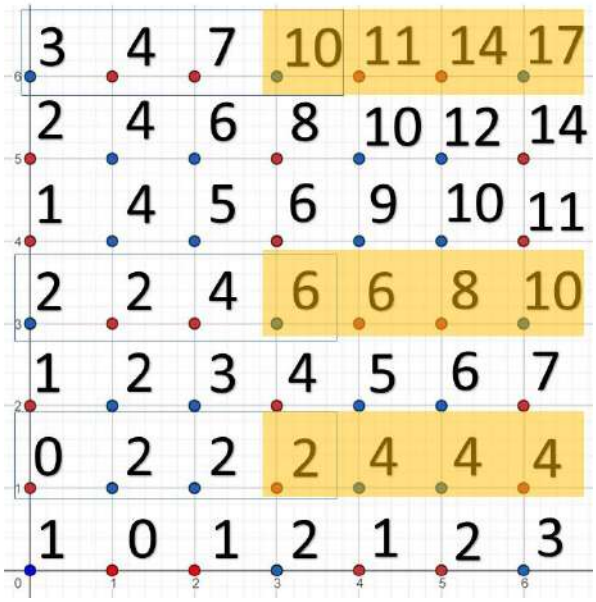
【**問題二**】 對於一個給定的奇質數 k，若相異的兩質數 p_1 與 p_2 均有 k −蜈蚣彘現象（假設最低次方解分別為 n_1 和 n_2），則是否存在 $1 \le \alpha < n_1$ 以及 $1 \le \beta < n_2$，使得是 $p_1^\alpha p_2^\beta$ 佩爾質數？

【問題三】 對於一個給定的奇質數 k，所產生的蜈蚣堯之最低次方解是否一定是質數，並且這樣的蜈蚣堯有無限多個呢？

【問題四】 對於一個給定的奇質數 k，是否有不同的蜈蚣堯，且最低次方解不相同的情況呢？

有關佩爾地毯

【問題五】 首先先看到我們的發現：。



這是三次方蜈蚣堯的佩爾地毯，在這張圖中，藍色點代表有不可約解的點 $\left(L\left(k,(\alpha,\beta)\right)>0\right)$，而紅色點代表全部的解都是可約解 $\left(L\left(k,(\alpha,\beta)\right)=0\right)$。我們觀察 $y=1$ 這條直線，我們發現最下方的藍色框框全部加 2 就會是橘色框框；觀察 $y=3$ 這條直線，我們發現最下方的藍色框框全部加 4 就會是橘色框框。不管 y 式多少，我們都有觀察到這個規律：在 $y=\alpha$ 這條線上，從知道藍色框框的解的長度，加上 $\alpha+1$ 就會橘色框框的解的長度。更神奇的是，這個不只是出現在 3-次方蜈蚣堯、5-次方蜈蚣堯兩種形狀的地毯也有這種現象。對於這現象，我們目前也是一無所知。

【問題六】 若 $x^2-ky^2=p_1$ 與 $x^2-ky^2=p_2$ 皆為 n-蜈蚣堯，且 $\alpha=n\cdot q_\alpha+\alpha'$、$\beta=n\cdot q_\beta+\beta'$，在幫佩爾地毯降次方時，我們發現把 x 座標降低 n 時，長度會變少 $\beta+1$；而把 y 座標降低 n 時，長度會變少 $\alpha+1$，因此我們有

$$L\left(k,p_1^{\alpha}p_2^{\beta}\right)=L\left(k,p_1^{\alpha'}p_2^{\beta'}\right)+q_\alpha(\beta+1)+q_\beta(\alpha+1)$$

最後我們用程式跑了 $k=37, p_1=3, p_2=7, p_3=11, p_4=41, p_5=47, p_6=53, p_7=71, p_8=73$ 這些方程式的解長度，結果如下表：

方程式	$L(k, \prod p_i)$
$\boldsymbol{x^2-37y^2=3\cdot 7=21}$	2
$\boldsymbol{x^2-37y^2=3\cdot 7\cdot 11=231}$	2
$\boldsymbol{x^2-37y^2=3\cdot 7\cdot 11\cdot 41=9471}$	6
$\boldsymbol{x^2-37y^2=3\cdot 7\cdot 11\cdot 41\cdot 47=445137}$	10
$\boldsymbol{x^2-37y^2=3\cdot 7\cdot 11\cdot 41\cdot 47\cdot 53=23592261}$	22
$\boldsymbol{x^2-37y^2=3\cdot 7\cdot 11\cdot 41\cdot 47\cdot 53\cdot 71=1675050531}$	42
$\boldsymbol{x^2-37y^2=3\cdot 7\cdot 11\cdot 41\cdot 47\cdot 53\cdot 71\cdot 73=122278688763}$	86

我們定義 $L_n=L(k, \prod_{i=1}^{n} p_i)$ 。仔細觀察上表中 L_n 的值，發現這似乎有滿足一個遞迴關係：

$$\begin{cases} L_1=0, L_2=2, L_3=2 \\ L_t=L_{t-1}+2L_{t-2} \end{cases}$$

利用以上遞迴式，我們可以用馬克勞林級數將公式簡化

設 $f(x)=\sum_{t=1}^{\infty} L_t x^t$ ，我們將以下三式做相加

$$f(x)=L_1x+L_2x^2+L_3x^3\cdots\cdots+L_tx^t\cdots\cdots$$

$$-xf(x)=\quad -L_1x^2-L_2x^3\cdots\cdots-L_{t-1}x^t\cdots\cdots$$

$$-2x^2f(x)=\quad -2L_1x^3\cdots\cdots-2L_{t-2}x^t\cdots\cdots$$

$$(1-x-2x^2)f(x)=L_1x+(L_2-L_1)x^2$$

$$f(x)=-\frac{2x^2}{2x^2+x-1}=-1-\left(\frac{-x+1}{(2x-1)(x+1)}\right)=-1+\frac{2}{3}\cdot\frac{1}{1+x}+\frac{1}{3}\cdot\frac{1}{1-2x}$$

展開成級數後會得到

$$f(x)=-1+\frac{2}{3}\sum_{t=0}^{\infty}(-x)^t+\frac{1}{3}\sum_{t=0}^{\infty}(2x)^t=\sum_{t=1}^{\infty}\left\{\left[\frac{1}{3}\cdot 2^t+\frac{2}{3}\cdot(-1)^t\right]x^t\right\}$$

因此我們猜測：

$$L_t = \frac{1}{3}\cdot 2^t + \frac{2}{3}\cdot(-1)^t$$

6. 參考資料

【1】 James K. Strayler（1994）Elementary Number theory. Waveland Press, Inc.

【2】 Titu Andreescu, Dorin Andrica（2015）Quadratic Diophantine Equations. Springer

【3】 許志農（無日期）佩爾方程式。

【4】 許志農（無日期）再談佩爾方程式。

【5】 黃唯宣，許立澄，鄭正杰（民 106）。有關廣義佩爾方程式的一些討論。新北市 105 學年度中小學科學展覽會作品。

【6】 鍾翔宇（民 109）。佩爾，又見佩爾！一些有關廣義佩爾方程式的研究。新北市 109 學年度中小學科學展覽會作品。

【7】 張耕宇（民 110）。被廣義佩爾方程式附身的蜈蚣。新北市 110 學年度中小學科學展覽會作品。

【8】 張耕宇，翁家宏（民 111）。不再附身於蜈蚣的廣義佩爾方程式。新北市 110 學年度中小學科學展覽會作品。

7. 附錄

1. 必要的證明

【定理 7.1.1】

設 $\omega = u + v\sqrt{k}$ 為 $x^2 - ky^2 = A$ 的一個不可約解 ，那麼對於任意的正整數 n， ω^n 是 $x^2 - ky^2 = A^n$ 的一個不可約解 ，其中奇質數 k 與奇數 A 互質。

【證明】

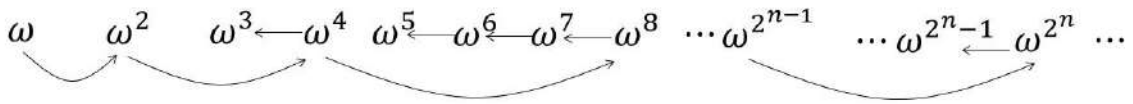
首先我們先證明對於任意的正整數 n， ω^2 是 $x^2 - ky^2 = A^2$ 的一個不可約解；已知 $\omega = u + v\sqrt{k}$ 是不可約解，那麼 $\omega^2 = (u^2 + kv^2) + 2uv\sqrt{k}$ 便會是 $x^2 - ky^2 = A^2$ 的一個解。假設質數 p 是 $\gcd\big((u^2 + kv^2), (2uv)\big)$ 的一個因數，這代表 p 可以整除$(u^2 + kv^2)^2 - k(2uv)^2 = A^2$，也因此 p 必為奇數。

由於 p 是 $\gcd\big((u^2 + kv^2), (2uv)\big)$ 的一個因數且 p 為奇數，根據 ω 的不可約性， p 必定只會整除 u 或 v 其中一個。但是 p 可以整除 A，這代表 p 可以整除 A，u 以及 v 其中兩者；

然而根據 $u^2 - kv^2 = A$，質數 p 定可以整除 u 以及 v，這便與 ω 的不可約性矛盾；故這樣的質數 p 不存在，也就是說 $\gcd\big((u^2 + kv^2), (2uv)\big) = 1$，即 ω^2 是不可約的。

根據上面的論證得知，ω 是不可約若且為若 ω^2 是不可約；因此，當 ω 是 $x^2 - ky^2 = A$ 的一個不可約解時，那麼對於任意的正整數 n， ω^{2^n} 是 $x^2 - ky^2 = A^{2^n}$ 的一個不可約解。接著，我們再利用 ω 是不可約若且為若 ω^2 是不可約，來證明 ω^n 的不可約性。

利用反證法，假設對於某個正整數 n， ω^n 是可約解，那麼存在一個足夠大的正整數 m，使得 $n < 2^m$，也因此 $\omega^{2^m} = \omega^n \cdot \omega^{2^m - n}$ 是可約的；然而這與 ω^{2^m} 的不可約性矛盾，故對於任意的正整數 n， ω^n 是 $x^2 - ky^2 = A^n$ 的一個不可約解。



利用上圖，以上的內容可以更加容易了解；故得證。■

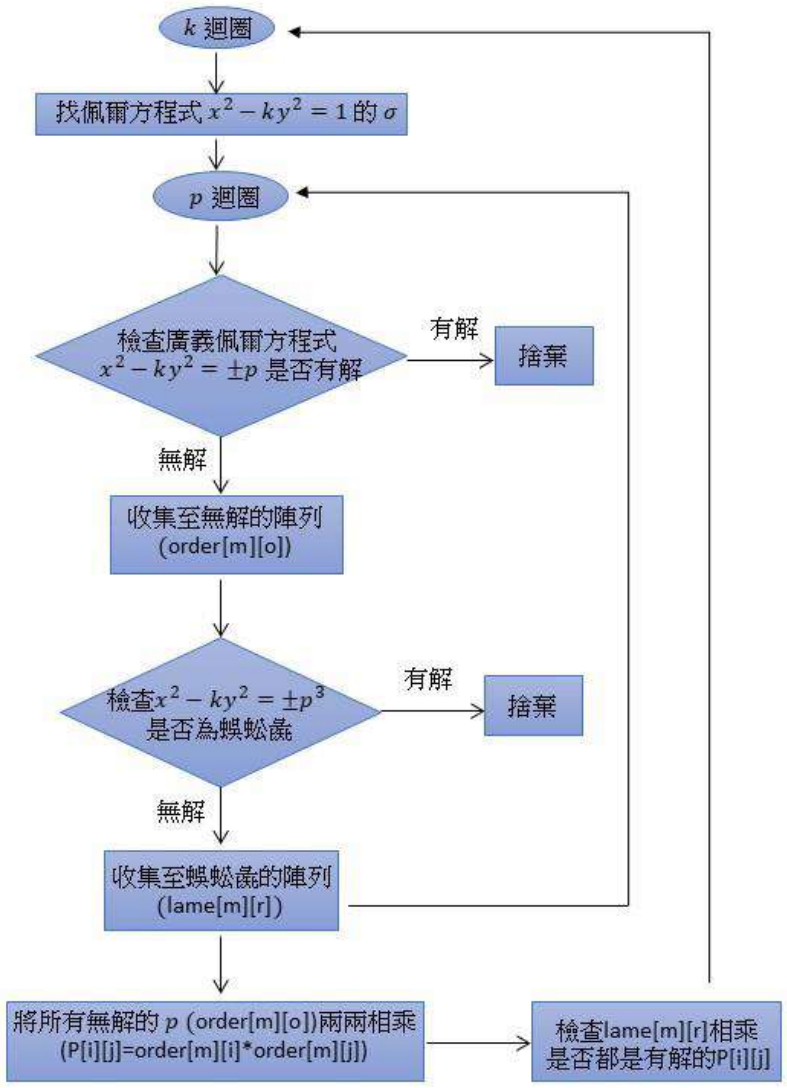
【備註 7.1.1】

若 $A = 2^m$，則 $x^2 - ky^2 = 2^m$ 會根據 k 給 8 除的餘數而有不同的結果；更多內容詳見**參考資料【8】【五、混亂的 $l(k, 2^n)$】**。

2. 【備註 3.2.4】第三點中提到的分解

ω	$\xrightarrow{\times\overline{\omega_1}}$	$-(\omega,\omega_1)=\frac{\omega\overline{\omega_1}}{p_1^{n_1}}$	$\xrightarrow{\times\overline{\omega_2}}$	$-(-(\omega,\omega_1),\omega_2)=\frac{\omega\overline{\omega_1\omega_2}}{p_1^{n_1}p_2^{n_2}}$	$\xrightarrow{\times\overline{\omega_3}}$	$-(-(-(\omega,\omega_1),\omega_2),\omega_3)=\frac{\omega\overline{\omega_1\omega_2\omega_3}}{p_1^{n_1}p_2^{n_2}p_3^{n_3}}(=1)$	$(E1)$
					$\xrightarrow{\times\omega_3}$	$+(-(-(\omega,\omega_1),\omega_2),\omega_3)=\frac{\omega\overline{\omega_1\omega_2}}{p_1^{n_1}p_2^{n_2}}\omega_3(=\omega_3^2)$	$(E2)$
			$\xrightarrow{\times\omega_2}$	$+(-(\omega,\omega_1),\omega_2)=\frac{\omega\overline{\omega_1}}{p_1^{n_1}}\omega_2$	$\xrightarrow{\times\overline{\omega_3}}$	$-(+(-(\omega,\omega_1),\omega_2),\omega_3)=\frac{\omega\overline{\omega_1\omega_3}}{p_1^{n_1}P_3^{n_3}}\omega_2(=\omega_2^2)$	$(E3)$
					$\xrightarrow{\times\omega_3}$	$+(+(-(\omega,\omega_1),\omega_2),\omega_3)=\frac{\omega\overline{\omega_1}}{p_1^{n_1}}\omega_2\omega_3(=\omega_2^2\omega_3^2)$	$(E4)$
	$\xrightarrow{\times\omega_1}$	$+(\omega,\omega_1)=\omega\omega_1$	$\xrightarrow{\times\overline{\omega_2}}$	$-(+(\omega,\omega_1),\omega_2)=\frac{\omega\omega_1\overline{\omega_2}}{p_2^{n_2}}$	$\xrightarrow{\times\overline{\omega_3}}$	$-(-(+(\omega,\omega_1),\omega_2),\omega_3)=\frac{\omega\omega_1\overline{\omega_2\omega_3}}{p_2^{n_2}p_3^{n_3}}(=\omega_1^2)$	$(E5)$
					$\xrightarrow{\times\omega_3}$	$+(-(+(\omega,\omega_1),\omega_2),\omega_3)=\frac{\omega\omega_1\overline{\omega_2}}{p_2^{n_2}}\omega_3(=\omega_1^2\omega_3^2)$	$(E6)$
			$\xrightarrow{\times\omega_2}$	$+(+(\omega,\omega_1),\omega_2)=\omega\omega_1\omega_2$	$\xrightarrow{\times\overline{\omega_3}}$	$-(+(+(\omega,\omega_1),\omega_2),\omega_3)=\frac{\omega\omega_1\omega_2\overline{\omega_3}}{p_3^{n_3}}(=\omega_1^2\omega_2^2)$	$(E7)$
					$\xrightarrow{\times\omega_3}$	$+(+(+(\omega,\omega_1),\omega_2),\omega_3)=\omega\omega_1\omega_2\omega_3$	$(E8)$

3. 程式碼



我們的作法是先輸入挑選範圍內的所有質數(我們是設定能夠讓 $x^2-ky^2=1$ 有比較小的解的質數 k ，例如 $x^2-61y^2=1$ 的第一個解有 10 位數，我們就不選 61 了)。首先，我們先讓 k 去迴圈，再讓 p 迴圈，一個一個去找 $x^2-ky^2=p$ 有沒有正整數解，將有正整數解的 p 捨棄掉，並將沒有正整數解的 p 儲存下來，接著將所有儲存下來的 p 兩兩互乘，看看有沒有得到有解的方程式 $x^2-ky^2=p_ip_j$ 。透過程式，我們找到三次方蜈蚣彘的「蜈蚣彘 × 蜈蚣彘」結果通通都是佩爾質數，我們也有設檢查機制檢驗我們的猜想是否正確。

```
#include<iostream>
#include<fstream>
#include<math.h>
#include <algorithm>
using namespace std;
int main ()
{
    long long int x,y,a,X2,KxY2,y_start,tan,X,Y,ppp,PPP,q;//2^63
    short int m,n,flag,order[45][45],lame[45][45],o=0,i,j,r=0,np=0;//2^15
    unsigned int alpha,beta,u,v,aukbv,buav,P[45][45];//2^32
    short int
k,p,prime[45]={3,5,7,11,13,17,19,23,29,31,37,41,43,47,53,59,67,71,73,79,83,101,103,107,109,113,127,131,137,139,14
```

```
9,151,157,163,167,173,179,181,191,193,197,199,211,223,227},max[45],maxr[45],pprime[45]={3,5,7,11,13,17,19,23,2
9,31,37,41,43,47,53,59,67,71,73,79,83,101,103,107,109,113,127,131,137,139,149,151,157,163,167,173,179,181,191,1
93,197,199,211,223,227};
      fstream pell_File;
      //Open file
      pell_File.open("pell prime.txt", ios::out);

       for(m=0;m<=44;m++)//k 迴圈
       {
            k=prime[m];
            cout<<"================================================="<<endl;
            for(x=1;x<=2000001;x++)//求 sigma
                  {     flag=0;
                        y_start=sqrt((x*x-1)/k);//speed up
                        if (y_start<=1) y_start=1;//speed up
                        X2=x*x;//speed up
                        for(y=y_start;y<=x;y++)
                        {
                              KxY2=k*y*y;
                              a=X2-KxY2;
                              if(a==1)
                              {
                                    cout<<"k="<<k<<" sigma=>"<<"x="<<x<<" y="<<y<<"      "<<X2<<"-
"<<KxY2<<"="<<x*x-k*y*y<<endl;
                                    //pell_File<<"k="<<k<<","<<"
sigma=>"<<","<<"x="<<x<<","<<"y="<<y<<","<<X2<<","<<"-"<<","<<KxY2<<","<<"="<<","<<a<<'\n';
                                    alpha=x;
                                    beta=y;
                                    flag++;
                              }
                              if(a<p)break;// speed up
                              if(flag==1)break;
                        }
                        if(flag==1)break;
                  }
            //求 x^2-ky^2=p
            for(n=0;n<=44;n++)//p 迴圈
            {
                  p=prime[n];
                  if(k==p)
```

```
{
	n=n+1;
	p=prime[n];
}
cout<<"k="<<k<<'\t'<<"p="<<p<<"########################\n";
//pell_File<<"k="<<k<<","<<"p="<<p<<"########################\n";
flag=0;
tan=sqrt(abs(p)*(alpha+1)/2);
for(x=1;x<=tan+5;x++)//x 迴圈
{
	y_start=sqrt((x*x-p)/k);//speed up
	if (y_start<=1) y_start=1;//speed up
	X2=x*x;//speed up

	for(y=y_start;y<=x;y++)//y 迴圈
	{
		KxY2=k*y*y;
		a=X2-KxY2;
		if(p==a)
			{
				flag++;
				if(flag==1)break;
			}
		if(flag==1)break;
		if(a<p)break;// speed up

	}
	if(flag==1)break;
}
//若 x^2-ky^2=p 無解，則試求 x^2-ky^2=-p
//求 x^2-ky^2=-p
if(flag==0)
{
	p=-prime[n];
	tan=sqrt(abs(p)*(alpha+1)/2);
	for(x=1;x<=tan+5;x++)//x 迴圈
	{
		y_start=sqrt((x*x-p)/k);//speed up
		if (y_start<=1) y_start=1;//speed up
		X2=x*x;//speed up
```

```
            for(y=y_start;y<=x;y++)//y 迴圈
            {
                KxY2=k*y*y;
                a=X2-KxY2;
                if(p==a)
                    {
                        flag++;
                        if(flag==1)break;
                    }
                if(flag==1)break;
                if(a<p)break;// speed up
            }
            if(flag==1)break;
        }
}
//如果無解就記錄下來
if(flag==0)
{
        order[m][o]=abs(p);
        cout<<"無解 order["<<m<<"]["<<o<<"] = "<<order[m][o]<<endl;
        o++;
        p=-p;
//檢驗是否為蜈蚣兿
//求 x^2-ky^2=p^3
        ppp=p*p*p;
        tan=sqrt(abs(ppp)*(alpha+1)/2);
        for(x=1;x<=tan+5;x++)//x 迴圈
        {
        X2=x*x;//speed up
        y_start=sqrt((X2-ppp)/k);//speed up
        if (y_start<=1) y_start=1;//speed up
            for(y=y_start;y<=x;y++)//y 迴圈
            {
                KxY2=k*y*y;
                a=X2-KxY2;
                if(ppp==a)
                {
                    cout<<"x="<<x<<'\t'<<"y="<<y<<'\t';
                    cout<<X2<<"-"<<KxY2<<"="<<a<<'\t'<<endl;
                    flag++;
```

```
                }
        if(flag==1)
        {
                cout<<"水啦!蜈蚣彘出現了!"<<endl;
                lame[m][r]=p;
                cout<<"lame["<<m<<"]["<<r<<"] = "<<lame[m][r]<<"為蜈蚣彘"<<endl;
                r++;
        }
        if(a<ppp)break;// speed up
        if(flag==1)break;
        }
        if(flag==1)break;
}
//  求 x^2-ky^2=-p^3
        if(flag==0)
        {
        ppp=-ppp;
        tan=sqrt(abs(ppp)*(alpha+1)/2);
        for(x=1;x<=tan+5;x++)//x 迴圈
        {
        X2=x*x;//speed up
        y_start=sqrt((X2-ppp)/k);//speed up
        if (y_start<=1) y_start=1;//speed up
        for(y=y_start;y<=x;y++)//y 迴圈
        {
        KxY2=k*y*y;
        a=X2-KxY2;
        if(ppp==a)
        {
                cout<<"x="<<x<<'\t'<<"y="<<y<<'\t';
                cout<<X2<<"-"<<KxY2<<"="<<a<<'\t'<<endl;
                flag++;
        }if(a<ppp)break;
        if(flag==1)
        {
                cout<<"水啦!蜈蚣彘出現了!"<<endl;
                lame[m][r]=-p;
                cout<<"lame["<<m<<"]["<<r<<"] = "<<lame[m][r]<<"為蜈蚣彘"<<endl;
                r++;
```

```
                                        }if(flag==1)break;
                                    }if(flag==1)break;
                                }


                                }
                        if(flag==0)
                        {
                                cout<<"三次方無互質解"<<endl;
                        }
                }
        }
        maxr[m]=r;
        r=0;
        max[m]=o;
        o=0;
}
//兩兩互乘
for(m=0;m<=44;m++)//k 迴圈
{
        k=pprime[m];
        cout<<"=================================================="<<endl;
        pell_File<<"==================================================\n";
        for(x=1;x<=2000001;x++)//求 sigma
        {
                flag=0;
                y_start=sqrt((x*x-1)/k);//speed up
                if (y_start<=1) y_start=1;//speed up
                X2=x*x;//speed up
                for(y=y_start;y<=x;y++)
                {
                        KxY2=k*y*y;
                        a=X2-KxY2;
                        if(a==1)
                        {
                                cout<<"k="<<k<<" sigma=>"<<"x="<<x<<" y="<<y<<"      "<<X2<<"-
"<<KxY2<<"="<<x*x-k*y*y<<endl;
                                alpha=x;
                                beta=y;
                                flag++;
                        }
```

```
                    if(a<p)break;// speed up
                    if(flag==1)break;
                }
                if(flag==1)break;
            }
            //找 omega
            //輸出幾個無解
            cout<<"k="<<k<<"  時  "<<max[m]<<"個無解"<<endl;
            pell_File<<"k="<<k<<"  時  "<<max[m]<<"個無解\n";
            for(int M=0;M<=max[m]-1;M++)
            {
                cout<<" "<< order[m][M];
                pell_File<<" "<< order[m][M];
            }
            cout<<endl;
            pell_File<<"\n";
            //輸出幾個無解
            //輸出幾個蜈蚣兿
            cout<<"蜈蚣兿"<<maxr[m]<<"個";
            pell_File<<"k="<<k<<"的蜈蚣兿"<<maxr[m]<<"個";
            for(int N=0;N<=maxr[m]-1;N++)
            {
                cout<<" "<< lame[m][N];
                pell_File<< " "<< lame[m][N];
            }
            cout<<endl;
            pell_File<<"\n";
            for(i=0;i<=max[m]-1;i++)
            {
                for(j=i+1;j<=max[m]-1;j++)
                {
                    P[i][j]=order[m][i]*order[m][j];//兩兩互乘
                    q=-order[m][i]*order[m][j];
                    cout<<"k="<<k<<'\t'<<"p="<<P[i][j]<<"="<<order[m][i]<<" * "<<order[m][j]<<" i="<<i<<"
j="<<j<<"########################\n";
                    //pell_File<<"k="<<k<<","<<"p="<<p<<"########################\n";
                    flag=0;
                    tan=sqrt(P[i][j]*(alpha+1)/2);
                    for(x=1;x<=tan+5;x++)//x 迴圈
                    {
```

```
                    y_start=sqrt((x*x-P[i][j])/k);//speed up
                    if (y_start<=1) y_start=1;//speed up
                    X2=x*x;//speed up
                    for(y=y_start;y<=x;y++)//y 迴圈
                    {
                        KxY2=k*y*y;
                        a=X2-KxY2;
                        if(P[i][j]==a)
                        {
                            flag++;
                            if(flag==1)
                            {
                                cout<<"x="<<x<<"    y="<<y<<endl;

    pell_File<<"k="<<k<<'\t'<<"p="<<P[i][j]<<"="<<order[m][i]<<"*"<<order[m][j]<<" i="<<i<<"
j="<<j<<"########################\n";
                                pell_File<<"x="<<x<<"    y="<<y<<"\n";
                                cout<<"發現佩爾質數了!發現佩爾質數了!"<<endl;
                                np++;
                                cout<<np;
                                u=x;
                                v=y;
                                cout<<"omaga=>"<<"x="<<u<<" y="<<v<<","<<x*x<<"-
"<<k*y*y<<"="<<a<<endl;
                                pell_File<<"omaga=>"<<",x="<<u<<","<<"
y="<<v<<","<<x*x<<","<<"-"<<","<<k*y*y<<","<<"="<<","<<a<<",\n";
                                aukbv=alpha*u+k*beta*v;
                                buav=beta*u+alpha*v;
                                cout<<"sigma*omaga=>"<<" x="<<aukbv<<" y="<<buav<<endl;
                                pell_File<<"sigma*omaga=>"<<",,"<<",x="<<aukbv<<","<<"
y="<<buav<<'\n';
                                flag=0;
                                for(X=1;X<=200000000;X++)//x 迴圈
                                {
                                    y_start=sqrt((X*X-P[i][j])/k);//speed up
                                    if (y_start<=1) y_start=1;//speed up
                                    X2=X*X;//speed up
                                    for(Y=y_start;Y<=X;Y++)//y 迴圈
                                    {
                                        KxY2=k*Y*Y;
```

```
                                        a=X2-KxY2;
                                    if(P[i][j]==a)
                                    {
                                        flag++;
                                        cout<<flag<<"."<<"x="<<X<<"    y="<<Y<<'\t';
                                        pell_File<<flag<<"."<<"x="<<X<<"    y="<<Y<<"\t";
                                        cout<<"x,y 的最大公因數:"<<__gcd(X,Y)<<endl;
                                        pell_File<<"x,y 的最大公因數:"<<__gcd(X,Y)<<"\n";
                                        if(Y==buav)
                                        {
                                            cout<<"L 長度為:"<<flag-1<<"\n";
                                            pell_File<<"L 長度為:"<<flag-1<<"\n";
                                            flag=100;
                                            break;
                                        }
                                        if(flag==100)break;
                                        }if(flag==100)break;
                                        if(a<P[i][j])break;
                                    }if(flag==100)break;
                                }
                            }
                        if(flag==100)break;
                        }
                    if(flag==100)break;
                    if(a<P[i][j])break;// speed up
                    }
                if(flag==100)break;
                }
                if(flag==0)
                {
                    cout<<"k="<<k<<'\t'<<"p="<<q<<"=-"<<order[m][i]<<" * "<<order[m][j]<<" i="<<i<<"
j="<<j<<"########################\n";
                    tan=sqrt(abs(q)*(alpha+1)/2);
                    for(x=1;x<=tan+5;x++)//x 迴圈
                    {
                        y_start=sqrt((x*x-q)/k);//speed up
                        if (y_start<=1) y_start=1;//speed up
                        X2=x*x;//speed up
                        for(y=y_start;y<=x;y++)//y 迴圈
                        {
```

```
                                        KxY2=k*y*y;
                                        a=X2-KxY2;
                                        if(q==a)
                                        {
                                            flag++;
                                            if(flag==1)
                                            {
                                                cout<<"x="<<x<<"    y="<<y<<endl;

    pell_File<<"k="<<k<<'\t'<<"p="<<P<<"="<<order[m][i]<<"*"<<order[m][j]<<" i="<<i<<"
j="<<j<<"########################\n";
                                                pell_File<<"x="<<x<<"    y="<<y<<"\n";
                                                cout<<"發現佩爾質數了!發現佩爾質數了!"<<endl;
                                                np++;
                                                cout<<np;
                                                u=x;
                                                v=y;
                                                cout<<"omaga=>"<<"x="<<u<<" y="<<v<<","<<x*x<<"-
"<<k*y*y<<"="<<a<<endl;
                                                pell_File<<"omaga=>"<<",x="<<u<<","<<"
y="<<v<<","<<x*x<<","<<"-"<<","<<k*y*y<<","<<"="<<","<<a<<",\n";
                                                aukbv=alpha*u+k*beta*v;
                                                buav=beta*u+alpha*v;
                                                cout<<"sigma*omaga=>"<<" x="<<aukbv<<"
y="<<buav<<endl;
                                                pell_File<<"sigma*omaga=>"<<",,"<<",x="<<aukbv<<","<<"
y="<<buav<<'\n';
                                                flag=0;
                                                for(X=1;X<=200000000;X++)//x 迴圈
                                                {
                                                    y_start=sqrt((X*X-q)/k);//speed up
                                                    if (y_start<=1) y_start=1;//speed up
                                                    X2=X*X;//speed up
                                                    for(Y=y_start;Y<=X;Y++)//y 迴圈
                                                    {
                                                        KxY2=k*Y*Y;
                                                        a=X2-KxY2;
                                        if(q==a)
                                        {
                                        flag++;
```

```
                                        cout<<flag<<"."<<"x="<<X<<"    y="<<Y<<'\t';
                                        pell_File<<flag<<"."<<"x="<<X<<"    y="<<Y<<"\t";
                                        cout<<"x,y 的最大公因數:"<<__gcd(X,Y)<<endl;
                                        pell_File<<"x,y 的最大公因數:"<<__gcd(X,Y)<<"\n";
                                            if(Y==buav)
                                            {
                                                cout<<"L 長度為:"<<flag-1<<"\n";
                                                pell_File<<"L 長度為:"<<flag-1<<"\n";
                                                flag=100;
                                                break;
                                            }
                                                    if(flag==100)break;
                                                    }if(flag==100)break;
                                                    if(a<q)break;
                                                }if(flag==100)break;
                                            }
                                        }
                                    if(flag==100)break;
                                    }
                                if(flag==100)break;
                                if(a<q)break;// speed up
                                }
                            if(flag==100)break;
                            }
                        }
                    if(flag==0)cout<<P[i][j]<<"無解"<<endl;
                    }
                }
                cout<<np<<"組佩爾質數"<<endl;
                pell_File<<np<<"組佩爾質數"<<endl;
                if(maxr[m]*(maxr[m]-1)/2==np) cout<<maxr[m]*(maxr[m]-1)/2<<"合理";
                else cout<<maxr[m]*(maxr[m]-1)/2<<"完蛋了完蛋了完蛋了完蛋了 ";
                np=0;
            }
        pell_File.close();
         return 0;
}
```

【評語】010018

作者首先證明廣義佩爾方程 $x^2-my^2=n$ 的解(x,y)具有唯一分解性，並且著手研究不可約解的相關性質，以此不可約性定義出佩爾質數。接著研究一般解分解成不可約解的過程，發現這些過程會形成作者自行定義的「蜈蚣彘」的現象。作者透過分類 m 與 n 的同餘性質，將這些不同的情況的蜈蚣彘一一計算出來，系統性的找出很多佩爾方程的解，並且將這些解對應到二維平面或三維空間中的格子點。透過其幾何性質，作者能夠更清楚的刻畫蜈蚣彘的性質。此外，作者也提出一些猜想，並寫程式驗證數值較小的特例，尚無反例出現。整體而言，本作品雖然提出一個具有原創性的想法(佩爾地毯)，但是作者並無法在本問題任何一個重要的方向上取得具體進展，使得作品結果呈現出太過瑣碎的樣態，是相當可惜之處。