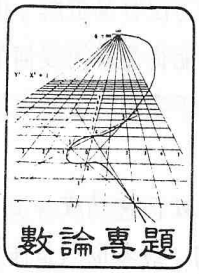


Diophantine方程

于 靖

第一部份 概 論

§ 1 Diophantine 方程式

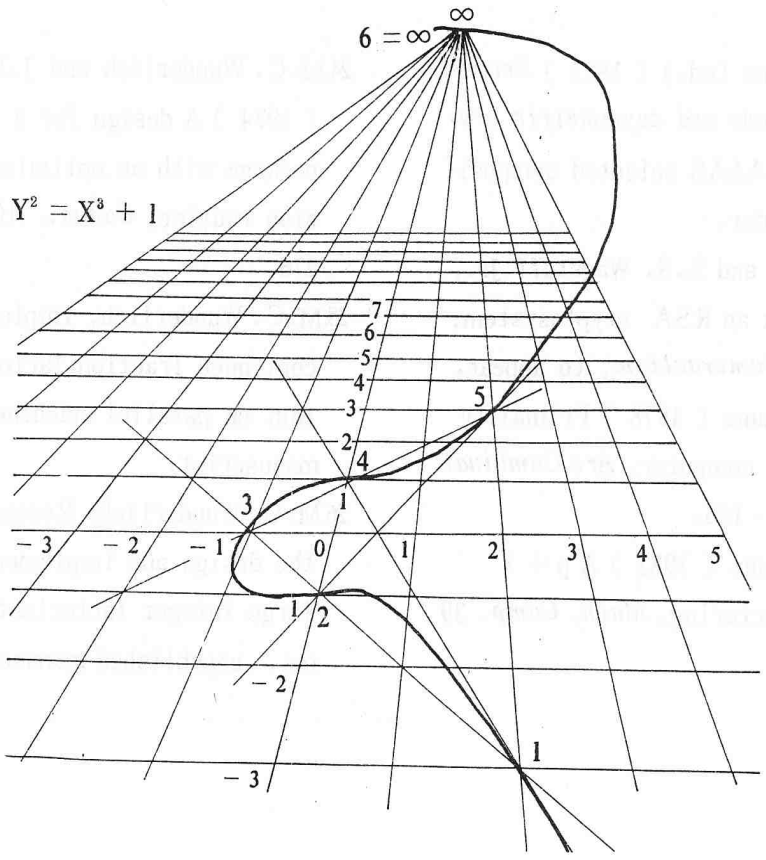
§ 2 曲線上的有理點，Mordell 定理與Faltings 定理

第二部份 Mordell 定理

§ 3 三次平滑曲線上的加法

§ 4 高度，無窮遞降與Mordell 定理的證明

§ 5 有理點羣與弱Mordell 定理的證明



Diophantus-Fermat 的割線切線法，圖中標示 1 到 5 的點代表 $Y^2 = X^3 + 1$ 所有的整數（有理數）解。

第一部份 概 論

§1 Diophantine方程式

所謂Diophantine 方程是指一組有限個方程式：

$$F_1(X_1, \cdots, X_n) = 0,$$
$$F_2(X_1, \cdots, X_n) = 0, \cdots,$$
$$F_t(X_1, \cdots, X_n) = 0$$

其中 F_i 是變元 $X_1, \cdots, X_n$ 的多項式，係數爲整數，對這樣一組方程我們當然希望找出它的整數解。這種方程的研究始於西元三世紀亞歷山大城的希臘數學家 Diophantus，他寫了一部書 Arithmetica 。後來 17 世紀 P. Fermat 就是受了這部書的影響而研究Diophantine方程。

一個Diophantine 方程並不一定有整數解，例如

$$15X^2 - 7Y^2 = 9$$

因此面對這樣的方程，首先必須確定它是否有解。對於某些特殊類的方程（如上述二元二次方程），我們是可以找到一個演算法則（Algorithm），然後依法則來判定方程式是否有整數解。有了法則之後剩下的工作電腦都可做，不再須要數學家，但是要去找好的法則就是數學家的事了。1900 年D. Hilbert 在國際數學會議（巴黎）上提出 23 個數學裏的大問題，其中第十問題就是要找一個演算法則來決定任何給定的Diophantine 方程是否有整數解。經過 70 年這個問題終於有了答案：俄國數學家Y. Matijasevic 證明出Hilbert所要的演算法則是不可能存在的。就好像不可能用直尺圓規三等分任意角一樣，問題是在沒有一種演算法則適用於任意Diophantine 方程而又是電腦會做的（請參考李國偉寫的Hilbert第十問題，徐氏基金會出版）。因此假使能對特殊類Diophantine 方程找到演算法則來決定它們是否有解，就已經是難能可貴的了。

給定一個已知有解的方程式，如

$$X^2 - 3Y^2 = 1$$

要找出它所有整數解仍然不是容易的事（當然偶而運氣好很快就把全部解找到）。首先是如何寫出所有的解的問題，因爲一個方程式的整數解可能無窮多。假使這種情形不發生，也就是說假定數學家能證明某類Diophantine方程只有有限個整數解，當然數學家會夢想有一天能找到全部解，最好是有計算法則把那類方程送入電腦，讓電腦印出它們的解。這是夢想，因爲實際情形是：對絕大多數已知有一個解的Diophantine 方程式，我們沒有任何辦法去找第二個解，或是判定第二個解不存在。數學家對Diophantine 方程能做的事往往只是證明它們是否有有限個解，而不是眞正的去解它們。

假使一個Diophantine 方程有無窮多解，找出它所有解的這個問題就必須重新檢討（formulate）。數學家是這樣做的：研究所有的解的性質，解與解之間的關係，然後把解集合特徵化。也就是要找出一些好的充分必要條件來決定一組整數是否是給定方程式的解。當然最好是找到的條件可以送上電腦，讓電腦來寫出適合條件的整數組。一個典型的例子是初

等數論書裏常提到的 Pell 方程式：

$$X^2 - dY^2 = 1$$

d 是一個沒有平方因子的正數。這種方程式有無窮多個整數解，其中有一個所謂“最小”解 (x_0, y_0)，其它解 (x, y) 都可以利用下面式子從最小解算出：

$$X + \sqrt{d}\, y = \pm (x_0 + \sqrt{d}\, y_0)^n$$
$$n \in \boldsymbol{Z}$$

因爲從 $\sqrt{d}$ 的連分數展開就可以找到最小解，所以雖然一個 Pell 方程式有無窮多解，我們仍然能夠找出它所有的解（請參考華寫的數論導引第十章 §9，凡異出版社）。

我們常常對齊次方程式有興趣，例如 Fermat 方程式 $X^n + Y^n = Z^n$，$n \geq 1$。因爲它是齊次，所以假如 (x, y, z) 是一解，則對任意整數 $\alpha \neq 0$，$(\alpha x, \alpha y, \alpha z)$ 也是一解。我們於是把 (x, y, z) 與 $(\alpha x, \alpha y, \alpha z)$ 看成同一解，也就是說只有在 x，y，z 的最大公因數是 1 的時候我們才算 (x, y, z) 是上述三元齊次方程式的解，而 $(0, 0, 0)$ 是不算作解的。這樣改變了解的定義之後，$X^3 + Y^3 = Z^3$ 就只有三個解，$(1, 0, 1)$，$(0, 1, 1)$ 與 $(1, -1, 0)$，因而一個整數三元序組滿足 $X^3 + Y^3 = Z^3$ 的充分必要條件就是它得是這三個解的整數倍。所謂 Fermat 最後定理是宣稱一般 Fermat 方程式（$n \neq 1, 2$）解的情形都是這樣的，除了那些由 0 與 ± 1 組成的“顯然解”就沒有其它解了。但是至今沒有人能對任意大的 n 證明 Fermat 所宣稱的這個“定理”（請參閱康明昌寫的 Fermat 問題上、下，數學傳播第七卷第四期與第八卷第一期）。對於任意 $n \geq 3$，我們今天只知道 Fermat 方程式有有限個解，這是 1983 年德國數學家 G. Faltings 證明的。

方程式 $X + Y = Z$ 與 $X^2 + Y^2 = Z^2$ 都有無窮多個解。前者是顯然的，任何人都會解，但是要解後者就不是太容易，因爲得先證明以下的數學定理：一整數三元序組 (x, y, z) 滿足 $X^2 + Y^2 = Z^2$，若且唯若存在兩個互質整數 m，n，一奇一偶，以及一個整數 k 使得下列等式成立：

$$x = (m^2 - n^2)\, k,$$
$$y = 2\, mnk,$$
$$z = (m^2 + n^2)\, k.$$

這個定理在任何初等數論書裏都可以找到（康明昌的文章裏有三種不同的證明）。

解多元方程式的困難其實是因爲每一個方程式都有它的個性。即使我們不在整數系裏解它們而到複數系裏解它們，不同方程式的解集合還是會有很大的差異。一個二元方程式的複數解集合可以看成是二維複數平面 $\boldsymbol{C}^2$ 的一代數曲線。三元齊次方程式的複數解也是取其齊次座標（成比例的解視爲相同），因而其解集合是看成二維複數射影平面（即平面 $\boldsymbol{C}^2$ 加上無窮遠直線）$\boldsymbol{CP}^2$ 裏的一代數曲線（這兒稱之爲曲線，因爲局部而言，它們總是可以一個複變數作參數，直觀上看它們實在是曲面）。由不同方程式寫下的曲線當然可能有很大的差異。

在本文裏我們只討論三元齊次 Diophantine 方程式以及二元 Diophantine 方程式。通常我們把三元齊次式看成是二元式經過以下齊次化的過程而來的：

$$F(X, Y) = 0 \to F\left(\frac{X}{Z}, \frac{Y}{Z}\right) Z^d = 0,\ d = \deg F$$
$$\| \qquad\qquad \|$$
$$G(X, Y, 1) \quad G(X, Y, Z)$$

直觀上來看，這是把左邊曲線（曲面）加上幾個無窮遠點，使它成爲封閉有限的曲線（曲面）。這兒無窮遠點就是那些 z 座標零的點，而 z 座標不等於零的點一一對應於原來 $F(X, Y) = 0$ 的解。因此三元序組 (x, y, z)，$z \neq 0$，是方程式 $G(X, Y, Z) = 0$ 的整數解若且唯若 $(x/z, y/z)$ 是二元方程式

$F(X,Y)=0$ 的有理數解。換句話說，在有理數系裏解 $F(X,Y)=0$ 和在整數系裏解 $G(X,Y,Z)=0$ 幾乎是一回事。

從下節起我們將用幾何語言，稱平面方程式爲曲線，其有理數解稱作有理點，整數解則稱爲整點。我們的工作就是在（整係數的）代數曲線上找尋它所有的有理點或它所有的整點。例如我們解方程式 $X^2+Y^2=Z^2$，其實就是把平面單位圓以有理參數方程式

$$\frac{X}{Z}=\frac{1-T^2}{1+T^2},\qquad \frac{Y}{Z}=\frac{2T}{1+T^2}$$

來表示，然後有理點就是那些對應於有理數參數 $T=\frac{n}{m}$ 的點。因此只要寫出了參數式，解 $X^2+Y^2=Z^2$ 是和解 $X+Y=Z$ 一樣容易的。

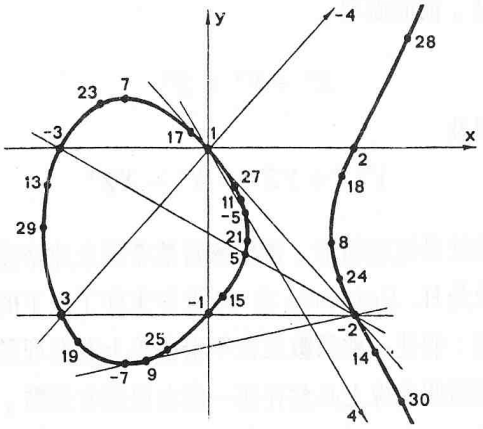
§2 曲線上的有理點；Mordell定理與Faltings定理

我們特別有興趣於平滑曲線。這兒所謂平滑是指曲線上每一點都可以劃唯一切線。假使一曲線在二維複數射影平面的齊次方程式是 $G(X,Y,Z)=0$，則它是平滑曲線的條件就是在它上面的每一點 (x,y,z) 都滿足：

$$\left(\frac{\partial G}{\partial X}\Big|_{(x,y,z)},\ \frac{\partial G}{\partial Y}\Big|_{(x,y,z)},\ \frac{\partial G}{\partial Z}\Big|_{(x,y,z)}\right)\neq(0,0,0)$$

所有上節中提到的曲線都是平滑曲線。

在第二部份裏我們的重點將放在三次平滑曲線。先前提過的三次曲線只有 Fermat 曲線 $X^3+Y^3=Z^3$，它除了無窮遠一點外有兩個有理點，而這兩點也正好是 $X^3+Y^3=1$ 的整點。一般而言，一個三次曲線上可能有無窮多個有理點，例如 $Y^2Z+YZ^2=X^3-XZ^2$。這個平滑曲線有顯然的有理點 $P=(0,0,1)$，其它任何有理點都可以從 P 點用割線法與切線法得到，過程是這樣的：我們從 P 點上開始，作過 P 點與無窮遠點 $\infty=(0,1,0)$ 的直線，因爲曲線是三次所以所作直線和曲線交於三點：P，∞ 與另外一點，以 $(-1)P$ 表示。再從 P 點作過 P 的切線，交曲線於另一點，以 $(-2)P$ 表示，然後作過 $(-2)P$ 與 ∞ 的直線交曲線於 $(-2)P$，∞ 及一點，以 $2P$ 表示。再作過 $2P$ 與 P 的直線與曲線相交得另點，以 $(-3)P$ 表示，然後作過 $(-3)P$ 與 ∞ 的直線與曲線相交而得點 $3P$，這樣一直作圖下去，得到點集合 $\{nP \mid n\neq 0, n\in \boldsymbol{Z}\}$ 就對應曲線 $Y^2+Y=X^3-X$ 上的所有有理點。如下圖：



圖中標示 n 的點就是 nP 在二維平面所對應的點。

割線切線法是很老的方法 — Diophantus 與 Fermat 的方法。它基於一個原理：假使一個有理系數三次多項式有兩個有理根，則其第三個根也必定是有理數。因此它可以適用於任意整數系數三次平滑回線，唯一條件是必須先有其它辦法找到至少一個有理點。一個三次曲線上並不一定有有理點，例如

$$3X^3+4Y^3=5Z^3$$

就可以證明是沒有任何有理點的。即使一個三次平滑曲線上確有有理點，我們不一定能找得到。就算找到幾個有理點，還有一種狀況可能發生，就是用割線切線法之後得不到新的有理

點，而是在幾個已知有理點間打轉。例如

$$X^3 + Y^3 = Z^3$$

用割線切線法從 $P = (0, 1, 1)$ 開始，就有

$$-P = (1, 0, 1)$$

而

$$-2P = P, \quad 2P = -P$$
$$3P = \infty = (1, -1, 0)$$

等等。

給定一整係數三次平滑曲線。運氣最好的情形是：我們能碰對幾個有理點，然後用割線切線法又能從那幾點得到這曲線上任何的有理點。前面處理

$$X^3 + Y^3 = Z^3$$

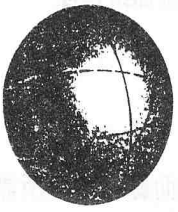
以及

$$Y^2Z + YZ^2 = X^3 - XZ^2$$

時就是這種情形。數學家當然希望永遠幸運，於是H. Poincare 在 19 世紀末作了以下的猜測：假使一整係數三次平滑曲線上有有理點，則這個曲線上必然存在一組有限個有理點，稱爲基本有理點，使得曲線上每一個有理點都可從這組點用割線切線法得到。這個猜測在1922年被英國劍橋大學數學家 L. J. Mordell 證明了，今天稱爲Mordell定理。Mordell 的證明不是 constructive 。對於任意整係數三次平滑曲線，它只告訴我們有可能找到曲線上所有的有理點，並沒有說如何去找。換句話說，Mordell定理是個存在定理。在數學裏存在和“找到”不見得是一回事。能找到的固然存在，但數學的本性之一就是常常在沒有找到時候也能證明存在，而且往往先證明了存在可以幫助我們在後來眞正找到（數學不是神學，不能證明完存在就算了）。

面對一整係數三次平滑曲線，要去找它所有的有理點。首先的困難是沒有任何演算法則可以告訴我們它是否有有理點。假使運氣不壞，碰到了有理點，下一步就是找出一組基本有理點，但是割線切線法對於找基本有理點毫無幫助，因此還有得靠運氣才行。即使運氣非常好，找到了一組基本有理點，我們還必須能證明他們的確是一組基本有理點。這件事是相當難的。例如曲線 $Y^2Z + YZ^2 = X^3 - XZ^2$ ，不難找到它的一組基本有理點，$\{(0,0,1)\}$ 就是；不容易的是證明這個曲線上任何有理點都可以用割線切線法從 $(0,0,1)$ 得到。

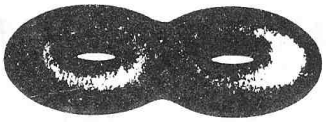
在上一節中我們曾提到，在二維複數射影平面的曲線局部可以一個複變數作參數。因而假使它是平滑的，它就是一個所謂 Riemann 曲面。19 世紀中B. Riemann 建立了這些代數曲線的Riemann 曲面理論，他引進了拓撲觀念以分類所有的封閉有限Riemann 曲面：每一封閉有限 Riemann 曲面都可經“橡皮變換”（可以拉，扭，但不可以剪破或黏貼）和以下的模型同胚（ homeomorphic ）：



$g = 0$

Torus

$g = 1$



Double torus

$g = 2$

.....

這兒 g 是封閉有限 Riemann 曲面的虧格（genus），它是一個拓撲不變量。假使

$$G(X, Y, Z) = 0$$

是 d 次的平滑曲線，其虧格可以算出是等於

$$\frac{(d-1)(d-2)}{2}$$

。

例如曲線 $X + Y = Z$ 以及 $X^2 + Y^2 = Z^2$ 的虧

格都是零，因此從拓撲上來看它們都是球面，也就是說可以把它們看成平面C加上無窮遠點。任何三次平滑曲線的虧格都是1，因而是和輪胎面同胚。

從上世紀末到本世紀初，數學家逐漸發現：對Diophantine 方程式所定義的代數曲線而言，拓撲本性和算術本性是相關的。解這些曲線的方程式可以依照曲線的虧格分爲三種情形：$g=0$，$g=1$，$g>1$。任何虧格零的的整係數平滑曲線總是類似$X^2+Y^2=Z^2$或$X^2+Y^2=3Z^2$，因爲它可以被全部參數化。假使它有有理係數的參數方程式，它上面就有無窮多個有理點，對應於所有有理參數，否則就不存在有理點。而且我們有演算法則，可以從這種曲線的方程式係數判定有理點不存在或找到有理點。有了有理點立刻就能寫出有理係數參數方程式，因而就找到這種曲線上所有的有理點。

虧格1的整係數平滑曲線都是三次。雖然數學家還無法保證解出這種Diophantine 方程式，但是由於Mordell定理，這種曲線的算術本性已逐漸被瞭解。至於虧格大於1的曲線，典型的例子就是Fermat曲線$X^n+Y^n=Z^n$，$n\geq 4$。1922年Mordell證出他的定理之後猜測：任何虧格大於1整係數曲線都只有有限個有理點。這個猜測在1983年被G. Faltings 用高深的代數幾何學證實。Faltings的證明也不是constructive，因此對於任意的虧格大於1的整係數曲線，去找那有限個有理點或者是去判定有理點不存在，都仍然是毫無頭緒的事。但是Faltings 定理使我們進一步瞭解曲線的拓撲和算術間的關聯。從Mordell到Faltings 的工作，可以代表20世紀數學發展的一個主流——算術，代數，拓撲與幾何的滙合。這些發展，至少對純數學而言，意義遠大於實際去解 Diophantine 方程。

第二部份　Mordell定理

利用割線切線法，我們要在三次平滑曲線上定義一種加法。有了這種加法運算，就可以藉代數語言來敍述Mordell定理：假使一整係數三次平滑曲線有有理點，則其所有有理點所成的集合在加法之下構成有限生成的交換群（finitely generated abelian group）。在本文的後半部份，我們將儘量詳細的介紹這個定理的證明。

§3　三次平滑曲線上的加法

給定一個有有理點的整係數三次平滑曲線，令Γ表示曲線上所有的有理點所成集合。在第2節裏我們講過割線切線法幾何作圖：假使P，$Q\in\Gamma$而$P\neq Q$，作連接P與Q的直線交曲線於第三點$PQ\in\Gamma$；假使$P=Q\in\Gamma$，作過P的切線交曲線於第三點$PP\in\Gamma$。利用這個幾何方法，我們只要固定一點$O\in\Gamma$就可以在Γ上引進一種加法運算：

定義3.1　對於P，$Q\in\Gamma$，作過PQ與O的直線（割線或切線，視$PQ\neq O$或$PQ=O$而定），這個直線和所予曲線相交的第三點就定爲$P+Q$。

我們需要證明Γ在這個加法之下構成交換群，以O爲加法單位元素。這並不困難，唯一必須驗證的是結合律：

$$(P+Q)+R=P+(Q+R)$$

這個結合律可以用以下很有意思的平面幾何原理來證：假使兩個三次（退化）曲線相交於九點，其中八點在另一個三次平滑曲線上，則第九點也必然在那個三次曲線上。

給定一整係數三次平滑曲線及其上一有理點O，我們總是可以找到所謂雙有理變換（birational transformation）把曲線化爲標準式：

$$Y^2Z = X^3 + aX^2Z + bXZ^2 + CZ^3$$

a，b，c都是整數

並且把O對應到無窮遠點$\infty = (0, 1, 0)$，例如對曲線

$$\bar{X}^3 + \bar{Y}^3 = \bar{Z}^3$$

以及

$$O = (1, -1, 0)$$

令$\bar{X} = 6Z + \frac{1}{6}Y$，$\bar{Y} = 6Z - \frac{1}{6}Y$，$\bar{Z} = X$

就得到曲線

$$Y^2Z = X^3 - 432Z^3$$

雖然標準化之後的曲線是不同的曲線，但仍然是平滑的，而且它上面有理點所成的群（以∞爲單位元素）在雙有理變換之下是同構於原先曲線上有理點所成的群（以給定爲O爲單位元素）。因此就Diophantine 方程的研究而言，我們只需要考慮寫成標準式的三次平滑曲線。這些曲線與無窮遠直線$Z = O$的所有交點重合於有理點$\infty = (0, 1, 0)$，我們以後在本文中都以這一點作爲這些曲線上的加法單位元素。

我們現在要從射影平面回到普通平面，每個曲線都以它在二維平面的非齊次方程式來表示。於是寫成標準式的三次曲線就是：

$$Y^2 = X^3 + aX^2 + bX + c = f(X)$$

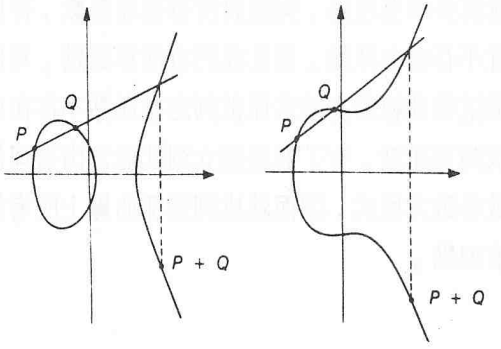
a，b，c是整數

這種曲線是平滑曲線的充要條件是多項式$f(X)$沒有重根，也就是說$f(X)$的判別式$\neq 0$。回到普通平面的優點是可以憑直觀來看圖，而且很容易以坐標來做解析幾何。但是因爲要在三次曲線上運算加法，無窮遠處的單位元素∞是不能忘掉的。我們把它想像成所有平行於y軸的直線在無窮遠處的交點。換句話說，在平面上通過∞的直線就是那些平行於y軸的直線。

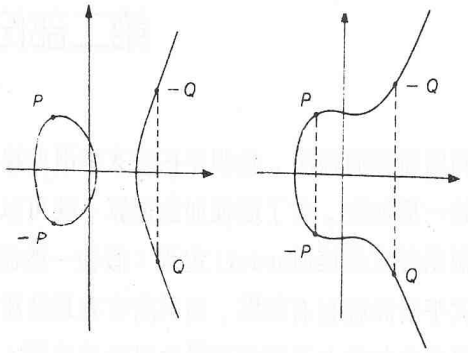
有了以上的共識，平滑曲線

$$Y^2 = f(X) = X^3 + aX^2 + bX + c$$

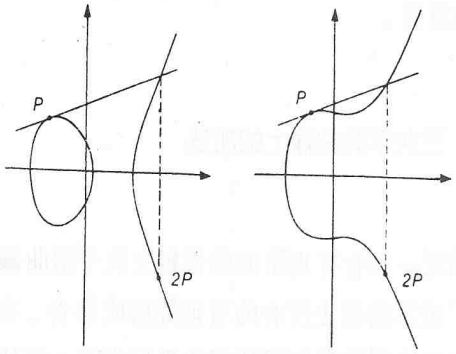
上面的加法就可以圖解如下：



圖一



圖二



圖三

如圖㈠，令 $P=(x_1, y_1)$

$Q=(x_2, y_2)$

$P \neq Q$

而且過P與Q的直線不通過∞。我們要計算

$$P+Q=(x_3, y_3)$$

假定過P與Q的直線是$Y=\lambda X+\nu$，就有

$$\lambda=\frac{y_1-y_2}{x_1-x_2}$$

$$\nu=y_1-\lambda x_1=y_2-\lambda x_2$$

假使$PQ=(x_0, y_0)$則x_0與y_0滿足以下的等式：

$$\begin{aligned} y^2 &= (\lambda x+\nu)^2 \\ &= x^3+ax^2+bx+c \\ x^3 &+ (a-\lambda^2)x^2+(b-2\lambda\nu)x \\ &+ (c-\nu^2)=0 \end{aligned}$$

最後這個三次方程式的根就是x_1，x_2，與$x_3=x_0$，因而得到**加法公式**：

$$x_3=\lambda^2-a-x_2-x_1$$

$$y_3=-\lambda x_3-\nu$$

假定$P=(x, y)$，而且過P點的切線不通過∞。我們可以用隱函數微分算出過P點切線的斜率λ：

$$2y\frac{dy}{dx}=f'(x)$$

$$\lambda=\frac{f'(x)}{2y}$$

再從這個斜率就得到了$2P=(\xi, \eta)$的座標；即**加倍公式**：

$$\begin{aligned} \xi &= \lambda^2-a-2x \\ &= \frac{(f'(x))^2-8xf(x)-4af(x)}{4f(x)} \\ &= \frac{x^4+\cdots}{4x^3+\cdots}=\frac{g(x)}{h(x)} \end{aligned}$$

因爲x的多項式$f(x)$沒有重根，所以這兒的$g(x)$與$h(x)$是互質的多項式。

我們能把三次平滑曲線上的兩個有理點相加，當然也可以照樣把兩個複數點相加。因此一個三次平滑曲線上所有複數點所成的集合在加法之下也一樣構成交換群，只是不再是有限生成的交換群而是所謂的緊緻交換Lie群。從十八世紀起，這些三次平滑曲線上複數點所構成的群和數學家捉了很久的迷藏。直到十九世紀中葉以後，由於橢圓函數理論的發展，整個來龍去脈才逐漸清楚。

在這兒我們就長話短說。考慮平滑曲線

$$Y^2=X^3+aX^2+bX+c$$

經由坐標平移我們可以把aX^2項消掉，然後以$\frac{1}{2}Y$代替Y就得到了Weierstrass 標準式：

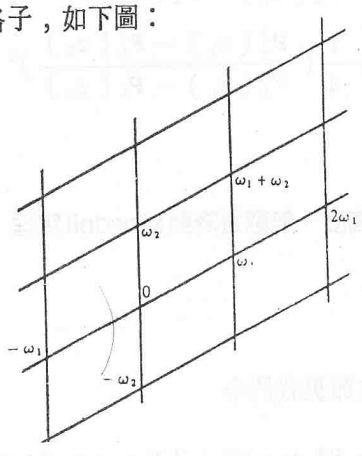
$$Y^2=4X^3-g_2X-g_3$$

g_2, g_3是複數

這些寫成Weierstrass 標準式的曲線可以用Weierstrass 橢圓函數參數化。過程是先作所謂的橢圓積分：

$$\int\frac{dx}{\sqrt{4x^3-g_2x-g_3}}$$

找出這個積分的一對基本複數週期ω_1，ω_2。然後讓ω_1，ω_2在複數平面經由向量加法生成加法群$L=\{n\omega_1+m\omega_2 \mid m, n\in Z\}$，即所謂的格子，如下圖：



有了格子，我們就可以定義Weierstrass橢圓函數：

$$\wp_L(z)=\frac{1}{z^2}+\sum_{\substack{\omega\in L\\ \omega\neq 0}}\left\{\frac{1}{(z-\omega)^2}-\frac{1}{\omega^2}\right\}$$

再作商群C/L面（就拓撲上而言，這個商群是一個和輪胎而同胚的曲面，因爲它是把上圖中一個平行四邊形的對邊黏貼起來而成的）。在這個商群上Weierstrass函數就給了我們以下的映像：

$$z\to(\wp_L(z),\ \wp_L'(z))$$

$$\begin{array}{ccc} C/L-\{0\}\cong\{(x,y)\mid y^2=4x^3-g_2x-g_3\}\subset C^2 \\ \cap \qquad\qquad\qquad\qquad \cap \\ C/L\cong\{(x,y,z)\mid y^2z=4x^3-g_2xz^2-g_3z^3\} \\ \cap \\ CP^2 \end{array}$$

這個映像不只是普通的一一對應，同胚或Riemann 曲面的同構，而且是交換群的同構。它把左邊的“向量加法”對到右邊的幾何加法（即用割線切線法定義的加法），因爲由 L. Euler的橢圓積分理論可以導出以下的加法定理：

$$\begin{aligned}&\wp_L(z_1+z_2)\\&=-\wp_L(z_1)-\wp_L(z_2)\\&\quad+\frac{1}{4}\left(\frac{\wp_L'(z_1)-\wp_L'(z_2)}{\wp_L(z_1)-\wp_L(z_2)}\right)^2\end{aligned}$$

§4 高度、無窮遞降與Mordell定理

在本節裏我們令

$$Y^2=X^3+aX^2+bX+c=f(X)$$

爲整係數三次平滑曲線，其所有有理點構成群Γ，以∞爲加法單位元素。對任一整數m，我們有一個Γ上的同態（homomorphism）$P\to mP$，其值域$m\Gamma$是Γ的子群，因而可以作商群$\Gamma/m\Gamma$。假使Γ是有限生成交換群，而$m\neq 0$，則$\Gamma/m\Gamma$必然是有限群。Mordell獨到的想法是先證明$\Gamma/2\Gamma$是有限群，然後用一個他所謂的無窮遞降法證明出Γ是有限生成的。對於一般交換群，這條路是走不通的，因爲一個無限生成群G也可以有有限商群$G/2G$。商群$\Gamma/2\Gamma$是有限（通常稱爲弱Mordell定理）的證明，我們將留到下一節。在本節裏我們要做的是從弱Mordell定理來證明Mordell定理。

我們先介紹高度（hight）的觀念。令$x=\frac{m}{n}$爲一有理數，寫成既約分數，即m，n爲互質整數。定義x的高度爲

$$H(x)=\max\{|m|,|n|\}$$

重要的事實是：給定任一整數M，永遠只有有限個有理數其高度小於M。這很容易經由數學歸納法證明。假使$P=(x,y)$是曲線$Y^2=f(X)$的有理點，我們定義P的高度$H(P)$爲其x座標的高度。對於$P=\infty$，我們讓$H(\infty)=1$。根據此定義，給定任一正數M就有有限集合$\{P\in\Gamma\mid H(P)\leq M\}$，因爲在這個集合中的有理點$P$其$x$座標只有有限種可能，而對每一$x$至多只有兩個$y$對應。因此假如能找出$\Gamma$的一組生成元，它們的高度都小於一因定正數，Mordell定理就得證。

我們須要兩個有關高度的引理。第一個引理告訴我們“平移”對高度的影響（至多平方），第二個引理告訴我們當一點加倍時其高度的變化（至少四次方）。

引理4.1 對每一點$P_0\in\Gamma$，存在一個常數$C_0>0$使得對所有的$P\in\Gamma$，下式恒成立

$$H(P+P_0)\leq C_0\{H(P)\}^2$$

引理4.2 存在有一常數$B>0$，使得所有$P\in\Gamma$都滿足

$$BH(2P)\geq\{H(P)\}^4$$

我們先證明Mordell定理，再回過頭來研究這兩個引理。由弱Mordell定理，我們可以在Γ中選取有限個元素$Q_1,\cdots,Q_n$使得Γ等於以下聯集：

$$(Q_1+2\Gamma)\cup(Q_2+2\Gamma)\cup\cdots\cdots\cup(Q_n+2\Gamma)$$

給定任何$P\in\Gamma$，就存在i_1，$1\leq i_1\leq n$使得

$$P-Q_{i_1}\in 2\Gamma$$

也就是說可以找到$P_1\in\Gamma$使$P-Q_{i_1}=2P_1$。繼續這個過程就有

$$\begin{aligned}P_1-Q_{i_2}&=2P_2\\P_2-Q_{i_3}&=2P_3\\&\vdots\\P_{m-1}-Q_{i_m}&=2P_m\end{aligned}$$

其中$P_1,\cdots,P_m$都在Γ中，於是就得到

$$\begin{aligned}P&=2P_1+Q_{i_1}\\&=Q_{i_1}+2Q_{i_2}+4P_2\\&\vdots\\&=Q_{i_1}+2Q_{i_2}+\cdots\\&\quad+2^{m-1}Q_{i_m}+2^mP_m\end{aligned}$$

換句話說P是在$Q_1,\cdots,Q_n$與P_m所產生的子群裏。

我們用引理4.1，4.2來比較P_m與P_{m-1}的高度。考慮$P_0=-Q_i$，引理4.1顯示：

$$H(P-Q_i)\leq C_i\{H(P)\}^2。$$

我們讓C'是所有C_i($i=1,\cdots,n$)中最大的數，就得到

$$H(P-Q_i)\leq C'\{H(P)\}^2$$

然後引理4.2給出以下不等式：

$$\begin{aligned}\{H(P_m)\}^4&\leq BH(2P_m)\\&=BH(P_{m-1}-Q_{i_m})\leq BC'\{H(P_{m-1})\}^2\\\{H(P_m)\}^4&\leq\frac{16BC'}{\{H(P_{m-1})\}^2}\left(\frac{H(P_{m-1})}{2}\right)^4\\H(P_m)&\leq\sqrt[4]{\frac{16BC'}{\{H(P_{m-1})\}^2}}\left(\frac{H(P_{m-1})}{2}\right)\end{aligned}$$

從P開始，作$P_1,P_2,\cdots$，一直繼續下去，假使$\{H(P_m)\}^2>16BC'$總是成立，就有

$$H(P_m)<\frac{H(P_{m-1})}{2}$$

$$m=1,2,\cdots$$

因而P_m的高度會一直遞降下去，降到比1小，這是不可能的(有理點的高度恆爲正整數)。所以我們對於任意$P\in\Gamma$總是可以找到m，使得

$$\{H(P_{m-1})\}^2\leq 16BC'=\text{固定常數}$$

這就是說，先前所找到的$Q_1,\cdots,Q_n$以及Γ中所有高度不超過$\sqrt{16BC'}$的元素是Γ的一組生成元。

在證明引理之前我們先把有理點$P=(x,y)$的座標寫成既約分數，

$$x=\frac{m}{M},\quad y=\frac{n}{N},\quad M>0,\quad N>0$$

代入曲線方程式之後得到的等式是

$$\begin{aligned}M^3n^2&=N^2m^3+aN^2Mm^2\\&\quad+bN^2M^2m+cN^2M^3\end{aligned}$$

因此$N^2\mid M^3n^2$，但是$(n,N)=1$，所以$N^2\mid M^3$。另一方面，以M除這個等式兩邊，就有$M\mid N^2m^3$，因而$M\mid N^2$；再以M^2除這個等式，得到$M^2\mid N^2$；然後以M^3除這個等

式，導出$M^3 \mid N^2$，所以$N^2 = M^3$。我們於是讓$e = \frac{N}{M}$，而有$e^2 = M$，$e^3 = N$。把$x = \frac{m}{e^2}$，$y = \frac{n}{e^3}$再代入方程式得

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6$$

因爲$H(P) = \max\{|m|, e^2\}$，取上式的絕對值就有下列不等式

$$|n|^2 \leq [H(P)]^3 + |a|[H(P)]^3 + |b|[H(P)]^3 + |c|[H(P)]^3$$
$$|n| \leq K[H(P)]^{3/2},$$
$$K = \sqrt{1 + |a| + |b| + |c|}$$

這顯示出P點的y座標的高度也受制於P的高度。

我們現在證明引理 4.1。假使$P_0 = \infty$，引理 4.1 是顯然的，因此我們假定$P_0 = (x_0, y_0) \neq \infty$。我們要從$P_0$找出常數$C_0$，使得所有的$P \in \Gamma$，$P \neq P_0$，$-P_0$，$\infty$，都滿足

$$H(P + P_0) \leq C_0 H(P)^2 。$$

然後我們調整常數C_0，就可以使上述不等式對於$P = P_0$，$-P_0$，或∞，也成立。

令$P = (x, y)$，$P + P_0 = (\xi, \eta)$。由上節加法公式我們有：

$$\xi + x + x_0 = \lambda^2 - a, \quad \lambda = \frac{y - y_0}{x - x_0}$$

$$\xi = \frac{(y-y_0)^2 + x(x-x_0)^2 + x_0(x-x_0)^2 - a(x-x_0)^2}{(x - x_0)^2}$$

把$x^3 = y^2 - ax^2 - bx - c$代入上式就得到以下的有理式：

$$\xi = \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}$$

其中A，B，…，G都是整數，而且是完全由a，b，c以及x_0，y_0所決定。把$x = \frac{m}{e^2}$，$y = \frac{m}{e^3}$代入上述有理式就有

$$\xi = \frac{Aen + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}$$

因爲

$$|Aen + Bm^2 + Cme^2 + De^4|$$
$$\leq (|AK| + |B| + |C| + |D|)[H(P)]^2$$
$$|Em^2 + Fme^2 + Ge^4|$$
$$\leq (|E| + |F| + |G|)[H(P)]^2$$

所以

$$H(\xi) \leq C_0[H(P)]^2$$
$$C_0 = \max\{|AK| + |B| + |C| + |D|, |E| + |F| + |G|\}$$

引理 4.2 的證明更有意思，令

$$P = (x, y), \quad 2P = (\xi, \eta) \neq \infty$$

由上節加倍公式知道

$$\xi = \frac{(f'(x))^2 - 8x f(x) - 4a f(x)}{4f(x)}$$
$$= \frac{x^4 + \cdots}{4x^3 + \cdots} = \frac{g(x)}{h(x)}$$

其中$g(X)$與$h(X)$是互質的整係數多項式。我們取有理係數多項式$k(X)$，$l(X)$使得下式成立：

$$k(X)\, g(X) + l(X)\, h(X) = 1$$

再取正整數$D \neq 0$，使得$Dk(X)$，$Dl(X)$都成爲整係數多項式。令ρ爲大於

$$\max[\deg k(X), \deg l(X)] + 4$$

的正整數。對於寫成既約分數的有理數$x = \frac{m}{n}$，我們就有以下的等式：

$$DM^{\rho-4}k\left(\frac{m}{M}\right)g\left(\frac{m}{M}\right)M^4$$

$$+DM^{\rho-4}l\left(\frac{m}{M}\right)h\left(\frac{m}{M}\right)M^4$$

$$=DM^{\rho}$$

假使 $C=C(m,M)$ 是 $g\left(\frac{m}{M}\right)M^4$ 與 $h\left(\frac{m}{M}\right)M^4$ 的最大公因數，則 $C\mid DM^{\rho}$。但

$$g\left(\frac{m}{M}\right)M^4\equiv m^4 \pmod M$$

而且 $(m,M)=1$，所以 $C\mid D$。於是得到

$$H(\xi)=H\left(\frac{g(x)}{h(x)}\right)$$

$$\geq\frac{1}{D}\max\left\{\left|M^4g\left(\frac{m}{M}\right)\right|,\left|M^4h\left(\frac{m}{M}\right)\right|\right\}$$

因此

$$\frac{H(2P)}{H(P)^4}\geq\frac{|g(x)|+|h(x)|}{2D\max\{|x|^4,1\}}$$

在最後這個不等式的右邊是 x 的一個連續函數，恆大於 0，而且當 $x\to\infty$ 時其函數值 $\to 1/2D$，所以我們可以找到常數 $B>0$，使得所有的 $P\in\Gamma$ 都滿足

$$BH(2P)\geq H(P)^4$$

§5 有理點群與弱Mordell定理的證明

令 $Y^2=X^3+aX^2+bX=f(X)$ 爲過原點 $(0,0)$ 的整係數三次平滑曲線

$$(b^2(a^2-4b)\neq 0)$$

其所有有理點以及單位元素 ∞ 構成交換群 Γ。我們要導出以下結果：假使 b 有 r 個不同的質因數而 a^2-4b 有 s 個不同的質因數，則 $\Gamma/2\Gamma$ 的元素個數小於或等於 2^{r+s+2}。換句話說，我們不僅要證明 $\Gamma/2\Gamma$ 是有限群，還要估計其元素個數。

我們首先考慮一個和所予曲線有密切關係的曲線：

$$Y^2=X^3+\bar{a}X^2+\bar{b}X$$

$$=\bar{f}(X)$$

$$=X^3-2aX^2+(a^2-4b)X$$

因爲

$$(a^2-4b)^2 16b\neq 0$$

所以這個曲線也是平滑的；它上面的有理點群記爲 $\bar{\Gamma}$。我們對以下的有理變換有興趣：

$$\bar{x}=x+a+\frac{b}{x}=\frac{y^2}{x^2}$$

$$\bar{y}=y\left(\frac{x^2-b}{x^2}\right)$$

這個變換把曲線 $Y^2=f(X)$ 變到曲線 $Y^2=\bar{f}(X)$。我們讓：

$$\varphi(0,0)=\varphi(\infty)=\bar{\infty}$$

$$\varphi(x,y)=(\bar{x},\bar{y})$$

假使 $(x,y)\in\Gamma$ 而且 $x\neq 0$，
就得到一個從 Γ 到 $\bar{\Gamma}$ 的映像，而且是同態映像：

引理5.1 $\varphi:\Gamma\to\bar{\Gamma}$ 是群同態

證明 令 $P_1,P_2,P_3\in\Gamma$，
而且 $P_1+P_2+P_3=\infty$
假使 P_1,P_2,P_3 是曲線 $Y^2=f(X)$ 與直線

$$Y=\lambda X+\nu,\quad \nu\neq 0$$

的三個交點，則 $\varphi(P_1)$，$\varphi(P_2)$ 與 $\varphi(P_3)$ 就是曲線 $Y^2=\bar{f}(X)$ 與直線

$$Y=\left(\frac{\nu\lambda-b}{\nu}\right)X+\frac{\nu^2-a\nu\lambda+b\lambda^2}{\nu}$$

的三個交點；假使P_1, P_2, P_3是$Y^2 = f(X)$與$Y = \lambda X$的三個交點，則$\varphi(P_1)$, $\varphi(P_2)$, 與$\varphi(P_3)$就是$Y^2 = \bar{f}(X)$與$X = \lambda^2$的三個交點；假使$P_3 = \infty$，則$P_1 = -P_2$，而且$\varphi(P_1) = -\varphi(P_2)$。因而

$$\varphi(P_1) + \varphi(P_2) + \varphi(P_3) = \bar{\infty}$$

總是成立。假使P_1, P_2是Γ裏任意兩個元素，我們取$P_3 = -(P_1 + P_2)$，就得到

$$\varphi(P_1 + P_2) = \varphi(P_1) + \varphi(P_2) \text{。}\#$$

從曲線$Y^2 = f(X)$可以變到曲線$Y^2 = \bar{f}(X)$，當然也可以從$Y^2 = \bar{f}(X)$變到

$$\begin{aligned} Y^2 &= \bar{\bar{f}}(X) \\ &= X^3 + \bar{\bar{a}}X^2 + \bar{\bar{b}}X \\ &= X^3 + 4aX^2 + 16bX \end{aligned}$$

但是最後這個曲線和原先所予曲線其實是一樣的（以$8Y$代替Y，以$4X$代替X）。因而我們也有一個同態ψ從$\bar{\Gamma}$到Γ，

$$\psi(\bar{x}, \bar{y}) = \left(\frac{\bar{x}}{4}, \frac{\bar{y}}{8}\right),$$

假使$\bar{x} \neq 0$。作合成映像$\psi \circ \varphi$，立刻就可以驗證出以下引理：

引理5.2 對於所有的$P \in \Gamma$，$\psi \circ \varphi(P) = 2P$；或者，對於所有的$P \in \Gamma$，$\psi \circ \varphi(P) = -2P$。

這就是說，我們藉$\bar{\Gamma}$之助把Γ的自同態$P \to 2P$分解成兩個同態映像的合成函數。因而我們要證明的事情也就可以分成兩個部份：

(*) $\bar{\Gamma}/\varphi(\Gamma)$是有限群，其元素個數$\leq 2^{s+1}$。

(**) $\Gamma/\psi(\Gamma)$是有限群，其元素個數$\leq 2^{r+1}$

這兩部份的道理當然是一樣的，我們只證明(*)。在證明它之前，我們還須要以下的引理：

引理5.3

(i) $(0,0) \in \varphi(\Gamma)$的充要條件是$\bar{b} = a^2 - 4b$必須是完全平方數。

(ii) 假使$(\bar{x}, \bar{y}) \in \bar{\Gamma}$，$\bar{x} \neq 0$，則$(\bar{x}, \bar{y}) \in \varphi(\Gamma)$的充要條件是$\bar{x}$必須是有理數平方。

証明：

(i) 假使存在$(x, y) \in \Gamma$，$\varphi(x, y) = (0,0)$，則$x \neq 0$而$y = 0$。因此

$$x^2 + ax + b = 0$$

有有理根，$a^2 - 4b$必須是完全平方。反過來假使$a^2 - 4b$是完全平方，解

$$x^2 + ax + b = 0$$

的有理根就得到所要的x。

(ii) 假使$(\bar{x}, \bar{y}) = \varphi(x, y)$，而$\bar{x} \neq 0$，根據定義$\bar{x}$就是有理數平方。反過來，假使$(\bar{x}, \bar{y}) \in \Gamma$，$\bar{x} = w^2$，$w \neq 0$，$w \in \boldsymbol{Q}$，我們令

$$x_1 = \frac{1}{2}\left(w^2 - a + \frac{\bar{y}}{w}\right)$$

$$y_1 = x_1 w$$

$$x_2 = \frac{1}{2}\left(w^2 - a - \frac{\bar{y}}{w}\right)$$

$$y_2 = x_2 w$$

很容易驗證

$$\begin{aligned} \varphi(x_1, y_1) &= \varphi(x_2, y_2) \\ &= (\bar{x}, \bar{y}) \end{aligned} \text{。}\#$$

令$\boldsymbol{Q}^*$爲所有非零有理數的乘法群，$(\boldsymbol{Q}^*)^2$爲所有非零有理數平方組成的子群。我們考慮以下的映像：

$$\alpha : \bar{\Gamma} \to \boldsymbol{Q}^*/(\boldsymbol{Q}^*)^2$$

$$\alpha(\infty) = 1 \mod (\boldsymbol{Q}^*)^2$$

$$\alpha(0,0) = b \mod (\boldsymbol{Q}^*)^2$$

$$\alpha(\bar{x}, \bar{y}) = \bar{x} \mod (\boldsymbol{Q}^*)^2$$

假使 $\bar{x} \neq 0$ 。

我們要證明這也是一個群同態。令

$$\bar{P}_1 = (\bar{x}_1, \bar{y}_1)$$
$$\bar{P}_2 = (\bar{x}_2, \bar{y}_2)$$
$$\bar{P}_3 = (\bar{x}_3, \bar{y}_3)$$

爲 $\bar{\Gamma}$ 的元素，

$$\bar{P}_1 + \bar{P}_2 + \bar{P}_3 = \bar{\infty} \text{ 。}$$

假使 $Y^2 = \bar{f}(X)$

與 $Y = \lambda X + \nu$ ， $\nu \neq 0$

交於 $\bar{P}_1, \bar{P}_2, \bar{P}_3$，則 $\bar{X}_1, \bar{X}_4, \bar{X}_3$ 是以下方程式的根

$$X^3 + (\bar{a} - \lambda^2) X^2 + (\bar{b} - 2\lambda\nu) X + \nu^2 = 0$$

因此有

$$\bar{x}_1 + \bar{x}_2 + \bar{x}_3 = \lambda^2 - \bar{a}$$
$$\bar{x}_1\bar{x}_2 + \bar{x}_2\bar{x}_3 + \bar{x}_3\bar{x}_1 = \bar{b} - 2\nu$$
$$\bar{x}_1\bar{x}_2\bar{x}_3 = \nu^2$$
$$\equiv \alpha(\bar{P}_1)\ \alpha(\bar{P}_2)\ \alpha(\bar{P}_3) \bmod (\boldsymbol{Q}^*)^2;$$

假使 $Y^2 = \bar{f}(X)$ 是與 $Y = \lambda X$ 交於 $\bar{P}_1, \bar{P}_2, \bar{P}_3$，令 $\bar{P}_1 = (0, 0)$ 就得到 $\bar{x}_2\ \bar{x}_3 = \bar{b}$ ；假使 $\bar{P}_3 = \bar{\infty}$ ，則 $\bar{P}_1 = -\bar{P}_2$ ，所以

$$\alpha(\bar{P}_1) = \alpha(\bar{P}_2) = \alpha(-\bar{P}_2) = \alpha(\bar{P}_2)^{-1} \text{ 。}$$

因而

$$\alpha(\bar{P}_1)\ \alpha(\bar{P}_2)\ \alpha(\bar{P}_3) = 1 \bmod (\boldsymbol{Q}^*)^2$$

恆成立。對於 $\bar{\Gamma}$ 中任意元素 $\bar{P}_1, \bar{P}_2$，我們取

$$\bar{P}_3 = -(\bar{P}_1 + \bar{P}_2) ,$$

就得到

$$\alpha(\bar{P}_1 + \bar{P}_2) = \alpha(\bar{P}_1)\ \alpha(\bar{P}_2)$$

根據引理 5.3 $\alpha(\bar{P}) = 1 \bmod (\boldsymbol{Q}^*)^2$ 的充要條件是 $\bar{P} \in \varphi(\Gamma)$ 。因而我們可以經由 α 把商群 $\bar{\Gamma}/\varphi(\Gamma)$ 看成 $\boldsymbol{Q}^*/(\boldsymbol{Q}^*)^2$ 的子群，$\bar{\Gamma}/\varphi(\Gamma)$ 的元素個數就是 $\alpha(\bar{\Gamma})$ 的元素個數。換句話說，我們所必須做的是證明 $\alpha(\bar{\Gamma})$ 是有限的，並且估計其元素個數。

令 $(\bar{x}, \bar{y}) \in \bar{\Gamma}$ 。上節中我們講過 $\bar{x}$ ， $\bar{y}$ 可以寫成：

$$\bar{x} = \frac{m}{e^2} , \qquad \bar{y} = \frac{n}{e^3}$$

$$(m, e) = 1 = (n, e)$$

其中整數 m ， n ， e 滿足以下的等式：

$$n^2 = m^3 + \bar{a}m^2e^2 + \bar{b}me^4$$
$$= m(m^2 + ame^2 + \bar{b}e^4)$$

令

$$d = (m, m^2 + \bar{a}me^2 + \bar{b}e^4)$$

則 $d \mid \bar{b}e^4$ ， $d \mid \bar{b}$ 。

把 m 分解因數：

$$m = \prod p^{a_p} \text{ 。}$$

假使 $p \nmid \bar{b}$ ，則 $p \nmid m$ ，所以 a_p 必然是偶數。於是就有

$$m = (\text{平方})(\pm p_1^{\varepsilon_1} \cdots p_r^{\varepsilon_r})$$

其中 $p_1, \cdots, p_r$ 是 $\bar{b} = a^2 - 4b$ 的不同質因數，而 $\varepsilon_i = 0$ 或 1 。這就證明了 $\alpha(\bar{\Gamma})$ 的元數個數是有限，而且不超過 2^{s+1} 。

假使一個整係數三次平滑曲線

$$Y^2 = f(X) = X^3 + aX^2 + bX + c$$

不通過原點，我們取 $f(X) = 0$ 的一個根，作代數擴張體 $\boldsymbol{Q}(\beta)$ ，然後以線性座標變換把 $(\beta, 0)$ 平移到原點。變換之後的曲線通過原點，但是其係數不再一定是整數，而是 $\boldsymbol{Q}(\beta)$ 中的代數整數。因此，只要藉助一些代數數論，本節的方法是可以用來證明一般情形的弱 Mordell 定理。我們在這兒不詳細寫了。