

丟番圖方程式

§1 問題的來源

「邊長為 3、5、7 的三角形中，三內角中的最大角為 120^0 」。

這是高二邊角關係這個單元中的一個簡單的例子，由餘弦定理可得到。

它的後面接了一個習作：

「三角形的三邊長為 $a=2t+1$ ， $b=t^2-1$ ， $c=t^2+t+1$ ，則 $\angle C = ?$ 」

由餘弦定理可以求得 $\angle C = 120^0$ 。取 $t=2$ 即得前述的三個邊長 3、5、7。

最大角為 120^0 的三角形，三邊長為 x 、 y 、 z 。若 120^0 角所對的邊長為 z ，則

$$z^2 = x^2 + y^2 - 2xy \cos 120^0 = x^2 + y^2 + xy$$

我的疑問是：

「 $z^2 = x^2 + y^2 + xy$ 的一般解是否即為 $x=2t+1$ ， $y=t^2-1$ ， $z=t^2+t+1$ ，其中 $(x, y, z) \neq 1$ 」？

§2 遇見資優生

2002 年左右，上午，衛道中學。

上課中偶然心血來潮，想到 $3^2 + 4^2 + 12^2 = 13^2$ ，於是請學生多找幾個例子，使滿足 $x^2 + y^2 + z^2 = t^2$ 。

下課後，桌上擺了兩張紙，一張上面只有簡單一行，寫著：

$$y=x+1, z=x(x+1), t=x(x+1)+1$$

另一張紙上寫著：

1, 4, 9, 16, 25, 36, 49, 64, 81, 100, 121, 144, 169, 196, 225, 256, 289,

324, 361, 400, 441, 484, 529, 576, 625, ... 所以有

$$2^2 + 10^2 + 11^2 = 15^2$$

$$8^2 + 9^2 + 12^2 = 17^2$$

$$1^2+4^2+8^2=9^2$$

$$4^2+5^2+20^2=21^2$$

前者找出部分解，後者由演算直接找到一些解，雖然不是完整的解答，但是對國三學生而言，實屬難得。這是 10 多年前的舊事，這兩位學生後來都進入了一中資優班。

§3 所謂丟番圖方程式

一般而言，若 $f(x_1, x_2, \dots, x_n)$ 是一個多變數的整係數多項式，求 $f(x_1, x_2, \dots, x_n)=0$ 的所有整數解就是丟番圖問題。

求 $x^2+y^2+z^2=t^2$ 的一般解(正整數解)就是一個丟番圖問題。

直角三角形 ABC 中， $z^2=x^2+y^2$ 這稱為畢氏定理或商高定理，盧米斯(Elisha Scott Loomis 1852~1940)在畢達哥拉斯命題(Pythagorean Proposition)一書中提到 370 種證法。

滿足 $x^2+y^2=z^2$ 的正整數稱為畢氏數，畢氏數的一般解(所有解)為何？

希臘數學家丟番圖(Diophantus 約 246~330)得到一般解:

$$x=2mn, y=m^2-n^2, z=m^2+n^2; \text{ 其中 } (m,n)=1, \text{ 且 } m>n; \text{ 當然假設 } (x,y,z)=1$$

§4 求 $z^2=x^2+y^2$ 的一般解

第一種解法：

$$\left(\frac{z}{x}\right)^2 - \left(\frac{y}{x}\right)^2 = 1, \left(\frac{z}{x} + \frac{y}{x}\right)\left(\frac{z}{x} - \frac{y}{x}\right) = 1$$

此式表示 $\frac{z}{x} + \frac{y}{x}$ 與 $\frac{z}{x} - \frac{y}{x}$ 互為倒數

$$\text{令 } \frac{z}{x} + \frac{y}{x} = \frac{m}{n}, \frac{z}{x} - \frac{y}{x} = \frac{n}{m}, \text{ 則 } \frac{z}{x} = \frac{1}{2}\left(\frac{m}{n} + \frac{n}{m}\right) = \frac{m^2+n^2}{2mn}, \frac{y}{x} = \frac{1}{2}\left(\frac{m}{n} - \frac{n}{m}\right) = \frac{m^2-n^2}{2mn}$$

取 $x=2mn$, 則 $y=m^2-n^2, z=m^2+n^2$, 此即為畢氏數的一般解。

第二種解法：

$$\text{設 } z=y+k, \text{ 則 } z^2-y^2=k(2y+k)$$

設 $k=p^2r$ 其中 p 是 k 的最大平方因數，

$$\text{則 } z^2-y^2=x^2=p^2r(2y+p^2r)$$

$r|2y+p^2r$ ，所以 $r|2y$

若 $r|y$ 則 $r|(x, y, z)$ ，此時 $r=1$ 。所以 $r=1$ 或 $r=2$

(1) $r=1$ 時

$$x^2=p^2(2y+p^2) \text{ 令 } 2y+p^2=q^2, \text{ 則 } y=\frac{q^2-p^2}{2}, x=pq, z=\frac{q^2+p^2}{2}$$

若 p, q 皆偶數，則 x, y, z 皆偶數不合；若 p, q 一奇一偶，則 y 不是整數，不合；所以 p, q 皆奇數，因為 x 是奇數所以 y 是偶數。

令 $q+p=2m$ ， $q-p=2n$ ，則 $q=m+n$ ， $p=m-n$ ，得到

$$x=m^2-n^2, y=2mn, z=m^2+n^2$$

(2) $r=2$ 時

$$x^2=2p^2(2y+2p^2)=4p^2(y+p^2) \text{ 令 } y+p^2=q^2$$

則 $y=q^2-p^2$ ， $x=2pq$ ， $z=q^2+p^2$ ，我們把符號換一下，令 $m=q, n=p$ ，則

$$x=2mn, y=m^2-n^2, z=m^2+n^2$$

由(1)(2)得解。(或者參看參考資料(2)。)

§5 求 $z^2=x^2+y^2+xy$ 的一般解

引理：

「若 x, y, z 滿足 $z^2=x^2+xy+y^2$ ，則 mx, my, mz 滿足 $z^2=x^2+xy+y^2$ 。反之亦成立。」

§1 中提到 $x=2t+1, y=t^2-1, z=t^2+t+1$ (1) 滿足 $x^2+xy+y^2=z^2$

$$\text{取 } t=\frac{m}{n}, \text{ 則 } x=2t+1=\frac{2mn+n^2}{n^2}, y=t^2-1=\frac{m^2-n^2}{n^2}, z=\frac{m^2+mn+n^2}{n^2}$$

由引理， $x=2mn+n^2$ ， $y=m^2-n^2$ ， $z=m^2+mn+n^2$ 也是 $x^2+xy+y^2=z^2$ 的解。... (2)

解(1)(2)，看起來形式上有很強的關聯性。確實關係為何？

我再次請教康明昌教授：

「教授在參考資料(2)中提到三次分圓體(cyclotomic field) $Q(\omega)$ 裡面的「整數」。

則 $z^2=x^2+y^2+xy=(x-\omega y)(x-\omega^2 y)$ ，其中 $\omega=\frac{-1+\sqrt{3}i}{2}$ 。是否可由 $Z[\omega]$ 求得

$z^2=x^2+y^2+xy$ 的一般解？」

以下是康教授的回函：

「Define $u=x/z$, $v=y/z$. Then $u^2+uv+v^2=1$. This is the same as the norm of $x:=u-\omega v=1$. By Hilbert Theorem 90. There is an element $y:=s-\omega t \in Q(\omega)$ such that $x=y/y'$ where $y'=s-\omega^2 t$ 。」

我把它改寫成如下：

設 $Q(r):=Q$ 的擴張體，其中 r 滿足 $x^2-x+1=0$

則 $x^2-x+1=(x-r)(x-\bar{r})$ ， $r+\bar{r}=1$, $r\bar{r}=1$

$$N\left(\frac{x+ry}{z}\right)=\left(\frac{x+ry}{z}\right)\left(\frac{x+\bar{r}y}{z}\right)=1$$

由 Hilbert 定理 90: 存在某個 $a \in (Q(r))^*$ 使得 $\frac{x+ry}{z} = \frac{a}{a}$

因此存在 $s \in Z$ ，使得 $\frac{x+ry}{z} = \frac{a}{a} = \frac{as}{as}$ ， $as \in Z[r]$ ，令 $as=m+nr$ ，其中 m 、 n 是整數

$$\begin{aligned} \text{因此 } \frac{x+ry}{z} &= \frac{a}{a} = \frac{as}{as} = \frac{m+nr}{m+nr} = \frac{m+nr}{m+(1-r)n} = \frac{(m+nr)^2}{m^2+mn+n^2} \\ &= \frac{(m^2-n^2)+r(2mn+n^2)}{m^2+mn+n^2} \end{aligned}$$

因為 $(x,y,z)=1$ ，所以 $x=m^2-n^2$ ， $y=2mn+n^2$ ， $z=m^2+mn+n^2$ 是原丟番圖方程式的一般解。

所以由 $x=2t+1$, $y=t^2-1$, $z=t^2+t+1$ 到 $x=2mn+n^2$, $y=m^2-n^2$, $z=m^2+mn+n^2$ 是正確的，只是中間需有一個代數數論的鋪陳。

§6 習作

1. 設直角 $\triangle ABC$ 的三邊長分別為 a, b, c ，且 $a < b < c$ 。若 $\frac{b}{c+a} - \frac{a}{c+b} = \frac{1}{6}$ ，則 $a : b : c =$ (建中通訊解題 84 期)
2. 滿足 $z^2 = x^2 + y^2$, $(x, y, z) = 1$ ，的正整數解中，(1) x, y 一個是奇數，另一個是偶數。(2) x, y 至少有一個是 3 的倍數。試證之。
3. 已知：一直角 $\triangle ABC$ 之兩股為 a, b ，斜邊為 c ， a, b, c 為整數且 a 為質數。試證： $2(a+b+1)$ 為完全平方數。
4. 求一組非零的有理數 x, y 滿足 $x^2 - 26y^2 = 1$
5. 試證對任意正整數 a ，存在異於 a 的正整數 b, c 使得 a^2, b^2, c^2 成等差數列
(104 年關西高中教師甄試)

◇解答◇

1. 令 $a=m^2-n^2, b=2mn, c=m^2+n^2$ 代入原式 可以化簡得 $7m^2 - 11mn - 6n^2 = 0$
 $(m-2n)(7m+3n)=0, m=2n$, 則 $a=3n^2, b=4n^2, c=5n^2$
所以 $a:b:c=3:4:5$
2. 略
3. 畢氏數 $a^2+b^2=c^2$ 的一般解為 $a=m^2-n^2, b=2mn, c=m^2+n^2$
今 $a=(m-n)(m+n)$ 為質數，所以 $m-n=1$, 即 $m=n+1$
代入後得 $2(a+b+1)=4(n+1)^2$ 為一完全平方數
4. 略
5. $2b^2=a^2+c^2$, $(2b)^2=(c+a)^2+(c-a)^2$; $2b=(m^2+n^2)k$, $c+a=(m^2-n^2)k$, $c-a=2mnk$;
 $a=(\frac{m^2-2mn-n^2}{2})k, b=(\frac{m^2+n^2}{2})k, c=(\frac{m^2+2mn-n^2}{2})k$ 取 $k=a, m=3, n=1$,
可得 $b=5a, c=7a$

§7 參考資料

1. 代數學之父 http://episte.math.ntu.edu.tw/people/p_diophantus/index.html
2. 費馬問題 http://episte.math.ntu.edu.tw/articles/mm/mm_07_4_01/ 康明昌
3. 畢氏數與 Hilbert Theorem 90
<http://www.math.harvard.edu/~elkies/Misc/hilbert.pdf> by Noam D. Elkies
4. 基礎數論講義 <http://math.ntnu.edu.tw/~li/ent-html/> 李華介教授

要證明一個丟番圖方程式無解，有兩個基本方法：(1)同餘理論 (2)無窮遞減法。

5. Catalan 問題：若 $x, y, m > 1, n > 1$ 都是正整數，則 $x^m - y^n = 1$ 的解只有 $x=3, y=2, m=2, n=3$ 。
6. 我把問題丟到 Math Pro 網站(<http://math.pro/db/index.php>)，馬上得到「thepiano 老師」的回應。以下是「thepiano」老師提供的解答，再度感謝他。
<http://math.pro/db/thread-2041-1-1.html>
7. 習作(5)的詳解 <http://math.pro/db/viewthread.php?tid=2316&extra=&page=2>

§8 後記

密碼學與數論有密切的關係，所以現在不會再有人質疑數論的實用性。

從畢氏數到 1996 年費馬最後定理的證明是一頁耀眼的數論發展史，想必也不會有人懷疑數論的深刻性。

高中數學 95 課程綱要中，高一有關初等數論(因數倍數)的部分在 99 課程綱要中被刪除了。因此第二章中方程式論裡，牛頓定理(整係數一次因是檢驗法)的證明也只能擺在附錄中，個人覺得有點遺憾。

不定方程式 $ax+by=c$ ，佩爾(Pell)方程式 $x^2-ny^2=1$ 的解已有定論。解決一道丟番圖方程式 $x^2+xy+y^2=z^2$ 對我而言就像下了一盤圍棋，是一個不錯的心靈遊戲。

$x^2+Axy+By^2=z^2$ 的一般解請看參考資料(3)。

至於§2 中， $x^2+y^2+z^2=t^2$ 的一般解為何，謹就教於各位賢達了。