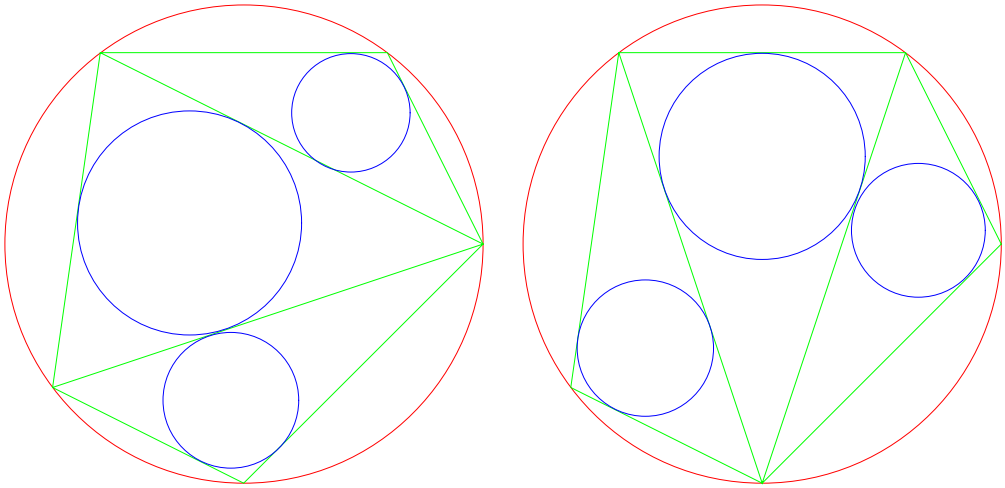
算術講義

許 志 農

國立台灣師範大學數學系

December 28, 2004



左圖三小圓半徑和＝右圖三小圓半徑和

目 錄

1 質多項式的問題

如果一個整係數多項式（以整數為係數的多項式）不能分解為兩個次數大於零次的整係數多項式的乘積則稱這個多項式為質多項式。本節的目的是要提出一些方法來判斷一個多項式是否為質多項式。

1.1 艾森斯坦判別法

定理 **1.1** 設 $f(x)=x^n+a_{n-1}x^{n-1}+\cdots+a_1x+a_0$ 為整係數多項式且存在一個質數 p 使得

$$\begin{cases} p \mid a_i (0 \le i \le n-1), \\ p^2 \ \text{不能整除} \ a_0. \end{cases}$$

證明 $f(x)$ 是一個質多項式。

【證明】利用反證法，假設 $f(x)$ 可以分解成兩個次數大於零次的整係數多項式的乘積，並令

$$\begin{cases} f(x) = & (x^m+\cdots+b_lx^l+p(b_{l-1}x^{l-1}+\cdots+b_0))\times \\ & (x^{n-m}+\cdots+c_1x+c_0), \\ \text{但是} \ \ p \ \ \text{不能整除} \ \ b_l, c_0. \end{cases}$$

現在比較 x^l 項的係數，由已知得到 $p \mid a_l$；但是由乘式

$$(x^m+\cdots+b_lx^l+p(b_{l-1}x^{l-1}+\cdots+b_0))(x^{n-m}+\cdots+c_1x+c_0)$$

得到 x^l 項的係數不為 p 的倍數，這與假設矛盾。因此 $f(x)$ 就是一個質多項式。 ☒

例題 **1.1** 如果 p 是一個質數，證明多項式

$$f(x)=x^{p-1}+x^{p-2}+\cdots+x+1$$

是一個質多項式。

【證明】假設

$$f(x)=x^{p-1}+x^{p-2}+\cdots+x+1=\frac{x^p-1}{x-1}$$

可分解，則多項式

$$\begin{aligned} g(x) &= f(x+1)=\frac{(x+1)^p-1}{x} \\ &= x^{p-1}+\tbinom{p}{1}x^{p-2}+\tbinom{p}{2}x^{p-3}+\cdots+\tbinom{p}{p-2}x+p \end{aligned}$$

也是可分解的多項式，但這與艾森斯坦判別法相矛盾。 ☒

1.2 利用同餘多項式判別質多項式

如果 p 是一個質數，$f(x)$ 與 $g(x)$ 是兩個整係數的多項式則用符號 $f(x) \equiv g(x) \pmod{p}$ 代表多項式差 $f(x) - g(x)$ 的每一 x 次方冪的係數都是 p 的倍數。此時我們稱多項式 $f(x)$ 與多項式 $g(x)$ 模 p 同餘。例如

$$\begin{aligned} x+1 &\equiv x-1 \pmod{2}, \\ x^2+3x+1 &\equiv x^2+x+1 \pmod{2}, \\ x^2+5x+13 &\equiv x^2+2x+1 \pmod{3}. \end{aligned}$$

我們容易推得：每一個首項係數為 1 的一次多項式必與 x 或 $x+1$ 模 2 同餘；每一個首項係數為 1 的二次多項式必與 x^2, x^2+x, x^2+1 或 x^2+x+1 模 2 同餘；每一個首項係數為 1 的三次多項式必與 $x^3, x^3+1, x^3+x^2, x^3+x^2+1, x^3+x^2+x, x^3+x^2+x+1, x^3+x$ 或 x^3+x+1 模 2 同餘。又因為

$$\begin{aligned} x^2 &\equiv x \cdot x \pmod{2}, \\ x^2+x &\equiv x(x+1) \pmod{2}, \\ x^2+1 &\equiv (x+1)(x+1) \pmod{2}, \end{aligned}$$

所以 $x^2+x+1 \pmod{2}$ 是唯一的一個二次模 2 質多項式（也就是說：此多項式模 2 之後不能分解）；同樣由

$$\begin{aligned} x^3 &\equiv x \cdot x \cdot x \pmod{2}, \\ x^3+1 &\equiv (x+1)(x^2+x+1) \pmod{2}, \\ x^3+x^2 &\equiv x^2 \cdot (x+1) \pmod{2}, \\ x^3+x^2+x &\equiv x \cdot (x^2+x+1) \pmod{2}, \\ x^3+x^2+x+1 &\equiv (x+1)^3 \pmod{2}, \\ x^3+x &\equiv x(x+1)^2, \end{aligned}$$

知道 $x^3+x^2+1 \pmod{2}$ 及 $x^3+x+1 \pmod{2}$ 是僅有的兩個三次模 2 質多項式。讀者是否可以仿照上述的方法找出所有的二次及三次模 3 的質多項式（限定首項係數為 1）。

例題 **1.2** 證明 $f(x) = x^4+3x^3+3x^2-4x+1$ 是一個質多項式。

【證明】四次多項式 $f(x)$ 的分解狀況有

$$\begin{cases} （一次）（一次）（一次）（一次）， \\ （一次）（一次）（二次）， \\ （一次）（三次）， \\ （二次）（二次）， \\ 質多項式。 \end{cases}$$

將 $x = \pm 1$ 代入得到 $f(1) = 4, f(-1) = 6$，由一次因式檢驗法知 $f(x)$ 沒有一次因式。因此第一、二、三種情形都不可能。

將 $f(x)$ 對 $p=2$ 取同餘（模 2）：因為模 2 的一次因式僅有 $x \pmod 2, x+1 \pmod 2$ 兩個，經逐一檢查得到

$$f(x) \equiv (x+1)(x^3+x+1) \pmod 2,$$

其中 $x^3+x+1 \pmod 2$ 已不可再分解。這說明了 $f(x)$ 沒有二次因式（你會說明嗎），所以第四種情形亦不可能。

由上述討論知道：多項式

$$f(x) = x^4+3x^3+3x^2-4x+1$$

必是一個質多項式。 ☒

如果 $f(x)$ 是一個首項係數為 1 的整係數多項式，p 是一個質數。我們判別的基本原理是這樣的：

(0) 如果 $f(x)$ 是可分解的，則 $f(x) \pmod p$ 是模 p 可分解的。

(1) 命題 (0) 的否逆命題為“如果 $f(x) \pmod p$ 是模 p 質多項式（不可分解的），則 $f(x)$ 必定是一個質多項（不可分解的）。”這是我們最常用的原理。

(2) 如果 $f(x) \pmod p$ 是可分解的，則不代表 $f(x)$ 可以分解。例如 $f(x)=x^2+x+2$，當 $p=2$ 時，

$$f(x) \equiv x(x+1) \pmod 2.$$

但是 $f(x)$ 是一個質多項式。

利用同餘判別質多項式是一種很重要且有效的判別方法，它的困難之處在於取那一個質數來做模，一般而言都是從較小的質數模起。

1.3 質數與質多項式

定理 **1.2** 如果質數 p 的十進位表示數為 $a_n a_{n-1}\cdots a_1 a_0$，其中

$$a_n, a_{n-1}, \cdots, a_1, a_0 \in \{0,1,2,3,4,5,6,7,8,9\}.$$

證明

$$f(z) = a_n z^n + a_{n-1}z^{n-1} + \cdots + a_1 z + a_0$$

是一個質多項式。

【證明】首先證明：若複數 z 滿足 $f(z)=0$，則 $\mathrm{Re}(z)<4$（ $\mathrm{Re}(z)$ 表示複數 z 的實部）。若 $x=\mathrm{Re}(z)>1$（如果 $x=\mathrm{Re}(z)\le 1$，則自然有 $\mathrm{Re}(z)<4$），則得到

$$\mathrm{Re}\left(\frac{1}{z}\right) = \frac{\mathrm{Re}(z)}{|\ z\ |^2} > 0.$$

再利用三角不等式

$$|\,a\,|+|\,b\,|\geq|\,a+b\,|\geq|\,a\,|-|\,b\,|$$

得到

$$\begin{aligned}
0=\left|\frac{f(z)}{z^n}\right| &\geq \left|a_n+\frac{a_{n-1}}{z}\right|-\left|\frac{a_{n-2}}{z^2}+\cdots+\frac{a_0}{z^n}\right| \\
&\geq \left|a_n+\frac{a_{n-1}}{z}\right|-\left(\frac{a_{n-2}}{|\,z\,|^2}+\cdots+\frac{a_0}{|\,z\,|^n}\right) \\
&\geq \mathrm{Re}\left(a_n+\frac{a_{n-1}}{z}\right)-\frac{9}{x^2}-\cdots-\frac{9}{x^n} \\
&\geq 1-\frac{9}{x^2-x} \\
\Rightarrow \qquad & \mathrm{Re}(z)<4 \quad (\text{因為假設 } x=\mathrm{Re}(z)>1).
\end{aligned}$$

其次假設多項式 $f(z)=g(z)h(z)$，其中 $g(z)$ 與 $h(z)$ 至少一次以上。對方程式 $h(z)=0$ 的每一實根 α，利用 $\mathrm{Re}(z)<4$ 得到 $10-\alpha\geq 10-4=6$；對方程式 $h(z)=0$ 的每一對共軛複根 $\alpha,\bar{\alpha}$，同理得到

$$(10-\alpha)(10-\bar{\alpha})=10^2-20\mathrm{Re}(\alpha)+|\,\alpha\,|^2\geq 10^2-20\times 4>1.$$

綜合得到 $|\,h(10)\,|>1$，同理也有 $|g(10)|>1$。

因為 $f(10)=g(10)h(10)$ 與 $f(10)=a_na_{n-1}\cdots a_1a_0=p$ 是質數矛盾，所以

$$f(z)=a_nz^n+a_{n-1}z^{n-1}+\cdots+a_1z+a_0$$

必須是一個質多項式。 ☒

習題 **1.1** 證明 $f(x)=x^4-x+1$ 是一個質多項式。

習題 **1.2** 證明 $f(x)=x^5+3x^4+x^3+7x+1$ 是一個質多項式。

習題 **1.3** 判別 $f(x)=x^5-x^2+1$ 是否為質多項式？

習題 **1.4** 證明 $f(x)=x^5+x^4+8x^3+5x^2+8x+9$ 是一個質多項式。

習題 **1.5** 證明 $f(x)=x^6-x^3+1$ 是一個質多項式。

習題 **1.6** 將多項式 $f(x)=x^7+x^5+x^3+x^2-1$ 分解成質多項式的乘積。

習題 **1.7** 證明 $f(x)=x^6+3x^4+1$ 是一個質多項式。 [1]

習題 **1.8** 試

(1) 列出所有模 3 的二次質多項式（限定首項係數為 1 者）。

[1] 可以考慮模 2 及模 3。

(2) 將多項式 $f(x)=x^6-6x^4+6x^3+12x^2+36x+1$ 對模 3 作分解。

(3) 證明 $f(x)$ 是一個質多項式。

習題 **1.9** 試

(1) 判別 x^3-3x+1 是否為質多項式。

(2) 證明：使多項式

$$(x^3-3x+1)(ax+b)+12-3x^2$$

是一個整數係數多項式的完全平方之整數解 (a,b) 至多僅有一組。

動手玩數學

三個同心圓，半徑分別為 $1, r_1, r_2$ $(1<r_1<r_2)$。甚麼時候可以在此三圓上各取一點，使它們構成一個正三角形。

挑戰題

試證明

(1) 如果整數 a,b 滿足

$$(x^3-3x+1)(ax+b)-3x^2+12=f(x)^2$$

其中 $f(x)$ 是整係數多項式，試確定所有 a,b 及多項式 $f(x)$ 的值。

(2) 若 α 為 $x^3-3x+1=0$ 的一根，試證明此三次方程式的另兩個根均可表為 α 的整係數多項式，並求此兩根。

科拉茨猜想

如果 n 是一個正整數，我們定義：

$$T(n)=\begin{cases}\frac{n}{2} & n \text{ 是偶數},\\ \frac{3n+1}{2} & n \text{ 是奇數}.\end{cases}$$

如此，給定任一個正整數 n, 我們就產生了一個數列如下：

$$n, T(n), T(T(n)), T(T(T(n))), \cdots .$$

例如： $n=7$ 時，產生的數列為

$$7, 11, 17, 26, 13, 20, 10, 5, 8, 4, 2, 1, 2, 1, \cdots .$$

科拉茨猜想是說：對任意的正整數 n, 我們所產生的數列

$$n, T(n), T(T(n)), T(T(T(n))), \cdots$$

至少有一項為 1（或者此數列最後一定是 1 與 2 交替出現）。