2003 基 礎 組 合

朱亮儒

國立臺灣師範大學數學系

在本單元中,我們將介紹生成函數的基本性質及其應用.對數列$a_0, a_1, a_2, \cdots, a_n, \cdots$作冪級數

$$A(x) = a_0 + a_1x + a_2x^2 + \cdots + a_nx^n + \cdots,$$

我們稱$A(x)$爲數列$\langle a_n\rangle$的(普通)生成函數(ordinary generating function),其中$1, x, x^2, x^3, \cdots$爲指示符號.生成函數的加法及乘法運算與一般多項式的運算相同,但因我們只對其有限項的係數有興趣,故不必考慮其斂散性.對於兩個生成函數$A(x) = \sum a_nx^n$與$B(x) = \sum b_nx^n$,若$a_n = b_n,\ \forall\, n$,就稱這兩個生成函數相等,記爲$A(x) = B(x)$.另外我們也可以定義數列$\langle a_n\rangle$的指數型生成函數(exponential generating function)如下:

$$E(x) := \sum_{n=0}^{\infty} \frac{a_n}{n!}x^n = a_0 + \frac{a_1}{1!}x + \frac{a_2}{2!}x^2 + \cdots.$$

例如:若$a_n = 1,\ \forall\, n$,則

$$A(x) := \sum_{n=0}^{\infty} a_nx^n = \frac{1}{1-x}\ ,\ E(x) := \sum_{n=0}^{\infty} \frac{a_n}{n!}x^n = e^x.$$

又如$a_n = n,\ \forall\, n$,則

$$A(x) := \sum_{n=0}^{\infty} a_nx^n = \frac{x}{(1-x)^2}\ ,\ E(x) := \sum_{n=0}^{\infty} \frac{a_n}{n!}x^n = xe^x.$$

[定理]:設$A(x), B(x), C(x)$分別是數列$\langle a_n\rangle, \langle b_n\rangle, \langle c_n\rangle$的(普通)生成函數.則

(a) $C(x) = A(x) + B(x) \Longleftrightarrow c_n = a_n + b_n,\ \forall\, n.$

(b) $C(x) = A(x)\cdot B(x) \Longleftrightarrow c_n = a_nb_0 + a_{n-1}b_1 + \cdots + a_1b_{n-1} + a_0b_n,\ \forall\, n.$

[推論]:設$A(x) = a_0 + a_1x + a_2x^2 + \cdots$.則$f(x) := A(x)\cdot \frac{1}{1-x}$的展開式中$x^n$的係數爲$c_n := a_0 + a_1 + \cdots + a_n$;即$f(x)$爲$\langle c_n\rangle$的生成函數.

1997 IMO的一道試題:令$f(n)$表示將正整數n表成2的非負冪次方之方法數,例如:$f(5) = 4$,其可能的情況爲:

(i) 5個$2^0 \longleftrightarrow 5 = 5\cdot 2^0 \longleftrightarrow x^5\cdot x^0 \cdots$

(ii) 3個2^0, 1個$2^1 \longleftrightarrow 5 = 3\cdot 2^0 + 1\cdot 2^1 \longleftrightarrow x^3\cdot x^1\cdot x^0\cdots$

(iii) 1個2^0, 2個$2^1 \longleftrightarrow 5 = 1\cdot 2^0 + 2\cdot 2^1 \longleftrightarrow x^1\cdot x^2\cdot x^0\cdots$

(iv) 1個2^0, 1個2^2 $\longleftrightarrow$ $5 = 1\cdot 2^0 + 1\cdot 2^2$ $\longleftrightarrow$ $x^1\cdot x^0\cdot x^2\cdot x^0\cdots$

這些表示法均可寫成:

$$x^{k_1}\cdot x^{2k_2}\cdot x^{4k_3},\ \text{其中}k_1 = 0,1,2,3,4,5,\ k_2 = 0,1,2,\ k_3 = 0,1,\ \text{且}\ k_1+2k_2+4k_3 = 5.$$

這樣的項正是以下無窮級數乘積展開後形成x^5的項:

$$(1+x+x^2+x^3+\cdots)(1+x^2+x^4+x^6+\cdots)(1+x^4+x^8+x^{12}+\cdots)(1+x^8+x^{16}+\cdots)\cdots.$$

因此,其對應的x^5之係數就代表我們要求的$f(5)$之值.更一般地,$f(n)$就是對應x^n項的係數.事實上,若不考慮級數是否發散,該無窮積可改寫成:

$$\frac{1}{(1-x)(1-x^2)(1-x^4)\cdots} = \prod_{k=0}^{\infty}\frac{1}{1-x^{2^k}}.$$

[例題]: (1996 Turkey) 設多項式

$$\prod_{n=1}^{2000}\left(1+nx^{3^n}\right) = 1 + a_1x^{k_1} + a_2x^{k_2} + \cdots + a_mx^{k_m},$$

其中$a_1, a_2, \cdots, a_m$都不爲零,且$k_1 < k_2 < \cdots < k_m$.試求k_{2000}及a_{2000}.

[解答]:注意:

$$\text{當}\ j = \sum_{i=0}^{t} r_i 2^i,\ \text{其中}\ r_i \in \{0,1\} \implies k_j = \sum_{i=0}^{t} r_i 3^{i+1}.$$

而a_j恰表示對應3的冪次方指數之積.因此由$2000 = 2^{10}+2^9+2^8+2^7+2^6+2^4$,可知$k_{2000} = 3^{11}+3^{10}+3^9+3^8+3^7+3^5$,而$a_{2000} = 11\cdot 10\cdot 9\cdot 8\cdot 7\cdot 5 = 277200$.

[定理]:設$A(x), B(x), C(x)$分別是數列$\langle a_n\rangle, \langle b_n\rangle, \langle c_n\rangle$的指數型生成函數.則

(a) $C(x) = A(x) + B(x) \iff c_n = a_n + b_n,\ \forall\, n.$

(b) $C(x) = A(x)\cdot B(x) \iff$

$$c_n = n!\left(\frac{a_nb_0}{n!} + \frac{a_{n-1}b_1}{(n-1)!1!} + \cdots + \frac{a_1b_{n-1}}{1!(n-1)!} + \frac{a_0b_n}{n!}\right) = \sum_{k=0}^{n} C_k^n a_{n-k}b_k,\ \forall\, n.$$

生成函數不僅是解決計數問題的有力工具,它也是證明或推導組合恆等式的一種重要方法,例如:

[例題]:試證:

$$\sum_{k=0}^{n}\frac{n!}{(n-k+1)!(k+1)!} = \frac{2(2^{n+1}-1)}{(n+1)(n+2)}.$$

[證明]：因爲

$$e^x = 1 + \frac{1}{1!}x + \frac{1}{2!}x^2 + \frac{1}{3!}x^3 + \cdots,$$

故

$$\frac{e^x - 1}{x} = 1 + \frac{1}{2!}x + \frac{1}{3!}x^2 + \frac{1}{4!}x^3 + \cdots.$$

因此，數列$\langle \frac{1}{n+1} \rangle$的指數型生成函數爲$\frac{e^x-1}{x}$. 由定理知

$$\sum_{k=0}^{n} C_k^n \cdot \frac{1}{(n-k+1)(k+1)} = \sum_{k=0}^{n} \frac{n!}{(n-k+1)!(k+1)!}$$

的指數型生成函數爲$\frac{(e^x-1)^2}{x^2}$. 另一方面，由於

$$\frac{(e^x-1)^2}{x^2} = \frac{1}{x^2}(e^{2x} - 2e^x + 1) = (\frac{2^2}{2!} - \frac{2}{2!}) + (\frac{2^3}{3!} - \frac{2}{3!})x + \cdots + (\frac{2^{n+2}}{(n+2)!} - \frac{2}{(n+2)!})x^n + \cdots,$$

故

$$\sum_{k=0}^{n} \frac{n!}{(n-k+1)!(k+1)!} = n!(\frac{2^{n+2}}{(n+2)!} - \frac{2}{(n+2)!}) = \frac{2(2^{n+1}-1)}{(n+1)(n+2)}.$$

生成函數的另一個應用是來求解遞迴數列的一般項，例如：費氏數列$a_0 = a_1 = 1, a_n = a_{n-1} + a_{n-2},\ \forall\ n \geq 2$,的生成函數爲

$$A(x) = \frac{1}{1-x-x^2} = \frac{1}{\sqrt{5}x}(\frac{1}{1-\frac{1+\sqrt{5}}{2}x} - \frac{1}{1-\frac{1-\sqrt{5}}{2}x})$$

$$= \sum_{n=0}^{\infty} \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{n+1} - (\frac{1-\sqrt{5}}{2})^{n+1})x^n,$$

故

$$a_n = \frac{1}{\sqrt{5}}((\frac{1+\sqrt{5}}{2})^{n+1} - (\frac{1-\sqrt{5}}{2})^{n+1}).$$

又如：Catalan數C_n表示一凸$(n+2)$邊形用$n-1$條互不相交（但可共端點）的對角線所分割之方法數，如：$C_0 = C_1 = 1, C_2 = 2, C_3 = 5$. 事實上，它滿足以下的遞迴關係：

$$C_n = C_0C_{n-1} + C_1C_{n-2} + \cdots + C_{n-1}C_0,\ \forall\ n.$$

我們可利用其生成函數$A(x) = \sum C_n x^n$來求解其一般式.

$$A(x)^2 = (\sum_{k=0}^{\infty} C_k x^k)(\sum_{l=0}^{\infty} C_l x^l) = C_0 \cdot C_0 + (C_1C_0 + C_0C_1)x + \sum_{n=2}^{\infty}(\sum_{k=0}^{n} C_kC_{n-k})x^n$$

$$= 1 + 2x + \sum_{n=2}^{\infty} C_{n+1}x^n = 1 + 2x + \frac{1}{x}(A(x) - 1 - x - 2x^2).$$

故 $x \cdot A(x)^2 - A(x) + 1 = 0$,得

$$A(x) = \frac{1-\sqrt{1-4x}}{2x} = \sum \frac{1}{n+1} C_n^{2n} x^n.$$

由此可導出 $C_n = \frac{1}{n+1} C_n^{2n}$.

[研究題]: (The Hanoi Tower Problem) 有三根木樁 A, B, C 直立於平面上,其中木樁 A 由上而下套著 n 個大小不同的環(越大的環必須放在越底層). 若我們想要將木樁 A 中的 n 個環搬到木樁 C, 且規定每次搬動只能移動一個環,木樁 A 中的環必須先被移到木樁 B 中,木樁 B 中的環必須被移到木樁 C 中,木樁 C 中的環必須被移到木樁 A 中,試問至少需要搬動幾次? Ans. $1 + \frac{1}{2\sqrt{3}}\left[(1+\sqrt{3})^{n+1} - (1-\sqrt{3})^{n+1}\right] + \frac{1}{2\sqrt{3}}\left[(1+\sqrt{3})^{n} - (1-\sqrt{3})^{n}\right]$.

生成函數的還有一個主要的應用,是用來計算正整數分割的個數,這種理論最早是 Euler 在1748年提出的. 首先,我們給出它的定義: 若正整數 n 可以寫成

$$n = n_1 + n_2 + \cdots + n_k,$$

其中 $n_1, n_2, \cdots, n_k$ 為正整數,則稱 $(n_1, n_2, \cdots, n_k)$ 為 n 的一個長度是 k 的分割 (partition) 或 k 分割.

符號:

$P(n)$ = n 的分割之個數

$P(n,k)$ = n 的分割中長度不超過 k 的個數

$Q(n,k)$ = n 的分割中每一項都不超過 k 的個數

$P_d(n)$ = n 的分割且每一項都相異的個數

$P_o(n)$ = n 的分割且每一項都是奇數的個數

$P_e(n)$ = n 的分割且每一項都是偶數的個數

例如:

$$P(5) = 7, P(5,3) = 5, P_3(5) = 2, P_d(5) = 3, P_o(5) = 3, P_e(5) = 0.$$

在研究正整數的分割時,一種直觀的幾何模型常常能幫助人們學習的思維,例如在 $n = n_1 + n_2 + \cdots + n_k$ 的分割中,每一分割項 n_i 對應到某一層的點(如圖 $n = 18 = 7+4+3+3+1$),第一層 n_1 個點,第二層 n_2 個點, $\cdots$,第 k 層 n_k 個點, $n_1 \geq n_2 \geq \cdots \geq n_k$. 像這樣的圖稱為 Ferrers 圖 (N. M. Ferrers, 1829-1903).

· · · · · · ·
· · · ·
· · ·
· · ·
·

若將Ferrers圖的行列對換，則可得到另一Ferrers圖，其仍是n的另一個分割，稱之爲共軛分割．例如：

$$18 = 7+4+3+3+1 \quad \longleftrightarrow \quad 18 = 5+4+4+2+1+1+1.$$

此時，由觀察得知原分割的項數即成爲新分割項的最大數，而原分割分割項的最大數即成爲新分割的項數．由於這是一種1-1對應，故有：$P(n,k) = Q(n,k)$.

[Andrews 定理]：

$$\lim_{n\to\infty} \sqrt[n]{P(n)} = 1.$$

關於$P(n)$的上界，Hardy-Ramanujan 曾對$P(n)$的估計問題作研究而得到了

$$P(n) = O\left(\frac{e^{\pi\sqrt{\frac{2}{3}n}}}{n}\right).$$

以下，我們給出$P(n)$的一個上界之估計值：

[定理]：

$$P(n) < e^{\pi\sqrt{\frac{2n}{3}}}, \ \forall\, n = 1, 2, 3, \cdots.$$

[證明]：令$f(x)$爲$P(n)$的生成函數，則

$$f(x) = (1-x)^{-1}(1-x^2)^{-1}(1-x^3)^{-1}\cdots.$$

對$0 < x < 1$，就有$P(n)x^n < f(x)$．故

$$\ln P(n) < \ln f(x) + n \ln \frac{1}{x}.$$

因爲

$$mx^{m-1} < 1 + x + x^2 + \cdots + x^{m-1} = \frac{1-x^m}{1-x}, \ \forall\, x \in (0,1),$$

得

$$\frac{1}{m} \cdot \frac{x^m}{1-x^m} < \frac{1}{m^2} \cdot \frac{x}{1-x}.$$

故

$$\ln f(x) = \ln(1-x)^{-1}(1-x^2)^{-1}(1-x^3)^{-1}\cdots = -\sum_{n=1}^{\infty} \ln(1-x^n) = \sum_{n=1}^{\infty}\sum_{m=1}^{\infty} \frac{x^{mn}}{m}$$

$$= \sum_{m=1}^{\infty} \frac{1}{m} \sum_{n=1}^{\infty} x^{mn} = \sum_{m=1}^{\infty} \frac{1}{m} \cdot \frac{x^m}{1-x^m} < \sum_{m=1}^{\infty} \frac{1}{m^2} \cdot \frac{x}{1-x} =: \frac{\pi^2}{6t}.$$

其中$t = \frac{1-x}{x}$．又因$\ln \frac{1}{x} = \ln(1+t) < t$，故

$$\ln P(n) < \ln f(x) + n\ln\frac{1}{x} < \frac{\pi^2}{6t} + nt =: g(t),\ \forall\, t > 0.$$

因$g(t) = \frac{\pi^2}{6t} + nt, t > 0,$的最小值爲$\pi\sqrt{\frac{2n}{3}}$,故得證.

[定理]:(a)數列$P(n)$的生成函數是

$$\frac{1}{(1-x)(1-x^2)(1-x^3)\cdots\cdots}.$$

(b)數列$P_e(n)$的生成函數是

$$\frac{1}{(1-x^2)(1-x^4)(1-x^6)\cdots\cdots}.$$

(c)數列$P_o(n)$的生成函數是

$$\frac{1}{(1-x)(1-x^3)(1-x^5)\cdots\cdots}.$$

(d)數列$P_d(n)$的生成函數是

$$(1+x)(1+x^2)(1+x^3)\cdots\cdots.$$

[Euler 定理]:$P_d(n) = P_o(n)$.

[證明]:因爲$P_d(n)$的生成函數爲

$$(1+x)(1+x^2)(1+x^3)\cdots = \frac{1-x^2}{1-x}\cdot\frac{1-x^4}{1-x^2}\cdot\frac{1-x^6}{1-x^3}\cdots$$
$$= \frac{1}{1-x}\cdot\frac{1}{1-x^3}\cdot\frac{1}{1-x^5}\cdots,$$

上式恰爲$P_o(n)$的生成函數,故得證.

[Sylvester 定理]:設p爲大於1的正整數,則每一正整數以p爲底的p進位表示法是唯一的.

[證明]:設$Q_p(n)$表示n分割成p的不同冪次方之方法數.則欲證

$$Q_p(n) = 1,\ \forall\, n = 1, 2, 3, \cdots,\ \forall\, p = 2, 3, \cdots.$$

我們知道數列$(1, 1, 1, 1, \cdots)$的生成函數爲

$$\frac{1}{1-x} = 1 + x + x^2 + x^3 + \cdots$$

$= (1+x+x^2+\cdots+x^{p-1})(1+x^p+x^{2p}+\cdots+x^{(p-1)p})(1+x^{p^2}+x^{2p^2}+\cdots+x^{(p-1)p^2})\cdots,$
又上式恰爲$Q_p(n)$的生成函數,故$Q_p(n)=1$.

[研究題]:對於$n\geq 3$的分割$(n_1,n_2,\cdots,n_k)$會使得$n_1\cdot n_2\cdots\cdot n_k$的值最大之充分且必要的條件是可選擇這些$n_i$中至多有兩個是2,其於都是3.

[研究題]:試證(Euler定理):設$P_{do}(n)$表示n的分割中每一項都相異且都是奇數的個數,而$P_{de}(n)$表示n的分割中每一項都相異且都是偶數的個數,則

$$P_{de}(n)=\begin{cases} P_{do}(n), \text{ 當 } n\neq \frac{3k^2\pm k}{2} \text{ (不是五角數)} \\ P_{do}(n)+(-1)^k, \text{ 當 } n=\frac{3k^2\pm k}{2} \text{ (五角數)} \end{cases}$$

在1995年加拿大舉辦的國際數學奧林匹亞競試中,出現一題與生成函數有關的試題:

[例題]:(1995 IMO)令p爲一奇質數.試求滿足下列條件的子集合A之個數:

(1) $A\subset\{1,2,3,\cdots,2p\}$

(2) 集合A中恰有p個元素,且它們的和是p的倍數.

[解答]:令$X=\{1,2,3,\cdots,2p\}$且定義

$$f_z(x)=(1+zx)(1+z^2x)(1+z^3x)\cdots(1+z^{2p}x),$$

其中$z=\cos\frac{2\pi}{p}+i\cdot\sin\frac{2\pi}{p}$.則$f_z$爲一$2p$次$x$的多項式,可令

$$f_z(x)=b_0+b_1x+b_2x^2+\cdots+b_{2p}x^{2p},$$

其中b_i是z的多項式.特別的,

$$b_p=\sum_{a_i\in X} z^{a_1+a_2+\cdots+a_p}.$$

因$z^p=1$,故

$$b_p=c_0+c_1z+c_2z^2+\cdots+c_{p-1}z^{p-1},$$

其中c_j是集合X的p元子集中,元素和以p除的餘數是j之子集合個數,$0\leq j\leq p-1$.
故我們的目標即求c_0之值.因爲$x^p=1$的根爲$1,z,z^2,\cdots,z^{p-1}$,故

$$x^p-1=(x-1)(x-z)(x-z^2)\cdots(x-z^{p-1}).$$

因p爲奇數,以$-x$代換x得

$$x^p+1=(x+1)(x+z)(x+z^2)\cdots(x+z^{p-1})=(1+x)(1+zx)(1+z^2x)\cdots(1+z^{p-1}x).$$

因此,

$$f_z(x) = (1+zx)(1+z^2x)(1+z^3x)\cdots(1+z^{2p}x)$$
$$= [(1+x)(1+zx)(1+z^2x)\cdots(1+z^{p-1}x)]^2 = (x^p+1)^2 = x^{2p}+2x^p+1.$$

故 $b_p = 2$,即
$$(c_0-2)+c_1z+c_2z^2+c_3z^3+\cdots+c_{p-1}z^{p-1}=0.$$

又由 Eisenstein 判別法知多項式 $1+x+x^2+\cdots+x^{p-1}$ 是一質式,且因每一 c_j 都是整數,故 $c_0-2=c_1=c_2=\cdots=c_{p-1}$.又因 X 的 p 元子集共有 C_p^{2p} 個,故
$$c_0+c_1+c_2+\cdots+c_{p-1}=C_p^{2p}.$$

由此可解得
$$c_0=\frac{C_p^{2p}-2}{p}+2.$$

[**研究題**]:令 p 爲一奇質數,k 爲一正整數.試求滿足下列條件的子集合 A 之個數:

(1) $A \subset \{1,2,3,\cdots,kp\}$

(2) 集合 A 中恰有 p 個元素,且它們的和是 p 的倍數.

[**例題**]:設 $a_0,a_1,a_2,\cdots$ 是一遞增的非負整數數列,且滿足每一非負整數都可唯一被表成 a_i+2a_j 的型式,其中 i,j 不必相異.試求 a_{2003} 之值.

[**證明**]:令
$$f(x)=x^{a_0}+x^{a_1}+x^{a_2}+\cdots,$$
則 $f(x^2)=x^{2a_0}+x^{2a_1}+x^{2a_2}+\cdots$.因此,
$$f(x)f(x^2)=\sum_{i,j}x^{a_i+2a_j}.$$

另一方面,因爲每一非負整數都可唯一被表成 a_i+2a_j 的型式,故
$$f(x)f(x^2)=1+x+x^2+\cdots=\frac{1}{1-x}.$$

由此可得
$$f(x^2)f(x^4)=\frac{1}{1-x^2}.$$

將上面兩式相除可得 $f(x)=(1+x)f(x^4)$.如此下去,我們可推得
$$f(x)=(1+x)(1+x^4)(1+x^{4^2})(1+x^{4^3})\cdots.$$

因此
$$\text{當 } j=\sum_{i=0}^{t}r_i\cdot 2^i,\ \text{其中 } r_i\in\{0,1\} \implies a_j=\sum_{i=0}^{t}r_i\cdot 4^i.$$

故由$2003=2^{10}+2^9+2^8+2^7+2^6+2^4+2^1+2^0$,可知

$$a_{2003}=4^{10}+4^9+4^8+4^7+4^6+4^4+4^1+4^0.$$

[研究題]:(1998 IMO 預選題)設$a_0,a_1,a_2,\cdots$是一遞增的非負整數數列,且滿足每一非負整數都可唯一被表成$a_i+2a_j+4a_k$的型式,其中i,j,k不必相異.試求a_{1998}之值.

[例題]:(1999 IMO)設p爲大於3的質數,對$T=\{0,1,2\}$,定義$E(T)$表示$(p-1)$重序對$(x_1,x_2,\cdots,x_{p-1})$所成的集合,其中每一個$x_i\in T$,且$x_1+2x_2+\cdots+(p-1)x_{p-1}$是$p$的倍數.試求$E(T)$的元素個數.

[解答]:令a_n表示非負整數n可表成

$$n=x_1+2x_2+\cdots+(p-1)x_{p-1}$$

的方法數,其中每一個$x_i\in T$.則

$$|E(T)|=\sum_{p|n}a_n=a_0+a_p+a_{2p}+a_{3p}+\cdots.$$

令$F(x)=\sum a_nx^n$爲$\langle a_n\rangle$的生成函數,則

$$F(x)=\left(1+x+x^2\right)\left(1+x^2+x^4\right)\left(1+x^3+x^6\right)\cdots\left(1+x^{p-1}+x^{2(p-1)}\right).$$

設$w=\cos\frac{2\pi}{p}+i\sin\frac{2\pi}{p}$爲1的$p$次原根,則$w^p=1$,且$1+w+w^2+\cdots+w^{p-1}=0$.更進一步地,

$$1+w^k+w^{2k}+\cdots+w^{(p-1)k}=\begin{cases}0\text{, 當 }p\text{ 不是 }k\text{ 的因數}\\ p\text{,當 }p\text{ 是 }k\text{ 的因數}\end{cases}.$$

而且,當p不是k的因數時,$1,w^k,w^{2k},\cdots,w^{(p-1)k}$爲$1,w,w^2,\cdots,w^{p-1}$的一重排.故有$F(w)=F(w^2)=\cdots=F(w^{p-1})$,且

$$F(1)+F(w)+F(w^2)+\cdots+F(w^{p-1})=p(a_0+a_p+a_{2p}+a_{3p}+\cdots)=p|E(T)|.$$

又$F(1)=3^p$且

$$\begin{aligned}F(w)&=\left(1+w+w^2\right)\left(1+w^2+w^4\right)\left(1+w^3+w^6\right)\cdots\left(1+w^{p-1}+w^{2(p-1)}\right)\\&=\frac{1-w^3}{1-w}\cdot\frac{1-w^6}{1-w^2}\cdot\frac{1-w^9}{1-w^3}\cdots\frac{1-w^{3p}}{1-w^p}=1.\end{aligned}$$

其中,最後一個等式成立是因爲$w^3,w^6,w^9,\cdots,w^{3p}$爲$1,w,w^2,\cdots,w^{p-1}$的一重排.因此,

$$|E(T)|=\frac{1}{p}\left(F(1)+F(w)+F(w^2)+\cdots+F(w^{p-1})\right)=\frac{3^p+p-1}{p}.$$