數學傳播　39卷1期, pp. 39-45

從費馬到拉格蘭日

沈淵源

摘要: 我們首先用數學歸納法證明費馬小定理; 然後本著模 p數系的乘法代數結構, 不僅導出了公式, 也同時證明了費馬小定理。而這個方法, 又很自然地可推廣到一般模 n的情況; 更有甚者, 同樣的論證適用於任何有限交換群。最後, 對非交換有限群; 可藉著拉格蘭日定理來建立同樣的公式, 而費馬小定理僅一特例也。

費馬小定理[3] (Fermat's Little Theorem) 乃是近代密碼學中瑞沙葉演算法[2, 4](RSA Algorithm) 的理論基礎。令 p爲一正質數, 費馬小定理告訴我們: 在模 p之下, 任何非 p之倍數的整數 a, 其 $p-1$次方就是乘法單位元素 1; 也就是說,

$$a^{p-1} \equiv 1 \pmod{p}, \quad \forall a \in \mathbb{Z},\, p \nmid a.$$

這個定理, 乍看之下似乎有點不可思議, 實在是太神奇了。所以我們試著從定理的證明著手, 分析非 p之倍數的整數在乘法之下的代數結構; 並推廣至非質數 n時對應的歐拉定理, 甚至還可繼續推廣到一般抽象群上的元素。此際, 這麼神奇的費馬小定理竟然只是群論上最基本的拉格蘭日定理的一個簡單推論而已。

一、數學歸納法證明費馬小定理

費馬小定理可以用數學歸納法證明, 雖說啟發性不大, 還是隱藏著某種程度的價值。怎麼說呢? 你知道數學歸納法僅適用於正整數, 所以理所當然的; 你得對 a作數學歸納法, 然後再去推廣到任意的整數。在數學歸納法中, 其主要的步驟從 a到 $a+1$時得取 $p-1$次方; 但是在模 p之下要將 $(a+1)$的 $p-1$次方 $(a+1)^{p-1}$展開並加以化簡, 看來是渺渺茫茫的, 我們似乎走進了一條死胡同。怎麼辦呢? 山不轉, 但路可以轉; 所以人生的經歷告訴我們, 是路轉的時候了。若是 $a+1$取 p次方, 在模 p之下那可就簡單極了。因爲取 p次方時, 二項式定理明示: 其係數除了頭尾兩項都是 1之外, 其餘都是 p的倍數; 也就是說,

$$p \,|\, \binom{p}{j} = \frac{p!}{j!(p-j)!}, \quad 1 \le j \le p-1\,。$$

此乃分母中所有的整數因子都比 p小, 這確保了分子的 p不會被消掉。所以在模 p之下, 二項的 p次方還是二項; 也就是說,

$$(a+1)^p \equiv a^p + 1 \pmod{p}。$$

當然, 這裡項數的 2可以取代爲任何的正整數; 換句話說,

和的 p 次方等於 p 次方的和。

所以, 爲了讓我們的日子過得更舒適安然一些; 在模 p的世界裡, 我們得先將結論中的次方修飾成 p次方。這不難, 只消在等式兩邊各乘上 a即可; 因此我們有, $a^p \equiv a \pmod{p}$。更帥的是, 當 a不是 p的倍數時; 這個同餘式與原先的同餘式是等價的。

現在回到原先的目標, 我們想對 a作數學歸納法; 而我們的 a卻被限制爲非 p之倍數, 數學歸納法必須對所有的正整數才行, 不能摒除 p的倍數。很幸運的, 修飾之後的版本 $a^p \equiv a \pmod{p}$對 p的倍數自動成立; 因爲在模 p之下, 同餘式兩邊都是 0。

因此我們可用數學歸納法證明 $a^p \equiv a \pmod{p}, \quad \forall a \in \mathbb{N} \quad (*)$ 如下:

(i) $a = 1$ 時同餘式 $(*)$ 成立, 因 $1^p \equiv 1 \pmod{p}$;

(ii) 假設 $a = k$ 時同餘式 $(*)$ 成立, 亦即 $k^p \equiv k \pmod{p}$。所以

$$(k+1)^p \equiv k^p + 1 \equiv k + 1 \pmod{p},$$

意味著 $a = k+1$ 時同餘式 $(*)$ 也成立; 故得證 $a^p \equiv a \pmod{p}, \quad \forall a \in \mathbb{N}.$

接下來, $a = 0$ 時同餘式 $(*)$ 當然成立; 那負整數 $a = -k,\ k \in \mathbb{N}$ 時又如何呢? 請看:

$$(-k)^p = -k^p \Longrightarrow a^p = (-k)^p = -(k^p) \equiv -k = a \pmod{p}。$$

所以關鍵在於等式 $(-k)^p = -k^p$對嗎? 若 p是奇數, 當然沒問題; p是偶數又怎麼樣呢? 一般而言, 是不對的; 因爲 $-k$ 的偶數次方, 符號會變成正的。然而, 我們的 p是質數; 除了 $p = 2$之外, 其他時候都是奇數。但當 $p = 2$時, 我們生活在一個沒有正負之分的世界; 因爲在模 2的世界裡, $1 + 1 \equiv 0 \pmod{2}$。所以, $-1 \equiv 1 \pmod{2}$; 也就是說, 負的就是正的, 減法就是加法。因而我們永遠有

$$(-k)^p = -k^p \pmod{p}。$$

這就完成了對同餘式 $a^p \equiv a \pmod{p}, \quad \forall a \in \mathbb{Z}$ 的證明, 也完成了費馬小定理的證明。

二、接下來呢?

用數學歸納法證明容易帶給人空虛的感覺, 因爲不知道公式從何而來? 空虛之餘, 接下來呢? 至少有兩件事情可以進行, 其一當然是希望把公式導出來; 其二則是可能的話, 將公式推廣或一般化。

整數無窮, 模 p之後只剩 p個餘數 $0, 1, 2, \ldots, p-1$; 通常用符號 $\mathbb{Z}_p$ 表示, 在模 p的加法及乘法之下 $(\mathbb{Z}_p, +, \cdot)$ 形成一個有限體的代數結構。費馬小定理所生存的空間就在這個有限體的乘法結構當中, 也就是 $(\mathbb{Z}_p^\times, \cdot)$當中; 此處 $\mathbb{Z}_p^\times = \{1, 2, 3, \ldots, p-1\}$, 這是一個交換群的代數結構[5]。

我們現在就從這個有限交換群的代數結構 $(\mathbb{Z}_p^\times = \{1, 2, \ldots, p-1\}, \cdot)$來建構費馬小定理。令整數 a爲非 p的倍數, 亦即與 p互質, 故 $a \in \mathbb{Z}_p^\times$。此群包含有 $p-1$個元素, 而這正是定理中 a的次冪。因而, 很自然地; 我們將 a乘上群中的每一個數, 如此得到包含有 $p-1$個 a之倍數的集合

$$\mathbb{Z}_p^\times a = \{1a,\, 2a,\, 3a,\, \ldots,\, (p-1)a\} \subseteq \mathbb{Z}_p^\times \text{。}$$

在模 p之下, 集合 $\mathbb{Z}_p^\times a$中的數是否兩兩相異呢? 不難看出, 只消利用群的消去律即可確認的確如此; 因而此二集合 $\mathbb{Z}_p^\times a$ 與 $\mathbb{Z}_p^\times$, 在模 p之下同歸於一: $\mathbb{Z}_p^\times a = \mathbb{Z}_p^\times$。將各自集合中所有的數相乘, 即得

$$(1a)(2a)\cdots(p-1)a \equiv 1 \cdot 2 \cdots (p-1) \pmod{p}\,,$$

或 $(p-1)!\, a^{p-1} \equiv (p-1)! \pmod{p}$; 消去律帶領我們抵達費馬小定理

$$a^{p-1} \equiv 1 \pmod{p}\text{。}$$

在上面的論證當中, 我們用到了 $(\mathbb{Z}_p^\times, \cdot)$是有限交換群的代數結構; 不僅導出了公式, 同時也證明了費馬小定理。

三、推廣到一般模 n

上一節的論證告訴我們, 費馬小定理此種論證的本質彰顯在 $(\mathbb{Z}_p^\times, \cdot)$是有限交換群的代數結構上。若將質數的假設拿掉, 公式會長的怎麼樣呢? 不需經過太多的思考, 很自然地我們會想到乘法群

$$\mathbb{Z}_n^\times = \{a \in \mathbb{Z}_n \mid \gcd(a, n) = 1\};$$

其元素個數就等於 $\phi(n)$, 也就是小於 n而又跟 n互質的正整數之個數。這同樣擁有交換群的代數結構[5]。

我們現在可優哉游哉輕輕鬆鬆地, 將上一節的論證依樣畫葫蘆地來建構費馬小定理推廣到一般模 n的公式。令 a爲與 n互質的整數且令 $\mathbb{Z}_n^\times = \{a_1,\, a_2,\, a_3,\, \ldots,\, a_{\phi(n)}\}$。仿上, 我們考

慮將 a乘上群 $\mathbb{Z}_n^\times$中每一個數所得到的集合

$$\mathbb{Z}_n^\times\, a = \{a_1a,\, a_2a,\, a_3a,\, \ldots,\, a_{\phi(n)}a\} \subseteq \mathbb{Z}_n^\times\,;$$

消去律告訴我們, 其中的元素兩兩互異; 故得到

$$\mathbb{Z}_n^\times\, a = \mathbb{Z}_n^\times \pmod n \Longrightarrow (a_1a)(a_2a)\cdots(a_{\phi(n)}a) \equiv a_1a_2\cdots a_{\phi(n)} \pmod n\,,$$

交換律允許我們將 a集中在一起寫成 a的 $\phi(n)$次方; 所以得到

$$(a_1a_2\cdots a_{\phi(n)})\, a^{\phi(n)} \equiv (a_1a_2\cdots a_{\phi(n)}) \pmod n\,。$$

最後再讓消去律施展發功一次, 得到費馬小定理的推廣 (即歐拉定理) : 若整數 a與 n互質, 則我們有同餘式

$$a^{\phi(n)} \equiv 1 \pmod n。$$

四、推廣到有限交換群

上兩節的論證中, 首先我們施展消去律, 讓看似不同的兩個集合 Ga 與 G 同歸於一。其次, 交換律提供給集合 Ga 一個機會; 當裡面所有元素相乘時, 其中的 a 可聚集在一起寫成 a 的一個次冪。最後, 再讓消去律發功一次, 得到所要的公式; 不管稱爲費馬小定理也好或是稱爲歐拉定理也好, 都是同一個模子。

這意味著什麼呢? 這意味著目前的論證, 其本質在 G 是有限交換群的代數結構上。因此之故, 推廣至有限交換群; 不僅是理所當然, 且是不費吹灰之力啊。令 G 爲擁有 m 個元素的交換群且令 $a \in G$ 爲當中的任何一個元素, 則 $a^m = e$, 此處 e 爲 G 的單位元素。其證明不言而喻! 令 $G = \{a_1, a_2, \ldots, a_m\}$, 則消去律告訴我們, $Ga = \{a_1a, a_2a, \ldots, a_ma\}$中的元素兩兩互異; 所以我們有, $Ga = G$。將 Ga 與 G各自集合裡面所有的元素相乘, 交換律使 a聚集一處; 故得

$$(a_1a_2\cdots a_m)\, a^m = (a_1a_2\cdots a_m)\,。$$

最後, 再一次的消去律; 我們抵達目的地 $a^m = e$, 帥呆了。

五、有限非交換群又如何?

若將交換性拿掉, 上面的論證可就行不通了。會有同樣的公式嗎? 也就是說, 在擁有 m個元素的非交換群 G裡, 是否 $a^m = e\ \forall a \in G$?

這是最後的挑戰! 我們面臨再一次的山不轉路轉之關鍵時刻。如何路轉? 沒有交換性, 元素 a要集中一處僅有的法子就是: 不可有任何其它元素的干擾。因此之故, 順理成章地我們考慮

群 G中由元素 a所生成的循環子群 $<a>=\{a^n \mid n \in \mathbb{Z}\} < G$。因爲 G是有限群, 必存在正整數 $i < j$使得 $a^i = a^j$; 所以 $a^{j-i} = e$。正整數$\mathbb{N}$之良序性應許我們必存在一最小正整數 k使得 $a^k = e$; 稱之爲 a的週期 (order), 通常以符號 $\circ(a)$表示之。所以在此種情況, 這個循環子群

$$<a>=\{a,\, a^2,\, a^3,\, \ldots,\, a^{\circ(a)} = e\}$$

僅包含有 $\circ(a)$ 個元素。若 $a^m = e$, 那麼週期 $\circ(a)$必定可以整除次冪 m; 亦即 $\circ(a) \mid m$。若否, 則將 m除以週期 $\circ(a)$, 得到商爲 q餘數爲 r, 此處 $0 < r < \circ(a)$。由此得知,

$$r = m - q \circ (a) \Longrightarrow a^r = a^m (a^{\circ(a)})^{-q} = e e^{-q} = e.$$

因而冒出來一個比週期 $\circ(a)$還小的正整數 r使得 $a^r = e$, 這顯然違背了週期的特性, 故得證。換句話說, 我們已經證明了: 欲達目的地 $a^m = e$ 之必要條件是 $\circ(a) \mid m$。反過來, 是否 $\circ(a) \mid m$ 也是目的地 $a^m = e$ 之充分條件呢? 很明顯的, 指數律告訴我們, 答案是肯定的。所以想要證明 $a^m = e$, 就等同於去證明 $\circ(a) \mid m$; 這就是下面所要進行的工作。

令 $A =<a>$且令 $k = \circ(a)$。若 $A = G$, 則 $m = \circ(a)$, 沒什好證的。故假設 $A \neq G$, 則存在有一元素 $b \in G$但 $b \notin A$, 然後將目前所有知道的元素列表如下:

$$a,\ a^2,\ a^3,\ \ldots,\ a^{k-1},\ e$$

$$ab, a^2b, a^3b, \ldots,\ a^{k-1}b, b$$

不難看出, 所有在第二列出現的元素兩兩相異 (根據消去律) 而且也迥異於在第一列出現的元素 ($a^i b = a^j \Rightarrow b = a^{j-i} \in A$ 違背了假設 $b \notin A$)。

至此, 我們已經列出了 $2 \circ (a)$元素; 若這就是 G所有的元素, 那麼證明完畢, 下台一鞠躬。否則的話, 就選取不在這兩列的元素 c並考慮下面新的表列:

$$\begin{aligned} &a,\ a^2,\ a^3,\ \ldots,\ a^{k-1},\ e \\ &ab, a^2b, a^3b, \ldots,\ a^{k-1}b, b \\ &ac, a^2c, a^3c, \ldots,\ a^{k-1}c, c \end{aligned}$$

同樣地不難看出, 所有在第三列出現的元素兩兩相異 (根據消去律) 而且也迥異於在前兩列出現的元素。因此上面列出來的元素總共有 $3\circ (a)$個。如此繼續進行下去的話, 每次所新製造出來的元素都是有 $\circ(a)$個。G的有限性保證我們在有限個步驟, 說是 s個步驟之後就會掃盡所有 G中的元素; 因而得到 $m = s \circ (a)$, 故得證 $\circ(a) \mid m$.

六、拉格蘭日定理 (Lagrange's Theorem)

我們若將上面由元素 a所生成的循環子群換成任意的子群 $H < G$, 那麼一模一樣的論證 (僅需將次冪移至下標 $H = \{a_1, \ldots, a_{k-1}, a_k = e\}$); 同樣可以得到 H的元素個數 $\circ(H)$是 G元素個數 $\circ(G)$的因子。這就是群論中鼎鼎有名而且最最基本的一個定理, 稱之爲拉格蘭日定理。

這就完成了從費馬到拉格蘭日的簡單旅程。我們從費馬小定理出發, 本著推導公式的方法; 推廣、推廣、再推廣, 卻靠著拉格蘭日從死胡同中路轉而出。下面, 我們恭恭敬敬地再一次敘述拉格蘭日定理並將其最重要的五個推論依序擺在你的面光之中[1]; 最後又再度回歸費馬小定理, 如此這般地我們瀟灑走一回。

拉格蘭日定理: 若 G 是有限群且 H 是 G 的子群, 則 $\circ(H) \mid \circ(G)$。

推論一: 若 G是元素個數爲質數 p的有限群, 則 G是循環群。

證明: 選取非單位元素 $a \in G$ 且令 $H = < a >$, 則

$$1 < \circ(H) \mid \circ(G) = p \Longrightarrow \circ(H) = p \Longrightarrow H = G,$$

故得證 G是循環群。

推論二: 若 G是有限群且 $a \in G$, 則 $\circ(a) \mid \circ(G)$。

證明: 令 $H = < a >$, 則 $\circ(a) = \circ(H) \mid \circ(G)$, 故得證。

推論三: 若 G是有限群且 $a \in G$, 則 $a^{\circ(G)} = e$.

證明: 推論二得知 $\circ(a) \mid \circ(G)$, 則 $\circ(G) = r \circ (a)$, 其中 $r \in \mathbb{N}$。故

$$a^{\circ(G)} = a^{r\circ(a)} = (a^{\circ(a)})^r = e^r = e.$$

推論四: 若 n是正整數且若整數 a與 n互質, 則我們有同餘式

$$a^{\phi(n)} \equiv 1 \pmod{n}。$$

證明: 將推論三執行在乘法群 $G = \mathbb{Z}_n^{\times}$, 即得。

推論五: 若 p是正質數且若整數 a不是 p的倍數, 則我們有同餘式

$$a^{p-1} \equiv 1 \pmod{p}。$$

證明: 將推論三執行在乘法群 $G = \mathbb{Z}_p^{\times}$, 即得。

參考資料

1. Herstein I.N.: Topics in Algebra, 2nd ed., John Wiley & Sons, Inc., 1975.
2. Rivest, R.L., Shamir A., and Adleman L.: A Method for Obtaining Digital Signatures and Public-Key Cryptosystems, *Communications of the ACM*, **21**(1978), 120-126.
3. 沈淵源, 數論輕鬆遊, 數學傳播第二十九卷第四期(116), 94年12月, 第45-71頁。全文見網頁 w3.math.sinica.edu.tw/media/pdf.jsp?m_file=ZDI5NC8yOTQwOA==
4. 沈淵源, 公鑰密碼之旅, 數學傳播第三十五卷第四期 (140), 100年12月, 第34-48頁。全文見網頁 w3.math.sinica.edu.tw/media/pdf.jsp?m_file=ZDM1NC8zNTQwNA==
5. 沈淵源,「抽象代數」真的抽象嗎? (上) , 數學傳播第三十六卷第二期 (142), 101年 6月, 第34-51頁。全文見網頁 w3.math.sinica.edu.tw/media/pdf.jsp?m_file=ZDM2Mi8zNjIwNA==

—本文作者任教東海大學數學系—