數論三講

于 靖

§1. 有關 Fermat 最後定理

你們當然都聽說過**Fermat**最後定理。這個著名問題可以作爲初等數論課的一個起點。藉由它我們可以熟悉好些種數論裡的基本方法。

P. Fermat 說: 方程式 $x^n + y^n = z^n$, $n > 2$ 沒有滿足 $xyz \neq 0$ 的整數解。他證明了 $n = 4$ 的情形:

定理1. 方程式 $x^4 + y^4 = z^2$ 沒有滿足 $xyz \neq 0$ 的整數解。

證明: Fermat 的方法現代稱爲遞降法。假定 (x, y, z) 滿足方程式而 $xyz \neq 0$。可以假定 $z > 0$。策略是去建構另一組解 (x_1, y_1, z_1), 仍然滿足 $x_1y_1z_1 \neq 0$, 而 $0 < z_1 < z$。假如我們的建構是對的, 就可持續做下去而得到一組無窮數列由遞降正整數組成。因此最先開始的解必定是不能存在的。

可以假定 x, y, z 沒有公因數, x 是奇數而 y 是偶數。我們有

$$y^4 = (z - x^2)(z + x^2),$$

$$(z - x^2, z + x^2) = 2。$$

因爲整數的唯一分解, 只有兩種可能性: $z - x^2 = 2a^4, z + x^2 = 8b^4$, 其中 $a > 0$ 是奇數而 $(a, b) = 1$, 或者是 $z + x^2 = 2a^4, z - x^2 = 8b^4$, 其中 $a > 0$ 是奇數而 $(a, b) = 1$。第一種情形是不可能的, 因爲可以導出 $x^2 = -a^4 + 4b^4$, 以至於 $1 \equiv -1 \pmod 4$。因此必定 $z = a^4 + 4b^4$, $a < z$, 而且 $z - x^2 = 8b^4$。因而 $4b^4 = (a^2 - x)(a^2 + x)$。仍然會有 $(a^2 - x, a^2 + x) = 2$。設 $a^2 - x = 2c^4, a^2 + x = 2d^4$ 就得到了 $a^2 = c^4 + d^4$。

由 Fermat 這個定理可以知道: 要證明**FLT**, 只須要考慮指數 n 是奇質數的情形。上述方法其實是數學歸納法的另一個形式。在這裡我們是用大小或高度來把解排序。

1823 年 Sophie Germain 證明了以下的結果:

定理2. 若 p 爲奇質數使 $2p + 1 = q$, 另一質數。則 $x^p + y^p + z^p = 0$ 沒有滿足 $(p, xyz) = 1$ 的整數解。

這兒的敍述, Fermat 方程式在奇質數時沒有有滿足 $(p, xyz) = 1$ 的解, 傳統上稱爲 Fermat 定理的第一類情形。1985 年

Adleman, Heath-Brown 與 Fouvry 證明了存在無窮多質數 p 使得在指數爲 p 時 **Fermat 定理**第一類情形成立。他們的工作起點仍是 Sophie Germain 的結果。

定理2 證明: 要點是考慮 mod 質數 q 的同餘。假定 $(x,y,z)=1$ 且 $p|xyz$。分解 $-x^p=(y+z)(z^{p-1}-z^{p-2}y+\cdots+y^{p-1})$。假設質數 l 滿足 $l|(y+z)$, 則 $l\neq p$ 且 $py^{p-1}\equiv 0\ (\mathrm{mod}\, l)$。因此 $l|y$, 這是不可能的。因而有

$$y+z=a^p,\ z^{p-1}-z^{p-2}y+\cdots+y^{p-1}=\alpha^p。$$

同樣, 可得到 $x+y=b^p$, 與 $x+z=c^p$。同時 $b^p+c^p-a^p=2x$。

由假設 $x^{(q-1)/2}+y^{(q-1)/2}+z^{(q-1)/2}\equiv 0\ (\mathrm{mod}\, q)$。因 $q>5$, 可假定 $q|x$。(回憶由 Fermat 小定理可推得 $q|m$, 則 $m^{(q-1)/2}\equiv \pm 1\ (\mathrm{mod}\, q)$)。因此 $b^p+c^p-a^p=2x\Rightarrow b^{(q-1)/2}+c^{(q-1)/2}-a^{(q-1)/2}\equiv 0\,(\mathrm{mod}\, q$。從 $q|x$, 可得 $q|bc$, 因此 $q|a$。

最後考慮 α^p mod q。我們有 $y\equiv b^p\ (\mathrm{mod}\ q)$, 因而

$$\alpha^p\equiv py^{p-1}\ (\mathrm{mod}\, q),$$

$$\pm 1\equiv \pm p\ (\mathrm{mod}\, q)。$$

此與假設 $2p+1=q$ 顯然是矛盾的。

數學家並不知道是否有無窮多個質數 p 使得 $2p+1$ 也是質數。但是 Legendre 就已經觀察到: 要證明 **FLT** 的第一類情形對指數 p 成立, 可以修改 Sophie Germain 的方法達成, 只要 $4p+1$ (或 $6p+1, 8p+1, 10p+1, 14p+1$ 或 $16p+1$) 也是質數。這些思考途逕終於在一百六十年後導致 Adleman, Heath-Brown 與 Fouvry 的結果。

一般而言, 要想證明有無窮多個質數滿足某種性質是很困難的事。這方面最成功的結果是 Dirichlet 的定理: 假如首項 a 與公比 d 互質, 則算術數列 $a+md$ 中有無窮多個質數。這個定理是用解析方法證得的。

把一個整數取 $(q-1)/2$ 次乘冪, 然後 mod q 往往是很有用的。這兒有所謂的二次逆換律使得我們可以很容易算出正負號。假使有必要, 當然也可以考慮「高次逆換律」。

我們現在繞道去看對於多項式的 **Fermat 最後定理**. 記得單變數多項式的集合與整數所成集合相似之處甚多。

給複係數多項式 $f(t)$。定義 $n_0(f)$ 爲 f 的相異根的數目。大約十年前, Mason 發現了以下的

定理3. 設 $a(t)$, $b(t)$, $c(t)$ 爲互質多項式使得 $a(t)+b(t)=c(t)$, 則

$$\begin{aligned}&\max\{\deg a(t),\deg b(t),\deg c(t)\}\\ \leq\ & n_0(a(t)b(t)c(t))-1。\end{aligned}$$

證明: 要點是用對數微分來處理根。設 $f=a(t)/c(t)$, $g=b(t)/c(t)$。則

$$f'+g'=\frac{f'}{f}f+\frac{g'}{g}g=0,$$

$$\frac{b(t)}{a(t)}=\frac{g}{f}=-\frac{f'/f}{g'/g}。$$

設

$$\begin{aligned}a(t)&=c_1\prod(t-\alpha_i)^{m_i},\\ b(t)&=c_2\prod(t-\beta_j)^{n_j},\end{aligned}$$

$$c(t) \;=\; c_3\prod(t-\gamma_k)^{r_k}\downarrow$$

因而

$$\frac{b(t)}{a(t)} = -\frac{f'/f}{g'/g} = -\frac{\sum\frac{m_i}{t-\alpha_i}-\sum\frac{r_k}{t-\gamma_k}}{\sum\frac{n_j}{t-\beta_j}-\sum\frac{r_k}{t-\gamma_k}}。$$

定義 $N_0=\prod(t-\alpha_i)\prod(t-\beta_j)\prod(t-\gamma_k)$, 則

$$\frac{b(t)}{a(t)} = -\frac{N_0f'/f}{N_0g'/g}。$$

這兒 N_0f'/f 與 N_0g'/g 都是多項式, 其次數不大於 $n_0(a(t)b(t)c(t))-1$。從 $a(t)$, $b(t)$ 互質的假設就得到我們所要結論。

推論. 方程式 $x^n+y^n=z^n,\ n>2$ 假使有多項式解 $(x(t),y(t),z(t)),\ x(t),\ y(t),\ z(t)$ 爲互質複係數多項式, 則 $(x(t),y(t),z(t))$ 中至少有一爲常數。

證明: 設 $x(t)$, $y(t)$, $z(t)$ 爲互質的複係數多項式, 不全爲常數, 而且滿足 Fermat 方程式。由定理 3 得到

$$n\deg x(t)\le \deg x(t)+\deg y(t)+\deg z(t)-1,$$

$$\begin{aligned} & n(\deg x(t)+\deg y(t)+\deg z(t)) \\ \le\ & 3(\deg x(t)+\deg y(t)+\deg z(t))-3。\end{aligned}$$

假如 $n>2$ 這是不可能的。

這個研究提供了對原先 **Fermat 問題**的另一種角度。給定整數 m, 定義 $N_0(m)$ 爲 m 的所有相異質因數的乘積。

abc 猜測. 固定 $\epsilon>0$, 存在有整數 $C(\epsilon)$ 具備以下性質。對給定 非零互質整數 a, b, c, $a+b=c$, 以下等式恆成立

$$\max\{|a|,|b|,|c|\}\le C(\epsilon)N_0(abc)^{1+\epsilon}。$$

由此可導出以下有關 **FLT** 的結果

定理4. 假設 **abc 猜測**爲眞, 則對所有充分大的 n, 方程式 $x^n+y^n=z^n$ 沒有滿足 $xyz\neq 0$ 的整數解。

定理 4 的證明與多項式的情形幾乎一樣。**abc 猜測**多出來的常數 $C(\epsilon)$ 是導致充分大 n 此一限制的原因。

直觀而言, **abc 猜測**是說很多質因數都只出現一次。假設一個小質數出現很多次, 則必須有出現一次的大質數來補償。從 $2^n\pm1$ 形式整數的分解就可看出端倪 (Fermat 質數, Mersenne 質數)。

在**abc 猜測**裡的 ϵ 對絕對必須的。對於任何正數 $C>0$, 都存在互質整數 a, b, c, 使 $a+b=c$, 而且 $|a|>CN_0(abc)$。例如考慮 $a_n=3^{2^n}$, $b_n=-1$, 注意對所有 n 恆有 $2^n|(3^{2^n}-1)$。

§2. 質數的分布

給定實數 $x>0$, 我們以 $\pi(x)$ 表示所有不超過 x 的質數個數。從x 增加時 $\pi(x)$ 的成長, 我們可以粗略的瞭解質數的分布。Gauss 首先猜測到:

$$\lim_{x\to\infty}\frac{\pi(x)}{x/\log x}=1。$$

這就是後來 Hadamard 與 de la Vallée Poussin 證明的所謂**質數定理**。這

個定理在約一百年前是經由高難度的解析方法得到的。對於初學者而言, 探索質數分布, 可以從 Chebyshev 的結果開始, 即證明存在常數 a 與 A, $0 < a < A$, 使得對所有實數 $x \geq 2$,

$$\frac{ax}{\log x} < \pi(x) < \frac{Ax}{\log x}。$$

事實上 Chebyshev 的工作已經相當深入, 他不僅對質數的 Asympototic 分布有研究, 也更進一步回答了所謂的 Bertrand 問題:

定理5 (Bertrand 假說) 對於任何整數 n, 存在質數 p 使得 $n < p \leq 2n$。

以下 p 將只用來表示質數。

定理6. 對於任何正整數 n, 我們有不等式 $\sum_{p \leq n} \log p < 2n \log 2$。

證明: 設 $\theta(n)$ 爲 Chebyshev 函數, $\theta(n) = \sum_{p \leq n} \log p$。假定對 $n < n_0$, 此定理成立。若 n_0 爲偶數, 則

$$\begin{aligned} \theta(n_0) &= \theta(n_0 - 1) < 2(n_0 - 1) \log 2 \\ &< 2n_0 \log 2 \end{aligned}$$

若 $n_0 = 2m + 1$, 我們可證明 $\theta(2m+1) - \theta(m+1) < 2m \log 2$。然後

$$\begin{aligned} \theta(n_0) &= \theta(2m+1) - \theta(m+1) + \theta(m+1) \\ &< 2m \log 2 + 2(m+1) \log 2 \\ &= 2n_0 \log 2。 \end{aligned}$$

考慮整數 $M = \frac{(2m+1)!}{m!(m+1)!}$。從二項式展開得到 $2M < 2^{2m+1}$, 因而 $M < 2^{2m}$。所以

$$\begin{aligned} &\theta(2m+1) - \theta(m+1) \\ = &\sum_{m+1 < p \leq 2m+1} \log p \leq \log M < 2m \log 2。 \end{aligned}$$

Bertrand 假說之證明: 首先知道階數乘 $n!$ 的分解

$$n! = \prod_p p^{\sum_{m \geq 1} \left[\frac{n}{p^m}\right]}。$$

假定對某一 $n > 512$, 不存在質數 p 使 $n < p \leq 2n$。

我們考慮整數 $N = \frac{(2n)!}{(n!)^2} = \prod_{p \leq 2n} p^{k_p}$, 其中

$$k_p = \sum_{m=1}^{\infty} \left(\left[\frac{2n}{p^m} \right] - 2 \left[\frac{n}{p^m} \right] \right)。$$

若 $p|N$, 則 $k_p \geq 1$ 且 $p \leq n$。假使 $2n/3 < p \leq n$, 則 $2p \leq 2n < 3p$ 而且 $p^2 > 4n^2/9 > 2n$。因此 $k_p = 0$。所以 N 的所有質因數均滿足 $p \leq 2n/3$, 而且由定理 6,

$$\sum_{p|N} \log p \leq \theta(2n/3) < \frac{4n}{3} \log 2。$$

由於 $\left[\frac{2n}{p^m}\right] - 2\left[\frac{n}{p^m}\right]$ 是 1 或 0, 根據 $\left[\frac{2n}{p^m}\right]$ 是偶數或奇數而定。因此 $k_p \leq [\log 2n / \log p]$。假使 $k_p \geq 2$, 就得到

$$2 \log p \leq k_p \log p \leq \log(2n),\ p \leq \sqrt{2n}。$$

因而

$$\sum_{k_p \geq 2} k_p \log p \leq \sqrt{2n} \log(2n),$$

$$\log N \leq \sum_{p|N} \log p + \sqrt{2n} \log(2n)$$

$$\leq \quad \frac{4n}{3}\log 2 + \sqrt{2n}\log(2n)。$$

另一方面, 由二項式展開得到 $2^{2n} \leq 2nN$, 因此

$$\begin{aligned} & 2n\log 2 \leq \log(2n) + \log N \\ \leq \quad & \frac{4n}{3}\log 2 + (1+\sqrt{2n})\log(2n)。 \end{aligned}$$

數學中有關質數的未解決的問題還有很多。例如: 有沒有無窮多對雙生質數 (即p 與 $p+2$ 均爲質數)? 另一個 Gauss 問的問題是: 是否有無窮多個質數 p, 使 $1/p$ 的小數展開的循環節長度正好是 $p-1$? 與此等價的另一敍述是: 是否存在無窮多個質數 p 使得 10 是 mod p 的原根? 有關質數在區間內的分布也有遠比 Bertrands 假說更困難的問題, 例如: 對任意正整數 n, 是否存在質數 p 使得 $n \leq p \leq n + \sqrt{n}$。

最後我們以 Chebyshev 函數來寫下質數定理的另一形式:

$$\lim_{x\to\infty} \frac{\pi(x)\log x}{\theta(x)} = 1, \ \lim_{x\to\infty} \frac{\theta(x)}{x} = 1。$$

§3. 數的幾何

數論中有一個很有用的原理叫做鴿龍原理。假如有 n 個籠子裡面有 $n+1$ 隻鴿子, 那一定有一個籠子裡至少有兩隻鴿子。Dirichlet 用這個原理來對無理數找接近的有理數, 他得到了「很好的有理近似」:

定理7. 對任意實數 γ, 及整數 $N > 1$, 存在整數 h, k, $0 < k < N$ 使得 $|\gamma - h/k| < 1/Nk$。

證明: 我們的鴿子是 N 個實數: $n\gamma - [n\gamma]$, $n = 1, 2, \ldots, N$。籠子則是區間 $(0, 1/N)$, $(1/N, 2/N), \cdots, (N-1/N, 1)$。假使第一個籠子有一隻鴿子, 則 $0 < m\gamma - [m\gamma] < 1/N$ 對某一 $m \leq N$ 成立。因此 $0 < \gamma - [m\gamma]/m < 1/Nm$ 成立。

另一方面, 假使第一個籠子沒有鴿子, 就一定有整數 m, n, $0 < m < n \leq N$, 而且

$$|(n-m)\gamma - ([n\gamma] - [m\gamma])| < 1/N。$$

我們取 $k = n - m$, 且 $h = [n\gamma] - [m\gamma]$ 就得到所要結論。

推論: 若 γ 是無理數, 則存在無窮多個有理數 h/k, 使得 $|\gamma - h/k| < 1/k^2$。

Hurwitz 更進一步加強了這個推論。對於任何常數 $c \leq \sqrt{5}$, 他都可得到無窮多個有理數 h/k 使 $|\gamma - h/k| < 1/ck^2$。對給定實數 γ 成立。另一方面, 確有無理數 γ_0, 使得對固定 $c > \sqrt{5}$, 只有有限個有理數 h/k 能滿足 $|\gamma_0 - h/k| < 1/ck^2$。

我們要根據 Minkowski 的一個原理, 給定理 7 另一個證明。這個原理也是鴿籠原理的一個較幾何的形式。以下我們稱 $\mathcal{R}^n$ 的一個子集 S 爲凸集合, 假設對所有的實數 $\mu, \nu > 0$, 而 $\mu + \nu = 1$, 它都滿足 $\mathrm{x}, \mathrm{y} \in S \Rightarrow \mu\mathrm{x} + \nu\mathrm{y} \in S$。假設 S 又滿足 $\mathrm{x} \in S \Rightarrow -\mathrm{x} \in S$, 就稱其爲對稱集合 (對原點對稱)。最後, 假如我們定義 $\mathcal{R}^n$ 一個子集 S 的體積, 也稱 S 爲可測度集合。

定理8.(Minkowski) 設 S 爲 $\mathcal{R}^n$ 中一個有界可測度的凸對稱集。假使 S 的體積

超過 2^n, 則必定包含有不同於原點的格子點(即座標均爲整數的點)。

證明: $n=1$ 的情形是顯然的。我們只證平面的情形。考慮 $\mathcal{R}^2$ 中所有邊長爲 2, 中心點 x 的座標是偶整數的正方形 $\square_{\mathrm{x}}$ 假如這樣一個正方形 $\square_{\mathrm{x}}$ 交到 S, 就平移 $S\cap\square_{\mathrm{x}}$ 到 $S\cap\square_{\mathrm{x}}-\mathrm{x}\subset\square_0$。

如此就把 S 中所有點都搬到 $\square_0$。因爲 S 的面積大於 4, S 中至少有兩點搬到同一點 $(x_0,y_0)\in\square_0$。再平移回去得得到那兩點座標爲 $(x_0,y_0)+(2r,2s)$ 與 $(x_0,y_0)+(2r',2s')$, 而整數對 $(r,s)\neq(r',s')$。因爲 S 是對稱的, $-(x_0+2r',y_0+2s')\in S$。由凸集合性質, 因而得到 S 中包含格子點

$$\left(\frac{x_0+2r-(x_0+2r')}{2},\frac{y_0+2s-(y_0+2s')}{2}\right)=(r-r',s-s')。$$

如果我們改變假設爲: S 的面積大於或等於 2^n, 則結論中找到的格子點就可能會在 S 的邊界上。

考慮下列不等式所給的平行四邊形區

$$|ax+by|\le\beta,\quad |cx+dy|\le\alpha,$$

其中 $\alpha,\beta>0$, $a,b,c,d\in\mathcal{R}$ 而 $\Delta=ad-bc\neq 0$。此平形四邊形區域面積是 $4\alpha\beta/\Delta$。因此假如 $\alpha\beta\ge\Delta$, 就必然有整數對 $(x,y)\neq 0$ 在此區域中。假如我們取 $a=d=1,c=0$, 就得到整數 x,y 使 $|x+by|\le\beta$ 且 $|y|\le 1/\beta$, 因而 $|b+x/y|\le 1/y^2$。

我們可以應用 Minkowski 的這個定理去做一組有理數的聯立近似:

定理9. 給定質數 $\alpha_1,\alpha_2,\ldots,\alpha_n$, 存在整數點 $(x_1,x_2,\ldots,x_n)$ 及整數 $y\ge 1$ 滿足

$$|\alpha_i-\frac{x_i}{y}|\ \le\ \frac{n}{(n+1)y^{(1+1/n)}},$$

對 $i=1,2,\ldots,n$。

證明: 固定 $r,t>0$, 考慮 $\mathcal{R}^{n+1}$ 中對稱凸集

$$|x_i-\alpha_i y|+|y/t|\le r,\quad 1\le i\le n。$$

用積分可以算出此集合體積爲 $2^{n+1}tr^{n+1}/(n+1)$。因此從定理 8 得到整數點 $(x_1,\ldots,x_n,y)\neq 0$。滿足 $|x_i-\alpha_i y|+|y/t|\le\left(\frac{n+1}{t}\right)^{\frac{1}{n+1}}$。

用算術平均與幾何平均不等式就得到, 對 $i=1,\ldots,n$,

$$\begin{aligned}&|(x_i-\alpha_i y)^n\left(\frac{ny}{t}\right)|^{\frac{1}{n+1}}\\ \le\ &\frac{n|x_i-\alpha_i y|+n|y/t|}{n+1}\\ \le\ &\frac{n}{n+1}\left(\frac{n+1}{t}\right)^{\frac{1}{n+1}},\end{aligned}$$

因此

$$|\alpha_i y-x_i|\le\frac{n}{(n+1)y^{1/n}}。$$

—本文作者任職於中央研究院數研所—