

基礎數論補充教材

Timo Chang

timo65537@protonmail.com

譯者: 仙女國公主

最後編輯: 2026 年 8 月 30 日

摘要

本講義為**基礎數論**課程的補充教材, 為作者在 2024 年春季擔任課程助教時所編撰, 並於演習課時講授. 此課程旨在涵蓋標準的導論課程之外的主題, 以及引領學生盡可能廣泛地探索數論的更多面向. 這門課預設學生具備最低限度的微積分及線性代數背景, 且無須抽象代數或數學分析的先備知識.

目錄

1	數論中的劉維爾定理與劉維爾數	2
2	黎曼 ζ 函數	5
3	狄利克雷密度定理	12
4	特徵的正交關係	18
5	高斯和與二次互反律	24
6	模 p 運算之下解的個數	24
7	仿射空間與射影空間	24
8	橢圓曲線及其群結構	24
9	p 進數	24
10	再論 p 進數	24
11	函數體中的基礎數論	24
12	再論函數體	24

1 數論中的劉維爾定理與劉維爾數

1.1 代數數與超越數

定理 1.1 若 $\alpha \in \mathbb{C}$ 是某非零多項式 $f \in \mathbb{Q}[x]$ ¹ 的根, 則稱 α 為代數數; 否則稱為超越數.

以符號 $\overline{\mathbb{Q}}$ 表示所有代數數的全體.

例 1.2 讀者不難想到代數數的一些例子, 比如說所有有理數、 $\sqrt{2}$ 、 $i = \sqrt{-1}$ 、 $(-1 + \sqrt{-3})/2$, 或更一般地, n 次單位根 $e^{2\pi i/n}$ 均為代數數.

事實上, 由「體論」(域論) 可證得: 只要 $\alpha, \beta \in \overline{\mathbb{Q}}$, 便有 $\alpha \pm \beta, \alpha\beta, \alpha/\beta \in \overline{\mathbb{Q}}$ (其中, α/β 中的 $\beta \neq 0$). 換言之, $\overline{\mathbb{Q}}$ 是「體」. (如果想要以構建式證明來說明此事實, 需要「結式」的概念, 其只需要線性代數的一些基本知識, 不妨參考我的講義 [2] 見更多相關的討論.)

例如, 取 $\alpha = \sqrt{2}$, $\beta = \sqrt{3}$, 令 $x = \sqrt{2} + \sqrt{3}$, 則 $x^2 = 5 + 2\sqrt{6}$, 從而

$$x^4 - 10x^2 + 1 = 0.$$

這意味著 x 亦為代數數.

例 1.3 對於超越數, 也許有人不禁會思考, 常數 e 和 π 是否是其中的例子. 的確, 已經證明出它們均為超越數, 亦即它們不是任何有理係數非零多項式的根. (參考我的講義 [1] 見只用微積分的工具來證明 e 的超越性.)

一些重要的「超越」函數也給出了超越數的例子. 舉例來說,

$$\log 2, \quad \zeta(2) := \sum_{n=1}^{+\infty} \frac{1}{n^2} = \frac{\pi^2}{6}, \quad \text{及} \quad \Gamma\left(\frac{1}{2}\right) = \int_0^{+\infty} t^{-\frac{1}{2}} e^{-t} dt = \sqrt{\pi}$$

均為超越數. (第 2 課將證明上述第二條等式, 見定理 2.3 及例 2.4.)

儘管常數 e 和 π 均為廣為人知的超越數, 但它們其實並非歷史上最早被證實的例子. 首個超越數實為劉維爾於 1844 年所構造; 他在發現了無理代數數的某項逼近性質後, 建構出了此一數字, 即現今所稱的「劉維爾常數」. 本週的課程將為大家介紹他的定理, 以及該常數的構造過程.

1.2 劉維爾在丟番圖逼近論中的定理

首先, 我們將證明下述定理.

定理 1.4 (劉維爾在丟番圖逼近論中的定理) 設 α 為滿足 n 次不可約多項式 $f(x) = \sum_{i=0}^n c_i x^i \in \mathbb{Z}[x]$ 的無理代數數. 那麼, 存在一數 $A > 0$ 使得對一切 $p, q \in \mathbb{Z}$, $q > 0$, 均有

$$\left| \alpha - \frac{p}{q} \right| > \frac{A}{q^n}.$$

¹ 記號 $\mathbb{Q}[x]$ 表示所有有理係數多項式的全體.

粗略來說, 定理 1.4 表明, 所有無理代數數 α 無法用有理數「很好地」去近似, 這是因為在 α 及任意有理數 p/q 之間一定有 A/q^n 的差距. 換言之, 若有無理數 α 可以由有理數很好地近似到一定程度, 則 α 必為超越數.

證明 由於 f 是多項式, 其導數 f' 必為連續函數, 故依最值定理, $M := \max_{[\alpha-1, \alpha+1]} |f'(x)|$ 必存在. 設 $\{\alpha_1, \dots, \alpha_m\}$ 為 f 的所有異於 α 的根構成的集合, 且設

$$0 < A < \min\{1, 1/M, |\alpha - \alpha_1|, \dots, |\alpha - \alpha_m|\},$$

我們斷言該 A 有定理描述中的性質.

假設不然, 即存在 $p, q \in \mathbb{Z}, q > 0$ 滿足

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{A}{q^n}, \quad (1.1)$$

由此可知,

$$\left| \alpha - \frac{p}{q} \right| \leq \frac{A}{q^n} \leq A < 1,$$

故 $p/q \in [\alpha - 1, \alpha + 1]$. 依均值定理, α 和 p/q 之間至少有一點 ξ 滿足

$$f(\alpha) - f\left(\frac{p}{q}\right) = f'(\xi) \left(\alpha - \frac{p}{q}\right). \quad (1.2)$$

因為 p/q 也在該區間中, 所以 $\xi \in [\alpha - 1, \alpha + 1]$. 於是, 根據 M 的定義, 我們有

$$M \geq |f'(\xi)|.$$

另外, α 是 f 的一根, 即 $f(\alpha) = 0$, 而由對於每個 $i = 1, \dots, m$, $|\alpha - p/q| \leq A < |\alpha - \alpha_i|$ 可知, $p/q \notin \{\alpha_1, \dots, \alpha_m\}$. 換言之, $f(p/q) \neq 0$. 有了這兩個條件, 連同 (1.2) 可推得 $f'(\xi) \neq 0$, 因此有

$$\left| \alpha - \frac{p}{q} \right| = \frac{|f(\alpha) - f(p/q)|}{|f'(\xi)|} = \frac{|f(p/q)|}{|f'(\xi)|}.$$

由此可見, 其分子

$$\begin{aligned} \left| f\left(\frac{p}{q}\right) \right| &= \left| c_0 + c_1 \frac{p}{q} + \dots + c_n \left(\frac{p}{q}\right)^n \right| \\ &= \frac{1}{q^n} |c_0 q^n + c_1 p q^{n-1} + \dots + c_n p^n| \\ &\geq \frac{1}{q^n}, \end{aligned}$$

其中, 最後一個等式成立是因為 $c_0, \dots, c_n, p, q$ 均為整數, 且它們在最後一個絕對值中的組合非零 (由於 $f(p/q) \neq 0$). 現在, 我們可將一切不等式綜合在一起, 可得

$$\left| \alpha - \frac{p}{q} \right| = \frac{|f(p/q)|}{|f'(\xi)|} \geq \frac{1}{|f'(\xi)| q^n} \geq \frac{1}{M q^n} > \frac{A}{q^n},$$

但這與 (1.1) 衝突. □

1.3 劉維爾數

在上一目中，我們介紹並證明了劉維爾關於無理代數數近似性的重要定理，正是憑藉著這個結果，他得以首次明確構造出一個超越數的例子。接下來，我們將具體探討他的構造方式。

定義 1.5 (劉維爾數) 設 $\alpha \in \mathbb{R}$ ，若對一切 $n \in \mathbb{N}$ ，皆存在 $a, b \in \mathbb{Z}$, $b > 1$ ，使得

$$0 < \left| \alpha - \frac{a}{b} \right| < \frac{1}{b^n}, \quad (1.3)$$

則稱 α 為劉維爾數。

根據定義，劉維爾數皆可在某種程度上被有理數良好地近似。定理 1.4 暗示了所有劉維爾數均為超越數——而事實也確實如此，我們將透過兩個步驟加以證明。

命題 1.6 所有劉維爾數均為無理數。

證明 假設不然，即存在有理劉維爾數 α ，則可記 $\alpha = p/q$ ，其中 $p, q \in \mathbb{Z}$, $q \geq 1$ 。取充分大的正整數 n 使得 $2^{n-1} > q$ 。我們斷言：此特定的 n 與定義 1.5 矛盾，即對一切 $a, b \in \mathbb{Z}$, $b > 1$ ，(1.3) 中其中一個不等式不成立（從而 α 不會是劉維爾數）。

注意到 $|\alpha - a/b| = |p/q - a/b| = |(pb - aq)/qb|$ 。

- 情況 1: $|pb - aq| = 0$ ，此時 $|\alpha - a/b| = 0$ ，但這與 (1.3) 的第一個不等式矛盾。
- 情況 2: $|pb - aq| \geq 1$ ，此時

$$\left| \alpha - \frac{a}{b} \right| \geq \frac{1}{bq} > \frac{1}{b2^{n-1}} \geq \frac{1}{b \cdot b^{n-1}} = \frac{1}{b^n},$$

第二個不等式成立於 n 的選取，而第三個不等式成立於 $b \geq 2$ ，但這與 (1.3) 中的第二個不等式矛盾。

得證。 □

命題 1.7 所有劉維爾數均為超越數。

證明 再次採矛盾證法，假設有劉維爾數 α 是代數數。依命題 1.6 可知 α 是無理數，故滿足定理 1.4 的假設，因此，存在 $n \in \mathbb{N}$ 及 $A > 0$ ，對於一切 $p, q \in \mathbb{Z}$, $q > 0$ ，均有

$$\left| \alpha - \frac{p}{q} \right| > \frac{A}{q^n}. \quad (1.4)$$

取充分大的正整數 r 使得 $2^r > 1/A$ ，那麼由於 α 是劉維爾數，依定義 1.5，存在 $a, b \in \mathbb{Z}$, $b > 1$ ，使得 $0 < |\alpha - a/b| < 1/b^{n+r}$ ，但由此可推得

$$0 < \left| \alpha - \frac{a}{b} \right| < \frac{1}{b^{n+r}} = \frac{1}{b^n b^r} \leq \frac{1}{b^n 2^r} < \frac{A}{b^n},$$

這與 (1.4) 矛盾，證畢。 □

我們已證明所有劉維爾數均為超越數，接下來將舉一個劉維爾數的例子，稱為**劉維爾常數**，是由劉維爾他自己提出的。

例 1.8 (劉維爾常數) 定義無窮和

$$L := \sum_{m=1}^{+\infty} \frac{1}{10^{m!}} = 0.110\,001\,000\,00\dots$$

注意到其小數表示在小數點後的每第 $m!$ 位均為 1，餘者均為 0。特別來說， L 是無理數。² 我們斷言 L 是劉維爾數，從而由命題 1.7 可推得 L 是超越數。

給定 $n \in \mathbb{N}$ ，將 L 寫成

$$L = \sum_{m=1}^n \frac{1}{10^{m!}} + \sum_{m=n+1}^{+\infty} \frac{1}{10^{m!}} = \frac{a'}{10^{n!}} + \sum_{m=n+1}^{+\infty} \frac{1}{10^{m!}},$$

其中， a' 是使得第一個和式可寫成單個分數的某數。現，取 $a := a'$ ， $b := 10^{n!}$ ，由此可得

$$\begin{aligned} 0 < \left| L - \frac{a}{b} \right| &= \sum_{m=n+1}^{+\infty} \frac{1}{10^{m!}} = \frac{1}{10^{(n+1)!}} + \frac{1}{10^{(n+1)!}} \sum_{m=n+2}^{+\infty} \frac{1}{10^{m!-(n+1)!}} \\ &\leq \frac{1}{10^{(n+1)!}} + \frac{1}{10^{(n+1)!}} \sum_{m=1}^{+\infty} \frac{1}{2^m} = \frac{2}{10^{(n+1)!}} < \frac{1}{10^{(n+1)!-1}} \leq \left(\frac{1}{10^{n!}} \right)^n, \end{aligned}$$

其中，最後一個不等式用到了 $(n+1)! - 1 \geq n(n!)$ ($n \in \mathbb{N}$)。因此，依定義 1.5， L 是劉維爾數。

練習 1.9 根據例 1.8 的思想，試給出劉維爾數的其他例子。

2 黎曼 ζ 函數

黎曼 ζ 函數實為數論中至關重要的函數之一，並以具備豐富的算術及分析性質著稱。例如，著名的黎曼猜想即在探討其「零點」之位置，該分佈與質數的分佈息息相關。本課程旨在證明此函數之若干基本性質，涵蓋歐拉乘積、正偶數點處之特殊值，以及黎曼的「解析延拓」與函數方程式。(本課程需要用到部分複分析工具，然所有技術性術語及證明過程皆會力求精簡。)

2.1 黎曼 ζ 函數的歐拉公式

定義 2.1 黎曼 ζ 函數為如下由級數定義的複變數函數：

$$\zeta(s) = \sum_{n=1}^{+\infty} \frac{1}{n^s}, \quad \operatorname{Re}(s) > 1. \quad (2.1)$$

將黎曼 ζ 函數與質數連結起來的首步為如下歐拉乘積。

²某實數是有理數的充要條件為：其小數表示或者只有有限位，或者有循環節。

命題 2.2 (歐拉) 對於 $\operatorname{Re}(s) > 1$, 有

$$\zeta(s) = \prod_p (1 - p^{-s})^{-1},$$

其中該無窮乘積遍及一切質數.

證明 由於對所有質數 p 及滿足 $\operatorname{Re}(s) > 1$ 的複數 s , 均有 $|p^{-s}| < 1$, 因此由幾何級數可看出等式右邊為

$$\begin{aligned} & \prod_p (1 - p^{-s})^{-1} \\ &= \left(\frac{1}{1} + \frac{1}{2^s} + \frac{1}{2^{2s}} + \cdots \right) \left(\frac{1}{1} + \frac{1}{3^s} + \frac{1}{3^{2s}} + \cdots \right) \left(\frac{1}{1} + \frac{1}{5^s} + \frac{1}{5^{2s}} + \cdots \right) \cdots \end{aligned}$$

現, 展開右式的乘積, 依算術基本定理³, 不難看出其結果與黎曼 ζ 函數的級數表達式 (2.1) 相符. $\square$

本節的主要目標是證明關於黎曼 ζ 函數的歐拉公式在正偶數點處的值的定理.

定理 2.3 (歐拉) 對於正偶數 $n \in \mathbb{N}$, 有

$$\zeta(n) = -\frac{B_n}{2 \cdot n!} (2\pi i)^n,$$

其中 $B_k \in \mathbb{Q}$ 為白努利數, 其由如下式子給出:

$$\frac{t}{e^t - 1} = \sum_{k=0}^{+\infty} B_k \frac{t^k}{k!}.$$

注意到由於 π 有超越性 (見例 1.3), 因此上述定理意味著黎曼 ζ 函數將正偶數點映至超越數. 必須指出, 關於其在正奇數點處之超越性的研究目前仍遙不可及.

例 2.4 由簡單的泰勒展開計算可得

$$\frac{t}{e^t - 1} = 1 - \frac{t}{2} + \frac{t^2}{12} - \frac{t^4}{720} + \cdots,$$

故有

$$B_0 = 1, \quad B_1 = -\frac{1}{2}, \quad B_2 = \frac{1}{6}, \quad B_3 = 0, \quad B_4 = -\frac{1}{30},$$

從而根據定理 2.3 (回顧一下例 1.3), 有

$$\zeta(2) = \frac{\pi^2}{6}, \quad \zeta(4) = \frac{\pi^4}{90},$$

等等.

³ 比如說, (2.1) 中的項 $1/12^s$ 來自

$$\frac{1}{12^s} = \frac{1}{(2^2 \cdot 3)^s} = \frac{1}{2^{2s}} \cdot \frac{1}{3^s} \cdot \frac{1}{1} \cdots$$

證明 複分析中, 正弦函數具有如下無窮乘積的公式:

$$\sin(\pi z) = \pi z \prod_{n=1}^{+\infty} \left(1 - \frac{z^2}{n^2}\right).$$

兩邊取對數後再求導, 可得

$$\pi \cot(\pi z) = \frac{\pi \cos(\pi z)}{\sin(\pi z)} = \frac{1}{z} + \sum_{n=1}^{+\infty} \frac{-\frac{2z}{n^2}}{1 - \frac{z^2}{n^2}} = \frac{1}{z} + \sum_{n=1}^{+\infty} \left(\frac{1}{n+z} - \frac{1}{n-z} \right). \quad (2.2)$$

另一方面, 由三角函數的指數表示式

$$\cos(z) = \frac{e^{iz} + e^{-iz}}{2} \quad \text{及} \quad \sin(z) = \frac{e^{iz} - e^{-iz}}{2i},$$

可得

$$\cot(z) = i \cdot \frac{e^{iz} + e^{-iz}}{e^{iz} - e^{-iz}} = i + \frac{2i}{e^{2iz} - 1},$$

從而

$$\pi \cot(\pi z) = \pi i + \frac{2\pi i}{e^{2\pi iz} - 1}. \quad (2.3)$$

由 (2.2) 及 (2.3), 得

$$\pi i + \frac{2\pi i}{e^{2\pi iz} - 1} = \frac{1}{z} + \sum_{n=1}^{+\infty} \left(\frac{1}{n+z} - \frac{1}{n-z} \right),$$

於是

$$\pi iz + \frac{2\pi iz}{e^{2\pi iz} - 1} = 1 + \sum_{n=1}^{+\infty} \left(\frac{2\pi iz}{2\pi in + 2\pi iz} - \frac{2\pi iz}{2\pi in - 2\pi iz} \right).$$

令 $t = 2\pi iz$, 則

$$\frac{t}{2} + \frac{t}{e^t - 1} = 1 + \sum_{n=1}^{+\infty} \left(\frac{t}{2\pi in + t} - \frac{t}{2\pi in - t} \right).$$

根據定義, 等式左邊為

$$\text{左式} = \frac{t}{2} + \sum_{k=0}^{+\infty} B_k \frac{t^k}{k!},$$

而等式右邊為

$$\begin{aligned}
\text{右式} &= 1 + \sum_{n=1}^{+\infty} \frac{t}{2\pi i n} \left(\frac{1}{1 + \frac{t}{2\pi i n}} - \frac{1}{1 - \frac{t}{2\pi i n}} \right) \\
&= 1 + \sum_{n=1}^{+\infty} \frac{t}{2\pi i n} \left(\sum_{k=0}^{+\infty} \left(-\frac{t}{2\pi i n} \right)^k - \sum_{k=0}^{+\infty} \left(\frac{t}{2\pi i n} \right)^k \right) \\
&= 1 + \sum_{n=1}^{+\infty} \frac{-2t}{2\pi i n} \left(\sum_{k=0}^{+\infty} \left(\frac{t}{2\pi i n} \right)^{2k+1} \right) \\
&= 1 - 2 \sum_{n=1}^{+\infty} \sum_{k=0}^{+\infty} \left(\frac{t}{2\pi i n} \right)^{2k+2} \\
&= 1 - 2 \sum_{k=0}^{+\infty} \left(\sum_{n=1}^{+\infty} \frac{1}{(2\pi i n)^{2k+2}} \right) t^{2k+2},
\end{aligned}$$

(在最後一個等式中, 交換兩求和符號的次序需要非常小心, 但此處我們略去詳細資訊.) 故有等式

$$\frac{t}{2} + \sum_{k=0}^{+\infty} B_k \frac{t^k}{k!} = 1 - 2 \sum_{k=0}^{+\infty} \left(\sum_{n=1}^{+\infty} \frac{1}{(2\pi i n)^{2k+2}} \right) t^{2k+2}. \quad (2.4)$$

現, 對於正偶數 m , 比較等式兩邊 t^m 的係數, 得

$$\frac{B_m}{m!} = -2 \sum_{n=1}^{+\infty} \frac{1}{(2\pi i n)^m} = \frac{-2}{(2\pi i)^m} \sum_{n=1}^{+\infty} \frac{1}{n^m} = \frac{-2}{(2\pi i)^m} \cdot \zeta(m),$$

因此,

$$\zeta(m) = -\frac{B_m}{2 \cdot m!} (2\pi i)^m.$$

□

系理 2.5 由於 $i \in \mathbb{C} \setminus \mathbb{R}$ 及 $B_k \in \mathbb{Q}$, 因此對於 $n \geq 2$,

$$\frac{\zeta(n)}{(2\pi i)^n} \in \mathbb{Q} \iff n \text{ 是偶數}.$$

系理 2.6 比較式 (2.4) 中的其他項, 有 (甲) $B_0 = 1$; (乙) $B_1 = -1/2$; (丙) 對於大於 1 的奇數, 有 $B_k = 0$. 這與我們在例 2.4 中的計算相吻合.

2.2 黎曼函數方程

在複分析中, 有一個概念稱為「解析⁴延拓」, 意為將某解析函數的定義域擴大並保持其解析性. 比如說, 考慮幾何級數 $1 + z + z^2 + \dots$, 其在 $D := \{z \in \mathbb{C} \mid |z| \leq 1\}$ 上定義一解析函數, 並且

$$1 + z + z^2 + \dots = \frac{1}{1 - z}, \quad z \in D.$$

⁴粗略地說, 所謂解析函數是指「局部」可展開成冪級數的函數.

然而, 等式右邊的函數不只在 D 上解析, 而且是 $\mathbb{C} \setminus \{1\}$ 上的解析函數. 因此, 可用此表達式來擴大該幾何級數的定義域, 並稱右式為其解析延拓.

有了對解析延拓大致的直觀想法, 本日將證明黎曼 ζ 函數 $\zeta(s)$ 具有解析延拓, 並推導其函數方程. 我們從以如下反常積分來定義的**歐拉伽瑪函數**開始:

$$\Gamma(s) := \int_0^{+\infty} t^s e^{-t} \frac{dt}{t}, \quad \operatorname{Re}(s) > 0. \quad (2.5)$$

定理 2.7 (黎曼) 令

$$\xi(s) := \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s), \quad \operatorname{Re}(s) > 1,$$

則可將 $\xi(s)$ 解析延拓至 $\mathbb{C} \setminus \{0, 1\}$ 上, 並且滿足函數方程

$$\xi(s) = \xi(1-s).$$

證明 於式 (2.5) 中作代換 $s \mapsto s/2$, 在等式兩邊乘以 $\pi^{-s/2} n^{-s}$, 且作變數變換, 得

$$\begin{aligned} \pi^{-\frac{s}{2}} n^{-s} \Gamma\left(\frac{s}{2}\right) &= \int_0^{+\infty} \pi^{-\frac{s}{2}} n^{-s} t^{\frac{s}{2}} e^{-t} \frac{dt}{t} \\ &= \int_0^{+\infty} \left(\frac{t}{\pi n^2}\right)^{\frac{s}{2}} e^{-t} \frac{dt}{t} \\ &= \int_0^{+\infty} t^{\frac{s}{2}} e^{-\pi n^2 t} \frac{dt}{t} \quad \left(\frac{t}{\pi n^2} \mapsto t\right). \end{aligned}$$

將上式關於 n 求從 1 至 $+\infty$ 的和, 得

$$\begin{aligned} \sum_{n=1}^{+\infty} \pi^{-\frac{s}{2}} n^{-s} \Gamma\left(\frac{s}{2}\right) &= \sum_{n=1}^{+\infty} \int_0^{+\infty} t^{\frac{s}{2}} e^{-\pi n^2 t} \frac{dt}{t} \\ &= \frac{1}{2} \sum_{\substack{n=-\infty \\ n \neq 0}}^{+\infty} \int_0^{+\infty} t^{\frac{s}{2}} e^{-\pi n^2 t} \frac{dt}{t} \\ &= \int_0^{+\infty} \left(\frac{\theta(it) - 1}{2}\right) t^{\frac{s}{2}} \frac{dt}{t}, \end{aligned} \quad (2.6)$$

此處,

$$\theta(z) := \sum_{n \in \mathbb{Z}} e^{\pi i n^2 z}$$

稱為**雅可比 θ 級數** (小心最後一個等式, 此處亦不加檢驗地交換了求和和積分的運算次序).

根據 $\xi(s)$ 的定義, 不難注意到 (2.6) 式的左邊為

$$\sum_{n=1}^{+\infty} \pi^{-\frac{s}{2}} n^{-s} \Gamma\left(\frac{s}{2}\right) = \pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \zeta(s) = \xi(s),$$

故得

$$\xi(s) = \int_0^{+\infty} \left(\frac{\theta(it) - 1}{2}\right) t^{\frac{s}{2}} \frac{dt}{t}. \quad (2.7)$$

為了計算 (2.7) 式的右邊, 需要下述 θ 級數的函數方程, 其可由「卜松求和公式」證得.

引理 2.8 θ 級數 $\theta(z)$ 滿足函數方程

$$\theta\left(-\frac{1}{z}\right) = \sqrt{\frac{z}{i}}\theta(z), \quad \text{Im}(z) > 0.$$

特別地,

$$\theta\left(\frac{i}{t}\right) = t^{\frac{1}{2}}\theta(it), \quad t > 0.$$

回到 (2.7) 式的右邊, 可見

$$\begin{aligned} & \int_0^{+\infty} \left(\frac{\theta(it) - 1}{2} \right) t^{\frac{s}{2}} \frac{dt}{t} \\ &= \frac{1}{2} \int_0^1 (\theta(it) - 1) t^{\frac{s}{2}} \frac{dt}{t} + \boxed{\frac{1}{2} \int_1^{+\infty} (\theta(it) - 1) t^{\frac{s}{2}} \frac{dt}{t}} \\ &= \frac{1}{2} \int_1^{+\infty} \left(\theta\left(\frac{i}{t}\right) - 1 \right) t^{-\frac{s}{2}} \frac{dt}{t} + \boxed{\phantom{\frac{1}{2} \int_1^{+\infty} (\theta(it) - 1) t^{\frac{s}{2}} \frac{dt}{t}}} \quad \left(t \mapsto \frac{1}{t} \right) \\ &= \frac{1}{2} \int_1^{+\infty} \left(t^{\frac{1}{2}}\theta(it) - 1 \right) t^{-\frac{s}{2}} \frac{dt}{t} + \boxed{\phantom{\frac{1}{2} \int_1^{+\infty} (\theta(it) - 1) t^{\frac{s}{2}} \frac{dt}{t}}} \quad (\text{引理 2.8}) \\ &= \frac{1}{2} \int_1^{+\infty} \left((\theta(it) - 1)t^{\frac{1}{2}(1-s)} + t^{\frac{1}{2}(1-s)} - t^{-\frac{s}{2}} \right) \frac{dt}{t} + \boxed{\phantom{\frac{1}{2} \int_1^{+\infty} (\theta(it) - 1) t^{\frac{s}{2}} \frac{dt}{t}}} \\ &= \frac{1}{2} \int_1^{+\infty} (\theta(it) - 1) t^{\frac{1}{2}(1-s)} \frac{dt}{t} - \frac{1}{1-s} - \frac{1}{s} + \boxed{\frac{1}{2} \int_1^{+\infty} (\theta(it) - 1) t^{\frac{s}{2}} \frac{dt}{t}}. \end{aligned}$$

故得

$$\xi(s) = \frac{1}{2} \int_1^{+\infty} (\theta(it) - 1) t^{\frac{1}{2}(1-s)} \frac{dt}{t} + \frac{1}{2} \int_1^{+\infty} (\theta(it) - 1) t^{\frac{s}{2}} \frac{dt}{t} - \frac{1}{1-s} - \frac{1}{s}. \quad (2.8)$$

可以證明, 式 (2.8) 中的各含參變數反常積分在 $\mathbb{C}$ 上解析. 因此, 由此等式, 可知 $\xi(s)$ 已解析延拓至 $\mathbb{C} \setminus \{0, 1\}$. (注意式 (2.8) 中的額外兩項 $-1/(1-s)$ 及 $-1/s$ 導致 $\xi(s)$ 在 $s = 0, 1$ 處沒有定義.) 另外也不難看出, 上式右邊在代換 $s \mapsto 1-s$ 之下保持不變, 因此對於左側來說應亦是如此, 換言之, 我們有

$$\xi(s) = \xi(1-s),$$

證畢. □

註記 2.9 以複分析的語言來說, 式 (2.8) 實際上證明了 $\xi(s)$ 具有整個複平面上的「亞純延拓」, 其在 $\mathbb{C} \setminus \{0, 1\}$ 上「全純」, 且在 $s = 0, 1$ 處具有「留數」分別為 $-1, 1$ 的「單極點」.⁵

系理 2.10 $\zeta(s)$ 可延拓為 $\mathbb{C} \setminus \{1\}$ 上的解析函數, 且滿足函數方程

$$\zeta(s) = 2^s \pi^{s-1} \sin\left(\frac{\pi s}{2}\right) \Gamma(1-s) \zeta(1-s).$$

⁵非常粗略地說, 其表示函數 $\xi(s)$ 可「良好地」(解析) 延拓至整個複平面, 除了在點 $s = 0, 1$ 的「行為」分別「像是」 $-1/s, -1/(1-s)$ (亞純函數).

證明 僅證明上述函數方程.⁶ 依定理 2.7, 在等式兩側乘上 $\Gamma(1 - s/2)$, 得

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \Gamma\left(1 - \frac{s}{2}\right) \zeta(s) = \pi^{-\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right) \Gamma\left(1 - \frac{s}{2}\right) \zeta(1-s). \quad (2.9)$$

依 Γ 函數的歐拉反射公式 (又稱餘元公式),

$$\Gamma(z)\Gamma(1-z) = \frac{\pi}{\sin(\pi z)}, \quad z \notin \mathbb{Z},$$

(2.9) 式左邊可化為

$$\pi^{-\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \Gamma\left(1 - \frac{s}{2}\right) \zeta(s) = \pi^{-\frac{s}{2}} \frac{\pi}{\sin\left(\frac{\pi s}{2}\right)} \zeta(s). \quad (2.10)$$

另一方面, 依 Γ 函數的雷建德倍元公式,

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

(2.9) 式右邊可寫成

$$\pi^{-\frac{1-s}{2}} \Gamma\left(\frac{1-s}{2}\right) \Gamma\left(1 - \frac{s}{2}\right) \zeta(1-s) = \pi^{-\frac{1-s}{2}} 2^{1-2\left(\frac{1-s}{2}\right)} \pi^{\frac{1}{2}} \Gamma(1-s) \zeta(1-s). \quad (2.11)$$

綜合 (2.10) 及 (2.11), 得

$$\pi^{-\frac{s}{2}} \frac{\pi}{\sin\left(\frac{\pi s}{2}\right)} \zeta(s) = \pi^{-\frac{1-s}{2}} 2^{1-2\left(\frac{1-s}{2}\right)} \pi^{\frac{1}{2}} \Gamma(1-s) \zeta(1-s),$$

化簡上式即為所證. □

設 s 為負偶數, 此時系理 2.10 中的正弦因子為 0, 餘者則非零, 故對於每個 $s \in \{-2n \mid n \in \mathbb{N}\}$, 均有 $\zeta(s) = 0$, 這些 s 稱為 $\zeta(s)$ 的**平凡零點**. 著名的千禧年大獎難題——黎曼猜想, 即關於 $\zeta(s)$ 之非平凡零點分佈的猜想.

猜想 2.11 (黎曼猜想) $\zeta(s)$ 的所有非平凡零點均落在直線 $\operatorname{Re}(s) = 1/2$ 上.

接下來, 我們將以白努利數表示黎曼 ζ 函數在負整數點處的值.

系理 2.12 對於 $k \in \mathbb{N}$, $k > 1$, 有

$$\zeta(1-k) = -\frac{B_k}{k},$$

其中 B_k 是第 k 個白努利數.

⁶函數解析延拓的證明思想大致如下: 根據定義, 有

$$\zeta(s) = \frac{\pi^{s/2}}{\Gamma(s/2)} \xi(s).$$

依註記 2.9, 可知 $\xi(s)$ 在點 $s = 0$ 處的行爲近似於 $-1/s$. 另一方面, 由複分析可知 $\Gamma(s)$ 在點 $s = 0$ 處的行爲近似於 $1/s$. 因此, 上述分式中「糟糕的行爲」相互抵消, 這表明 $\zeta(s)$ 實際上在點 0 處可定義.

證明 依系理 2.10 及定理 2.3, 當 $k > 1$ 為偶數時, 有

$$\begin{aligned}\zeta(1-k) &= 2^{1-k} \pi^{-k} \sin\left(\frac{\pi(1-k)}{2}\right) \Gamma(k) \zeta(k) \\ &= 2^{1-k} \pi^{-k} (-1)^{\frac{k}{2}} (k-1)! \left(-\frac{B_k}{2 \cdot k!} (2\pi i)^k\right) \\ &= -\frac{B_k}{k}.\end{aligned}$$

當 $k > 1$ 為奇數時, 由於 $1-k$ 是平凡零點, 故有 $\zeta(1-k) = 0$. 另外, 我們也注意到, 對所有大於 1 的奇數 k , 均有 $B_k = 0$ (參見系理 2.6), 證畢. $\square$

注意 2.13 由系理 2.12, 取 $k = 2$, 可得 (回顧例 2.4)

$$\zeta(-1) = -\frac{B_2}{2} = -\frac{1}{6} \cdot \frac{1}{2} = -\frac{1}{12}.$$

有人或許會將此式看作

$$\zeta(-1) = \sum_{n=1}^{+\infty} \frac{1}{n} = 1 + 2 + 3 + 4 + \cdots = -\frac{1}{12},$$

並宣稱一切自然數之和為 $-1/12$, 但這是一派胡言, 因為 $\zeta(s)$ 的級數表達式 (2.1) 僅對於 $\operatorname{Re}(s) > 1$ 成立.

3 狄利克雷密度定理

長久以來, 質數的奧秘一直是數論學家難以解開的謎團. 一方面, 質數的出現帶有極大的隨機性而難以預測. 比如說, 相鄰質數間的距離 (即質數間隙問題) 變化莫測且毫無規律. 但另一方面, 數學家卻又在質數之中發現了許多優美的規律, 如「質數定理」. 本週的課程將證明一個探討質數分佈的絕妙結果——狄利克雷密度定理.

3.1 狄利克雷密度與主要目標

定義 3.1 設 $\mathcal{P}$ 為質數集的一個子集, 則極限 (若存在)

$$d(\mathcal{P}) := \lim_{s \rightarrow 1^+} \frac{\sum_{p \in \mathcal{P}} \frac{1}{p^s}}{\sum_p \frac{1}{p^s}}$$

稱為 $\mathcal{P}$ 的**狄利克雷 (解析) 密度**, 其中分母的和遍及一切質數.

注意到若 $\mathcal{P}$ 是有限集, 則因為分母趨向 $+\infty$ (為何?), 所以其狄利克雷密度為 0. 另一方面, 質數集的狄利克雷密度為 1. 一般上, 若密度存在, 則其值必介於 0 和 1 之間. 不難發現, 若 $\mathcal{P}_1, \mathcal{P}_2$ 相離且均有狄利克雷密度, 則 $d(\mathcal{P}_1 \cup \mathcal{P}_2) = d(\mathcal{P}_1) + d(\mathcal{P}_2)$.

本週課程的核心目標, 旨在證明下列歸功於狄利克雷的定理.

定理 3.2 (狄利克雷) 設 $a, m \in \mathbb{N}$, $\gcd(a, m) = 1$, 定義

$$P(a; m) := \{\text{質數 } p : p \equiv a \pmod{m}\},$$

則

$$d(P(a; m)) = \frac{1}{\phi(m)},$$

其中 ϕ 是歐拉 ϕ 函數.

注意到上述定理立刻可推得 $P(a; m)$ 必為無限集, 即有無窮多個質數模 m 同餘 a . 然而, 此結論所揭示的意涵還要更加深刻. 不難發現, 對每個固定的 $m \in \mathbb{N}$, 若質數 p 不整除 m , 則存在滿足 $p \in P(a; m)$ 且 $\gcd(a, m) = 1$ 的正整數 a . 換言之, 滿足上述條件的質數的全體可以根據其各元素除以 m 所得的餘數來分割. 既然那樣的同餘類恰好有 $\phi(m)$ 個, 那麼該定理亦指出: 質數 (除了有限多個狄利克雷密度為零的例外) 會均勻地分佈在這些 $P(a; m)$ 集合當中.

比如說, 取 $m = 4$, 則由定理 3.2 可得

$$d(P(1; 4)) = d(P(3; 4)) = \frac{1}{2}.$$

換言之, 有一半的奇質數模 4 同餘 1, 而另一半的則模 4 同餘 3.

3.2 狄利克雷密度的等價定義

為了證明定理 3.2, 我們首先給出狄利克雷密度的一個等價定義. 為此, 我們將進一步探討黎曼 ζ 函數 (回顧定義 2.1) 的解析性質:

$$\zeta(s) := \sum_{n=1}^{+\infty} \frac{1}{n^s}, \quad \operatorname{Re}(s) > 1.$$

命題 3.3

$$\lim_{s \rightarrow 1^+} (s-1)\zeta(s) = 1.$$

證明 設 $s > 1$, 則由 t^{-s} 單調遞減, 得

$$\frac{1}{(n+1)^s} \leq \int_n^{n+1} \frac{1}{t^s} dt \leq \frac{1}{n^s}.$$

於上述不等式各邊取 $n = 1$ 至 $+\infty$ 的和, 並計算不等式中間的定積分, 得

$$\zeta(s) - 1 \leq \frac{1}{s-1} \leq \zeta(s),$$

從而

$$1 \leq (s-1)\zeta(s) \leq s-1 \leq s.$$

取 $s \rightarrow 1^+$, 則依夾擠定理即得證. □

系理 3.4

$$\lim_{s \rightarrow 1^+} \frac{\log \zeta(s)}{\log(s-1)^{-1}} = 1.$$

證明 由

$$\log \zeta(s) = \log \zeta(s)(s-1) - \log(s-1)$$

可得

$$\frac{\log \zeta(s)}{\log(s-1)^{-1}} = -\frac{\log \zeta(s)(s-1)}{\log(s-1)} + 1.$$

只要取 $s \rightarrow 1^+$, 便可從命題 3.3 得出結論. □

命題 3.5

$$\log \zeta(s) = \sum_p \frac{1}{p^s} + R(s),$$

其中 $R(s)$ 當 $s \rightarrow 1^+$ 時仍有界.

證明 證明此命題需要如下泰勒展開式:

$$-\log(1-x) = \sum_{m=1}^{+\infty} \frac{x^m}{m}, \quad -1 \leq x < 1.$$

依命題 2.2, 對於 $s > 1$, 有

$$\log \zeta(s) = \sum_p -\log(1-p^{-s}) = \sum_p \sum_{m=1}^{+\infty} \frac{p^{-sm}}{m} = \sum_p \frac{1}{p^s} + \sum_p \sum_{m=2}^{+\infty} \frac{1}{mp^{sm}}.$$

稍微估計上式第二項雙重和, 可知當 $s \rightarrow 1^+$ 時,

$$\sum_p \sum_{m=2}^{+\infty} \frac{1}{mp^{sm}} \leq \sum_p \sum_{m=2}^{+\infty} \frac{1}{p^{sm}} = \sum_p \frac{p^{-2s}}{1-p^{-s}} \leq \frac{1}{1-2^{-s}} \sum_p \frac{1}{p^{2s}} \leq 2\zeta(2s) < +\infty,$$

證畢. □

系理 3.6

$$\lim_{s \rightarrow 1^+} \frac{\sum_p \frac{1}{p^s}}{\log(s-1)^{-1}} = 1.$$

證明 依命題 3.5, 有

$$\frac{\log \zeta(s)}{\log(s-1)^{-1}} = \frac{\sum_p \frac{1}{p^s}}{\log(s-1)^{-1}} + \frac{R(s)}{\log(s-1)^{-1}},$$

取 $s \rightarrow 1^+$, 則由系理 3.4 及命題 3.5 即得證. □

回顧一下定義 3.1, 質數集的子集 $\mathcal{P}$ 的狄利克雷密度由如下極限定義:

$$d(\mathcal{P}) = \lim_{s \rightarrow 1^+} \frac{\sum_{p \in \mathcal{P}} \frac{1}{p^s}}{\sum_p \frac{1}{p^s}},$$

現由系理 3.6, 可看出其也定義作

$$d(\mathcal{P}) = \lim_{s \rightarrow 1^+} \frac{\sum_{p \in \mathcal{P}} \frac{1}{p^s}}{\log(s-1)^{-1}}. \quad (3.1)$$

註記 3.7 注意到, 系理 3.6 亦可推得質數有無窮多個 (若不然, 則極限為 0).

3.3 狄利克雷特徵

在本目, 固定 $m \in \mathbb{N}$, 令 $G := (\mathbb{Z}/m\mathbb{Z})^\times$, 其包含所有與 m 互質的整數模 m 的同餘類. 為了證明定理 3.2, 我們接下來要引入的關鍵工具, 便是**狄利克雷特徵**的概念.

定義 3.8 所謂 G 的**特徵** χ , 是指滿足對一切 $a, b \in G$, 均有

$$\chi(ab) = \chi(a)\chi(b)$$

的函數 $\chi: G \rightarrow \mathbb{C}^\times := \mathbb{C} \setminus \{0\}$. 將 G 的特徵的全體記作 $\widehat{G}$.

一個特徵的簡單例子, 是對所有 $a \in G$ 都定義成 $\chi_0(a) := 1$ 的**平凡特徵** $\chi_0 \in \widehat{G}$. 一般地, 不難觀察出, 對任何 $\chi \in \widehat{G}$, 均有 $\chi(1) = \chi(1^2) = \chi(1)^2$, 且根據定義有 $\chi(1) \neq 0$, 從而 $\chi(1) = 1$.

例 3.9 取 $m = 4$, 則 $G = (\mathbb{Z}/4\mathbb{Z})^\times = \{1, 3\}$. 由於 $3^2 \equiv 1 \pmod{4}$, 因此 $\chi(3)^2 = \chi(3^2) = \chi(1) = 1$, 故 $\chi(3) = \pm 1$. 於是在此情形下, G 有兩個特徵. 不妨將 G 的**特徵表**列出如下:

$(\mathbb{Z}/4\mathbb{Z})^\times$	1	3
χ_0	1	1
χ_1	1	-1

例 3.10 接著, 取 $m = 10$, 則 $G = (\mathbb{Z}/10\mathbb{Z})^\times = \{1, 3, 7, 9\}$. 注意到在 G 中, 有

$$\begin{aligned} 3^1 &\equiv 3 \pmod{10}, \\ 3^2 &\equiv 9 \pmod{10}, \\ 3^3 &\equiv 7 \pmod{10}, \\ 3^4 &\equiv 1 \pmod{10}. \end{aligned}$$

換言之, 同餘類 3「生成」 G 的其他元素. 因此, 欲求出 G 的所有特徵, 只需確定其在 3 處的值即可. 更進一步地, 注意到 $\chi(3)^4 = \chi(3^4) = \chi(1) = 1$, 故有 $\chi(3) = \pm 1, \pm i$, 從而 G 有四個特徵.

練習 3.11 列出 $G = (\mathbb{Z}/10\mathbb{Z})^\times$ 的特徵表.

定義 3.12 將 $\chi \in \widehat{G}$ 的定義域延伸至 $\mathbb{Z}$ 如下:

- 若 $\gcd(a, m) > 1$, 則規定 $\chi(a) := 0$;
- 對所有 $a \in \mathbb{Z}$, 規定 $\chi(a) := \chi(a \bmod m)$.

延伸定義域後的特徵稱為**模 m 的狄利克雷特徵**.

練習 3.13 證明狄利克雷特徵是完全積性函數, 即對所有 $a, b \in \mathbb{Z}$ 都滿足 $\chi(ab) = \chi(a)\chi(b)$.

3.4 狄利克雷密度定理其中一特殊情形之證明

有了上述準備, 現在可以開始證明定理 3.2. 實際上, 我們將僅針對 $m = 4$ 的情形給出證明, 因其已足以呈現該證明之核心思想. 我們亦將說明, 一般的情形如何透過完全相同的流程推導得出 (當然, 過程中會伴隨較多技術上的細節).

證明 ($m = 4$) 依例 3.9 及定義 3.12, 存在兩個模 4 的狄利克雷特徵:

$$\chi_0(n) = \begin{cases} 1, & n \text{ 為奇數}, \\ 0, & n \text{ 為偶數}, \end{cases} \quad \text{及} \quad \chi_1(n) = \begin{cases} 1, & n \equiv 1 \pmod{4}, \\ -1, & n \equiv 3 \pmod{4}, \\ 0, & n \text{ 為偶數}. \end{cases} \quad (3.2)$$

接著, 對於 $s > 1$, 定義關於 χ_0, χ_1 的狄利克雷 L 函數作

$$\begin{cases} L(s, \chi_0) := \sum_{n=1}^{+\infty} \frac{\chi_0(n)}{n^s} = 1 + \frac{1}{3^s} + \frac{1}{5^s} + \frac{1}{7^s} + \cdots, \\ L(s, \chi_1) := \sum_{n=1}^{+\infty} \frac{\chi_1(n)}{n^s} = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots. \end{cases}$$

由練習 3.13, 特徵均為完全積性函數, 故根據與命題 2.2 類似的證明, 可得

$$\begin{cases} L(s, \chi_0) = \prod_{p \text{ 為奇數}} (1 - p^{-s})^{-1} = (1 - 2^{-s})\zeta(s), \\ L(s, \chi_1) = \prod_{p \text{ 為奇數}} (1 - \chi_1(p)p^{-s})^{-1}. \end{cases}$$

有了這些歐拉乘積的表達式, 由與命題 3.5 類似的證明, 可得

$$\begin{cases} \log L(s, \chi_0) = \sum_{p \text{ 為奇數}} \frac{1}{p^s} + R_1(s), \\ \log L(s, \chi_1) = \sum_{p \text{ 為奇數}} \frac{\chi_1(p)}{p^s} + R_2(s), \end{cases}$$

其中, $R_1(s), R_2(s)$ 當 $s \rightarrow 1^+$ 時仍有界. 依 (3.2) 式, 這意味著

$$\begin{cases} \log L(s, \chi_0) + \log L(s, \chi_1) = 2 \sum_{p \equiv 1 \pmod{4}} \frac{1}{p^s} + R_3(s), \\ \log L(s, \chi_0) - \log L(s, \chi_1) = 2 \sum_{p \equiv 3 \pmod{4}} \frac{1}{p^s} + R_4(s), \end{cases} \quad (3.3)$$

其中, $R_3(s), R_4(s)$ 當 $s \rightarrow 1^+$ 時仍有界. 兩邊同除以 $\log(s-1)^{-1}$, 可得

$$\frac{\log L(s, \chi_0)}{\log(s-1)^{-1}} + \frac{\log L(s, \chi_1)}{\log(s-1)^{-1}} = \frac{2 \sum_{p \equiv 1 \pmod{4}} \frac{1}{p^s}}{\log(s-1)^{-1}} + \frac{R_3(s)}{\log(s-1)^{-1}} \quad (3.4)$$

及

$$\frac{\log L(s, \chi_0)}{\log(s-1)^{-1}} - \frac{\log L(s, \chi_1)}{\log(s-1)^{-1}} = \frac{2 \sum_{p \equiv 3 \pmod{4}} \frac{1}{p^s}}{\log(s-1)^{-1}} + \frac{R_4(s)}{\log(s-1)^{-1}}. \quad (3.5)$$

現, 由 (3.1) 式, 可知 (3.4) 式及 (3.5) 式的右邊當 $s \rightarrow 1^+$ 時分別趨於 $2d(\mathcal{P}(1; 4))$ 及 $2d(\mathcal{P}(3; 4))$. 而關於等式左邊, 注意到依系理 3.4, 當 $s \rightarrow 1^+$ 時, 有

$$\frac{\log L(s, \chi_0)}{\log(s-1)^{-1}} = \frac{\log(1-2^{-s})}{\log(s-1)^{-1}} + \frac{\log \zeta(s)}{\log(s-1)^{-1}} \rightarrow 1.$$

另一方面, 注意到對於 $s > 1$, 有

$$L(s, \chi_1) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots = \left(1 - \frac{1}{3^s}\right) + \left(\frac{1}{5^s} - \frac{1}{7^s}\right) + \cdots \geq \frac{2}{3}$$

及

$$L(s, \chi_1) = 1 - \frac{1}{3^s} + \frac{1}{5^s} - \frac{1}{7^s} + \cdots = 1 - \left(\frac{1}{3^s} - \frac{1}{5^s}\right) - \left(\frac{1}{7^s} - \frac{1}{9^s}\right) + \cdots \leq 1.$$

因此, 依夾擠定理, 有

$$\frac{\log L(s, \chi_1)}{\log(s-1)^{-1}} \rightarrow 0.$$

綜合上述得到的一切資訊, 可推得

$$d(\mathcal{P}(1; 4)) = d(\mathcal{P}(3; 4)) = \frac{1}{2},$$

定理即得證. □

3.5 一般情形

最後, 我們將透過重新審視上述證明的各個步驟來為本週課程作結, 並指明哪些部分易於推廣, 而哪些環節需要更進一步的處理. 設 $a, m \in \mathbb{N}$ 且 $\gcd(a, m) = 1$.

首個步驟列舉了所有模 4 的狄利克雷特徵. 對於一般的 m , 可藉由「群論」對 $(\mathbb{Z}/m\mathbb{Z})^\times$ 之特徵加以刻畫. 值得一提的是, 模 m 的狄利克雷特徵數量恰為 $\phi(m)$, 亦即與 $(\mathbb{Z}/m\mathbb{Z})^\times$ 的基數相等 (見例 3.9 及例 3.10).

接下來, 對於一切模 m 的狄利克雷特徵 χ , 可以同樣的方式定義狄利克雷 L 函數 $L(s, \chi)$, 即對於 $s > 1$, 定義

$$L(s, \chi) := \sum_{n=1}^{+\infty} \frac{\chi(n)}{n^s}.$$

因為由練習 3.13, 一切 χ 皆為完全積性函數, 所以可得如同命題 2.2 中的歐拉乘積

$$L(s, \chi) = \prod_p (1 - \chi(p)p^{-s})^{-1}.$$

據此, 亦可建立 $\log L(s, \chi)$ 之與命題 3.5 類似的估計, 即有⁷

$$\log L(s, \chi) = \sum_{p \nmid m} \frac{\chi(p)}{p^s} + R_\chi(s),$$

其中, $R_\chi(s) \rightarrow 1^+$ 時仍有界.

在證明的下個核心步驟中, 於等式左側對 $\log L(s, \chi)$ 取適當的線性組合, 從而「生成」下列等式:

$$\sum_{\chi \in \widehat{G}} c_\chi \log L(s, \chi) = \phi(m) \sum_{p \equiv a \pmod{m}} \frac{1}{p^s} + R_a(s) \quad (3.6)$$

其中, $R_a(s)$ 當 $s \rightarrow 1^+$ 時仍有界. 實際上, 此類線性組合的存在性是由線性代數所保證的. 更確切地說, 可以證明 $(\mathbb{Z}/m\mathbb{Z})^\times$ 的所有特徵構成了定義於 $(\mathbb{Z}/m\mathbb{Z})^\times$ 上所有複數值函數之 $\mathbb{C}$ -向量空間的一組「正交基」⁸. 第 4 課中將深入探討此主題.

最後的步驟中再次將式 (3.6) 兩端同除以 $\log(s-1)^{-1}$. 令 $s \rightarrow 1^+$, 由式 (3.1) 可知, 右端同樣將收斂於 $\phi(m)d(\mathcal{P}(a; m))$. 對於左端, 藉由系理 3.4, 仍不難證明:

$$\lim_{s \rightarrow 1^+} \frac{\log L(s, \chi_0)}{\log(s-1)^{-1}} = 1,$$

(χ_0 為模 m 的平凡特徵). 整個證明中最具挑戰性的部分, 在於證明對於非平凡的 χ , 下列恆等式成立:

$$\lim_{s \rightarrow 1^+} \frac{\log L(s, \chi)}{\log(s-1)^{-1}} = 0.$$

此條件等價於要求證明: 對於所有此類 χ , $L(1, \chi)$ 均不為零. 然而, 這是一項極為深奧的數論結果, 其證明已遠超出本課程所能探討的範疇.

4 特徵的正交關係

我們於上週的課程中證明了狄利克雷密度定理 (定理 3.2) 的一個特例, 並且說明了其證明如何推廣至任意情形, 其中也提到了某關鍵的步驟牽涉到 $(\mathbb{Z}/m\mathbb{Z})^\times$ 之特徵的正交性, 而本週的課程將針對這個部分進行詳細說明.

⁷ 此處將浮現一項技術性細節. 由於特徵一般而言取複數值, 故狄利克雷 L 函數 $L(s, \chi)$ 亦然. 因此, 在進行取對數的操作時須格外謹慎, 因其在複分析中實為一多值函數.

⁸ 此概念與 $(\mathbb{Z}/m\mathbb{Z})^\times$ 上的「傅立葉分析」密切相關.

4.1 $(\mathbb{Z}/m\mathbb{Z})^\times$ 的特徵群

本週課程中, 我們總固定 $m \in \mathbb{N}$, 並設 $G := (\mathbb{Z}/m\mathbb{Z})^\times$ 為所有模 m 且與 m 互質的整數的全體. 回顧一下定義 3.8, G 的特徵 χ 是指對所有 $a, b \in G$, 皆滿足

$$\chi(ab) = \chi(a)\chi(b)$$

的函數 $\chi: G \rightarrow \mathbb{C}^\times = \mathbb{C} \setminus \{0\}$. 亦將 G 的所有特徵的全體記作 $\widehat{G}$.

現將在 $\widehat{G}$ 上賦予自然的二元運算. 給定 $\chi, \lambda \in \widehat{G}$, 對所有 $a \in G$, 將 $\chi\lambda: G \rightarrow \mathbb{C}^\times$ 規定作 $\chi\lambda(a) := \chi(a)\lambda(a)$, 則有如下簡單的觀察:

- (封閉性) 因 χ, λ 均為特徵, 故對所有 $a, b \in G$, 有

$$\chi\lambda(ab) = \chi(ab)\lambda(ab) = \chi(a)\chi(b)\lambda(a)\lambda(b) = \chi(a)\lambda(a)\chi(b)\lambda(b) = \chi\lambda(a)\chi\lambda(b).$$

換言之, $\chi\lambda$ 也是特徵.

- (交換性) 對所有 $a \in G$, 均有

$$\chi\lambda(a) = \chi(a)\lambda(a) = \lambda(a)\chi(a) = \lambda\chi(a),$$

亦即 $\chi\lambda = \lambda\chi$.

- (么元) §3.3 中提到了定義為 $\chi_0(a) := 1$ ($a \in G$) 的平凡特徵 $\chi_0 \in \widehat{G}$, 其對所有 $\chi \in \widehat{G}$ 及 $a \in G$ 都滿足

$$\chi\chi_0(a) = \chi(a)\chi_0(a) = \chi(a),$$

即 $\chi\chi_0 = \chi$.

- (逆元) 給定 $\chi \in \widehat{G}$, 定義 $\chi^{-1}: G \rightarrow \mathbb{C}^\times$ 作 $\chi^{-1}(a) := \chi(a)^{-1}$ ($a \in G$), 則 χ^{-1} 亦為 G 的特徵 (見練習 4.1), 且其滿足對所有 $a \in G$,

$$\chi\chi^{-1}(a) = \chi(a)\chi^{-1}(a) = \chi(a)\frac{1}{\chi(a)} = 1 = \chi_0(a),$$

也就是說, $\chi\chi^{-1} = \chi_0$.

- (結合性) 對一切 $\chi, \lambda, \psi \in \widehat{G}$, 均有 (見練習 4.1)

$$(\chi\lambda)\psi = \chi(\lambda\psi).$$

練習 4.1 補齊上述討論中缺失的細節.

總的來說, 這意味着 $\widehat{G}$ 與上述二元運算組成「交換群」, 稱其為 G 的特徵群.

我們先前已在 §3.3 中觀察出所有 $\chi \in \widehat{G}$ 都滿足 $\chi(1) = 1$, 現將作更多如下的觀察. 設 ϕ 為歐拉 ϕ 函數. 依歐拉定理, 對一切 $a \in G$, 均有

$$a^{\phi(m)} \equiv 1 \pmod{m},$$

故對所有 $\chi \in \widehat{G}$,

$$\chi(a)^{\phi(m)} = \chi(a^{\phi(m)}) = \chi(1) = 1,$$

這表示 $\chi(a)$ 是 $\phi(m)$ 次單位根. 特別地, $\chi(a)$ 是代數數 (見例 1.2). 而且, 若 $a^{-1} \in G$ 為滿足 $aa^{-1} \equiv 1 \pmod{m}$ 的元素, 則

$$\chi(a)\chi(a^{-1}) = \chi(aa^{-1}) = \chi(1) = 1,$$

因此

$$\chi(a^{-1}) = \chi(a)^{-1} = \overline{\chi(a)}.$$

此恆等式意味著, $a \in G$ 的逆、 $\chi(a) \in \mathbb{C}^\times$ 的逆, 以及 $\chi \in \widehat{G}$ 的逆實際上是相容的. 另外, 作為單位根, $\chi(a)$ 落在複平面中的單位圓上, 故其滿足 $\chi(a)^{-1} = \overline{\chi(a)}$, 其中 $\bar{\cdot}$ 表示複共軛.

4.2 正交關係

我們曾在 §3.5 中不加證明地提及過, $\widehat{G}$ 的特徵群含有 $\phi(m)$ 個元素, 故

$$\#(G) = \#(\widehat{G}) = \phi(m).$$

本節中, 我們將建立特徵的兩個正交關係, 並說明它們在線性代數之下的觀點.

命題 4.2 (特徵的正交關係) 對一切 $\chi, \lambda \in \widehat{G}$, 有

$$\sum_{a \in G} \chi(a) \overline{\lambda(a)} = \begin{cases} \phi(m), & \chi = \lambda, \\ 0, & \chi \neq \lambda. \end{cases}$$

證明 注意到

$$\sum_{a \in G} \chi(a) \overline{\lambda(a)} = \sum_{a \in G} \chi(a) \lambda^{-1}(a) = \sum_{a \in G} \chi \lambda^{-1}(a),$$

故只需證明

$$\sum_{a \in G} \chi(a) = \begin{cases} \phi(m), & \chi = \chi_0, \\ 0, & \chi \neq \chi_0. \end{cases} \quad (4.1)$$

當 $\chi = \chi_0$ 為平凡特徵時, 不難看出

$$\sum_{a \in G} \chi(a) = \sum_{a \in G} 1 = \#(G) = \phi(m).$$

當 $\chi \neq \chi_0$ 時, 必存在滿足 $\chi(t) \neq 1$ 的 $t \in G$. 注意到

$$\chi(t) \sum_{a \in G} \chi(a) = \sum_{a \in G} \chi(t)\chi(a) = \sum_{a \in G} \chi(ta) = \sum_{a \in G} \chi(a). \quad (4.2)$$

最後一個等式成立的理由如下: 設有滿足 $at = bt$ 的 $a, b \in G$, 這表示 $at \equiv bt \pmod{m}$. 由於 $\gcd(t, m) = 1$, 因此 $a \equiv b \pmod{m}$, 或等價地說, 在 G 中有 $a = b$. 於是, 在 G 上的乘 t 映射是單射, 從而是雙射.

現, 由 (4.2) 式, 得

$$(\chi(t) - 1) \sum_{a \in G} \chi(a) = 0.$$

由於根據假設, $\chi(t) \neq 1$, 因此該和式為 0. □

例 4.3 由例 3.9, $(\mathbb{Z}/4\mathbb{Z})^\times$ 的特徵表為

$(\mathbb{Z}/4\mathbb{Z})^\times$	1	3
χ_0	1	1
χ_1	1	-1

那麼, 命題 4.2 (或更確切地說, (4.1)) 指出, 第一列 χ_0 的總和為 $\phi(4) = 2$, 而第二列 χ_1 的總和為 0.

例 4.4 練習 3.11 要求求出 $(\mathbb{Z}/10\mathbb{Z})^\times$ 的特徵表. 答案如下:

$(\mathbb{Z}/10\mathbb{Z})^\times$	1	3	7	9
χ_0	1	1	1	1
χ_1	1	-1	-1	1
χ_2	1	i	-i	-1
χ_3	1	-i	i	-1

可以看出, 第一列 χ_0 的總和為 $\phi(10) = 4$, 而其餘列各總和為 0.

現在要以線性代數的觀點詮釋命題 4.2. 考慮由所有 G 上的複數值函數組成的複線性空間 $\mathcal{F}(G, \mathbb{C})$.

定義 4.5 在 $\mathcal{F}(G, \mathbb{C})$ 上定義內積如下: 設 $f_1, f_2 \in \mathcal{F}(G, \mathbb{C})$,

$$(f_1 | f_2) := \frac{1}{\phi(m)} \sum_{a \in G} f_1(a) \overline{f_2(a)}.$$

練習 4.6 檢查 $(\cdot | \cdot)$ 確實是 $\mathcal{F}(G, \mathbb{C})$ 上的內積.

以此定義, 可將命題 4.2 的結論寫成: 對所有 $\chi, \lambda \in \widehat{G}$,

$$(\chi | \lambda) = \frac{1}{\phi(m)} \sum_{a \in G} \chi(a) \overline{\lambda(a)} = \begin{cases} 1, & \chi = \lambda, \\ 0, & \chi \neq \lambda, \end{cases}$$

即 G 的所有特徵組成的群 $\widehat{G}$ 在 $\mathcal{F}(G, \mathbb{C})$ 中是正交的 (實際上是規範正交的, 因為我們將其內積以 $\#(G)^{-1} = \phi(m)^{-1}$ 來歸一化). 特別地, 它們線性獨立, 從而

$$\phi(m) \leq \dim_{\mathbb{C}} \mathcal{F}(G, \mathbb{C}).$$

另一方面, 設 $G = \{a_1, \dots, a_{\phi(m)}\}$. 對每個 $i \in \{1, \dots, \phi(m)\}$, 只要 $a = a_i$, 便將 $f_i \in \mathcal{F}(G, \mathbb{C})$ 定義成 $f_i(a) := 1$, 否則定義成 0. 也就是說, f_i 是 $\{a_i\} \subseteq G$ 的指示函數. 那麼, 顯而易見 $\{f_1, \dots, f_{\phi(m)}\}$ 生成複向量空間 $\mathcal{F}(G, \mathbb{C})$. 特別地, 有

$$\phi(m) \geq \dim_{\mathbb{C}} \mathcal{F}(G, \mathbb{C}).$$

總的來說, 我們證明了 $\mathcal{F}(G, \mathbb{C})$ 的維數恰為 $\phi(m)$, 並且特徵群 $\widehat{G}$ 是 $\mathcal{F}(G, \mathbb{C})$ 的一組 (規範) 正交基.

命題 4.7 (鉛直正交關係) 對一切 $a, b \in G$, 有

$$\sum_{\chi \in \widehat{G}} \chi(a) \overline{\chi(b)} = \begin{cases} \phi(m), & a = b, \\ 0, & a \neq b. \end{cases}$$

證明 由於 $\widehat{G}$ 是群, 可給出與命題 4.2 類似的證明, 此處使用線性代數.

固定 $b \in G$, 將 $f_b \in \mathcal{F}(G, \mathbb{C})$ 定義成單點集 $\{b\}$ 的指示函數的 $\phi(m)$ 倍, 即

$$f_b(a) := \begin{cases} \phi(m), & a = b, \\ 0, & a \neq b. \end{cases}$$

因特徵組成 $\mathcal{F}(G, \mathbb{C})$ 的一組規範正交基, 故有

$$f_b = \sum_{\chi \in \widehat{G}} (f_b | \chi) \chi.$$

對於內積 $(f_b | \chi)$, 依定義 4.5, 可看出

$$(f_b | \chi) = \frac{1}{\phi(m)} \sum_{a \in G} f_b(a) \overline{\chi(a)} = \frac{1}{\phi(m)} \cdot f_b(b) \overline{\chi(b)} = \overline{\chi(b)}.$$

這意味著

$$f_b(a) = \sum_{\chi \in \widehat{G}} \overline{\chi(b)} \chi(a) = \begin{cases} \phi(m), & a = b, \\ 0, & a \neq b. \end{cases}$$

此式即為所證. □

註記 4.8 注意到命題 4.7 等價於

$$\sum_{\chi \in \widehat{G}} \chi(a) = \begin{cases} \phi(m), & a = 1, \\ 0, & a \neq 1. \end{cases}$$

這表明了如例 4.3 中第一行 ($a = 1$ 的情形) 總和為 $\phi(4) = 2$ 及第二行 ($a = 3$ 的情形) 總和為 0. 例 4.4 也有類似的觀察.

結束這堂課之前, 讓我們再看看狄利克雷定理一般情形的證明 (回憶一下 §3.5). 假設在證明的時候, 我們找到了所有模 m 的狄利克雷特徵, 並建立了估計

$$\log L(s, \chi) = \sum_{p \nmid m} \frac{\chi(p)}{p^s} + R_\chi(s).$$

現在想要對每個 $\chi \in \widehat{G}$ 取相應的 $c_\chi \in \mathbb{C}$ 使得式 (3.6) 成立.

應用命題 4.7, 可看出只要取 $c_\chi := \overline{\chi(a)}$ 並對所有 $\chi \in \widehat{G}$ 求和, 將得到

$$\begin{aligned} \sum_{\chi \in \widehat{G}} \overline{\chi(a)} \log L(s, \chi) &= \sum_{\chi \in \widehat{G}} \sum_{p \nmid m} \frac{\chi(p) \overline{\chi(a)}}{p^s} + \sum_{\chi \in \widehat{G}} \overline{\chi(a)} R_\chi(s) \\ &= \sum_{p \nmid m} \frac{1}{p^s} \sum_{\chi \in \widehat{G}} \chi(p) \overline{\chi(a)} + R_a(s) \\ &= \phi(m) \sum_{p \equiv a \pmod{m}} \frac{1}{p^s} + R_a(s), \end{aligned}$$

而這恰好就是式 (3.6) 中所求.

的確, 考慮在 §3.4 中證明的特殊情形 $m = 4$, 取 $a = 3 \in (\mathbb{Z}/4\mathbb{Z})^\times$, 則從 $(\mathbb{Z}/4\mathbb{Z})^\times$ 的特徵表 (見例 3.9), 宜令

$$c_{\chi_0} = \overline{\chi_0(3)} = 1 \quad \text{及} \quad c_{\chi_1} = \overline{\chi_1(3)} = -1,$$

這恰與式 (3.3) 的第二式相吻合, 其中

$$\sum_{\chi \in \widehat{G}} c_\chi \log L(s, \chi) = \log L(s, \chi_0) - \log L(s, \chi_1).$$

- 5 高斯和與二次互反律
- 6 模 p 運算之下解的個數
- 7 仿射空間與射影空間
- 8 橢圓曲線及其群結構
- 9 p 進數
- 10 再論 p 進數
- 11 函數體中的基礎數論
- 12 再論函數體

參考資料

- [1] Timo Chang. e 的超越性. 仙女國公主譯. 原標題: *The Transcendence of e* . 網址: https://timomath.com/the_transcendence_of_e_zh-tw.pdf.
- [2] Timo Chang. 結式與其應用. 仙女國公主譯. 原標題: *Resultant and its Applications*. 網址: https://timomath.com/resultant_and_its_applications_zh-tw.pdf.