

# 数论基础

Lectured by Prof. Zhao Lili

Adaus

2022 年 4 月 9 日

# 前言

预备知识: 初等数论, 高等代数 (线性代数和多项式), 数学分析, 复变函数, 近世代数.

参考文献: 代数数论入门 by 冯克勤

课程内容包括解析数论和代数数论, 如果课时允许, 会补充组合数论的内容.

由于各种各样的原因, 这份笔记与教学的内容和顺序并不完全重合, 笔记中可能出现的所有的笔误和数学错误完全是我个人的原因, 若您发现任何问题请与我联系.

Adaus

# 目录

<b>I</b>	<b>解析理论</b>	<b>1</b>
<b>1</b>	<b>素数分布 ( 初等证明 )</b>	<b>1</b>
1.1	基本定理 . . . . .	1
1.2	一些数论函数及其性质 . . . . .	4
<b>2</b>	<b>Riemann zeta 函数与素数定理</b>	<b>8</b>
2.1	Riemann zeta 函数的基本性质 . . . . .	8
2.2	素数定理 . . . . .	13
<b>3</b>	<b>算术级数中的素数分布 I</b>	<b>16</b>
3.1	有限 Abel 群的特征 . . . . .	16
3.2	Dirichlet L 函数及其性质 . . . . .	19
3.3	Dirichlet 定理的证明 . . . . .	28
<b>4</b>	<b>算术级数中的素数分布 II</b>	<b>30</b>
4.1	算术级数中的素数定理 . . . . .	30
<b>II</b>		<b>31</b>
	<b>附录</b>	<b>31</b>
<b>A</b>	<b>分圆多项式</b>	<b>31</b>
<b>B</b>	<b>分析学</b>	<b>33</b>
B.1	解析延拓 . . . . .	33
B.2	Poisson 求和公式 . . . . .	33

<b>C “初等” 方法</b>	<b>35</b>
C.1 Dirichlet 除数问题 . . . . .	35
C.2 Chebyshev 估计 . . . . .	36
<b>D <math>\pi</math> 是无理数</b>	<b>39</b>

## Part I

# 解析理论

## 1 素数分布 ( 初等证明 )

本章旨在回顾一些初等的内容, 并同接下来的解析方法做一个对比. 为有助于回顾复习, 要用到的一些初等数论的结果会以引理的形式给出.

### 1.1 基本定理

**定理 1.1.** 有无穷多个素数.

证明. 用反证法. □

下面我们看 Euler 怎么证明 **定理 1.1.**.

证明. 考虑算术基本定理, 当  $s > 1$  时,

$$\sum_{n=1}^{\infty} \frac{1}{n^s} = \prod_p \left(1 + \frac{1}{p^s} + \frac{1}{p^{2s}} + \cdots\right) \quad (1)$$

$$= \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \quad (2)$$

而

$$\lim_{s \rightarrow 1^+} \sum_{n=1}^{\infty} \frac{1}{n^s} = \infty$$

于是 (1.2) 等号右边是一个无穷乘积, 即素数有无穷多个. □

**定义 1.2.** 我们称

$$\zeta(s) = \sum_{n=1}^{\infty} \frac{1}{n^s} \quad (s \in \mathbb{C}, \operatorname{Re}(s) > 1)$$

为 *Riemann zeta* 函数.

注. 设  $a(n)$  是积性的数论函数, 且对于固定的  $\epsilon_0 \geq 0$ ,  $|a(n)| \leq n^{\epsilon_0}$ , 则当  $s > 1 + \epsilon_0$  时,

$$\sum_{n=1}^{\infty} \frac{a(n)}{n^s} = \prod_p \left(1 + \frac{a(p)}{p^s} + \frac{a(p^2)}{p^{2s}} + \cdots\right) \quad (3)$$

等号右边的式子一般称为 *Euler* 乘积.

我们再给一个拓扑的证明 (Hillel Furstenberg, 2020 年 Abel 奖得主).

证明. 对  $a \in \mathbb{Z}, b \in \mathbb{Z}^+$ , 引入记号

$$a(\bmod b) := \{n \in \mathbb{Z} \mid n \equiv a(\bmod b)\}$$

我们引入一个  $\mathbb{Z}$  上的拓扑  $(\mathbb{Z}, \tau)$  如下. 对于任意子集  $A \subset \mathbb{Z}$ ,  $A \in \tau$  当且仅当要么  $A = \emptyset$ , 要么  $\forall a \in A, \exists b \in \mathbb{Z}^+, \text{ s.t. } a(\bmod b) \subset A$ .

验证这是一个拓扑是容易的.

根据定义,  $\emptyset \in \tau, \mathbb{Z} = 0(\bmod 1) \in \tau$ .

如果  $\{A_\lambda\} \in \tau (\lambda \in \Lambda)$ , 则只需考虑它们不全是空集的情况, 根据定义,  $\forall a \in \bigcup_\lambda A_\lambda, \exists b \in \mathbb{Z}^+, \text{ s.t. } a(\bmod b) \subset \bigcup_\lambda A_\lambda$ .

如果  $A_1, A_2 \in \tau$  非空, 则  $\forall a \in A_1 \cap A_2, \exists b \in \mathbb{Z}^+, \text{ s.t. } a(\bmod b) \subset A_1 \cap A_2$ .

易见  $a \in \mathbb{Z}, b \in \mathbb{Z}^+, a(\bmod b) \in \tau$ .

对任意  $n \neq \pm 1 (n \in \mathbb{Z})$ , 都存在素数  $p$ , s.t.  $p \mid n$ , i.e.  $n \in 0(\bmod p)$ , 并且对于  $\pm 1$ , 不存在这样的素数.

因此

$$\mathbb{Z} \setminus \{1, -1\} = \bigcup_p 0(\bmod p)$$

而

$$\{1, -1\} = \bigcap_p (\mathbb{Z} \setminus 0(\bmod p)) \notin \tau$$

故

$$\bigcap_p (\mathbb{Z} \setminus 0(\bmod p)) = \bigcap_p (1(\bmod p) \cup \cdots \cup (p-1)(\bmod p))$$

等式右边不是有限交

□

**思考.**  $4k+1$  型素数是否有无穷多个.

$4k-1$  型素数是否有无穷多个.

**定理 1.3.** 设  $q$  是固定的正整数, 则有无穷多个形如  $qk+1$  形素数 ( $k \in \mathbb{Z}^+$ )

证明. 考虑分圆多项式

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^n (x - e^{2\pi i \frac{k}{n}}) \in \mathbb{Z}[x]$$

它与  $x^k - 1$  ( $1 \leq k < n$ ) 在  $\mathbb{Z}[x]$  中互素.

假设只有有限个素数  $p_1, \dots, p_m \equiv 1 \pmod{q}$

取  $t$  为充分大的正整数, 记  $a = tq p_1 \dots p_m$ . 考虑  $\Phi_q(tp p_1 \dots p_m)$  的素因子  $p$ .

于是  $p|a^q - 1$ . 因此  $p \neq p_1, \dots, p \neq p_m, p \nmid q$ . 于是  $p|\Phi_q(a)|a^q - 1$ .

设  $k$  是使得  $p|a^j - 1$  ( $j \in \mathbb{Z}^+$ ) 成立的最小的  $j$ .

**断言.**  $k = q$ .

下面我们证明断言. 记  $r = \frac{q}{k} \in \mathbb{Z}^+$ . 假设  $k < q$ , 即  $r < 1$ .

我们有如下多项式的整除关系

$$\Phi_q(x)|x^q - 1 = (x^k - 1)(x^{k(r-1)} + \dots + x^k + 1)$$

则

$$\Phi_q(x)|(x^{k(r-1)} + \dots + x^k + 1)$$

因此, 代入  $a$  有

$$\Phi_q(a)|(a^{k(r-1)} + \dots + a^k + 1)$$

而  $a^k \equiv 1 \pmod{p}$ , 于是

$$p|\sum_{j=0}^{r-1} (a^k)^j \equiv r \pmod{p}$$

因此  $p|r|a$ , 与假设矛盾. 这证明了断言.

接下来根据费马小定理, 我们有  $p|a^{p-1} - 1$ , 则  $q|p-1$ . 因此  $p \equiv 1 \pmod{q}$ .

与假设矛盾.  $\square$

**注.**  $m=0$  的情况是有可能的.

## 1.2 一些数论函数及其性质

现在我们介绍一些函数.

1. Von Mangoldt 函数  $\Lambda : \mathbb{Z}^+ \rightarrow \mathbb{R}$

$$\Lambda(n) = \begin{cases} \log p & n = p^k, p \text{ 是素数}, k \in \mathbb{Z}^+, \\ 0 & \text{otherwise.} \end{cases}$$

2. 对一个固定的实数  $x$ , 所有比  $x$  小的素数个数给出一个函数

$$\begin{aligned} \pi(x) &= \sum_{n \leq x} \mathbf{1}_{\mathbb{P}}(n) \\ &= \sum_{p \leq x} 1 \end{aligned}$$

其中  $\mathbf{1}_{\mathbb{P}}$  是素数集合的特征函数.

3. 在  $\pi(x)$  的和式中考虑一个权重

$$\begin{aligned} \theta(x) &= \sum_{n \leq x} \mathbf{1}_{\mathbb{P}}(n) \log n \\ &= \sum_{p \leq x} \log p \end{aligned}$$

4.  $\psi(x) = \sum_{n \leq x} \Lambda(n)$

我们给出一些 Von Mangoldt 函数的性质.

**命题 1.4.**  $\sum_{d|n} \Lambda(d) = \log n$

证明. 循定义验证即可. □

**命题 1.5.** 当  $\operatorname{Re}(s) > 1$  时,  $\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$  绝对收敛.



证明. 由**命题 1.4.**, 我们有

$$\Lambda(n) \leq \sum_{d|n} \Lambda(d) = \log n$$

$$\text{于是 } \frac{\Lambda(n)}{n^s} \leq \frac{\log n}{n^s}$$

□

至此, 我们粗略的看看下列两个无穷级数的乘积.

$$\begin{aligned} \left( \sum_{n=1}^{\infty} \frac{1}{n^s} \right) \left( \sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} \right) &= \sum_{m=1}^{\infty} \sum_{k=1}^{\infty} \frac{1}{m^s} \frac{\Lambda(k)}{k^s} \\ &= \sum_{n=1}^{\infty} \sum_{\substack{m,k \\ mk=n}} \frac{1}{m^s} \frac{\Lambda(k)}{k^s} \\ &= \sum_{n=1}^{\infty} \frac{\log n}{n^s} = -\zeta'(s) \end{aligned}$$

这几乎得到了  $\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s}$  的表达式, 但我们还不清楚  $\zeta(s)$  的零点, 不能将它挪到等式右边. 某种程度上它也推动着我们去探索  $\zeta(s)$  的零点. 之后我们会看到这实际上给出了 Von Mangoldt 函数的 Dirichlet 级数.

为了证明素数定理, 我们需要做一些准备工作.

**定理 1.6.** 下列叙述等价.

1.  $\pi(x) \sim \frac{x}{\log x}$
2.  $\theta(x) \sim x$
3.  $\psi(x) \sim x$

证明.  $(2 \Leftrightarrow 3)$ :

$$\begin{aligned}
 0 \leq \psi(x) - \theta(x) &= \sum_{\substack{k \geq 2 \\ p^k \leq x}} \log p \\
 &\leq \sum_{\substack{k \geq 2 \\ p^k \leq x}} \log x \\
 &\leq \sum_{p \leq \sqrt{x}} \log p \sum_{2 \leq k \leq \frac{\log x}{\log p}} 1 \\
 &\leq \sqrt{x} \log x
 \end{aligned}$$

于是  $\frac{\psi(x)}{x} - \frac{\theta(x)}{x} \rightarrow 0 \ (x \rightarrow +\infty)$

$(1 \Leftrightarrow 2)$  只需看下列两个不等式:

对任意正数  $\epsilon > 0$

$$\begin{aligned}
 \theta(x) &\leq \pi(x) \log x \\
 \theta(x) &\geq \sum_{x^{1-\epsilon} \leq p \leq x} \log x^{1-\epsilon} = (1-\epsilon)(\pi(x) + O(x^{1-\epsilon})) \log x
 \end{aligned}$$

等价性立即可得 □

**注** (Chebyshev). 存在常数  $c_1, c_2$  满足  $0 < c_1 < 1 < c_2$  使得

$$c_1 < \frac{\pi(x)}{x/\log x} < c_2$$

我们将在附录证明这个结果.

**注** (Riemann).  $\zeta(s)$  可以解析延拓到  $\mathbb{C} \setminus \{1\}$ , 并且  $1$  是单极点. *Riemann* 还证明了在  $\operatorname{Re}(s) < 0$  的范围内所有的零点是  $-2, -4, \dots$ , 即所有负偶数, 且它们是单零点.

**猜想 1.7** (Riemann). 若  $0 \leq \operatorname{Re}(s) \leq 1$ , 且  $\zeta(s) = 0$ , 则  $\operatorname{Re}(s) = \frac{1}{2}$ .

**注.** *Riemann* 猜想  $\Rightarrow$  素数定理.

$\zeta(1+it) \neq 0 \ \forall t \in \mathbb{R} \Rightarrow$  素数定理.

**引理 1.8.** 若  $\int_1^\infty \frac{\psi(x) - x}{x^2} dx$  收敛, 则  $\psi(x) \sim x$ .

证明. 用反证法. 假设  $\psi(x) \sim x$  不成立. 则要么存在  $c_1 > 1$ , 使得有一个严格递增趋于无穷的序列  $\{x_n\}$  满足

$$\psi(x_n) \geq c_1 x_n$$

要么存在  $0 < c_2 < 1$ , 使得有一个严格递增趋于无穷的序列  $\{y_n\}$  满足

$$\psi(y_n) \leq c_2 y_n$$

若第一种情况成立, 则

$$\begin{aligned} \int_{x_n}^{c_1 x_n} \frac{\psi(x) - x}{x^2} dx &\geq \int_{x_n}^{c_1 x_n} \frac{c_1 x_n - x}{x^2} dx \\ &= c_1 - 1 - \log c_1 > 0 \end{aligned}$$

这同假设矛盾. 类似地, 若第二种情况成立, 则

$$\begin{aligned} \int_{c_2 y_n}^{y_n} \frac{\psi(x) - x}{x^2} dx &\leq \int_{c_2 y_n}^{y_n} \frac{c_2 y_n - x}{x^2} dx \\ &= -c_2 + 1 + \log c_2 < 0 \end{aligned}$$

这也同假设矛盾. □

## 2 Riemann zeta 函数与素数定理

我们约定复变量的符号为  $s = \sigma + it$ .

### 2.1 Riemann zeta 函数的基本性质

**定理 2.1.** 当  $\operatorname{Re}(s) > 1$  时,  $\zeta(s) \neq 0$ .

证明.  $s$  是实数时结论是显然的.

我们考察 Euler 乘积的形式

$$\begin{aligned} |\zeta(s)| &= \left| \prod_p \left(1 - \frac{1}{p^s}\right)^{-1} \right| \\ &= \prod_p \left| \left(1 - \frac{1}{p^s}\right)^{-1} \right| \\ &\geq \prod_p \left(1 + \frac{1}{p^\sigma}\right)^{-1} \\ &\geq \prod_p \left(1 - \frac{1}{p^\sigma}\right) \\ &\geq \left( \prod_p \left(1 - \frac{1}{p^\sigma}\right)^{-1} \right)^{-1} \\ &\geq \frac{1}{\zeta(\sigma)} \in \mathbb{R}^+ \end{aligned}$$

即  $\zeta(s) \neq 0$ . □

**注.** 现在回过头看第一节的结果, 我们有当  $\operatorname{Re}(s) > 1$  时,

$$\sum_{n=1}^{\infty} \frac{\Lambda(n)}{n^s} = -\frac{\zeta'(s)}{\zeta(s)}$$

**定理 2.2.** 当  $\operatorname{Re}(s) > 1$  时, 我们有

$$\zeta(s) = \frac{s}{s-1} - s \int_1^{+\infty} \{x\} x^{-s-1} dx \quad (4)$$

并且 (4) 给出了  $\zeta(s)$  在  $\operatorname{Re}(s) > 0 (s \neq 1)$  的解析延拓且  $s = 1$  是单极点.

证明. 当  $Re(s) > 2$  时, 我们有

$$\begin{aligned}
 \sum_{n=1}^{\infty} n(n^{-s} - (n+1)^{-s}) &= \sum_{n=1}^{\infty} nn^{-s} - \sum_{n=1}^{\infty} n(n+1)^{-s} \\
 &= \sum_{n=1}^{\infty} n^{-s+1} - \sum_{n=1}^{\infty} (n+1)^{-s+1} + \sum_{n=1}^{\infty} (n+1)^{-s} \\
 &= \zeta(s)
 \end{aligned}$$

继续计算有

$$\begin{aligned}
 \zeta(s) &= \sum_{n=1}^{\infty} n(n^{-s} - (n+1)^{-s}) \\
 &= s \sum_{n=1}^{\infty} n \int_n^{n+1} x^{-s-1} dx \\
 &= s \sum_{n=1}^{\infty} \int_n^{n+1} [x] x^{-s-1} dx \\
 &= s \sum_{n=1}^{\infty} \int_n^{n+1} (x - \{x\}) x^{-s-1} dx \\
 &= s \sum_{n=1}^{\infty} \int_n^{n+1} x^{-s} dx - s \sum_{n=1}^{\infty} \int_n^{n+1} \{x\} x^{-s-1} dx \\
 &= \frac{s}{s-1} - s \int_1^{+\infty} \{x\} x^{-s-1} dx
 \end{aligned}$$

不难发现  $\frac{s}{s-1} - s \int_1^{+\infty} \{x\} x^{-s-1} dx$  是  $\zeta(s)$  到  $Re(s) > 0 (s \neq 1)$  的延拓且  $s = 1$  是单极点.  $\square$

现在为了将  $\zeta(s)$  延拓到整个复平面上, 我们需要回顾一些关于 Gamma 函数  $\Gamma$  的重要性质. 更多细节请读者查阅 [3], Ch.6.

在  $Re(s) > 0$  上我们定义 Gamma 函数为

$$\Gamma(s) = \int_0^{+\infty} x^{s-1} e^{-x} dx.$$

不难验证我们有

$$\Gamma(s+1) = s\Gamma(s)$$

由此我们可以将  $\Gamma$  延拓成复平面上的亚纯函数且只有单极点  $s = 0, -1, -2, \dots$ , 且没有零点 (考察  $\Gamma(s)\Gamma(1-s) = \frac{\pi}{\sin \pi s}$ ).

接下来我们就可以着手将  $\zeta(s)$  延拓到整个复平面上.

对  $x > 0$ , 引入函数  $\theta(x) = \sum_{n=-\infty}^{+\infty} e^{-n^2 x \pi} (= 1 + 2 \sum_{n=1}^{\infty} e^{-n^2 x \pi})$ .

**引理 2.3.**  $x > 0$  时,  $\theta(\frac{1}{x}) = \sqrt{x}\theta(x)$ .

证明. 考虑 Poisson 公式有

$$\begin{aligned}\theta(x) &= \sum_{n \in \mathbb{Z}} \int_{-\infty}^{+\infty} e^{u^2 x \pi - 2\pi i n u} du \\ &= \sum_{n \in \mathbb{Z}} \int_{-\infty}^{+\infty} e^{-x\pi(u+in\frac{1}{x})^2 - \pi n^2 \frac{1}{x}} du \\ &= \sum_{n \in \mathbb{Z}} e^{-\pi n^2 \frac{1}{x}} \int_{-\infty}^{+\infty} e^{-\pi x(u+in\frac{1}{x})^2} du \\ &= \sum_{n \in \mathbb{Z}} e^{-\pi n^2 \frac{1}{x}} \int_{-\infty}^{+\infty} e^{-\pi x u^2} du \\ &= \theta(\frac{1}{x}) \frac{1}{\sqrt{x}}\end{aligned}$$

□

**定理 2.4.** 对  $s \in \mathbb{C}$ ,

$$\pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = -\frac{1}{s(1-s)} + \int_1^{+\infty} (x^{\frac{s}{2}-1} + x^{\frac{1-s}{2}-1}) \frac{\theta(x) - 1}{2} dx.$$

一个立即得到的推论是

**推论 2.5.**  $\pi^{-\frac{s}{2}} \Gamma(\frac{s}{2}) \zeta(s) = \pi^{-\frac{1-s}{2}} \Gamma(\frac{1-s}{2}) \zeta(1-s)$  ( $s \neq 0, 1$ ).

**思考.** 如何判断  $\zeta(s)$  的零点问题.

下面我们来证明**定理 2.4**.

证明.

$$\begin{aligned}
\Gamma\left(\frac{s}{2}\right)\zeta(s) &= \int_0^{+\infty} x^{\frac{s}{2}-1} e^{-x} dx \sum_{n=1}^{\infty} \frac{1}{n^s} \\
&= \sum_{n=1}^{\infty} \frac{1}{n^s} \int_0^{+\infty} x^{\frac{s}{2}-1} e^{-x} dx \\
&\stackrel{(x=\pi n^2 y)}{=} \sum_{n=1}^{\infty} \frac{1}{n^s} \int_0^{+\infty} \pi^{\frac{s}{2}-1} n^{s-2} y^{\frac{s}{2}-1} e^{-\pi n^2 y} \pi n^2 dy \\
&= \pi^{\frac{s}{2}} \sum_{n=1}^{\infty} \int_0^{+\infty} y^{\frac{s}{2}-1} e^{-\pi n^2 y} dy \\
&= \pi^{\frac{s}{2}} \int_0^{+\infty} y^{\frac{s}{2}-1} \sum_{n=1}^{\infty} e^{-\pi n^2 y} dy \\
&= \pi^{\frac{s}{2}} \int_0^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy
\end{aligned}$$

将积分拆开如下

$$\begin{aligned}
\pi^{\frac{s}{2}} \int_0^{\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy &= \pi^{\frac{s}{2}} \int_1^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy + \pi^{\frac{s}{2}} \int_0^1 y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy \\
&\stackrel{(y=\frac{1}{x})}{=} \pi^{\frac{s}{2}} \int_1^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy + \pi^{\frac{s}{2}} \int_1^{+\infty} x^{-\frac{s}{2}-1} \frac{\theta(\frac{1}{x}) - 1}{2} dx \\
&= \pi^{\frac{s}{2}} \int_1^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy + \pi^{\frac{s}{2}} \int_1^{+\infty} x^{-\frac{s}{2}-1} \frac{\sqrt{x}\theta(x) - 1}{2} dx \\
&= \pi^{\frac{s}{2}} \int_1^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy + \pi^{\frac{s}{2}} \int_1^{+\infty} x^{-\frac{s}{2}-1} \frac{\sqrt{x}(\theta(x) - 1) + \sqrt{x} - 1}{2} dx \\
&= \pi^{\frac{s}{2}} \int_1^{+\infty} y^{\frac{s}{2}-1} \frac{\theta(y) - 1}{2} dy + \pi^{\frac{s}{2}} \int_1^{+\infty} x^{-\frac{s}{2}-\frac{1}{2}} \frac{\theta(x) - 1}{2} dx - \pi^{\frac{s}{2}} \frac{1}{s(1-s)}.
\end{aligned}$$

上面证明了  $\operatorname{Re}(s) > 2$  时原式成立. 由解析函数的性质, 我们有原式对  $\operatorname{Re}(s) > 0$  时也成立, 并且它给出了等式左边到  $\mathbb{C} \setminus \{0, 1\}$  的延拓.  $\square$

**推论 2.6.** 上述定理给出了  $\zeta(s)$  到  $\mathbb{C} \setminus \{1\}$  的解析延拓, 且  $s = 1$  是单极点. 并且  $\zeta(0) \neq 0$ ,  $\zeta(-2) = \zeta(-4) = \dots = 0$  是单零点 (有时称作平凡零点).

**推论 2.7.**  $\operatorname{Re}(s) < 0$  时, 负偶数是  $\zeta(s)$  的所有零点.

事实上我们现在才能真正叙述 Riemann 猜想, 除去之前给出的叙述, 我们还能将其叙述为:  $\zeta(s)$  的所有非平凡零点的实部为  $\frac{1}{2}$ .

**定理 2.8.**  $\zeta(1+it) \neq 0$  ( $\forall t \in \mathbb{R}$ ).

证明. 不妨  $t \neq 0$ . 考虑  $s = \sigma + it$ .

$$\begin{aligned}\zeta(\sigma + it) &= \prod_p \left(1 - \frac{1}{p^{\sigma+it}}\right) \\ &= \exp\left(\log \prod_p \left(1 - \frac{1}{p^{\sigma+it}}\right)\right) \\ &= \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{1}{mp^{m(\sigma+it)}}\right) \\ &= \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{\cos(\log p)mt - i \sin(\log p)mt}{mp^{m\sigma}}\right).\end{aligned}$$

于是

$$|\zeta(\sigma + it)| = \exp\left(\sum_p \sum_{n=1}^{\infty} \frac{\cos(\log p)mt}{mp^{m\sigma}}\right).$$

考察

$$|\zeta(\sigma)^3 \zeta(\sigma + it)^4 \zeta(\sigma + 2it)| = \exp\left(\sum_p \sum_{m=1}^{\infty} \frac{3 + 4 \cos(\log p)mt + \cos(\log p)m2t}{mp^{m\sigma}}\right).$$

对于等号右边的分子, 我们有

$$3 + 4 \cos(\log p)mt + \cos(\log p)m2t = 2(\cos mt \log p + 1)^2 \geq 0.$$

于是

$$|\zeta(\sigma)^3 \zeta(\sigma + it)^4 \zeta(\sigma + 2it)| \geq 1.$$

倘若对某个  $t$ ,  $1 + it$  是零点, 则下述不等式

$$(\zeta(\sigma)(\sigma - 1))^3 \left|\frac{\zeta(\sigma + it)}{\sigma - 1}\right|^4 |\zeta(\sigma + 2it)| \geq \frac{1}{\sigma - 1}$$

令  $\sigma \rightarrow 1^+$  时左边是常数而右边趋于无穷, 矛盾. □



## 2.2 素数定理

**引理 2.9.** 设  $f(u)$  是 (可积, 间断点离散) 实函数.

1. 存在  $M > 0$ , s.t.  $|f(u)| \leq \frac{M}{u}$  ( $\forall u \geq 1$ ).

2.  $g(s) = \int_1^{+\infty} \frac{f(u)}{u^s} du$  ( $Re(s) > 0$ ) 可以延拓到  $Re(s) \geq 0$ .

则积分  $\int_1^{+\infty} f(u) du$  收敛.

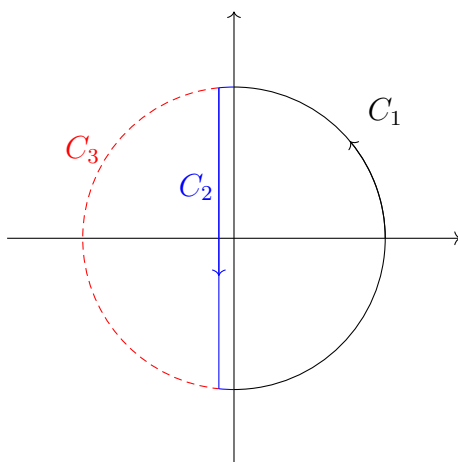
证明. 引入  $g_x(s) = \int_1^x \frac{f(u)}{u^s} du$  ( $\forall s$ ), 要证结论即转为  $\lim_{x \rightarrow +\infty} g_x(0) = g(0)$ . 对充分大的  $R$ , 存在  $h_R > 0$ , s.t.  $g(s)$  在  $Re(s) \geq -h_R$  且  $|Im(s)| \leq R$  的范围内解析. 任取正数  $h < h_R$ , 存在  $M_R$ , s.t.  $|g(s)| \leq M_R$  ( $\forall s \in D_R$ ). 其中  $D_R$  是由积分围道  $C(= C_1 + C_2)$  围成的闭集, 虚轴右端的半圆记为  $C_1$ , 即

$$C_1 = \{s \mid Re(s) \geq 0, |s| = R\}$$

$C_2 = C - C_1$ , 虚轴左边的半圆记为  $C_3$ , 即

$$C_3 = \{s \mid Re(s) \leq 0, |s| = R\}$$

如下图所示.



根据 Cauchy 积分公式, 我们有

$$g_x(0) - g(0) = \frac{1}{2\pi i} \int_C \frac{g_x(s) - g(s)}{s} x^s \left( \frac{s^2}{R^2} + 1 \right) ds$$

于是原积分改写为

$$\begin{aligned} \frac{1}{2\pi i} \int_C \frac{g_x(s) - g(s)}{s} x^s \left( \frac{s^2}{R^2} + 1 \right) ds &= \frac{1}{2\pi i} \int_{C_1} \frac{g_x(s) - g(s)}{s} x^s \left( \frac{s^2}{R^2} + 1 \right) ds \\ &\quad + \frac{1}{2\pi i} \int_{C_2} \frac{g_x(s) - g(s)}{s} x^s \left( \frac{s^2}{R^2} + 1 \right) ds \end{aligned}$$

其中

$$\begin{aligned} \frac{1}{2\pi i} \int_{C_2} \frac{g_x(s) - g(s)}{s} x^s \left( \frac{s^2}{R^2} + 1 \right) ds &= \frac{1}{2\pi i} \int_{C_3} \frac{g_x(s)}{s} x^s \left( \frac{s^2}{R^2} + 1 \right) ds \\ &\quad - \frac{1}{2\pi i} \int_{C_2} \frac{g(s)}{s} x^s \left( \frac{s^2}{R^2} + 1 \right) ds \end{aligned}$$

下面我们分别考虑这些积分.

在  $C_1$  上, 有  $|x^s| = x^\sigma$ ,  $|\frac{1}{s}| = \frac{1}{R}$ ,  $|\frac{s^2}{R^2} + 1| = \frac{2\sigma}{R}$ . 当  $\sigma > 0$  时

$$\begin{aligned} |g_x(s) - g(s)| &= \left| \int_x^{+\infty} \frac{f(u)}{u^s} du \right| \\ &\leq M \left| \int_x^{+\infty} \frac{1}{u^{\sigma+1}} du \right| = \frac{M}{\sigma} x^{-\sigma} \end{aligned}$$

于是

$$\begin{aligned} \left| \frac{1}{2\pi i} \int_{C_1} \frac{g_x(s) - g(s)}{s} x^s \left( \frac{s^2}{R^2} + 1 \right) ds \right| &\leq \left| \frac{1}{2\pi i} \pi R \cdot \frac{M}{\sigma} x^{-\sigma} \cdot x^\sigma \cdot \frac{1}{R} \cdot \frac{2\sigma}{R} \right| \\ &\leq \frac{M}{R} \quad (\sigma \geq 0, s \in C_1) \end{aligned}$$

类似地有

$$\left| \frac{1}{2\pi i} \int_{C_3} \frac{g_x(s)}{s} x^s \left( \frac{s^2}{R^2} + 1 \right) ds \right| \leq \frac{M}{R} \quad (\sigma \leq 0, s \in C_3)$$

而在  $C_2$  上, 我们把它分为两个小弧段和直线, 依次有

$$\begin{aligned} \left| \frac{1}{2\pi i} \int_{C_2} \frac{g(s)}{s} x^s \left( \frac{s^2}{R^2} + 1 \right) ds \right| &\leq \left| \frac{1}{2\pi i} \cdot 2\pi h \left( \frac{M_R}{R} x^\sigma \frac{2\sigma}{R} \right) \right| + \left| \frac{1}{2\pi i} \cdot \frac{M_R}{h} \cdot x^{-h} \cdot 2 \right| \\ &\leq \frac{M_R h^2}{R^2} + x^{-h} \frac{2R M_R}{\pi h} \end{aligned}$$

综上, 我们有

$$|g_x(0) - g(0)| \leq \frac{2M}{R} + \frac{M_R h^2}{R^2} + x^{-h} \frac{2RM_R}{\pi h}$$

于是对于任意的  $\varepsilon > 0$ , 能够 ( 依次 ) 取到合适的  $R, h$ , s.t.  $\exists x_0$ , 对任意的  $x > x_0$ ,  $|g_x(0) - g(0)| \leq \varepsilon$ . □

**定理 2.10.**  $\psi(x) \sim x$ .

证明. 根据引理 1.8. 和引理 2.9., 要证素数定理, 只需证  $f(u) = \frac{\psi(u)-u}{u^2}$  满足引理 2.9. 的两个条件. 我们已经知道存在正常数  $c_1, c_2$  使得  $c_1 x \leq \psi(x) \leq c_2 x$ , 这就满足了第一个条件. 对于第二个条件,  $Re(s) > 0$  时, 我们考虑

$$\begin{aligned} g(s) &= \int_1^{+\infty} \frac{\psi(u) - u}{u^{s+2}} du = \int_1^{+\infty} \frac{\sum_{n \leq u} \Lambda(n)}{u^{s+2}} du - \frac{1}{s} \\ &= \sum_{n=1}^{\infty} \Lambda(n) \int_n^{+\infty} \frac{1}{u^{s+2}} du - \frac{1}{s} \\ &= -\frac{1}{s+1} \frac{\zeta'(s+1)}{\zeta(s+1)} - \frac{1}{s} \end{aligned}$$

只用代入延拓后的 Riemann zeta 函数 (4) 即可证得其满足第二个条件. □

### 3 算术级数中的素数分布 I

本章目的是证明如下的 Dirichlet 定理

**定理 3.1** (Dirichlet). 给定  $a, q \in \mathbb{Z}^+, (a, q) = 1$ . 则有无穷多个素数形如  $p \equiv a \pmod{q}$ . 即

$$\{a + qk \mid k \in \mathbb{Z}^+\}$$

中有无穷多个素数.

为了证明这个定理, 我们需要做一些准备工作. 若无特殊声明, 本节提到的群均为有限 Abel 群.

#### 3.1 有限 Abel 群的特征

群的特征是 Dedekind 研究所谓群行列式的时候发现的, 这实际上也是群表示论的开端. 感兴趣的读者仅需要高等代数和一些抽象代数的知识就可以阅读 [3], 有更强大背景的读者想必可以从 [7] 中汲取大量营养.

**定义 3.2.** 从群  $G$  到  $\mathbb{C}^\times = \mathbb{C} \setminus \{0\}$  的群同态

$$\chi : G \rightarrow \mathbb{C}^\times$$

称为群  $G$  的一个特征. 所有特征构成的集合记为  $G^*$

**注.** 不难看出  $G^*$  非空, 因为  $[g \mapsto 1] \in G^*$

**注.** 若记  $|G| = n$ , 则对任意  $g \in G$ ,  $\chi(g)$  都是  $n$  次单位根.

我们称上述恒映到 1 的特征为主特征, 记为  $\chi_0$ . 本文中有时为了强调它作为单位元, 也记作  $\text{id}_{G^*}$ , 引入乘法

$$\chi_1 * \chi_2 : G \rightarrow \mathbb{C}^\times$$

$$g \mapsto [\chi_1 * \chi_2(g) := \chi_1(g)\chi_2(g)]$$

于是不难验证有

**引理 3.3.**  $G^*$  构成有限 Abel 群.

**注.** 由于特征  $\chi$  都是单位根, 它的逆可以写成  $\chi^{-1} : g \mapsto \chi^{-1}(g) = \chi(g^{-1}) = \overline{\chi(g)}$ .

**定理 3.4.** 我们有如下群同构

$$G \cong G^*.$$

**证明. Step 1.** 我们首先证明结论对循环群成立.

记  $G = \langle g \rangle$ ,  $|g| = |G| = n$ . 于是对任意  $\chi \in G^*$ ,

$$\chi(g) \in \{e^{2\pi i \frac{k}{n}} \mid 0 \leq k \leq n-1\}.$$

定义

$$\chi_k : G \rightarrow \mathbb{C}^*$$

$$g^j \mapsto [\chi_k(g^j) = e^{2\pi i \frac{kj}{n}}] \quad (0 \leq j \leq n-1)$$

不难验证  $\chi_k \in G^*$ , 更进一步  $G^*$  是循环群.

**Step 2.** 我们现在证明对有限 Abel 群  $A, B$ ,  $(A \times B)^* \equiv A^* \times B^*$ .

引入

$$\rho : A^* \times B^* \rightarrow (A \times B)^*$$

$$(\sigma, \tau) \mapsto [\rho(\sigma, \tau) : (a, b) \mapsto \sigma(a)\tau(b)]$$

不难验证这样定义的  $\rho(\sigma, \tau)$  确实是  $A \times B$  上的特征, 更进一步  $\rho$  是一个群同态. 要证它是同构, 只需证它既是单射又是满射.

(单射) 若对任意  $a \in A, b \in B$ ,  $\rho(\sigma, \tau)(a, b) = \sigma(a)\tau(b) = 1$ . 取定  $a = \text{id}_A$ , 则  $\forall b, \tau(b) = 1$ , 于是  $\tau = \text{id}_{B^*}$ . 取定  $b = \text{id}_B$ , 则  $\forall a, \sigma(a) = 1$ , 于是  $\sigma = \text{id}_{A^*}$ .

(满射) 对任意  $f \in (A \times B)^*$ , 取  $\sigma : a \rightarrow f(a, \text{id}_B) \quad \forall a \in A, \tau : b \rightarrow f(\text{id}_A, b) \quad \forall b \in B$ . 不难验证  $\sigma \in A^*, \tau \in B^*$ , 且  $\rho(\sigma, \tau) = f$ .

于是根据有限 Abel 群的结构定理即证. □

**定理 3.5** (正交关系). 设  $G$  为有限 Abel 群,

$$(1) \frac{1}{|G|} \sum_{g \in G} \chi(g) = \begin{cases} 1 & \chi = \chi_0, \\ 0 & \text{otherwise.} \end{cases}$$

$$(2) \frac{1}{|G|} \sum_{\chi \in G^*} \chi(g) = \begin{cases} 1 & g = \text{id}_G, \\ 0 & \text{otherwise.} \end{cases}$$

证明. (1) 只需考虑  $\chi \neq \chi_0$  的情况. 此时  $\exists s \in G$  s.t.  $\chi(s) \neq 1$ , 则

$$\begin{aligned} \sum_{g \in G} \chi(g) &= \sum_{g \in G} \chi(sg) \\ &= \chi(s) \sum_{g \in G} \chi(g) \end{aligned}$$

于是  $(1 - \chi(s)) \sum_{g \in G} \chi(g) = 0$ .

(2) 只需考虑  $g \neq \text{id}_G$  的情况. 我们首先证明对这样的  $g$ , 存在  $\tau \in G^*$  s.t.  $\tau(g) \neq 1$ . 如果不然, 即对任意的  $\chi \in G^*$ ,  $\chi(g) = 1$ .  $\chi$  自然诱导从商群  $G/\langle g \rangle$  到  $\mathbb{C}^*$  的同态

$$\begin{aligned} \tilde{\chi} : G/\langle g \rangle &\rightarrow \mathbb{C}^\times \\ h \cdot \langle g \rangle &\mapsto \chi(h) \end{aligned}$$

于是  $|G| = |G^*| \leq |(G/\langle g \rangle)^*| = |G/\langle g \rangle|$ , 矛盾. 其余部分与 (1) 同理.  $\square$

**注.** 我们也可以从另一个角度看这个定理. 对有限 Abel 群  $G$ ,  $G^* \cong G$  也是有限 Abel 群, 于是我们可以考虑  $G^*$  的特征, 它由  $G$  中的元素给出:

$$\begin{aligned} g : G^* &\rightarrow \mathbb{C}^\times \\ \chi &\mapsto \langle g, \chi \rangle := \chi(g) \end{aligned}$$

不难验证他们同样构成一个有限 Abel 群  $(G^*)^*$ . 于是有  $G \cong G^* \cong (G^*)^*$ . 那么

**定理 3.5.** 中的 (2) 就可以由 (1) 直接推出:

$$\sum_{\chi \in G^*} \chi(g) = \sum_{\chi \in G^*} \langle g, \chi \rangle.$$

这立刻给出下面两条推论.

**推论 3.6.** 对  $\chi_1, \chi_2 \in G^*$ ,

$$\frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} = \begin{cases} 1 & \chi_1 = \chi_2, \\ 0 & \text{otherwise.} \end{cases}$$

证明. 我们有

$$\frac{1}{|G|} \sum_{g \in G} \chi_1(g) \overline{\chi_2(g)} = \frac{1}{|G|} \sum_{g \in G} \chi_1 \chi_2^{-1}(g)$$

由定理 3.5. (1) 立即可得. □

**推论 3.7.** 对  $g_1, g_2 \in G$ ,

$$\frac{1}{|G|} \sum_{\chi \in G^*} \chi(g_1) \overline{\chi(g_2)} = \begin{cases} 1 & g_1 = g_2, \\ 0 & \text{otherwise.} \end{cases}$$

证明. 注意到对任意特征  $\chi$ ,  $\chi(g) \overline{\chi(g)} = \chi(g) \chi(g^{-1}) = 1$ , 于是

$$\frac{1}{|G|} \sum_{\chi \in G^*} \chi(g_1) \overline{\chi(g_2)} = \frac{1}{|G|} \sum_{\chi \in G^*} \chi(g_1 g_2^{-1})$$

由定理 3.5. (2) 立即可得. □

## 3.2 Dirichlet L 函数及其性质

现在我们着手把上述理论应用到  $G = (\mathbb{Z}/q\mathbb{Z})^\times$  上.

**定义 3.8** (Dirichlet 特征). 对  $q \in \mathbb{Z}^+ (\geq 2)$ ,  $\chi \in G^*$ ,  $\overline{m} \in G$ . 我们称

$$\chi_D(m) = \begin{cases} \chi(\overline{m}) & (m, q) = 1, \\ 0 & (m, q) > 1. \end{cases}$$

给出的函数

$$\chi_D : \mathbb{Z} \rightarrow \mathbb{C}$$

为  $(\text{mod } q)$  的 Dirichlet 特征.

注. 一共有  $\varphi(q)$  个  $\bmod q$  的 Dirichlet 特征. 其中  $\varphi$  是 Euler 函数.

下面给出一些关于 Dirichlet 特征 (的由定义和正交关系立即可得) 的性质.

**命题 3.9.** 设  $\chi$  是  $\bmod q$  的特征, 则  $\chi$  是完全积性的, 即  $a, b \in \mathbb{Z}$ ,

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

**命题 3.10.** 对  $a, b \in \mathbb{Z}$ ,

$$\frac{1}{\varphi(q)} \sum_{\chi(\bmod q)} \chi(a) \overline{\chi(b)} = \begin{cases} 1 & a \equiv b(\bmod q) \text{ 且 } (ab, q) = 1, \\ 0 & \text{otherwise.} \end{cases}$$

其中  $\sum_{\chi(\bmod q)}$  表示对所有  $\bmod q$  的特征求和.

**命题 3.11.** 对  $a \in \mathbb{Z}$ ,

$$\frac{1}{\varphi(q)} \sum_{1 \leq a \leq q} \chi(a) = \begin{cases} 1 & \chi = (\text{id}_{G^*})_D, \\ 0 & \text{otherwise.} \end{cases}$$

**命题 3.12.**  $\chi$  是周期为  $q$  的函数.

**定义 3.13** (Dirichlet L-函数). 在  $\text{Re}(s) > 1$  时, 我们定义

$$\begin{aligned} L(s, \chi) &:= \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \\ &= \prod_p \left( 1 + \frac{\chi(p)}{p^s} + \frac{\chi(p^2)}{p^{2s}} + \dots \right) \\ &= \prod_p \left( 1 - \frac{\chi(p)}{p^s} \right)^{-1} \\ &= \prod_{p \nmid q} \left( 1 - \frac{\chi(p)}{p^s} \right)^{-1} \end{aligned}$$

$L(s, \chi)$  称为 Dirichlet L-函数.



称  $G^*$  中单位元给出的 Dirichlet 特征为 (Dirichlet) 主特征, 在无歧义的情况下仍记为  $\chi_0$ . 即

$$\chi_0(m) = \begin{cases} 1 & (m, q) = 1, \\ 0 & (m, q) > 1. \end{cases}$$

**注.** 若非主特征  $\chi(n)$  总是实数, 则称为非主实特征. 非实特征称为复特征, 即  $\exists n$  s.t.  $\chi_n \notin \mathbb{R}$ .

**引理 3.14.** 设  $\chi$  是 mod  $q$  的 Dirichlet 特征,  $x \geq 1$ .

(1) 若  $\chi$  不是主特征, 则

$$|\sum_{n \leq x} \chi(n)| \leq \varphi(q)$$

2 若  $\chi = \chi_0$ , 则

$$|\sum_{n \leq x} \chi(n) - \frac{\varphi(q)}{q}x| \leq 2\varphi(q)$$

**证明.** 由于周期性, 我们可以把求和写成如下形式:

$$\sum_{n \leq x} \chi(n) = \left[ \frac{x}{q} \right] \sum_{1 \leq a \leq q} \chi(a) + R,$$

其中  $|R| \leq \sum_{1 \leq a \leq q} |\chi(a)| \leq \varphi(q)$ . 于是当  $\chi \neq \chi_0$  时, 由**命题 3.11** 可知  $\sum_{1 \leq a \leq q} \chi(a) = 0$ . 当  $\chi = \chi_0$  时,  $\sum_{1 \leq a \leq q} \chi(a) = \varphi(q)$ . □

**命题 3.15.** 对正实数  $s$ , 当  $\chi$  不是主特征时,  $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$  收敛, 但不绝对收敛. 当  $\chi = \chi_0$  时,  $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$  不收敛.

**证明.**  $\chi \neq \chi_0$  时, 由于  $|\sum_{n=1}^N \chi(n)| \leq \varphi(q)$ , 根据 Dirichlet 关于条件收敛的判据可知  $s > 0$  时,  $\sum_{n=1}^{\infty} \frac{\chi(n)}{n^s}$  收敛. □

**命题 3.16.**  $L(s, \chi_0)$  可以延拓到整个复平面,  $s = 1$  是单极点.

证明. 注意到  $L(s, \chi_0) = \prod_{p|q} (1 - \frac{1}{p^s}) \zeta(s)$ . □

**命题 3.17.** 当  $\chi \neq \chi_0$ ,  $\operatorname{Re}(s) > 1$  时, 有

$$L(s, \chi) = \frac{1}{s} \int_1^\infty F_\chi(u) u^{-s-1} du$$

其中  $F_\chi(u) = \sum_{1 \leq a \leq u} \chi(a)$ . 并且上式给出了  $L(s, \chi)$  在  $\operatorname{Re}(s) > 0$  上的解析延拓.

证明. 由分部求和有

$$\begin{aligned} \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} &= \sum_{n=1}^{\infty} \frac{F_\chi(n) - F_\chi(n-1)}{n^s} \\ &= \sum_{n=1}^{\infty} F_\chi(n) (n^{-s} - (n+1)^{-s}) \\ &= \frac{1}{s} \sum_{n=1}^{\infty} F_\chi(n) \int_n^{n+1} u^{-s-1} du \\ &= \frac{1}{s} \sum_{n=1}^{\infty} \int_n^{n+1} F_\chi(u) u^{-s-1} du \\ &= \frac{1}{s} \int_1^{+\infty} F_\chi(u) u^{-s-1} du. \end{aligned}$$

根据引理 3.14. 可知上式最后的积分的收敛性. □

**推论 3.18.** 设  $q \geq 3$ , 则有  $\chi \neq \chi_0$  时的  $\varphi(q) - 1$  个 Dirichlet 函数中至多有一个函数在  $s = 1$  处为零. 且若  $L(1, \chi) = 0$  ( $\chi \neq \chi_0$ ), 则  $s = 1$  是  $L(s, \chi)$  的单零点.

证明. 对实数  $s > 1$  考察

$$\begin{aligned}
 \prod_{\chi(\bmod q)} L(s, \chi) &= \prod_{\chi(\bmod q)} \prod_p \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \\
 &= \exp \left( \sum_{\chi(\bmod q)} \sum_p \log \left(1 - \frac{\chi(p)}{p^s}\right)^{-1} \right) \\
 &= \exp \left( \sum_{\chi} \sum_p \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}} \right) \\
 &= \exp \left( \sum_{\chi} \sum_p \sum_{k=1}^{\infty} \frac{\chi(p^k)}{kp^{ks}} \right) \\
 &= \exp \left( \varphi(q) \sum_k \sum_{p^k \equiv 1(\bmod q)} \frac{1}{kp^{ks}} \right) \geq 1.
 \end{aligned}$$

我们知道  $s = 1$  是  $L(s, \chi_0)$  的一个单极点, 而  $\chi \neq \chi_0$  时  $L(s, \chi)$  在  $s = 1$  处是解析的. 于是若有超过一个函数在  $s = 1$  处为零则乘积为 0, 与上述计算结果矛盾. □

**推论 3.19.** 设  $\chi$  是复特征, 则  $L(1, \chi) \neq 0$ .

证明. 取  $\chi$  的共轭函数  $\bar{\chi}$ , 它也是  $\bmod q$  的 Dirichlet 特征.  $\chi$  和  $\bar{\chi}$  是不同的函数, 且  $L(1, \chi) = 0 \Leftrightarrow L(1, \bar{\chi}) = 0$ . 当实数  $s > 1$  时有  $L(s, \bar{\chi}) = \overline{L(s, \chi)}$ . 取  $s \rightarrow 1^+$  即证. □

我们介绍一个非常重要的公式, 并给出一些估计.

**定理 3.20** (Abel 求和公式 (部分求和公式)). 对于任意  $y \in \mathbb{R}$ ,  $y \geq 1$ , 我们有

$$\sum_{1 \leq n \leq y} a(n)b(n) = \sum_{1 \leq n \leq y} a(n)b(y) - \int_1^y \left( \sum_{1 \leq n \leq t} a(n) \right) b'(t) dt$$

证明. 注意到

$$\int_1^y \left( \sum_{1 \leq n \leq t} a(n) \right) b'(t) dt = \sum_{1 \leq n \leq y} a(n) \int_n^y b'(t) dt = \sum_{1 \leq n \leq y} a(n)(b(y) - b(n)).$$

易见等式成立. □

我们首先给出一个在数学分析中已经知道的估计.

**推论 3.21.** 我们有

$$\sum_{n=1}^y \frac{1}{n} = \log y + \gamma + O\left(\frac{1}{y}\right)$$

其中  $\gamma$  称为 *Euler* 常数.

证明.

$$\begin{aligned} \sum_{n=1}^y \frac{1}{n} &= 1 + \int_1^y [t] \frac{1}{t^2} dt \\ &= 1 + \int_1^y \frac{1}{t} dt - \int_1^y \{t\} \frac{1}{t^2} dt \\ &= \log y + 1 - \int_1^{+\infty} \{t\} \frac{1}{t^2} dt + O\left(\frac{1}{y}\right) \\ &= \log y + \gamma + O\left(\frac{1}{y}\right). \end{aligned}$$

其中  $\gamma = 1 - \int_1^{+\infty} \{t\} \frac{1}{t^2} dt$ . □

下面给出两个在之后的证明中要用到的估计.

**推论 3.22.** 我们有

$$\sum_{n=1}^y \frac{1}{\sqrt{n}} = 2\sqrt{y} + A + O\left(\frac{1}{\sqrt{y}}\right)$$

其中  $A$  是一个常数.

证明.

$$\begin{aligned} \sum_{n=1}^y \frac{1}{\sqrt{n}} &= y \frac{1}{\sqrt{y}} + \frac{1}{2} \int_1^y [t] t^{-\frac{3}{2}} dt \\ &= \sqrt{y} + \frac{1}{2} \int_1^y t^{-\frac{1}{2}} dt - \frac{1}{2} \int_1^y \{t\} t^{-\frac{3}{2}} dt \\ &= 2\sqrt{y} - 1 - \frac{1}{2} \int_1^{+\infty} \{t\} t^{-\frac{3}{2}} dt + O(y^{-\frac{1}{2}}) \\ &= 2\sqrt{y} + A + O\left(\frac{1}{\sqrt{y}}\right). \end{aligned}$$

其中  $A = -1 - \frac{1}{2} \int_1^{+\infty} \{t\} t^{-\frac{3}{2}} dt$ . □

**推论 3.23.** 对于非主的  $\text{mod } q$  特征  $\chi$ ,  $\beta > 0$ ,  $y \geq 1$  是实数. 我们有

$$\sum_{n=1}^y \frac{\chi(n)}{n^\beta} = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^\beta} + O\left(\frac{1}{y^\beta}\right)$$

证明. 任取  $Y \in \mathbb{Z}^+$  ( $y \leq Y$ ), 对  $n \leq Y$ , 我们取  $a(n) = \chi(n)$  ( $y \leq n \leq Y$ ), 其余情况取 0,  $b(n) = \frac{1}{n^\beta}$ . 套用 Abel 求和公式我们有

$$\begin{aligned} \sum_{y \leq n \leq Y} \frac{\chi(n)}{n^\beta} &= \sum_{y \leq n \leq Y} \frac{\chi(n)}{y^\beta} - \int_1^y \sum_{y \leq n \leq t} \chi(n) t^{-\beta-1} dt \\ &\leq \varphi(q) y^{-\beta} + \varphi(q) y^{-\beta} \\ &\leq 2\varphi(q) y^{-\beta} \end{aligned}$$

此式对任意  $Y \in \mathbb{Z}^+$  ( $y \leq Y$ ) 都成立. 推论即证. □

**定理 3.24.** 设  $\chi$  是  $\text{mod } q$  的非主特征, 则有

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

证明. 对于实数  $s > 1$ , 取  $y$ ,

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

于是有

$$|L(s, \chi) - \sum_{n=1}^y \frac{\chi(n)}{n^s}| \leq 2\varphi(q)y^{-s} \leq 2\varphi(q)y^{-1}$$

则

$$|L(1, \chi) - \sum_{n=1}^y \frac{\chi(n)}{n}| \leq 2\varphi(q)y^{-1}.$$

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

□

注. 设  $\{a(n)\}_n$  是  $\mathbb{Z}^+$  的一个重排. 于是当  $\operatorname{Re}(s) > 1$  时有

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

**引理 3.25.** 设  $\chi$  是非主实特征,  $y \geq 1$ , 令  $D(n) = \sum_{d|n} \chi(d)$ .

$$\sum_{n \leq y} D(n)n^{-\frac{1}{2}} = 2L(1, \chi)y^{\frac{1}{2}} + O(1).$$

证明. 我们用 Dirichlet 双曲律 (**定理 C.1.**) 证明这个引理.

$$\begin{aligned} \sum_{n \leq y} \frac{D(n)}{\sqrt{n}} &= \sum_{\substack{a, b \leq y \\ ab \leq y}} \frac{\chi(a)}{\sqrt{ab}} \\ &= \sum_{a \leq \sqrt{y}} \frac{\chi(a)}{\sqrt{a}} \sum_{b \leq \frac{y}{a}} \frac{1}{\sqrt{b}} + \sum_{b \leq \sqrt{y}} \frac{1}{\sqrt{b}} \sum_{a \leq \frac{y}{b}} \frac{\chi(a)}{\sqrt{a}} \\ &\quad - \sum_{a \leq \sqrt{y}} \frac{\chi(a)}{\sqrt{a}} \sum_{b \leq \sqrt{y}} \frac{\chi(b)}{\sqrt{b}} \end{aligned}$$

我们分别估计这三项.

$$\begin{aligned}
\sum_{a \leq \sqrt{y}} \frac{\chi(a)}{\sqrt{a}} \sum_{b \leq \frac{y}{a}} \frac{1}{\sqrt{b}} &= \sum_{a \leq \sqrt{y}} \frac{\chi(a)}{\sqrt{(a)}} \left( 2\sqrt{\frac{y}{a}} + A + O\left(\sqrt{\frac{a}{y}}\right) \right) \\
&= 2\sqrt{y} \left( \sum_{n=1}^{\infty} \frac{\chi(a)}{a} + O\left(\frac{1}{\sqrt{y}}\right) \right) + A \left( \sum_{n=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} + O(y^{-\frac{1}{4}}) \right) + O(1) \\
&= 2\sqrt{y}L(1, \chi) + O(1) \\
\sum_{b \leq \sqrt{y}} \frac{1}{\sqrt{b}} \sum_{a \leq \frac{y}{b}} \frac{\chi(a)}{\sqrt{a}} &= \sum_{b \leq \sqrt{y}} \frac{1}{\sqrt{b}} \left( \sum_{a=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} + O\left(\sqrt{\frac{b}{y}}\right) \right) \\
&= \sum_{a=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} \left( 2y^{\frac{1}{4}} + A + O(y^{-\frac{1}{4}}) \right) + O(1) \\
&= 2y^{\frac{1}{4}} \sum_{a=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} + O(1) \\
\sum_{a \leq \sqrt{y}} \frac{\chi(a)}{\sqrt{a}} \sum_{b \leq \sqrt{y}} \frac{\chi(b)}{\sqrt{b}} &= \left( \sum_{a=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} + O(y^{-\frac{1}{4}}) \right) \left( 2y^{\frac{1}{4}} + A + O(y^{-\frac{1}{4}}) \right) \\
&= 2y^{\frac{1}{4}} \sum_{a=1}^{\infty} \frac{\chi(a)}{\sqrt{a}} + O(1).
\end{aligned}$$

于是我们得到

$$\sum_{n \leq y} D(n)n^{-\frac{1}{2}} = 2L(1, \chi)y^{\frac{1}{2}} + O(1). \quad \square$$

**定理 3.26.** 设  $\chi$  是非主实特征, 则  $L(1, \chi) \neq 0$ .

证明. 设  $p$  是素数,  $a \in \mathbb{Z}^+$ , 则

$$D(p^a) = \sum_{d|p^a} \chi(d) = 1 + \chi(p) + \cdots + \chi(p)^a.$$

由于  $\chi$  是实特征, 不难得到若  $n$  是完全平方数,  $D(n) \geq 1$ , 且对任意  $n$ ,  $D(n) \geq 0$ .

于是

$$\sum_{n \leq y} \frac{D(n)}{\sqrt{n}} \geq \sum_{m^2 \leq y} \frac{D(m^2)}{\sqrt{m^2}} \geq \sum_{m \leq \sqrt{y}} \frac{1}{m}. \quad (5)$$

若  $L(1, \chi) = 0$ , 根据引理 3.25. 我们有  $\sum_{n \leq y} \frac{D(n)}{\sqrt{n}} = O(1)$ . 这同 (5) 矛盾.  $\square$

**推论 3.27.** 对  $q \in \mathbb{Z}^+$  (不妨  $q \geq 3$ ). 由

$$\sum_{p \equiv 1 \pmod{q}} \frac{1}{p} = \infty$$

特别地, 有无穷多个素数  $p \equiv 1 \pmod{q}$ .

### 3.3 Dirichlet 定理的证明

**引理 3.28.**  $\sum \frac{\Lambda(a)\chi(a)}{n^s} = -\frac{L'(s, \chi)}{L(s, \chi)}.$

下面我们证明 Dirichlet 定理 (**定理 3.1.**).

**证明.** 由**引理 3.28.**, 有

$$\begin{aligned} \sum_{\substack{n=1 \\ n \equiv a \pmod{q}}}^{\infty} \frac{\Lambda(n)}{n^s} &= \frac{1}{\varphi(q)} \sum_{\chi \pmod{q}} \overline{\chi(a)} \sum_{n=1}^{\infty} \frac{\Lambda(n)\chi(n)}{n^s} \\ &= -\frac{1}{\varphi(q)} \frac{L'(s, \chi_0)}{L(s, \chi_0)} + \frac{1}{\varphi(q)} \sum_{\substack{\chi \pmod{q} \\ \chi \neq \chi_0}} \overline{\chi(a)} (-1) \frac{L'(s, \chi)}{L(s, \chi)} \end{aligned}$$

下只考虑  $s$  为大于 1 的实数, 考虑  $s \rightarrow 1^+$ . 当  $\chi = \chi_0$  时有  $\frac{1}{s-1}g(s)$ , 其中  $g(s)$  是一个在 1 的邻域内的解析函数且  $g(1) \neq 0$ . 则有

$$\begin{aligned} -\frac{L'(s, \chi_0)}{L(s, \chi_0)} &= -\frac{-\frac{1}{(s-1)^2}g(s) + \frac{1}{s-1}g'(s)}{\frac{1}{s-1}g(s)} \\ &= \frac{1}{s-1} - \frac{g'(s)}{g(s)} \rightarrow +\infty \quad (s \rightarrow 1^+). \end{aligned}$$

而对任意  $\chi \neq \chi_0$ , 有

$$\frac{L'(s, \chi)}{L(s, \chi)} \rightarrow \frac{L'(1, \chi)}{L(1, \chi)} \quad (s \rightarrow 1^+).$$

因此

$$\sum_{\substack{n=1 \\ n \equiv a \pmod{q}}}^{\infty} \frac{\Lambda(n)}{n^s} \rightarrow +\infty \quad (s \rightarrow 1^+).$$



即

$$\sum_{\substack{n=1 \\ n \equiv a \pmod{q}}}^{\infty} \frac{\Lambda(n)}{n} = +\infty. \quad (6)$$

注意到

$$\sum_p \sum_{k \geq 1} \frac{\log p}{p^k} = +\infty$$

而

$$\begin{aligned} \sum_p \sum_{k \leq 2} \frac{\log p}{p^k} &= \sum_p \log p \frac{1}{p(p-1)} \\ &\leq 2 \sum_p \frac{\log p}{p^2} \\ &\leq 2 \sum_{n=2}^{\infty} \frac{\log n}{n^2} \leq +\infty. \end{aligned}$$

且上式对  $p \equiv a \pmod{q}$  求和也是收敛的, 于是由 (6) 可知

$$\sum_{p \equiv a \pmod{q}} \frac{\log p}{p} = +\infty.$$

可知这样的  $p$  有无穷多个. □

## 4 算术级数中的素数分布 II

本章证明算术级数中的素数定理.

### 4.1 算术级数中的素数定理

我们首先引入  $\pi(y; q, a) = \sum_{\substack{p \leq y \\ p \equiv a \pmod{q}}} 1$ . 其中记号与条件同定理 3.1..

**定理 4.1** (算术级数中的素数定理). 对  $(a, q) = 1$ , 有

$$\pi(y; q, a) \sim \frac{y}{\varphi(q) \log y} \quad (y \rightarrow +\infty).$$

我们首先给出同证明素数定理类似的引理.

**引理 4.2.** 令  $\psi(y; q, a) = \sum_{\substack{p \leq y \\ p \equiv a \pmod{q}}} \Lambda(n)$ . 如果  $\lim_{y \rightarrow +\infty} \frac{\psi(y; q, a)}{y/\varphi(q)} = 1$ , 则定理 4.1..

成立, 即  $\lim_{y \rightarrow +\infty} \frac{\pi(y; q, a)}{y/\varphi(q) \log y} = 1$ .

**引理 4.3.** 若  $\int_1^{+\infty} \frac{\psi(y; q, a)\varphi(q) - y}{y^2} dy$  收敛, 则  $\lim_{y \rightarrow +\infty} \frac{\psi(y; q, a)}{y/\varphi(q)} = 1$ .

**引理 4.4.**  $\psi(y; q, a) \leq \psi(y) = O(y)$ .

**引理 4.5.**  $\int_1^{+\infty} \frac{\psi(t; q, a)\varphi(q) - t}{y^{2+s}} dt \quad (Re(s) > 0)$  可以延拓成  $Re(s) \geq 0$  上的解析函数.

上述引理以及定理的证明同素数定理的证明过程是完全平行的.

## Part II

### 附录 A 分圆多项式

本节旨在初步介绍分圆多项式并给出一些基本性质. 我们记  $\xi_n = e^{\frac{2\pi i}{n}}$ .

**定义 A.1.** 我们称

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^n (x - e^{2\pi i \frac{k}{n}})$$

为  $n$  次分圆多项式.

**注.**  $n$  次分圆多项式 (*nth cyclotomic polynomial*) 的  $n$  次来自于  $n$  次本原单位根 (*nth primitive root*), 而不是说它的次数 (*degree*) 是  $n$ .

**命题 A.2.**  $x^n - 1 = \prod_{d|n} \Phi_d(x)$

证明. 首先

$$x^n - 1 = \prod_{k=0}^{n-1} (x - \xi_n^k) = \prod_{d|n} \prod_{(k,n)=d} (x - \xi_n^k)$$

于是只需证明假设  $(k, n) = d$ , 设  $k = dj$ , 则  $\xi_n^k = \xi_n^{dj} = \xi_{\frac{n}{d}}^j$  且  $(j, \frac{n}{d}) = 1$ . 因此

$$\prod_{(k,n)=d} (x - \xi_n^k) = \prod_{j, \frac{n}{d}} (x - \xi_{\frac{n}{d}}^j) = \Phi_{\frac{n}{d}}(x)$$

而

$$\prod_{d|n} \Phi_{\frac{n}{d}}(x) = \prod_{d|n} \Phi_d(x) \quad \square$$

**推论 A.3.**  $\deg \Phi_n(x) = \varphi(n)$ , 其中  $\varphi(n)$  是 Euler 函数.

证明. 对**命题 A.2.** 式两边取次数得

$$n = \sum_{d|n} \deg \Phi_d(x)$$

应用 Möbius 变换和 Euler 函数的性质立即可得. □

**推论 A.4.**  $\Phi_n(x) \in \mathbb{Z}[x]$ .

证明. 用归纳法.  $n = 1$  时显然. 设对  $\Phi_k(x)$  ( $1 < k < n$ ) 命题都成立, 则对  $\Phi_n(x)$ , 我们有

$$\Phi_n(x) = \frac{x^n - 1}{\prod_{\substack{k|n \\ 1 < k < n}} \Phi_k(x)}$$

记  $f(x) = \prod_{\substack{k|n \\ 1 < k < n}} \Phi_k(x)$ , 我们可以做多项式的带余除法

$$x^n - 1 = f(x)g(x) + r(x)$$

其中  $r(x) = 0$  或  $\deg r(x) < \deg f(x)$ .

则  $r(x) = f(x)(\Phi(x) - g(x))$ . 若  $r(x) \neq 0$ , 则  $\Phi(x) \neq g(x)$ , 于是  $\deg r(x) \geq \deg f(x)$ , 矛盾. 于是  $r(x) = 0$ ,  $\Phi(x) = g(x) \in \mathbb{Z}[x]$  且是首一的.  $\square$

**定理 A.5.**  $\Phi_n(x)$  不可约且是任意  $n$  次本原单位根的极小多项式.

## 附录 B 分析学

本附录旨在回顾正文中可能用到的分析学背景知识. 附录中的结论几乎不会给出证明, 读者可以自行参考分析学的相关著作如 [2],[3].

### B.1 解析延拓

**定理 B.1.** 设  $f, g$  是在一个区域  $\Omega \subset \mathbb{C}$  上的全纯函数, 并且在某个非空开子集  $S \subset \Omega$  上,  $f(z) = g(z) \forall z \in S$ , 则  $f(z) = g(z) \forall z \in \Omega$

**注.** 更一般地,  $S$  可以替换成聚点在  $\Omega$  内的 (不同点构成的) 点列.

**定义 B.2.** 给定函数  $f, F$  使得它们分别在区域  $\Omega, \Omega'$  上解析, 并且  $\Omega \subset \Omega'$ . 如果  $f(z) = F(z) \forall z \in \Omega$ , 我们就称  $F$  是  $f$  到  $\Omega'$  上的解析延拓.

如果解析延拓存在, **定理 B.1** 保证了解析延拓的唯一性.

事实上, 正文中出现的大多是延拓成亚纯函数, 不难证明亚纯延拓也是唯一的.

### B.2 Poisson 求和公式

Poisson 求和公式或可归于调和分析, 欲探求具体细节和一般形式的读者可查阅 [4].

**定义 B.3.** 设  $f: \mathbb{R} \rightarrow \mathbb{C}$  是  $L^1$  函数 (即可积函数).  $f$  的 Fourier 变换  $\hat{f}: \mathbb{R} \rightarrow \mathbb{C}$  由

$$\hat{f}(\xi) = \int_{-\infty}^{+\infty} f(x) e^{-2\pi i x \xi} dx$$

给出. 这是一致连续的.

**定义 B.4.** 我们定义 Schwarz 函数空间如下

$$\mathcal{S}(\mathbb{R}) = \{f: \mathbb{R} \rightarrow \mathbb{C} \mid f \in C^\infty(\mathbb{R}), |f^{(n)}(t)| = o(|t|^{-c})(t \rightarrow \pm\infty) \forall n \in \mathbb{N}_{\geq 0}, c \in \mathbb{R}\}$$

**引理 B.5.** 设  $f, g \in \mathcal{S}(\mathbb{R})$ . 则有

1.  $\hat{f}, \hat{g} \in \mathcal{S}(\mathbb{R})$ .

2.  $\hat{f}(t) = \hat{f}(-t)$ .

3. 对卷积

$$(f \star g)(t) = \int_{-\infty}^{\infty} f(t-u)g(u)du$$

有

$$\widehat{f \star g}(s) = \hat{f}(s)\hat{g}(s).$$

**定理 B.6** (Poisson 求和公式). 若  $f \in \mathcal{S}(\mathbb{R})$ , 则

$$\sum_{n \in \mathbb{Z}} f(n) = \sum_{n \in \mathbb{Z}} \hat{f}(n).$$

## 附录 C “初等”方法

本附录将介绍一些只用到数学分析的方法, 主要内容都是关于均阶估计的.

### C.1 Dirichlet 除数问题

考虑除数函数  $d(n) = \sum_{m|n} 1$ .

$$\begin{aligned} \sum_{n \leq x} d(n) &= \sum_{n \leq x} \sum_{m|n} 1 \\ &\stackrel{(n=mq)}{=} \sum_{\substack{m, q \\ mq \leq x}} 1 = \sum_{m \leq x} \sum_{q \leq \frac{x}{m}} 1 \\ &= \sum_{m \leq x} \left[ \frac{x}{m} \right] = \sum_{m \leq x} \left( \frac{x}{m} - \left\{ \frac{x}{m} \right\} \right) \\ &= x \sum_{m \leq x} \frac{1}{m} - \sum_{m \leq x} \left\{ \frac{x}{m} \right\} \end{aligned}$$

注意到

$$\sum_{m \leq x} \frac{1}{m} = \log x + \gamma + O\left(\frac{1}{x}\right)$$

其中  $\gamma$  是 Euler 常数.

于是

$$\sum_{n \leq x} d(n) = x \log x + O(x).$$

为了改进上述结果, 观察上述对  $mq \leq x$  的求和, 我们给出它的几何描述, 即第一象限的双曲线同坐标轴之间的区域有多少整点. 这启发我们考虑如下等式

$$\begin{aligned} \sum_{n \leq x} d(n) &= 2 \sum_{m \leq x} \left[ \frac{x}{m} \right] - [\sqrt{x}]^2 \\ &= 2(x(\log \sqrt{x} + \gamma + O(\frac{1}{\sqrt{x}})) - \sum_{m \leq \sqrt{x}} \left\{ \frac{x}{m} \right\}) - (\sqrt{x} - \{\sqrt{x}\})^2 \\ &= x \log x + (2\gamma - 1)x + O(\sqrt{x}). \end{aligned}$$

注. 比较上述结果, 我们不难得出

$$\sum_{n \leq x} \left\{ \frac{x}{n} \right\} = (1 - \gamma)x + O(\sqrt{x}).$$

上面的办法可以推广到一般的数论函数即为所谓 Dirichlet 双曲律,

**定理 C.1** (Dirichlet 双曲律). 设  $f, g$  是两个数论函数, 其部分和函数分别记为  $F, G$ . 于是对任意的  $1 \leq y \leq x$  有

$$\sum_{md \leq x} f(m)g(d) = \sum_{d \leq y} g(d)F(x/d) + \sum_{m \leq x/y} f(m)G(x/m) - F(x/y)G(y).$$

证明是显然的.

此外, 从上面的过程中我们可以总结一套通行的做法, 考虑一般的数论函数  $f: \mathbb{N} \rightarrow \mathbb{C}$ ,

$$\begin{aligned} \sum_{n \leq x} \sum_{d|n} f(d) &\stackrel{(n=dq)}{=} \sum_{d \leq x} f(d) \left[ \frac{x}{d} \right] \\ &= \sum_{d \leq x} f(d) \frac{x}{d} - \sum_{d \leq x} f(d) \left\{ \frac{x}{d} \right\} \\ &= x \sum_{d \leq x} \frac{f(d)}{d} + O\left(\sum_{d \leq x} |f(d)|\right). \end{aligned}$$

## C.2 Chebyshev 估计

本节的主要结果是下面的定理:

**定理 C.2** (Chebyshev). 对于  $x > 2$ , 我们有

1.  $\psi(x) \asymp x$ ,
2.  $\varphi(x) \asymp x$ ,
3.  $\pi(x) \asymp \frac{x}{\log x}$ .



证明. 首先证明存在正常数  $c_1, c_2$  使得

$$c_1 x \leq \psi(x) \leq c_2 x. \quad (7)$$

我们考虑

$$\begin{aligned} T(x) &:= \sum_{n \leq x} \log n = \sum_{n \leq x} \sum_{d|n} \Lambda(d) \\ &\stackrel{(n=dq)}{=} \sum_{\substack{d, q \\ dq \leq x}} \Lambda(d) = \sum_{d \leq x} \sum_{q \leq \frac{x}{d}} \Lambda(d) \\ &= \sum_{n \leq x} \psi\left(\frac{x}{n}\right) = \sum_{n=1}^{\infty} \psi\left(\frac{x}{n}\right) \end{aligned}$$

不难看出  $T(x) = \sum_{n \leq x} \log n = x \log x - x + O(\log x)$ . 回忆对于单调递减趋于 0 的数列  $\{a_n\}$ , 有

$$a_1 - a_2 \leq \sum_{n=1}^{\infty} (-1)^{n-1} a_n \leq a_1 - a_2 + a_3$$

我们将其应用到  $\psi(\frac{x}{n})$  上. 首先

$$\sum_{n=1}^{\infty} (-1)^{n-1} \psi\left(\frac{x}{n}\right) = \sum_{n=1}^{\infty} \psi\left(\frac{x}{n}\right) - 2 \sum_{n=1}^{\infty} \psi\left(\frac{x}{2n}\right) = T(x) - 2T\left(\frac{x}{2}\right),$$

于是

$$\psi(x) - \psi\left(\frac{x}{2}\right) \leq T(x) - 2T\left(\frac{x}{2}\right) \leq \psi(x) - \psi\left(\frac{x}{2}\right) + \psi\left(\frac{x}{3}\right).$$

我们有一组不等式

$$\psi\left(\frac{x}{2^k}\right) - \psi\left(\frac{x}{2^{k+1}}\right) \leq \frac{x}{2^k} \log 2 + O(\log \frac{x}{2^k}) \quad (k = 1, 2, 3, \dots)$$

把它们加起来可得

$$\psi(x) \leq (2 \log 2)x + O((\log x)^2).$$

另一边, 我们有

$$\begin{aligned} \psi(x) &\geq \psi(x) - \psi\left(\frac{x}{2}\right) \geq T(x) - 2T\left(\frac{x}{2}\right) - \psi\left(\frac{x}{3}\right) \\ &\geq \frac{\log 2}{3}x + O(\log x) \end{aligned}$$

其余部分效仿定理 1.6. 即可. □

注. *Chebyshev* 利用更精细的办法, 得到 (5) 中的常数大致分别为  $c_1 = 0.92\dots, c_2 = 1.10\dots$ .

现在我们可以证明 Bertrand 假设, 即下述定理

**定理 C.3** (Bertrand). 对任意  $n \in \mathbb{Z}^+$ ,  $(n, 2n]$  至少包含一个素数.

## 附录 D $\pi$ 是无理数

**命题 D.1.**  $\pi$  是无理数

证明. 用反证法. 假设  $\pi = \frac{a}{b}$ ,  $a, b \in \mathbb{Z}^+$ . 引入

$$f(x) = f_n(x) = \frac{x^n(a - bx)^n}{n!} \quad n \in \mathbb{Z}^+$$

不难看出  $f(0) = f(\pi) = 0$ ,  $f(x) = f(\pi - x)$ .

**断言.** 对每一个  $j \in \mathbb{Z}^+$ ,  $f^{(j)}(0) \in \mathbb{Z}$ . 下面我们证明断言. 我们可以将  $f(x)$  的分子部分写成

$$x^n(a - bx)^n = c_n x^n + \cdots + c_{2n} x^{2n}$$

其中  $c_n, \dots, c_{2n} \in \mathbb{Z}$ .

当  $j < n$  时,  $f^{(j)}(0) = 0 \in \mathbb{Z}$ .

当  $j \geq n$  (不妨  $n \leq 2n$ ) 时, 考虑  $(x^j)^{(j)} = j!$ , 有

$$\left( \frac{c_j x^j}{n!} \right)^{(j)} = \frac{c_j j!}{n!} \in \mathbb{Z}$$

因此断言成立. 同理我们有  $\forall j \in \mathbb{Z}^+$ ,  $f^{(j)}(\pi) \in \mathbb{Z}$ .

下引入

$$\begin{aligned} F(x) &= f(x) - f^{(2)}(x) + f^{(4)}(x) + \cdots + (-1)^n f^{(2n)}(x) \\ &= \sum_{j=0}^n (-1)^j f^{(2j)}(x). \end{aligned}$$

约定  $f^{(0)}(x) = f(x)$ . 于是  $f(x) = F(x) + F^{(2)}(x)$ . 观察到

$$\begin{aligned} (F'(x) \sin x - F(x) \cos x)' &= F''(x) \sin x + F(x) \sin x \\ &= f(x) \sin x. \end{aligned}$$

于是

$$\begin{aligned} \int_0^\pi f(x) \sin x &= (F'(x) \sin x - F(x) \cos x) \Big|_0^\pi \\ &= F(\pi) + F(0) \in \mathbb{Z}^+ \end{aligned}$$

而当  $0 < x < \pi$  时,  $f(x) \sin x > 0$ . 于是有

$$1 \leq \int_0^\pi f(x) \sin x \leq \frac{\pi^{n+1} a^n}{n!} \rightarrow 0 \quad (n \rightarrow \infty)$$

矛盾.

□

## 参考文献

- [1] 冯克勤. 代数数论入门.
- [2] G. 特伦鲍姆. 解析与概率数论导引. 陈华一 译
- [3] 朱富海. 有限群表示论
- [4] Serge Lvovski. Principles of Complex Analysis.
- [5] Elias M.Stein. Complex Analysis.
- [6] Loukas Grafakos. Classical Fourier Analysis. GTM249.
- [7] J-P Serre. Linear Representations of Finite Groups. GTM42.