数论基础

Lectured by Prof. Zhao Lilu

Adaus

2022 年 3 月 11 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.

Adaus

目录

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,

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

$$= \prod_p (1-\frac{1}{p^s})^{-1} \tag{2}$$

而

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

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*

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

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,

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

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

$$a(\text{mod } b) := \{n \in \mathbb{Z} | n \equiv a(\text{mod } b)\}$$

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 $\forall a \in A, \exists b \in \mathbb{Z}^+$, s.t. $a(\text{mod } b) \subset A$.

验证这是一个拓扑是容易的.

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

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, $\forall a \in \bigcup_\lambda A_\lambda, \exists b \in \mathbb{Z}^+$, s.t. $a(\text{mod } b) \subset \bigcup_\lambda A_\lambda$.

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

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

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

因此

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

而

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

故

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

等式右边不是有限交 $\square$

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

假设只有有限个素数 $p_1, \ldots, p_m \equiv 1 (\bmod q)$

取 t 为充分大的正整数, 考虑 $\Phi_q(tqp_1 \ldots p_m)$ 的素因子 p, 且 $p \neq p_1, \ldots, p \neq p_m, p \nmid q$. 记 $a = tqp_1 \ldots p_m$, 于是 $p | \Phi_q(a) | a^{p-1} - 1$.

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

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

则

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

因此, 代入 a 有

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

而 $a^k \equiv 1 (\bmod p)$, 于是

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

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 $p \equiv 1 (\bmod q)$. 与假设矛盾. □

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 $\Lambda : \mathbb{Z}^+ \to \mathbb{R}$

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

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

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

   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

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

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

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

证明. 由**命题 1.4.**, 我们有

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

于是 $\dfrac{\Lambda(n)}{n^s} \leq \dfrac{\log n}{n^s}$ □

至此, 我们粗略的看看下列两个无穷级数的乘积.

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

这几乎得到了 $\sum_{n=1}^{\infty} \dfrac{\Lambda(n)}{n^s}$ 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. $\pi(x) \sim \dfrac{x}{\log x}$
2. $\theta(x) \sim x$
3. $\psi(x) \sim x$

证明. $(2 \Leftrightarrow 3)$:

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

于是 $\dfrac{\psi(x)}{x} - \dfrac{\theta(x)}{x} \to 0 \ (x \to +\infty)$

$(1 \Leftrightarrow 2)$ 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 $Re(s) < 0$ 的范围内所有的零点是 $-2, -4, \ldots$, 即所有负偶数, 且它们是单零点.*

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

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

$$\psi(x_n)\geq c_1x_n$$

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

$$\psi(y_n)\leq c_2y_n$$

若第一种情况成立, 则

$$\begin{aligned}\int_{x_n}^{c_1x_n}\frac{\psi(x)-x}{x^2}dx &\geq \int_{x_n}^{c_1x_n}\frac{c_1x_n-x}{x^2}dx\\ &= c_1-1-\log c_1>0\end{aligned}$$

这同假设矛盾. 类似地, 若第二种情况成立, 则

$$\begin{aligned}\int_{c_2y_n}^{y_n}\frac{\psi(x)-x}{x^2}dx &\leq \int_{c_2y_n}^{y_n}\frac{c_2y_n-x}{x^2}dx\\ &= -c_2+1+\log c_2<0\end{aligned}$$

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 $Re(s)>1$ 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

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

即 $\zeta(s) \neq 0$. □

注. 现在回过头看第一节的结果, 我们有当 $Re(s) > 1$ 时,

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

定理 2.2. 当 $Re(s) > 1$ 时, 我们有

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

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

证明. 当 $Re(s) > 2$ 时, 我们有

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

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 $\dfrac{s}{s-1} - s\displaystyle\int_1^{+\infty}\{x\}x^{-s-1}dx$ 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 Γ 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 Γ 延拓成复平面上的亚纯函数且只有单极点 $s = 0, -1, -2, \ldots$, 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 $\theta(x) = \displaystyle\sum_{-\infty}^{+\infty} e^{-n^2 x\pi} (= 1 + 2\sum_{n=1}^{\infty} e^{-n^2 x\pi})$.

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

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.

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

将积分拆开如下

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

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

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 $\zeta(0)\neq 0$, $\zeta(-2)=\zeta(-4)=\cdots=0$ 是单零点 (有时称作平凡零点).

推论 2.7. $Re(s) < 0$ 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. $\zeta(1+it) \neq 0$ $(t \in \mathbb{R})$.

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

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

于是

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

考察

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

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

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

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

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

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

□

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

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

记 $f(x)=\prod\limits_{\substack{k|n\\1<k<n}}\Phi_k(x)$, 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 Ω 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 Ω, Ω' 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 Ω' 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 $f : \mathbb{R} \to \mathbb{C}$ 是 L^1 函数 (即可积函数). f 的 *Fourier* 变换 $\hat{f} : \mathbb{R} \to \mathbb{C}$ 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

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

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. $\hat{\hat{f}}(t) = f(-t)$.
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 $d(n) = \sum_{m|n} 1$.

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

注意到

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

其中 γ 是 Euler 常数.

于是

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

为了改进上述结果, 观察上述对 $mq\le x$ 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

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

注. 比较上述结果, 我们不难得出

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

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, 感兴趣的读者不妨自行查阅相关资料.

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 $f:\mathbb{N}\to\mathbb{C}$,

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

C.2 Chebyshev 估计

本节的主要结果是下面的定理:

定理 C.1 (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

$$c_1x\le\psi(x)\le c_2x. \tag{5}$$

我们考虑

$$
\begin{aligned}
T(n) := \sum_{n\le x} \log x &= \sum_{n\le x}\sum_{d\mid n}\Lambda(d) \\
&\xlongequal{(n=dq)} \sum_{\substack{d,q\\ dq\le x}} \Lambda(d) = \sum_{d\le x}\sum_{q\le \frac{x}{d}}\Lambda(d) \\
&= \sum_{n\le} \psi(\frac{x}{n}) = \sum_{n=1}^{\infty}\psi(\frac{x}{n})
\end{aligned}
$$

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

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

我们将其应用到 $\psi(\frac{x}{n})$ 上. 首先

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

于是

$$
\psi(x) - \psi(\frac{x}{2}) \le T(x) - 2T(\frac{x}{2}) \le \psi(x) - \psi(\frac{x}{2}) + \psi(\frac{x}{3}).
$$

我们有一组不等式

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

把它们加起来可得

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

另一边, 我们有

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

其余部分效仿**定理 1.6.** 即可. $\square$

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

现在我们可以证明 Bertrand 假设, 即下述定理

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

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] Serge Lvovski. Principles of Complex Analysis.

[4] Elias M.Stein. Complex Analysis.

[5] Loukas Grafakos. Classical Fourier Analysis. GTM249.