中国科学: 数学 2024 年 第 54 卷 第 9 期: 1197 ~ 1206
SCIENTIA SINICA Mathematica
论 文

p- 进解析簇上的 zeta 函数

献给陆洪文教授 85 寿辰

曹炜[1*], 万大庆[2]

1. 闽南师范大学数学与统计学院, 漳州 363000;
2. Department of Mathematics, University of California at Irvine, Irvine, CA 92697, USA
E-mail: caow2286@mnnu.edu.cn, dwan@math.uci.edu

收稿日期: 2023-05-16; 接受日期: 2023-06-22; 网络出版日期: 2023-10-30; * 通信作者
国家自然科学基金 (批准号: 11871291) 和福建省自然科学基金 (批准号: 2022J02046) 资助项目

摘要 本文引进定义在 p- 进数域上 p- 进解析簇的 zeta 函数, 该 zeta 函数计算解析簇上 Techmüller 点的个数. 利用 Witt 向量的加法运算、Dwork 有理性定理以及 Hilbert 基定理, 本文证明该 zeta 函数是一个有理函数. 本文还提出若干问题以促进对这类新的 zeta 函数的研究.

关键词 zeta 函数 p- 进解析簇 Witt 环 Teichmüller 提升

MSC (2020) 主题分类 11D88, 11S40, 13F35, 11T55

1 引言

设 p 是一个有理素数, $q=p^h$, 其中 h 是一个正整数. 设 $\mathbb{F}_q$ 为 q 元有限域. 设 $\mathbb{Q}_p$ 为 p- 进有理数域, $\mathbb{Q}_q$ 为 $\mathbb{Q}_p$ 的一个非分歧扩张, 其剩余域为 $\mathbb{F}_q$. 更一般地, 设 K 为 $\mathbb{Q}_p$ 的一个有限 (可能分歧) 扩张, 其剩余域为 $\mathbb{F}_q$, 此时 K 是 $\mathbb{Q}_q$ 的一个完全分歧的有限扩张. 用 $\mathbb{Z}_q$ (或 $\mathbb{Z}_K$) 表示 $\mathbb{Q}_q$ (或 K) 中的整数环. 用 $\mathbb{Z}_K\langle\langle x_1,\dots,x_n\rangle\rangle$ 表示 $\mathbb{Z}_K$ 上 p- 进收敛的 n 元幂级数环, 即其中幂级数的系数在 $\mathbb{Z}_K$ 上且收敛于 0. 令 V 表示由下列多项式方程组确定的 p- 进解析簇:

$$f_1(x_1,\dots,x_n)=\cdots=f_s(x_1,\dots,x_n)=0,$$

其中 $f_i(x_1,\dots,x_n)\in\mathbb{Z}_K\langle\langle x_1,\dots,x_n\rangle\rangle$ 是 p- 进收敛的幂级数. 更多关于 p- 进数域和 p- 进分析的内容, 可参见经典的教材 [6].

用 $\mathcal{T}_q$ 表示 $\mathbb{F}_q$ 在 $\mathbb{Z}_q$ 中的 Teichmüller 提升, 即 $\mathcal{T}_q=\{x\in\mathbb{Z}_q\mid x^q=x\}=\{0\}\cup\mu_{q-1}$, 其中 μ_{q-1} 表示由 $\mathbb{Z}_q$ 中 $q-1$ 次单位根构成的群. 本文感兴趣的是计算 V 中 Techmüller 点的个数, 即 V 中的点 $(x_1,\dots,x_n)$, 其中 $x_i\in\mathcal{T}_{q^e}$, e 是一个正整数. V 中这样的点也称为 V 中的 $\mathcal{T}_{q^e}$- 有理点. 下文用 $\mathbb{N}$ 表示正整数集, 并简记 $X:=(x_1,\dots,x_n)$.

英文引用格式: Cao W, Wan D Q. Zeta functions of p-adic analytic varieties (in Chinese). Sci Sin Math, 2024, 54: 1197–1206, doi: 10.1360/SSM-2023-0143

定义 1.1 对于 $e \in \mathbb{N}$, 令

$$N_e(V) = \#\{X \in \mathcal{T}_{q^e}^n \mid f_1(X) = \cdots = f_s(X) = 0\},$$

则 $\mathbb{Z}_K$ 上关于 V 的 zeta 函数定义为

$$Z(V,T) = \exp\left(\sum_{e=1}^{\infty} \frac{T^e}{e} N_e(V)\right) \in 1 + T\mathbb{Q}[[T]].$$

显而易见, $N_e(V)$ 为 V 中 $\mathcal{T}_{q^e}$- 有理点的个数. 如同其他 zeta 函数, $Z(V,T)$ 也可定义为用闭的 Teichmüller 点表示的 Euler 乘积, 它们是 $\mathcal{T}_{q^e}$- 有理点的 Galois 轨道, 其中 $e \in \mathbb{N}$. 由此可得 $Z(V,T) \in 1 + T\mathbb{Z}[[T]]$. 一个自然的问题是, 当 e 变化时, 序列 $N_e(V)$ 是否有递推的公式. 更准确地问, zeta 函数 $Z(V,T)$ 是否是一个关于 T 的有理函数. 本文的主要结果对该问题给出了一个肯定的回答, 即证明了 $Z(V,T)$ 是一个关于 T 的有理函数. 特别地, 序列 $N_e(V)$ $(e = 1, 2, \ldots)$ 满足一个线性的递推关系.

定理 1.1 (定理 4.3) $Z(V,T) \in \mathbb{Q}(T)$.

证明上述定理的策略是, 先将定义在 p- 进数域上的 zeta 函数归约为定义在有限 Witt 环上的 zeta 函数, 再进一步将其归约为定义在有限域上的 zeta 函数, 最后利用 Dwork 有理性定理和 Hilbert 基定理得到定理的结论. 为此, 需要引进定义在有限 Witt 环上的 V 的有限层次的 zeta 函数序列. 固定一个正整数 $m \in \mathbb{N}$.

定义 1.2 对于 $e \in \mathbb{N}$, 令

$$N_{e,m}(V) = \#\{X \in \mathcal{T}_{q^e}^n \mid f_1(X) \equiv \cdots \equiv f_s(X) \equiv 0 \pmod{p^m}\},$$

则 $\mathbb{Z}_K/p^m\mathbb{Z}_K$ 上关于 V 的 zeta 函数定义为

$$Z_m(V,T) = \exp\left(\sum_{e=1}^{\infty} \frac{T^e}{e} N_{e,m}(V)\right).$$

该 zeta 函数计算 V 中 "近似" Teichmüller- 有理点的个数. 这种 "近似" 随着 m 的增大而愈来愈佳. 由此可得到一个有限层次的 zeta 函数的无限序列: $Z_m(V,T)$, $m = 1, 2, \ldots$ 而 zeta 函数 $Z(V,T)$ 则可以看作是当 $m = \infty$ 时的无限层次的 zeta 函数, 它是有限层次的 zeta 函数当 m 趋于无穷时的极限. 有两个关于有限层次的 zeta 函数 $Z_m(V,T)$ 的重要性质.

定理 1.2 (定理 4.1) 对于任意 $m \in \mathbb{N}$, 都有 $Z_m(V,T) \in \mathbb{Q}(T)$.

定理 1.3 (定理 4.2) 对于序列 $Z_m(V,T)$, $m \in \mathbb{N}$, 当 m 充分大时会变得稳定, 即存在一个依赖于 V 的正整数 M 使得 $Z_M(V,T) = Z_{M+1}(V,T) = Z_{M+2}(V,T) = \cdots = Z(V,T)$.

沿用文献 [1] 中的术语, 集合 $\mathcal{T}_q^n$ 称为 Teichmüller 盒子, 更一般地, $\mathbb{Z}_q^n$ 中的一个盒子 $\mathcal{B}$ 被定义为 $\mathbb{F}_q^n$ 在 $\mathbb{Z}_q^n$ 中的一个完全代表系. 可将上述关于 Teichmüller 盒子的定义和定理推广到一般的盒子上去.

本文余下内容结构如下. 第 2 节将分歧的 $\mathbb{Z}_K$- 情形归约为非分歧的 $\mathbb{Z}_q$- 情形. 第 3 节回顾关于 Witt 环的一些基本的预备知识. 第 4 节给出关于 Teichmüller 盒子的主要结果及其证明; 同时提出若干问题, 以促进未来对这类新的 zeta 函数的研究. 第 5 节给出关于一般盒子的类似结果.

2 归约到非分歧情形

设 $a, b \in \mathbb{R}$, 记 $[a,b] := \{x \in \mathbb{Z} \mid a \leqslant x \leqslant b\}$, 并记 $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$. 设 K 为 $\mathbb{Q}_p$ 的一个有限扩张, 其剩余域为 $\mathbb{F}_q$, 用 $\mathbb{Z}_K$ 表示 K 中的整数环, π 为其一致化子 (uniformizer), 分歧指数为 r. 用 v_p 表示

$\mathbb{Z}_K$ 上满足 $v_p(p)=1$ 的 p- 进赋值. 则有 $v_p(\pi)=\frac{1}{r}$, 且可得 $\mathbb{Z}_K$ 关于自由 $\mathbb{Z}_q$- 模的直和分解

$$\mathbb{Z}_K=\mathbb{Z}_q[\pi]=\mathbb{Z}_q+\mathbb{Z}_q\pi+\cdots+\mathbb{Z}_q\pi^{r-1}.$$

令

$$\mathbb{Z}_K\langle\langle X\rangle\rangle=\left\{\sum_{u\in\mathbb{N}_0^n}a_uX^u\,\middle|\,a_u\in\mathbb{Z}_K,\ \lim_{|u|\to\infty}a_u=0\right\}.$$

$\mathbb{Z}_K\langle\langle X\rangle\rangle$ 称为系数在 $\mathbb{Z}_K$ 中收敛的 n 元幂级数环. 设 $f(X)\in\mathbb{Z}_K\langle\langle X\rangle\rangle$, 可将其唯一地表示为

$$f(X)=\sum_{i=0}^{r-1}\pi^if_i(X),$$

其中每个 $f_i(X)\in\mathbb{Z}_q\langle\langle X\rangle\rangle$ 是一个系数在更小的非分歧的环 $\mathbb{Z}_q$ 中收敛的幂级数.

引理 2.1 设 $X\in\mathbb{Z}_{q^e}^n$, 则有 $f(X)=0$ 当且仅当

$$f_0(X)=f_1(X)=\cdots=f_{r-1}(X)=0.$$

证明 充分性是显然的. 下面证明必要性. 假设 $X\in\mathbb{Z}_{q^e}^n$ 且有 $f(X)=0$. 接下来证明 $f_0(X)=\cdots=f_{r-1}(X)=0$. 因为每个 $f_i(X)$ 的系数在 $\mathbb{Z}_q$ 中, 所以 $f_i(X)\in\mathbb{Z}_{q^e}$, 其中 $\mathbb{Z}_{q^e}$ 在 $\mathbb{Z}_q$ 上非分歧. 假设存在某个 $j\in[0,r-1]$, 使得 $f_j(X)\neq0$, 则有 $v_p(f_j(X))\in\mathbb{Z}$. 注意到当 $i\in[0,r-1]$ 时, p- 进赋值 $v_p(\pi^i)=\frac{i}{r}$ 模 $\mathbb{Z}$ 是互不相同的. 由此可知, 当 $i\in[0,r-1]$ 且 $f_i(X)\neq0$ 时, 有限个 p- 进赋值 $v_p(\pi^if_i(X))$ 模 $\mathbb{Z}$ 也是互不相同的. 故有

$$c:=\min_{0\leqslant i\leqslant r-1,f_i(X)\neq0}v_p(\pi^if_i(X))<\infty,$$

其中最小值在某个唯一的 i 达到. 由此可得

$$v_p(f(X))=v_p\left(\sum_{i=0}^{r-1}\pi^if_i(X)\right)=c<\infty.$$

从而有 $f(X)\neq0$. 这与 $f(X)=0$ 的假设矛盾. 因此, 对于所有的 $i\in[0,r-1]$, 均有 $f_i(X)=0$. □

上面的引理说明, 如果只关心 $\mathbb{Z}_{q^e}^n$- 有理点 (特别地, $\mathcal{T}_{q^e}$- 有理点), 则每个系数在 $\mathbb{Z}_K$ 中收敛的幂级数可替换为 r 个系数在 $\mathbb{Z}_q$ 中收敛的幂级数. 因此, 为证明 $Z(V,T)$ 的有理性, 可将分歧的 $\mathbb{Z}_K$- 情形归约为非分歧的 $\mathbb{Z}_q$- 情形. 对于有限层次的 zeta 函数 $Z_m(V,T)$ 的有理性, 也有类似的归约. 我们需要下面的引理 2.1 在有限层次的版本.

引理 2.2 设 $m\in\mathbb{N}$, $X\in\mathbb{Z}_{q^e}^n$. 则有 $f(X)\equiv0\pmod{p^m}$ 当且仅当

$$f_0(X)\equiv f_1(X)\equiv\cdots\equiv f_{r-1}(X)\equiv0\pmod{p^m}.$$

证明 只证明必要性. 设 $X\in\mathbb{Z}_{q^e}^n$ 且 $f(X)\equiv0\pmod{p^m}$. 若有某个 $f_j(X)\not\equiv0\pmod{p^m}$, 则

$$c_m:=\min_{0\leqslant i\leqslant r-1,f_i(X)\not\equiv0\pmod{p^m}}v_p(\pi^if_i(X))\leqslant m-1+\frac{r-1}{r}<m,$$

其中最小值在某个唯一的 i 达到. 由此可得

$$v_p(f(X))=v_p\left(\sum_{i=0}^{r-1}\pi^if_i(X)\right)=c_m<m.$$

从而有 $f(X)\not\equiv0\pmod{p^m}$. 这与 $f(X)\equiv0\pmod{p^m}$ 的假设矛盾. 因此, 对于所有的 $i\in[0,r-1]$, 均有 $f_i(X)\equiv0\pmod{p^m}$. □

从现在起, 假设 $\mathbb{Z}_K=\mathbb{Z}_q$ 是非分歧的, 其剩余域为 $\mathbb{F}_q$.

3 预备知识

首先回顾经典的 Witt 和 Teichmüller 关于 p- 典型 (p-typical) Witt 向量的构造及其简单性质 (参见文献 [8,10]). 通过 p- 典型 Witt 向量, 可以从特征为 p 的完全域 F 过渡到剩余域为 F 且商域特征为 0 的非分歧的完全离散赋值环.

设 R 为一个含幺元的交换环, 并记 $\mathbb{N}_0 = \{0\} \cup \mathbb{N}$. 则 R 上 p- 典型 Witt 环的集合为 $W(R) = R^{\mathbb{N}_0} = \{(a_0, a_1, \dots) \mid a_i \in R\}$. 设 $n \in \mathbb{N}_0$, 则第 n 个 Witt 多项式定义为

$$\omega_n(x_0, x_1, \dots, x_n) := x_0^{p^n} + px_1^{p^{n-1}} + \cdots + p^n x_n. \tag{3.1}$$

利用 Witt 多项式, 可以构建所谓的 "幽灵" 映射

$$\omega : W(R) \to R^{\mathbb{N}_0}, \quad \boldsymbol{a} = (a_0, a_1, \dots) \mapsto \omega(\boldsymbol{a}) = (\omega_0(a_0), \omega_1(a_0, a_1), \dots), \tag{3.2}$$

其中 $\omega_n(a_0, a_1, \dots, a_n)$ 称为 $\boldsymbol{a}$ 的第 n 个幽灵分量. R 上的 p- 典型 Witt 环 $W(R)$ 中的对应分量之间的加法和乘法是通过幽灵分量定义的, 这是由 Witt [10] 发现的. 用 $\oplus$ 和 $\odot$ 分别表示环 $W(R)$ 中加法和乘法.

定理 3.1 [10] 存在两族整系数的多项式

$$S_n(x_0, y_0; x_1, y_1; \dots; x_n, y_n), \quad M_n(x_0, y_0; x_1, y_1; \dots; x_n, y_n), \quad n \in \mathbb{N}_0,$$

使得对于任意 $\boldsymbol{a} = (a_0, a_1, \dots), \boldsymbol{b} = (b_0, b_1, \dots) \in W(R)$, 都有

(i) $\boldsymbol{a} \oplus \boldsymbol{b} = (S_0(a_0, b_0), S_1(a_0, b_0; a_1, b_1), \dots)$;

(ii) $\boldsymbol{a} \odot \boldsymbol{b} = (M_0(a_0, b_0), M_1(a_0, b_0; a_1, b_1), \dots)$;

(iii) $\omega(\boldsymbol{a} \oplus \boldsymbol{b}) = \omega(\boldsymbol{a}) + \omega(\boldsymbol{b})$, $\omega(\boldsymbol{a} \odot \boldsymbol{b}) = \omega(\boldsymbol{a})\omega(\boldsymbol{b})$.

如果 p 在环 R 中可逆, 则由 (3.2) 诱导的环同态 $\omega : W(R) \to R^{\mathbb{N}_0}$ 是一个同构映射, 即有 $W(R) \cong R^{\mathbb{N}_0}$. 显然, 多项式 S_n 和 M_n 由 Witt 向量的前 $n+1$ 个分量决定, 且它们的系数不依赖于环 R. 设 $r \in \mathbb{N}$, $j \in [1, r]$, 记 $X_j = (x_{0j}, \dots, x_{nj}, \dots)$ 及

$$X_1 \oplus \cdots \oplus X_r = (S_0^{(r)}, \dots, S_n^{(r)}, \dots). \tag{3.3}$$

引理 3.1 [1] $S_n^{(r)}$ 是一个变量为 x_{ij} ($i \in [0, n]$, $j \in [1, r]$) 的整系数多项式. 如果对于 $i \in [0, n]$, $j \in [1, r]$, 令加权次数 $\mathrm{wt}(x_{ij}) = p^i$, 则 $S_n^{(r)}$ 是一个加权次数为 p^n 的加权齐次多项式. 更一般地, 对于 $i \in [0, n]$, $j \in [1, r]$, $d \in \mathbb{N}$, 若加权次数 $\mathrm{wt}(x_{ij}) \leqslant dp^i$, 则 $S_n^{(r)}$ 的加权次数小于等于 dp^n.

注 3.1 $S_n^{(r)}$ 的加权次数不依赖于 r. 为了明确表示 $S_n^{(r)}$ 中的变量及其顺序, 记

$$S_n^{(r)} := S_n^{(r)}(x_{01}, \dots, x_{0r}; x_{11}, \dots, x_{1r}; \dots; x_{n1}, \dots, x_{nr}).$$

现设 R 是一个特征为 p 的完全环, 这意味着 Frobenius 映射 $\phi : a \mapsto a^p$ 是一个自同构. 用 $W(R)$ 表示 R 上的 Witt 环. 则 Teichmüller 提升定义为

$$\tau : R \hookrightarrow W(R), \quad a \mapsto \tau(a) = (a, 0, 0, \dots),$$

这里 $\tau(a)$ 称为元素 a 的 Teichmüller 表示. 令

$$K_R := \{\tau(a_0) + \tau(a_1)p + \tau(a_2)p^2 + \cdots \mid a_i \in R, i = 0, 1, 2, \dots\},$$

则 K_R 成为一个在通常的加法和乘法下与 $W(R)$ 同构的 p- 进环. 进一步地, 如果 R 是一个域, 则 K_R 是一个零特征的完全离散赋值环, 其剩余域为 R, 最大理想为 pK_R. $W(R)$ 中的每一个元素 $(a_0,a_1,a_2,\dots)$ 均可唯一地表示成 K_R 中的元素 $\tau(a_0)+\tau(a_1)p+\tau(a_2)p^2+\cdots$. 但该双射并不是 $W(R)$ 与 K_R 之间的一个环同构, 因为它不能保持加法运算. 由于 R 是特征为 p 的完全环, 由 Frobenius 映射 $\phi: a\mapsto a^p$, 有 $R\cong R^p$. $W(R)$ 与 K_R 之间真正的环同构, 仍记为 τ, 由下面的映射给出:

$$\tau: W(R)\to K_R,\quad (a_0,a_1,a_2,\dots)\mapsto \tau(a_0)+\tau(a_1)^{p^{-1}}p+\tau(a_2)^{p^{-2}}p^2+\cdots.$$

通常采用 τ 的另一种表示如下:

$$\tau: W(R)\to K_R,\quad (a_0,a_1^p,a_2^{p^2},\dots)\mapsto \tau(a_0)+\tau(a_1)p+\tau(a_2)p^2+\cdots. \tag{3.4}$$

例 3.1 一个著名的例子是 $W(\mathbb{F}_q)\cong\mathbb{Z}_q$. 特别地, 有 $W(\mathbb{F}_q)/p^mW(\mathbb{F}_q)\cong\mathbb{Z}_q/p^m\mathbb{Z}_q$.

设 $r\in\mathbb{N}$, 讨论 K_R 中的 r 重加法运算. 设 $j\in[1,r]$, 令 $X_j=(x_{0j},x_{1j}^p,x_{2j}^{p^2},\dots)\in W(R)$, 则有

$$\tau(X_j)=\sum_i^{\infty}\tau(x_{ij})p^i\in K_R.$$

我们希望找到一个函数 $\widetilde{s}_n^{(r)}$, 它像在引理 3.1 中定义的 $S_n^{(r)}$ 一样, 使得

$$\sum_{j=1}^{r}\Big(\sum_{i=0}^{\infty}\tau(x_{ij})p^i\Big)=\sum_{n=0}^{\infty}\tau(\widetilde{s}_n^{(r)})p^n. \tag{3.5}$$

定理 3.2 [1,7] 记号如上, 设 $n\in\mathbb{N}_0$, 则有

$$\widetilde{s}_n^{(r)}=S_n^{(r)}(x_{01}^{1/p^n},\dots,x_{0r}^{1/p^n};x_{11}^{1/p^{n-1}},\dots,x_{1r}^{1/p^{n-1}};\dots;x_{n1},\dots,x_{nr}).$$

令 $s_n^{(r)}:=(\widetilde{s}_n^{(r)})^{p^n}$, 则有

$$s_n^{(r)}=S_n^{(r)}(x_{01},\dots,x_{0r};x_{11}^p,\dots,x_{1r}^p;\dots;x_{n1}^{p^n},\dots,x_{nr}^{p^n}),$$

其中 $s_n^{(r)}$ 是变量为 x_{ij} 次数为 p^n 次的整系数齐次多项式.

注 3.2 在下文中, 简单地记作 $s_n^{(r)}$, 即默认它的变量为 $\{x_{ij}^{p^i}\mid i\in[0,n],j\in[1,r]\}$. 虽然 $x_{ij}^{p^i}$ 的顺序可能会影响 $s_n^{(r)}$ 的表达式, 但这并不影响 $s_n^{(r)}$ 的齐次次数. 所以当变量需要标明时, 我们不太严谨地简记为 $s_n^{(r)}=s_n^{(r)}(x_{ij}^{p^i}\mid i\in[0,n],\,j\in[1,r])$.

引理 3.2 [1] 设 R 是一个特征为 p 的完全环. 设 $m,r\in\mathbb{N}$, $\sum_{i=0}^{\infty}\tau(x_{ij})p^i\in K_R$, 其中 $x_{ij}\in R$, $j\in[1,r]$. 设 $\sum_{j=1}^{r}(\sum_{i=0}^{\infty}\tau(x_{ij})p^i)=\sum_{n=0}^{\infty}\tau(\widetilde{s}_n^{(r)})p^n$, 对于 $n\in\mathbb{N}_0$, 令 $s_n^{(r)}:=(\widetilde{s}_n^{(r)})^{p^n}$, 则下列条件等价:

(i) $\sum_{j=1}^{r}\sum_{i=0}^{\infty}\tau(x_{ij})p^i\equiv 0\pmod{p^m}$;

(ii) $\widetilde{s}_0^{(r)}=\widetilde{s}_1^{(r)}=\cdots=\widetilde{s}_{m-1}^{(r)}=0$;

(iii) $s_0^{(r)}=s_1^{(r)}=\cdots=s_{m-1}^{(r)}=0$.

本文还需要下面两个众所周知的结论. 第一个是 Hilbert 基定理.

定理 3.3 Noether 环上的一元多项式环仍是 Noether 的.

定理 3.4 有限域上代数簇的 zeta 函数是有理函数.

定理 3.4 是 Weil 系列猜想的一部分, 它最早由 Dwork [4] 用 p- 进分析方法证明. Weil 系列猜想的其他部分由 Grothendieck [5] 和 Deligne [2,3] 证明. Wan [9] 证明了有限域上代数簇的部分 zeta 函数是有理函数, 从而极大推广了定理 3.4.

4 主要结论

记 $X^u = x_1^{d_1}\cdots x_n^{d_n}$, 其中 $u=(d_1,\dots,d_n)\in\mathbb{N}_0^n$. 在文献 [1] 中, 本文作者观察到 $\mathbb{Z}_q$ 中的每一个多项式均可写成 Teichmüller 展开形式. 设 $f=\sum_{j=1}^r a_jX^{u_j}\in\mathbb{Z}_q[X]$, 其中 $0\neq a_j\in\mathbb{Z}_q$. 设系数 a_j 的 Teichmüller 展开为 $a_j=\sum_{i=0}^\infty a_{ij}p^i$, 其中 $a_{ij}\in\mathcal{T}_q$. 则多项式 f 的 Teichmüller 展开可由下式给出:

$$f=\sum_{j=1}^r\sum_{i=0}^\infty a_{ij}p^iX^{u_j}=\sum_{i=0}^\infty p^i\sum_{j=1}^r a_{ij}X^{u_j}=:\sum_{i=0}^\infty p^if_i,\quad a_{ij}\in\mathcal{T}_q,$$

其中每个 $f_i=\sum_{j=1}^r a_{ij}X^{u_j}$ 称为 Teichmüller 多项式. 不难将上述 Teichmüller 展开推广到 p- 进收敛的幂级数上去. 假设 $f=\sum_{j=1}^\infty a_jX^{u_j}\in\mathbb{Z}_q\langle\langle X\rangle\rangle$, 其中 $a_j=\sum_{i=0}^\infty a_{ij}p^i$, $a_{ij}\in\mathcal{T}_q$. 固定 $i\in\mathbb{N}_0$, 我们断言在集合 $\{a_{ij}\mid j\in\mathbb{N}_0\}$ 中只有有限个非零元素, 否则将与 f 是 p- 进收敛的假设矛盾. 因此, 可将 f 写成 Teichmüller 展开的形式如下:

$$f=\sum_{i=0}^\infty p^i\sum_{j=1}^{r_i}a_{ij}X^{u_j},\quad a_{ij}\in\mathcal{T}_q.$$

设 $W(\mathbb{F}_q)$ 为 $\mathbb{F}_q$ 上的 Witt 向量环, 相应的 Teichmüller 提升为 $\tau:\mathbb{F}_q\to\mathbb{Z}_q$, $a\mapsto\tau(a)$, 则有 $\mathcal{T}_q=\{\tau(a)\mid a\in\mathbb{F}_q\}$, 且对于每个 $a\in\mathbb{F}_q$, 有 $\tau(a)^q=\tau(a)$ 和 $\tau(a)\equiv a\pmod p$. 对于每个 $a\in\mathcal{T}_q$, 用 $\widetilde{a}$ 表示 $\mathbb{F}_q$ 中唯一的元素使得 $\tau(\widetilde{a})=a$. 如同在第 3 节中所介绍的, 环 $\mathbb{Z}_q$ 可由 Witt 环 $W(\mathbb{F}_q)$ 构造如下:

$$\tau:W(\mathbb{F}_q)\to\mathbb{Z}_q,\quad (a_0,a_1^p,a_2^{p^2},\dots)\mapsto\tau(a_0)+\tau(a_1)p+\tau(a_2)p^2+\cdots. \tag{4.1}$$

若 $q=p$, 则 $W(\mathbb{F}_p)\cong\mathbb{Z}_p$. 由于对于所有的 $a\in\mathbb{F}_p$, 均有 $a^p=a$, 所以映射 (4.1) 变为

$$\tau:W(\mathbb{F}_p)\to\mathbb{Z}_p,\quad (a_0,a_1,a_2,\dots)\mapsto\tau(a_0)+\tau(a_1)p+\tau(a_2)p^2+\cdots. \tag{4.2}$$

定理 4.1 设 $m\in\mathbb{N}$, 则有 $Z_m(V,T)\in\mathbb{Q}(T)$.

证明 为了符号的简洁起见, 假设 V 由一个收敛的幂级数 $f(X)\in\mathbb{Z}_q\langle\langle X\rangle\rangle$ 所定义. 设 $s_n^{(r)}$ 为在第 3 节中定义的多项式函数. 将 f 写成 Teichmüller 展开形式如下:

$$f=\sum_{i=0}^\infty p^i\sum_{j=1}^{r_i}a_{ij}X^{u_j},\quad a_{ij}\in\mathcal{T}_q.$$

设 $e\in\mathbb{N}$. 由定义 1.2 可知, $N_{e,m}(V)=\#\{X\in\mathcal{T}_{q^e}^n\mid f(X)\equiv0\pmod{p^m}\}$. 由引理 3.2 知, 对于给定的 $X\in\mathcal{T}_{q^e}^n$, $f(X)\equiv0\pmod{p^m}$ 当且仅当

$$g_k(\widetilde{X}):=s_k^{(r_i)}((\widetilde{a}_{ij}\widetilde{X}^{u_j})^{p^i}\mid i\in[0,k],j\in[1,r_i])=0$$

对于所有 $k\in[0,m-1]$ 都成立. 注意到 $\widetilde{a}_{ij}\in\mathbb{F}_q$, $\widetilde{X}\in\mathbb{F}_{q^e}^n$, 其中 $X\in\mathcal{T}_{q^e}^n$. 由此可得

$$N_{e,m}(V)=\#\{X\in\mathbb{F}_{q^e}^n\mid g_0(X)=g_1(X)=\cdots=g_{m-1}(X)=0\}=\#V_m(\mathbb{F}_{q^e}),$$

其中 V_m 是 $\mathbb{A}^n/\mathbb{F}_q$ 中由多项式方程组 $g_0(X)=g_1(X)=\cdots=g_{m-1}(X)=0$ 的公共零点所定义的仿射代数簇, 即

$$V_m=\{X\in\bar{\mathbb{F}}_q^n\mid g_0(X)=g_1(X)=\cdots=g_{m-1}(X)=0\}\hookrightarrow\mathbb{A}^n/\mathbb{F}_q. \tag{4.3}$$

设 $Z(V_m,T)$ 为 V_m 在 $\mathbb{F}_q$ 上的 zeta 函数, 即

$$Z(V_m,T)=\exp\left(\sum_{e=1}^{\infty}\frac{T^e}{e}\#V_m(\mathbb{F}_{q^e})\right).$$

由定理 3.4 可知, $Z_m(V,T)=Z(V_m,T)\in\mathbb{Q}(T)$. 以上关于单个收敛的幂级数的证明很容易推广到一组收敛的幂级数上去. □

一个自然的问题是, 序列 $Z_m(V,T)$ 将如何随着 m 的变化而变化. 下面的定理将回答这个问题.

定理 4.2 当 m 充分大时, $Z_m(V,T)$ 将变得稳定.

证明 如同定理 4.1 的证明, 假设 V 由单个收敛的幂级数 $f(X)\in\mathbb{Z}_q\langle\langle X\rangle\rangle$ 所定义, 这一情形很容易推广到 V 由一组收敛的幂级数所定义的一般情形上去. 由 (4.3) 可得多项式环 $\mathbb{F}_q[X]$ 中一个无限上升的理想链:

$$(g_0)\subseteq(g_0,g_1)\subseteq\cdots\subseteq(g_0,\ldots,g_{m-1})\subseteq\cdots$$

由定理 3.3 知, 该理想链必趋于稳定, 即存在 $M\in\mathbb{N}$, 使得 $(g_0,\ldots,g_M)=(g_0,\ldots,g_M,g_{M+1})=\cdots$. 由代数簇与理想之间的反序对应关系可以得到一个无限下降的代数簇链

$$V_0\supseteq V_1\supseteq\cdots\supseteq V_m\supseteq\cdots\supseteq V_\infty=\bigcap_{m=1}^{\infty}V_m.$$

它必将趋于稳定, 即 $V_M=V_{M+1}=\cdots$. 所以当 $m\to\infty$ 时, $Z_m(V,T)$ 会稳定, 即

$$Z_M(V,T)=Z_{M+1}(V,T)=\cdots=Z(V_\infty,T).$$

证毕. □

记号 4.1 设 V 为 p- 进解析簇. 令 M_V 表示最小的正整数 M, 使得对于所有的 $m\geqslant M$, 均有 $Z_m(V,T)=Z_M(V,T)$.

定理 4.3 $Z(V,T)=Z_M(V,T)\in\mathbb{Q}(T)$.

证明 沿用定理 4.1 的证明中使用的记号, 设 $M=M_V$, 则对于任意 $e\in\mathbb{N}$, 都有

$$V_M(\mathbb{F}_{q^e})=V_{M+1}(\mathbb{F}_{q^e})=V_{M+2}(\mathbb{F}_{q^e})=\cdots=V_\infty(\mathbb{F}_{q^e}).$$

故

$$N_e(V)=N_e(V_\infty)=N_{e,M}(V)=N_{e,M+1}(V)=\cdots.$$

由定理 4.1 和 4.2 可得

$$Z(V,T)=Z_M(V,T)=Z_{M+1}(V,T)=\cdots\in\mathbb{Q}(T),$$

其中 $Z_m(V,T)=Z(V_m,T)$ 是有限域 $\mathbb{F}_q$ 上代数簇 V_m 的 zeta 函数, $m\in\mathbb{Z}$. 定理得证. □

注 4.1 注意到 V 和 V_∞ 是两个不同的簇. 第一个是 p- 进解析簇, 而第二个则是定义在有限域 $\mathbb{F}_q$ 上的簇, 尽管对于所有的 $e\in\mathbb{N}$, 均有 $|V_\infty(\mathbb{F}_{q^e})|=|V(\mathcal{T}_{q^e})|$.

由定理 4.3, 可假设

$$Z(V,T)=\frac{\prod_{i=1}^{d_1}(1-\alpha_iT)}{\prod_{j=1}^{d_2}(1-\beta_jT)},\tag{4.4}$$

其中有限个 α_i 与 β_j 均是非零的代数整数且 $\alpha_i \neq \beta_j$. 因此, 对于任意 $e \in \mathbb{N}$, 都有

$$N_e(V) = \sum_{j=1}^{d_2} \beta_j^e - \sum_{i=1}^{d_1} \alpha_i^e,$$

其中 α_i、β_j 和 $d_1 + d_2$ 分别称为 $Z(V,T)$ 的零点倒数、极点倒数和总次数. 用 v_q 表示 q-adic 加法赋值且满足 $v_q(q) = 1$, 则 $v_q(\alpha_i)$ (或 $v_q(\beta_j)$) 也称为 α_i (或 β_j) 的 q- 进斜率.

为了促进对这类新的 zeta 函数的研究, 我们提出以下问题:

(i) 给出 M_V 一个有效的上界. 由于 $Z_m(V,T)$ 可以对有限个 m 进行有效计算, 因此这同时也将给计算 $Z(V,T)$ 提供一个有效算法.

(ii) 给出关于 $Z(V,T)$ 的零点和极点的更多信息. 例如, 零点和极点的倒数是否具有 $q^k\zeta$ 这种特殊形式, 其中 $k \in \mathbb{N}_0$, ζ 是一个单位根?

(iii) 找到 $Z(V,T)$ 总次数的一个明确上界.

(iv) 给出 $Z(V,T)$ 第一条 q- 进斜率的非平凡下界.

当 $m = 1$ 时, $Z_1(V,T)$ 的第一条 q- 进斜率的非平凡下界可由著名的 Ax-Katz 定理给出. 该结论被本文作者 [1] 推广到了所有的 $m \in \mathbb{N}$. 关于 M_V 的有效上界也可以提供关于 $Z(V,T)$ 的第一条 q- 进斜率的相关信息.

引理 4.1 [1] 设 $f \in \mathbb{Z}_q[X]$ 是次数为 d 的非零多项式. 对于给定的 $m \in \mathbb{N}$, 令

$$N_{e,m}(V) = \#\{X \in \mathcal{T}_{q^e}^n \mid f(X) \equiv 0 \pmod{p^m}\},$$

则有

$$v_{q^e}(N_{e,m}(V)) \geqslant \left\lceil \frac{n - \frac{p^m-1}{p-1}d}{p^{m-1}d} \right\rceil.$$

设 V 是由 $f(X) = 0$ 所确定的仿射代数簇, 并设 $M = M_V$. 若 $(p-1)n > (p^M - 1)d$, 则对于任意 $m \geqslant M$, 由引理 4.1 可以得到关于 $N_m(V)$ 的一个非平凡的 p- 进估计:

$$v_{q^e}(N_e(V)) = v_{q^e}(N_{e,m}(V)) = v_{q^e}(N_{e,M}(V)) \geqslant \left\lceil \frac{n - \frac{p^M-1}{p-1}d}{p^{M-1}d} \right\rceil. \tag{4.5}$$

这就得到了 $Z(V,T)$ 的牛顿多边形的第一条 q- 进斜率的非平凡下界. 我们相信这个依赖于条件 $(p-1)n > (p^M - 1)d$ 的下界很弱. 找到 $Z(V,T)$ 的第一条 q- 进斜率的无条件的非平凡下界将是一项有意义的工作.

5 推广到一般盒子上

设 $e \in \mathbb{N}$. 在上一节中, 集合 $\mathcal{T}_{q^e}^n$ 称为 $\mathbb{Z}_{q^e}^n$ 中的 Teichmüller 盒子. 更一般地, $\mathbb{Z}_{q^e}^n$ 中的一个盒子 $\mathcal{B}$ 定义为 $\mathbb{F}_{q^e}^n$ 在 $\mathbb{Z}_{q^e}^n$ 中的完全代表系. 我们将利用一组 p- 进收敛的幂级数的像来描述盒子 $\mathcal{B}$.

用 $\mathbb{Q}_q^{nr}$ 表示 $\mathbb{Q}_q$ 的极大非分歧扩张, $\mathbb{Z}_q^{nr}$ 为 $\mathbb{Q}_q^{nr}$ 的整数环. 令 $\bar{\mathcal{T}}_q := \{\tau(a) \mid a \in \bar{\mathbb{F}}_q\}$, 其中 τ 表示从 $\bar{\mathbb{F}}_q$ 到 $\mathbb{Z}_q^{nr}$ 的 Teichmüller 提升. 设 φ 为映射

$$\varphi : \mathbb{Z}_q^{nr} \to \mathbb{Z}_q^{nr}, \quad X \mapsto \varphi(X) = X + (pg_1(X), \ldots, pg_n(X)),$$

其中 $g_1,\dots,g_n\in\mathbb{Z}_q\langle\langle x_1,\dots,x_n\rangle\rangle$ 为 p- 进收敛的幂级数. 定义盒子

$$\mathcal{B}_e:=\varphi(\mathcal{T}_{q^e}^n)=\{X+(pg_1(X),\dots,pg_n(X))\mid X\in\mathcal{T}_{q^e}^n\}. \tag{5.1}$$

显然, 若对于所有的 $i\in[1,n]$, 均有 $g_i=0$, 则 $\mathcal{B}_e=\mathcal{T}_{q^e}^n$. 因此, $\mathcal{B}_e$ 推广了 Teichmüller 盒子 $\mathcal{T}_{q^e}^n$. 如同第 1 节, 设 $f_1,\dots,f_s\in\mathbb{Z}_q\langle\langle x_1,\dots,x_n\rangle\rangle$ 为 p- 进收敛的幂级数, 设 V 为由下列多项式方程组定义的 p- 进解析簇:

$$f_1(x_1,\dots,x_n)=\cdots=f_s(x_1,\dots,x_n)=0.$$

特别地, 用 $V_{\mathcal{B}}$ 表示由下列方程组定义的 p- 进解析簇:

$$\{(f_1\circ\varphi)(X)=\cdots=(f_s\circ\varphi)(X)=0\}\hookrightarrow\mathbb{A}^n/\mathbb{Z}_q.$$

定义 5.1 对于 $e\in\mathbb{N}$, 令

$$V_{\mathcal{B},e}=\{X\in\mathcal{B}_e\mid f_1(X)=\cdots=f_s(X)=0\}.$$

定义 zeta 函数

$$Z(V_{\mathcal{B}},T)=\exp\left(\sum_{e=1}^{\infty}\frac{T^e}{e}\#V_{\mathcal{B},e}\right).$$

定理 5.1 $Z(V_{\mathcal{B}},T)\in\mathbb{Q}(T)$.

证明 由 (5.1) 知, 对于每个 $X\in\mathcal{B}_e$, 存在唯一的元素 $Y=(y_1,\dots,y_n)\in\mathcal{T}_{q^e}^n$, 使得 $X=\varphi(Y)$. 故

$$\begin{aligned}\#V_{\mathcal{B},e}&=\#\{X\in\mathcal{B}_e\mid f_1(X)=\cdots=f_s(X)=0\}\\&=\#\{Y\in\mathcal{T}_{q^e}^n\mid f_1(\varphi(Y))=\cdots=f_s(\varphi(Y))=0\}\\&=\#\{Y\in\mathcal{T}_{q^e}^n\mid (f_1\circ\varphi)(Y)=\cdots=(f_s\circ\varphi)(Y)=0\}\\&=\#V_{\mathcal{B}}(\mathcal{T}_{q^e}),\end{aligned}$$

其中合成 $f_i\circ\varphi\in\mathbb{Z}_q\langle\langle y_1,\dots,y_n\rangle\rangle$ 为 p- 进收敛的幂级数. 由定理 4.3 即可得到结论. □

参考文献

1 Cao W, Wan D Q. Divisibility on point counting over finite Witt rings. Finite Fields Appl, 2023, 91: 102254
2 Deligne P. La conjecture de Weil. I. Publ Math Inst Hautes Études Sci, 1974, 43: 273–307
3 Deligne P. La conjecture de Weil. II. Publ Math Inst Hautes Études Sci, 1980, 52: 137–252
4 Dwork B. On the rationality of the zeta function of an algebraic variety. Amer J Math, 1960, 82: 631–648
5 Grothendieck A. Formule de Lefschetz et rationalité des fonctions L. Sém N Bourbaki, 1966, 279: 41–55
6 Koblitz N. p-Adic Numbers, p-Adic Analysis and Zeta-Functions. Graduate Texts in Mathematics, vol. 58. New York: Springer-Verlag, 1984
7 Rabinoff J. The theory of Witt vectors. arXiv:1409.7445, 2014
8 Serre J P. Local Fields. Graduate Texts in Mathematics, vol. 67. New York: Springer-Verlag, 1979
9 Wan D Q. Rationality of partial zeta functions. Indag Math NS, 2003, 14: 285–292
10 Witt E. Zyklische Körper und Algebren der Charakteristik p vom Grad p^n. Struktur diskret bewerteter perfekter Körper mit vollkommenem Restklassenkörper der Charakteristik p. J Reine Angew Math, 1937, 176: 126–140

Zeta functions of p-adic analytic varieties

Wei Cao & Daqing Wan

Abstract In this paper, we introduce the zeta function of a p-adic analytic variety defined over a p-adic number field. This zeta function counts Techmüller points on the analytic variety. We prove that this zeta function is a rational function. Our approach is based on the addition operation of Witt vectors, Dwork's rationality theorem, and Hilbert's basis theorem. We also propose some problems to prompt the research on this new kind of zeta function.

Keywords **zeta function, p-adic analytic variety, Witt ring, Teichmüller lifting**

MSC(2020) **11D88, 11S40, 13F35, 11T55**

doi: 10.1360/SSM-2023-0143