Kloosterman 和的生成域

张神星

第八届全国数论会议　江苏金坛

2021 年 6 月 30 日

指数和

设 p 是一个素数, $\mathbb{F}_q$ 是含有 $q = p^d$ 个元素的有限域. 对于 $\mathbb{F}_q$ 上的一元多项式 $f(x)$, 定义指数和

$$S_1(f) := \sum_{x \in \mathbb{F}_q} \zeta_p^{\mathrm{Tr}(f(x))} \in \mathbb{Z}[\zeta_p],$$

其中 $\mathrm{Tr} = \mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}$, $\zeta_p \in \mu_p$ 是一个选定的 p 次本原单位根.

我们要问:

1. 作为一个复数, $|S_1(f)| = ?$
2. 作为一个 p 进数, $|S_1(f)|_p = ?$
3. 作为一个代数 (整) 数, $\deg S_1(f) = ?$

L 函数

前两个问题已经有相当多的文献中研究过，包括本次会议也有关于指数和的估计的报告．我们简要回顾下指数和的基本性质．

定义 f 的 L 函数为

$$L(t,f) := \prod_{x\in\overline{\mathbb{F}}_p} \left(1 - \mathrm{Tr}_{\mathbb{F}_q(x)/\mathbb{F}_p}(f(x))\, t^{\deg x}\right)^{-1} = \exp\left(\sum_k S_k(f)\frac{t^k}{k}\right)$$

其中 $S_k(f) := \sum_{x\in\mathbb{F}_{q^k}} \zeta_p^{\mathrm{Tr}(f(x))} \in \mathbb{Z}[\zeta_p]$.

定理 (Dwork-Bombieri-Grothendieck)

$L(t,f)$ 是有理函数.

ℓ 进层

记

$$L(t,f)=\frac{\prod_j(1-\beta_j t)}{\prod_i(1-\alpha_i t)},\quad \alpha_i\neq\beta_j,$$

则

$$S_k(f)=\sum_i \alpha_i^k-\sum_j \beta_j^k.$$

我们称 α_i,β_j 为特征根. 为了估计特征根, 我们需要 ℓ 进方法.

一般地, 设 X 是一个概形, $X_{\text{ét}}$ 是 (小) étale site. 固定素数 $\ell\neq p$, 设 E 是 $\mathbb{Q}_\ell$ 的有限扩张. $X_{\text{ét}}$ 上系数为 E 的 ℓ 进层是这个 site 上的层 (实际上是 $\mathcal{O}_E$ 有限商上的模层的逆向系, 态射扩充至 E), 使得在每个有限商上是可构造的. 若在每个有限商上是局部常值的, 则称之为 lisse 的.

Swan 导子

为了刻画 lisse 层的一些性质, 我们需要 Swan 导子的概念. 设 K 是完备离散赋值域, $I^{(x)}, x \geq 0$ 为其高阶分歧群. 对于分歧群 P 的 E 表示 M, 我们有满足如下性质的分解 $M = \oplus M(x)$,

$$M(0) = M^P, \quad M(x)^{I^{(x)}} = 0, \quad M(x)^{I(y)} = M(x), \; y > x > 0.$$

称 $M(x) \neq 0$ 的 x 为 M 的断点. 定义 M 的 Swan 导子为

$$\mathrm{Sw}(M) = \sum x \dim M(x).$$

它总是一个整数.

曲线

令 C 是特征 p 完全域 $\mathbb{F}$ 上一射影光滑几何连通代数曲线, $K=\mathbb{F}(C)$ 为其函数域. 对于任意闭点 $x\in C(\mathbb{F})$, 我们有完备化 K_x.

对于非空开集 $U\subset C$, 我们有阿贝尔范畴等价

$$\begin{aligned}\{U\text{ 上的 lisse } E \text{ 层}\} &\longrightarrow \mathrm{Rep}_E^c\pi_1(U,\overline{\eta})\\ \mathcal{F} &\longmapsto \mathcal{F}_{\overline{\eta}}.\end{aligned}$$

由于基本群 $\pi_1(U,\overline{\eta})$ 是伽罗瓦群 $\mathrm{Gal}(\overline{K}/K)$ 的商, 因此分解群 D_x 作用在 $\mathcal{F}_{\overline{\eta}}$ 上. 于是我们可以定义 $\mathcal{F}$ 在 x 处的 Swan 导子. 对于 $x\in U$, 由于惯性群 I_x 作用平凡, 因此 $\mathrm{Sw}_x(\mathcal{F})=0$.

我们将会取 $C=\mathbb{P}^1$ and $U=\mathbb{G}_m$.

ℓ 进方法

假设 $\mu_p \subseteq E$. Deligne 在 $\mathbb{G}_{a,\overline{\mathbb{F}}_p}$ 上构造了一个局部自由秩 1 的 ℓ 进层 $\mathcal{F}_\ell(f)$, 它满足

$$L(t,f) = \prod_i \det(1 - t\mathrm{Frob}, \mathrm{H}^i_c)^{(-1)^{i+1}}$$

及由此

$$S_k(f) = \sum_i (-1)^i \mathrm{Tr}(\mathrm{Frob}^k, \mathrm{H}^i_c).$$

这里 Frob 是几何 Frobenius, $\mathrm{H}^i_c = \mathrm{H}^i_c(\mathbb{G}_{a,\overline{\mathbb{F}}_p}, \mathcal{F}_\ell(f))$ 是紧支撑上同调.

ℓ 进方法之续

记 ω_{ij} 为 Frob 在 H_c^i 上的特征值, 则

$$S_k(f) = \sum_{ij} (-1)^i \omega_{ij}^k.$$

记 $B_i = \dim_E \mathrm{H}_c^i$ 为 Betti 数.

定理 (Deligne)

ω_{ij} 是代数整数, 且存在整数 $0 \leq r_{ij} \leq i$ 使得它的所有 $\mathbb{Q}$ 共轭的绝对值均为 $q^{r_{ij}/2}$.

由此

$$|S_k| \leq \sum_i B_i q^{ki/2}.$$

一般情形

更一般地, 设

1. V 是 $\mathbb{F}_q$ 上 $\mathbb{A}^N$ 的闭子簇,
2. ψ 是 $\mathbb{F}_q$ 上非平凡加性特征, $\psi_k := \psi \circ \mathrm{Tr}_{\mathbb{F}_{q^k}/\mathbb{F}_q}$,
3. f 是 V 上定义在 $\mathbb{F}_q$ 上的正则函数,
4. χ 是 $\mathbb{F}_q^\times$ 上乘性特征, $\chi_k := \chi \circ \mathbf{N}_{\mathbb{F}_{q^n}/\mathbb{F}_q}$,
5. g 是 V 上定义在 $\mathbb{F}_q$ 上的可逆正则函数.

定义指数和

$$S_k = \sum_{x \in V(\mathbb{F}_{q^k})} \psi_k(f(x))\chi_k(g(x)),$$

则前面的方法仍然是有效的. 这时候, Bombieri 证明了特征根个数不超过

$$(4 \max\{\deg V + 1, \deg f\} + 5)^{2N+1}.$$

Kloosterman 和

取
$$V = V(X_1 \cdots X_n - a), \quad f = X_1 + \cdots + X_n.$$
设 $\chi = \{\chi_1, \ldots, \chi_n\}$ 是无序的 n 个乘性特征 $\chi_i : \mathbb{F}_q^\times \to \mu_{q-1}$. 定义 Kloosterman 和
$$\mathrm{Kl}_n(\psi, \chi, q, a) = \sum_{\substack{x_1 \cdots x_n = a \\ x_i \in \mathbb{F}_q}} \chi_1(x_1) \cdots \chi_n(x_n) \psi\left(\mathrm{Tr}_{\mathbb{F}_q/\mathbb{F}_p}(x_1 + \cdots + x_n)\right).$$

此时特征根个数为 n 个. 因此 $|\mathrm{Kl}_n| \le nq^{(n-1)/2}$.

伽罗瓦作用

但我们并不是想要对其大小进行估计，而是想要知道第三个问题的答案，即它生成的数域是哪个．显然 $\mathrm{Kl}_n \in \mathbb{Z}[\mu_{pc}]$，其中 $c = \mathrm{lcm}_i \{\mathrm{ord}(\chi_i)\}$ 整除 $q-1$．我们将伽罗瓦群表示为

$$\mathrm{Gal}(\mathbb{Q}(\mu_{pc})/\mathbb{Q}) = \left\{\sigma_t\tau_w \mid t \in (\mathbb{Z}/p\mathbb{Z})^\times, w \in (\mathbb{Z}/c\mathbb{Z})^\times\right\},$$

其中

$$\sigma_t(\zeta_p) = \zeta_p^t, \quad \sigma_t(\zeta_c) = \zeta_c,$$
$$\tau_w(\zeta_p) = \zeta_p, \quad \tau_w(\zeta_c) = \zeta_c^w.$$

容易看出

$$\sigma_t\tau_w\mathrm{Kl}_n(\psi,\chi,q,a) = \prod \chi(t)^{-w}\mathrm{Kl}_n(\psi,\chi^w,q,at^n).$$

因此我们需要研究两个 Kloosterman 和何时相差一个 $(q-1)$ 次单位根．

平凡特征

若 $\chi = \mathbf{1} = \{1, \ldots, 1\}$ 均为平凡特征, 则易知

$$a, b \text{ 共轭} \implies \mathrm{Kl}_n(\psi, \mathbf{1}, q, a) = \mathrm{Kl}_n(\psi, \mathbf{1}, q, b).$$

当 $p > (2n^{2d} + 1)^2$ (Fisher), 或 $p \geq (d-1)n + 2$ 且 p 不整除一个特定整数 (万大庆) 时, 反过来也是成立的. 一般猜测 $p \geq nd$ 就足够了. 在这些情形下,

$$\deg \mathrm{Kl}_n(\psi, \mathbf{1}, q, a) = \frac{p-1}{(p-1, n)}.$$

Kloosterman 层

Deligne 和 Katz 在 $\mathbb{G}_m \otimes \mathbb{F}_q$ 上定义了一个 lisse 层

$$\mathcal{K}\mathrm{l} = \mathcal{K}\mathrm{l}_{n,q}(\psi, \chi),$$

它满足如下性质

1. $\mathcal{K}\mathrm{l}$ 秩为 n, 权为纯 $n-1$.
2. 对任意 $a \in \mathbb{F}_q^{\times}$, $\mathrm{Tr}\big(\mathrm{Frob}_a, \mathcal{K}\mathrm{l}_{\bar{a}}\big) = (-1)^{n-1}\mathrm{Kl}_n(\psi, \chi, q, a)$.
3. $\mathcal{K}\mathrm{l}$ 在 0 处温和 $(\mathrm{Sw}_0 = 0)$.
4. $\mathcal{K}\mathrm{l}$ 在 ∞ 处完全野, $Swan_\infty = 1$. 于是它的 ∞ 断点均为 $1/n$.

Fisher 的下降

Fisher 给了 Kloosterman 层沿着有限域的扩张的下降. 对于 $a \in \mathbb{F}_q^\times$, 他定义了 $\mathbb{G}_m \otimes \mathbb{F}_p$ 上的一个 lisse 层 $\mathcal{F}_a(\chi)$, 使得 $\mathcal{F}_a(\chi)|\mathbb{G}_m \otimes \mathbb{F}_q = \bigotimes_{\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)} \left(t \mapsto \sigma(a)t^n\right)^* \mathcal{K}\mathrm{l}_n(\psi \circ \sigma^{-1}, \chi \circ \sigma^{-1})$ 并满足如下性质:

1. $\mathcal{F}_a(\chi)$ 秩为 n^d, 权为纯 $d(n-1)$.
2. 对任意 $t \in \mathbb{F}_p^\times$, $\mathrm{Tr}\left(\mathrm{Frob}_t, \mathcal{F}_a(\chi)_{\bar{t}}\right) = (-1)^{(n-1)d}\mathrm{Kl}_n(\psi, \chi, q, at^n)$.
3. $\mathcal{F}_a(\chi)$ 在 0 处温和.
4. $\mathcal{F}_a(\chi)$ 的 ∞ 断点均不超过 1.

关键的估计

引理

设 $\mathcal{F}, \mathcal{F}'$ 是 $\mathbb{G}_m \otimes \mathbb{F}_p$ 上秩均为 r, 权均为纯 w 的 *lisse* 层. 假设存在单位根 λ 使得对任意 $t \in \mathbb{F}_p^\times$ 有

$$\mathrm{Tr}\big(\mathrm{Frob}_t, \mathcal{F}_{\bar{t}}\big) = \lambda \mathrm{Tr}\big(\mathrm{Frob}_t, \mathcal{F}'_{\bar{t}}\big).$$

设 $\mathcal{G}$ 是 $\mathbb{G}_m \otimes \mathbb{F}_p$ 上一几何不可约秩为 s, 权为纯 w 的层, 使得 $\mathcal{G} \mid \mathbb{G}_m \otimes \overline{\mathbb{F}}_p$ 在 $\mathcal{F} \mid \mathbb{G}_m \otimes \overline{\mathbb{F}}_p$ 中恰好出现一次, 则它在 $\mathcal{F}' \mid \mathbb{G}_m \otimes \overline{\mathbb{F}}_p$ 中至少出现一次, 其中我们要求 $p > [2rs(M_0 + M_\infty) + 1]^2$, M_η 是 $\mathcal{F} \oplus \mathcal{F}'$ 的最大 η 断点.

关键的估计之证明概述

反证法. 通过平移我们不妨设 $w=0$. 我们将 Lefschetz 迹公式应用到 $\mathcal{G}^\vee \otimes \mathcal{F}$ 和 $\mathcal{G}^\vee \otimes \mathcal{F}'$ 上,

$$\sum_{i=0}^{2}(-1)^i \mathrm{Tr}\big(\mathrm{Frob}, \mathrm{H}_c^i(\mathcal{G}^\vee \otimes \mathcal{F})\big) = \lambda \sum_{i=0}^{2}(-1)^i \mathrm{Tr}\big(\mathrm{Frob}, \mathrm{H}_c^i(\mathcal{G}^\vee \otimes \mathcal{F}')\big).$$

我们有

$$\mathrm{H}_c^0 = 0 = \mathrm{H}_c^2(\mathcal{G}^\vee \otimes \mathcal{F}')$$

$\mathrm{H}_c^2(\mathcal{G}^\vee \otimes \mathcal{F})$ 为 1 维, 权为纯 2, H_c^1 的权不超过 1 (Weil II). 结合 Euler-Poincaré 公式

$$h_c^0(\mathcal{F}) - h_c^1(\mathcal{F}) + h_c^2(\mathcal{F}) = -\mathrm{Sw}_0(\mathcal{F}) - \mathrm{Sw}_\infty(\mathcal{F})$$

我们可以得到 p 的估计.

Kummer 诱导的

称 χ 是 Kummer 诱导的, 若存在非平凡特征 Λ 使得作为无序数组 $\chi = \chi\Lambda := \{\chi_1\Lambda, \ldots, \chi_n\Lambda\}$. 此时, $\prod\chi = \prod(\chi\Lambda) = \Lambda^n\prod\chi$. 因此 $\Lambda^n = 1$.

假设 $p > 2n+1$ 且 χ 不是 Kummer 诱导的, 则 $\mathcal{F}_a(\chi)$ 有一个重数为 1 的最高权. 考虑对应的李代数 $\mathfrak{g}(\mathcal{F}_a(\chi))$ 表示, 它对应一个子层 $\mathcal{G}_a(\chi)$. 而且这个子层是几何不可约的, 且在 $\mathcal{F}_a(\chi)|\mathbb{G}_m \otimes \overline{\mathbb{F}}_p$ 中只出现一次.

推论

推论

设 $a, b \in \mathbb{F}_q^\times$, χ 和 ρ 为乘性特征 $\chi_i, \rho_j : \mathbb{F}_q^\times \to \overline{\mathbb{Q}}_\ell^\times$ 构成的 n 元无序数组. 假设 $p > (2n^{2d}+1)^2$, χ 不是 *Kummer* 诱导的, 且存在 $\lambda \in \mu_{q-1}$ 使得

$$\mathrm{Kl}_n(\psi, \chi, q, a) = \lambda \mathrm{Kl}_n(\psi, \rho, q, b).$$

则 $\mathcal{G}_a(\chi) \otimes \mathcal{L}_{\prod \overline{\chi}} \mid \mathbb{G}_m \otimes \overline{\mathbb{F}}_p$ 在 $\mathcal{F}_b(\rho) \otimes \mathcal{L}_{\prod \overline{\rho}} \mid \mathbb{G}_m \otimes \overline{\mathbb{F}}_p$ 中出现.

这里 $\mathcal{L}_\chi$ 是 $\mathbb{G}_m \otimes \mathbb{F}_p$ 上由 Lang torsor 定义的秩 1 lisse 层, 使得对任意 $t \in \mathbb{F}_p^\times$,

$$\mathrm{Tr}(\mathrm{Frob}_t, (\mathcal{L}_\chi)_{\overline{t}}) = \chi(t).$$

推论的证明

令

$$\mathcal{F}=\mathcal{F}_a(\boldsymbol{\chi})\otimes\mathcal{L}_{\prod\overline{\chi}},\ \mathcal{F}'=\mathcal{F}_b(\boldsymbol{\rho})\otimes\mathcal{L}_{\prod\overline{\rho}},\ \mathcal{G}=\mathcal{G}_a(\boldsymbol{\chi})\otimes\mathcal{L}_{\prod\overline{\chi}}.$$

由于对任意 $t\in\mathbb{F}_p^\times$, $\sigma_t\lambda=\lambda$, 因此

$$\begin{aligned}&(-1)^{(n-1)d}\mathrm{Tr}\big(\mathrm{Frob}_t,\mathcal{F}_{\overline{t}}\big)=\prod\overline{\chi}(t)\cdot\mathrm{Kl}_n(\psi,\boldsymbol{\chi},q,at^n)\\=&\sigma_t\big(\mathrm{Kl}_n(\psi,\boldsymbol{\chi},q,a)\big)=\lambda\sigma_t\big(\mathrm{Kl}_n(\psi,\boldsymbol{\rho},q,b)\big)\\=&\lambda\prod\overline{\rho}(t)\cdot\mathrm{Kl}_n(\psi,\boldsymbol{\rho},q,bt^n)=(-1)^{(n-1)d}\lambda\mathrm{Tr}\big(\mathrm{Frob}_t,\mathcal{F}'_{\overline{t}}\big).\end{aligned}$$

应用前述引理即可, 其中 $r=s=n^d, M_0=0, M_\infty\leq 1.$

Kloosterman 和的不同

现在

$$\mathcal{G}_a(\boldsymbol{\chi}) \otimes \mathcal{L}_{\prod \overline{\chi}} \hookrightarrow \mathcal{F}_b(\boldsymbol{\rho}) \otimes \mathcal{L}_{\prod \overline{\rho}}, \quad \mathcal{G}_b(\boldsymbol{\rho}) \otimes \mathcal{L}_{\prod \overline{\rho}} \hookrightarrow \mathcal{F}_a(\boldsymbol{\chi}) \otimes \mathcal{L}_{\prod \overline{\chi}}.$$

我们有最高权 $\lambda_a(\boldsymbol{\chi}) = \lambda_b(\boldsymbol{\rho})$. 由此, 通过 Fisher 的论述可得:

定理

设 $a, b \in \mathbb{F}_q^\times$. 假设 $\boldsymbol{\chi}, \boldsymbol{\rho}$ 不是 *Kummer* 诱导的且它们都不是 $(\xi_1, \xi_1^{-1}, 1, \Lambda_2)\xi_2$ 型. 若 $p > (2n^{2d}+1)^2$ 以及存在 $\lambda \in \mu_{q-1}$ 使得

$$\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a) = \lambda \mathrm{Kl}_n(\psi, \boldsymbol{\rho}, q, b),$$

则存在 $\sigma \in \mathrm{Gal}(\mathbb{F}_q/\mathbb{F}_p)$ 和乘性特征 η, 使得 $\boldsymbol{\rho} = \eta \cdot (\boldsymbol{\chi} \circ \sigma^{-1})$ 以及 $b = \sigma(a)$. 更进一步, 要么两个 *Kloosterman* 和均为零, 要么 $\eta(b) = \lambda^{-1}$.

非零性

最后一步我们需要证明 Kloosterman 和非零.

定理

若 $p > (3n-1)C_\chi - n$, 且对任意 i, j, $\chi_i = \chi_j$ 或它们不相差一个 n 次 (未必本原) 特征, 则 $\mathrm{Kl}_n(\psi, \boldsymbol{\chi}, q, a)$ 非零. 其中

$$C_\chi = \max_{i,j} \mathrm{lcm}\big(\mathrm{ord}(\chi_i), \mathrm{ord}(\chi_j)\big) \tag{1}$$

是任两个特征的阶的最小公倍数的最大值.

非零性的证明概述

通过 $\mathbb{F}_q^\times$ 上的傅里叶变换，我们可以将 Kl_n 表达为高斯和的组合

$$(q-1)\mathrm{Kl}_n(\psi, \chi, q, a) = \sum_{m=0}^{q-2} \omega^m(a) \prod_{i=1}^{n} g(m+s_i),$$

其中我们固定一个 Teichmüller 特征并记 $\chi_i = \omega^{s_i}$. 通过小心的估计，我们可以证明存在唯一的 m 使得 $\prod_{i=1}^n g(m+s_i)$ 最小，由此可知非零性.

对于平凡特征情形，$m=0$.

生成域

定理

若 $p > \max\left\{(2n^{2d}+1)^2, (3n-1)C_\chi - n\right\}$ 且对任意 i, j, $\chi_i = \chi_j$ 或它们不相差一个 n 次特征, 则 $\mathrm{Kl}_n(\psi, \chi, q, a)$ 生成 $\mathbb{Q}(\mu_{pc})^H$, 其中 H 包含的 $\sigma_t\tau_w$ 满足: 存在整数 β 和特征 η 使得

$$t = \lambda a_1^\beta, \lambda^{n_1} = 1,\ \chi^w = \eta\chi^{q_1^\beta},\ \eta(a) = \prod \chi^w(t).$$

这里, $n_1 = (n, p-1)$, $q_1 = \#\mathbb{F}_p(a^{(p-1)/n_1})$, $a_1 \in \mathbb{F}_p^\times$ 满足 $a_1^{n/n_1} = \mathrm{N}_{\mathbb{F}_{q_1}/\mathbb{F}_p}(a^{(1-p)/n_1}) = a^{(1-q_1)/n_1}$.

例子: $n=2$ 情形

设 $\boldsymbol{\chi}=\{1,\chi\}$, 其中乘性特征 χ 的阶为 $c\neq 2$. 若 $p>\max\left\{(2^{2d+1}+1)^2, 5c-2)\right\}$, 则 $\mathrm{Kl}(\psi,\boldsymbol{\chi},p^d,a)$ 生成 $\mathbb{Q}(\mu_{pc})^H$, 其中

$$H=\begin{cases}\langle \tau_{q_1}\sigma_{a_1},\sigma_{-1},\tau_{-1}\rangle, & \text{若 } \chi(-1)=1,\chi(a)=1;\\ \langle \tau_{-q_1}\sigma_{a_1},\sigma_{-1}\rangle, & \text{若 } \chi(-1)=1,\chi(a)=\chi(a_1)=-1;\\ \langle \tau_{q_1^\alpha}\sigma_{a_1^\alpha},\sigma_{-1}\rangle, & \text{若 } \chi(-1)=1,\chi(a)^\alpha\neq 1;\\ \langle \tau_{q_1}\sigma_{-a_1},\tau_{-1}\sigma_{-1}\rangle, & \text{若 } \chi(-1)=-1,\chi(a)=\chi(a_1)=-1;\\ \langle \tau_{q_1}\sigma_{a_1},\tau_{-1}\rangle & \text{若 } \chi(-1)=-1,\chi(a)=1;\\ \langle \tau_{q_1}\sigma_{a_1},\tau_{-1}\sigma_{-1}\rangle, & \text{若 } \chi(-1)=-1,\chi(a)=-1,\chi(a_1)=1;\\ \langle \tau_{q_1^{\alpha/2}}\sigma_{-a_1^{\alpha/2}}\rangle, & \text{若 } \chi(-1)=-1,2\mid\alpha,\chi(a)\neq\pm 1;\\ \langle \tau_{q_1^\alpha}\sigma_{a_1^\alpha}\rangle, & \text{若 } \chi(-1)=-1,2\nmid\alpha,\chi(a)\neq\pm 1.\end{cases}$$

$q_1=\#\mathbb{F}_p(a^{(1-p)/2})$, $a_1=a^{(1-q_1)/2}$, α 是 $\chi(a_1)\in\mu_{p-1}$ 的阶.

注记

考虑 Kloosterman 和

$$S_k = \mathrm{Kl}(\psi, \chi \circ \mathbf{N}_{\mathbb{F}_{q^k}/\mathbb{F}_q}, q^k, a).$$

若 $p > \max\left\{(2n^{2dk}+1)^2, (3n-1)C_\chi - n\right\}$, 则 $\mathbb{Q}(S_k) = \mathbb{Q}(\mu_{pc})^H$, 其中 H 包含的 $\sigma_t\tau_w$ 满足: 存在整数 β 和 $\mathbb{F}_q^\times$ 上的特征 η 满足

$$t = \lambda a_1^\beta, \lambda^{n_1} = 1, \quad \chi^w = \eta\chi^{q_1^\beta}, \quad \eta(a) = \gamma \cdot \prod \chi^w(t), \gamma^k = 1.$$

于是 $\mathbb{Q}(S_k) = \mathbb{Q}(S_{k-c})$, 因为 $\gamma^c = 1$.

注记之续

由于 L 函数

$$L(T)=\exp\left(\sum_{k=1}^{\infty}\frac{T^k}{k}S_k\right)$$

是一个有理函数, 序列 $\{S_k\}_k$ 是一个线性递推序列. 万大庆和尹航证明了存在 N 使得序列 $\{\mathbb{Q}(S_k)\}_{k\geq N}$ 是周期的. 设 r 为其周期, 则 $p>\max\left\{\left(2n^{2d(N+r)}+1\right)^2,(3n-1)C_\chi-n\right\}$ 时, $\mathbb{Q}(S_k)$ 由前文所描述. 因此我们需要将下界 $(2n^{2d}+1)^2$ 缩小, 并需要对 r 和 N 进行尽可能小的估计. 我们 (大胆) 猜测下 $p>3ndc$ 时成立.

感谢各位的倾听!