Algebraic Theory of Exponential Sums over Finite Fields

Daqing Wan

Lecture Notes at HIT Math Summer School 2019

Contents

Abstract. Exponential sums over finite fields are of central importance in number theory and its applications. Much of the modern study focuses on their analytic estimates as complex numbers or as p-adic numbers. In these lecture notes[1], we view exponential sums as algebraic numbers in the p-th cyclotomic field and estimate their degrees as algebraic

[1]Notes taken by Mingkuan Zhang

numbers. This is a new direction. Various examples, results and open problems will be presented along the way.

§ 1. Exponential sums over finite field $\mathbb{F}_p$

Let p be a prime number, $\zeta_p = e^{\frac{2\pi i}{p}}$, a primitive p-th root of unity, and $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z} = \{\overline{0}, \overline{1}, \cdots, \overline{p-1}\}$, the finite prime field of p elements.

Definition 1.1. For $f(x) \in \mathbb{F}_p[x]$, we define the exponential sum

$$S_p(f) := \sum_{x \in \mathbb{F}_p} \zeta_p^{f(x)} \in \mathbb{Z}[\zeta_p].$$

A basic problem in number theory is the following

Question 1.2. Study the number $S_p(f)$.

(1) as a complex number, $|S_p(f)| =?$
(2) as a p-adic number, $|S_p(f)|_p =?$
(3) as an algebraic number, $\deg S_p(f) =?$

The first two questions have been studied extensively in the literature. It is surprising that the third question has not received much attention so far, other than a couple of sporadic examples such as Gauss sums (Gauss periods) and Kloosterman sums. The aim of these lecture notes is to explore the third question in a more systematic way. Due to the undergraduate nature of the audience (some first year students), we shall keep the background as little as possible.

Degrees of algebraic numbers: Let $\alpha \in \mathbb{C}$ be algebraic with minimal polynomial $f(x) \in \mathbb{Q}[x]$. Then

$$\deg \alpha = \deg f = \ [\mathbb{Q}(\alpha) : \mathbb{Q}].$$

Remark 1.3. $\mathbb{Q}[\alpha] = \mathbb{Q}(\alpha)$:
Let $\phi: \ \mathbb{Q}[x] \to \mathbb{Q}[\alpha]$, which maps $g(x)$ to $g(\alpha)$. It is a surjective ring homomorphism. $\mathbb{Q}[x]/ker(\phi) = \mathbb{Q}[x]/f(x) \simeq \mathbb{Q}[\alpha]$ is a field.

Question 1.4. Irreducibility of polynomials over $\mathbb{Q}$

Lemma 1.5. (Gauss lemma) A monic integral polynomial $g(x) = x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$ is irreducible over $\mathbb{Q}$ if and only if $g(x)$ is irreducible over $\mathbb{Z}$.

Definition 1.6. A polynomial $g(x) = x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$ is p-Eisenstein for some prime p if $p \mid a_i$ for all $1 \leq i \leq d$ and $p^2 \nmid a_d$. The polynomial $g(x)$ is called generalized p-Eisenstein if for all $1 \leq i \leq d$,

$$v_p(a_i) \geq \frac{i}{d} v_p(a_d), \text{ and } (d, v_p(a_d)) = 1,$$

where v_p denotes the p-adic valuation on $\mathbb{Z}$ defined by $v_p(0) = \infty$ and $v_p(p^r b) = r$ when $(p, b) = 1$.

Lemma 1.7. If $g(x) = x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{Z}[X]$ is p-Eisenstein, then it is irreducible over $\mathbb{Q}$. If $g(x)$ is generalized p-Eisenstein, then $g(x)$ is also irreducible over $\mathbb{Q}$, see [W3].

Example 1.8. $deg(\zeta_p) =?$, where ζ_p is a root of the p-th cyclotomic polynomial

$$\phi_p(x) = \frac{x^p - 1}{x - 1} = x^{p-1} + x^{p-2} + \cdots + x + 1.$$

One checks that

$$\phi_p(x+1) = \frac{(x+1)^p - 1}{x} = x^{p-1} + \binom{p}{1} x^{p-1} + \cdots + \binom{p}{p-2} x + \binom{p}{p}$$

is p-Eisenstein. It follows that $\phi_p(x)$ is irreducible and thus $\deg(\zeta_p) = [\mathbb{Q}(\zeta_p) : \mathbb{Q}] = p - 1$.

Recall: $S_p(f) \in \mathbb{Q}(\zeta_p)$ implies $\mathbb{Q}(S_p(f)) \subseteq \mathbb{Q}(\zeta_p)$. Since $\mathbb{Q} \subseteq \mathbb{Q}(S_p(f)) \subseteq \mathbb{Q}(\zeta_p)$, we deduce $\deg S_p(f) | (p-1)$ and we can calculate $[\mathbb{Q}(S_p(f)) : \mathbb{Q}]$ by discussing $[\mathbb{Q}(\zeta_p) : \mathbb{Q}(S_p(f))]$. Galois theory implies

$$\#\{\text{Fields } K \mid \mathbb{Q} \subseteq K \subseteq \mathbb{Q}(\zeta_p)\} = \tau(p-1),$$

the number of divisors of $p - 1$.

1.1. **Galois theory-example.**

Since $\phi_p(x) = \prod_{k=1}^{p-1} (x - \zeta_p^k)$ is irreducible in $\mathbb{Q}[x]$, $\mathbb{Q}(\zeta_p) = \mathbb{Q}(\zeta_p, \zeta_p^2, \ldots, \zeta_p^{p-1})$ is the splitting field of ϕ_p over $\mathbb{Q}$. This implies that $\mathbb{Q}(\zeta_p)/\mathbb{Q}$ is a Galois extension and the Galois group is

$$G := Gal\ (\mathbb{Q}(\zeta_p)/\mathbb{Q}) = Aut_{\mathbb{Q}}(\mathbb{Q}(\zeta_p)) = \{\sigma | \sigma : \mathbb{Q}(\zeta_p) \xrightarrow{\sim} \mathbb{Q}(\zeta_p)\}.$$

For $h(x) \in \mathbb{Q}[x]$ and $\sigma \in G$, we have $\sigma(h(\alpha)) = h(\sigma(\alpha))$, which implies that

$$\sigma(\phi_p(\zeta_p)) = \phi_p(\sigma(\zeta_p)) = 0.$$

Hence $\sigma(\zeta_p) = \zeta_p^k$ for some $1 \leq k \leq p-1$. As σ is determined by its image on ζ_p, σ is determined by k. Therefore $\#G \leq p-1$. Since

$$\mathbb{Q}[x]/(\phi_p(x)) \cong \mathbb{Q}(\zeta_p),\ x \mapsto \zeta_p$$

$$\mathbb{Q}[x]/(\phi_p(x)) \xrightarrow{\sim} \mathbb{Q}(\zeta_p^k) = \mathbb{Q}(\zeta_p),\ x \mapsto \zeta_p^k,$$

we can combine these to get an automorphism $\sigma_k : \sigma_k(\zeta_p) = \zeta_p^k$. It follows that

$$G = \{\sigma_k | k \in \mathbb{F}_p^*\} \simeq \mathbb{F}_p^*,$$

$$\sigma_k \mapsto k,\ \sigma_{k_1 k_2} \mapsto k_1 k_2 = \sigma_{k_1}\sigma_{k_2}.$$

Remark 1.9. Let α be a primitive root of $\mathbb{F}_p^*$. The discrete logarithm

$$\log_\alpha : \mathbb{F}_p^* \to \mathbb{Z}/(p-1)\mathbb{Z}$$

$$\beta = \alpha^j \mapsto j,\ j = 1, 2, \ldots, p-1.$$

has important applications.

1.2. **Galois correspondence.**

There exists a one to one correspondence between subfields K of $\mathbb{Q}(\zeta_p)$ and subgroups H of $G = \mathbb{F}_p^*$.

$$\begin{array}{ccc} \mathbb{Q}(\zeta_p) & \text{——} & 1 \\ | & & | \\ \mathrm{K} & \longleftrightarrow & \mathrm{H} \\ | & & | \\ \mathbb{Q} & \text{——} & \mathbb{F}_p^* = G. \end{array}$$

The one to one correspondence is given by

$$K = \mathbb{Q}(\zeta_p)^H = \{\alpha \in \mathbb{Q}(\zeta_p) \mid h(\alpha) = \alpha,\ \forall h \in H\},$$

$$H = Gal\ (\mathbb{Q}(\zeta_p)/K) = \{\sigma \in G\ :\ \sigma|_K = 1\}.$$

The subgroups of $\mathbb{F}_p^*$ are parameterized by $H_d = \{\alpha^d \mid \alpha \in \mathbb{F}_p^*\}$ for $d\ |(p-1)$. Here $|H_d| = \frac{p-1}{d}$. The subfield of $\mathbb{Q}(\zeta_p)$ corresponding to H_d is

$$K_d = \mathbb{Q}(\zeta_p)^{H_d} = \{\beta \in \mathbb{Q}(\zeta_p)\ |\sigma_{\alpha^d}(\beta) = \beta,\ \forall \alpha \in \mathbb{F}_p^*\}.$$

Question 1.10. Given $S_p(f)$, how can we determine $\mathbb{Q}(S_p(f)) = K_d$ for the unique $d\ |(p-1)$? This is trivial if $p = 2$. We assume that $p > 2$ from now on.

Example 1.11.

(1) $d = 1$, $K_d = \mathbb{Q}$, $H_d = \mathbb{F}_p^*$.

(2) $d = p-1$, $K_d = \mathbb{Q}(\zeta_p)$, $H_d = 1$.
(3) $d = \frac{p-1}{2}$,

$$H_{\frac{p-1}{2}} = \{\alpha^{\frac{p-1}{2}} | \alpha \in \mathbb{F}_p^*\} = \{\pm 1\},$$
$$K_{\frac{p-1}{2}} = \{\alpha \in \mathbb{Q}(\zeta_p) | \overline{\alpha} = \alpha\} = \mathbb{Q}(\zeta_p + \zeta_p^{-1}).$$

Let $\eta_p = \zeta_p + \zeta_p^{-1}$. This is a real number. Since $\zeta_p \cdot \eta_p = \zeta_p^2 + 1$, we see that ζ_p is a root of the real irreducible polynomial

$$x^2 - \eta_p x + 1 = 0.$$

Hence

$$[\mathbb{Q}(\zeta_p) : \mathbb{Q}(\eta_p)] = 2.$$

(4) $d = 2$,

$$H_2 = \{\alpha^2 | \alpha \in \mathbb{F}_p^*\}$$
$$K_2 = \{\beta \in \mathbb{Q}(\zeta_p) | \sigma_{\alpha^2}(\beta) = \beta, \forall \alpha \in \mathbb{F}_p^*\}$$
$$= \mathbb{Q}\left(\sqrt{(-1)^{\frac{p-1}{2}} p}\right) \text{ (Gauss, 1804).}$$

To see this, let $S_p(x^2) = \sum\limits_{x \in \mathbb{F}_p} \zeta_p^{x^2}$. Then for all $a^2 \in H_2$,

$$\sigma_{a^2}(S_p(x^2)) = \sum_{x \in \mathbb{F}_p} \zeta_p^{a^2 x^2} = \sum_{x \in \mathbb{F}_p} \zeta_p^{(ax)^2} = \sum_{y \in \mathbb{F}_p} \zeta_p^{y^2} = S_p(x^2), \ \forall a^2 \in H_2$$

Hence $\mathbb{Q}(S_p(x^2)) \subseteq \mathbb{Q}(\zeta_p)^{H_2} := K_2$. Gauss proved that

$$S_p(x^2) = \sqrt{(-1)^{\frac{p-1}{2}} p}$$

which implies that $\mathbb{Q}(S_p(x^2)) = K_2$.

1.3. **Construction of K_d via Gauss sums (Gauss periods).**

Let $d|(p-1)$, $H_d = \{a^d \mid a \in \mathbb{F}_p^*\}$ and $S_p(x^d) = \sum\limits_{x \in \mathbb{F}_p} \zeta_p^{x^d}$. This is called a Gauss sum in some literature. It is also a Gauss period up to a rational linear transformation. For any $a^d \in H_d$,

$$\sigma_{a^d}(S_p(x^d)) = \sum_{x \in \mathbb{F}_p} \zeta_p^{a^d x^d} = \sum_{y \in \mathbb{F}_p} \zeta_p^{y^d} = S_p(x^d).$$

Hence $S_p(x^d) \in \mathbb{Q}(\zeta_p)^{H_d} = K_d$, we have $\mathbb{Q} \subseteq \mathbb{Q}(S_p(x^d)) \subseteq K_d$. Therefore

$$\mathbb{Q}(S_p(x^d)) = K_d \Leftrightarrow \deg S_p(x^d) = d.$$

The minimal polynomial of $S_p(x^d)$ has been studied extensively in the literature for small values of d, see [BE] for a comprehensive survey. For general d, we have

Theorem 1.12. ([W1]) The monic integral polynomial

$$F(x) = \prod_{\sigma \in \mathbb{F}_p^*/H_d} (x - \sigma(S_p(x^d))) \in \mathbb{Z}[x]$$

is p-Eisenstein of degree d, hence it is the minimal polynomial of $S_p(x^d)$.

As a consequence, we deduce the following corollary due to Gauss, see [My].

Corollary 1.13. $\forall d \mid (p-1),\ K_d = \mathbb{Q}(S_p(x^d)),\ \deg S_p(x^d) = d.$

Proof. We give a proof of the theorem, following the method in [W1]. The ideas of this method will be used several times later on.

We need to find an irreducible polynomial in $\mathbb{Q}[x]$ of degree d vanishing at $S_p(x^d)$. For this purpose, we define

$$F(x) = \prod_{\sigma \in \mathbb{F}_p^*/H_d} (x - \sigma(S_p(x^d))) \in \mathbb{Q}[x].$$

It is clear that

- $S_p(x^d)$ is a root of $F(x)$.
- $\deg F(x) = [\mathbb{F}_p^* : H_d] = d$.
- $F(x)$ is invariant under G-action, i.e. $\sigma(F(x)) = F(x), \forall \sigma \in G$. This means that $F(x)$ has coefficients in $\mathbb{Q}$.

To prove that $F(x)$ is p-Eisenstein, we write

$$F(x) = \prod_{\sigma \in \mathbb{F}_p^*/H_d} (x - \sigma(S_p(x^d))) = x^d + b_1 x^{d-1} + \cdots + b_d.$$

For $1 \le k \le d$, we compute the k-th power sum

$$\begin{aligned} M_k &= \sum_{\sigma \in \mathbb{F}_p^*/H_d} \sigma(S_p(x^d))^k \\ &= \frac{1}{\frac{p-1}{d}} \sum_{\sigma \in \mathbb{F}_p^*} \sigma(S_p(x^d))^k \\ &= \frac{d}{p-1} \sum_{a \in \mathbb{F}_p^*} (\sum_{x \in \mathbb{F}_p} \zeta_p^{ax^d})^k \\ &= \frac{d}{p-1} \sum_{x_1,\ldots,x_k \in \mathbb{F}_p} \sum_{a \in \mathbb{F}_p^*} \zeta_p^{a(x_1^d + \cdots + x_k^d)}. \end{aligned}$$

Lemma 1.14. For $b \in \mathbb{F}_p$, we have

$$\sum_{a\in\mathbb{F}_p} \zeta_p^{ab} = \begin{cases} p, & b = 0, \\ 0, & 1 \le b \le p-2. \end{cases}$$

Now

$$\begin{aligned} M_k &= \frac{d}{p-1}\left(\sum_{x_1,\dots,x_k\in\mathbb{F}_p} \sum_{a\in\mathbb{F}_p} \zeta_p^{a(x_1^d+\cdots+x_k^d)} - p^k \right) \\ &= \frac{d}{p-1}(\ pN_k - p^k\ ) \equiv 0\ (\mod\ p\ ), \end{aligned}$$

where $N_k = \#\{(x_1,\dots,x_k) \in \mathbb{F}_p | x_1^d + \cdots + x_k^d = 0\}$. The Newton formula on elementary and power symmetric polynomials gives

$$\begin{cases} 0 = M_1 + b_1, \\ 0 = M_2 + b_1 M_1 + 2b_2, \\ \cdots \\ 0 = M_d + b_1 M_{d-1} + \cdots + b_{d-1} M_1 + d b_d. \end{cases}$$

Hence $p \mid M_k, 1 \le k \le d$ implies that $p \mid k b_k, 1 \le k \le d < p$. Therefore $p \mid b_k, \forall\ 1 \le k \le d$. Since $M_d + d b_d \equiv 0\ (\mod\ p^2\ )$, we have

$$p^2 \mid b_d \Leftrightarrow p^2 \mid d b_d \Leftrightarrow p^2 \mid M_d.$$

Claim 1.15.

$$p^2 \nmid M_d = \frac{d}{p-1} p(N_d - p^{d-1}),\ d > 1,\ i.e.\ p \nmid N_d.$$

Lemma 1.16. For $b \in \mathbb{F}_p$,

$$\#\{x \in \mathbb{F}_p | x^d = b\} = \begin{cases} 1, & if\ b = 0 \\ d, & if\ b = c^d\ for\ some\ c \in \mathbb{F}_p^* \\ 0, & if\ b\ \notin (\mathbb{F}_p^*)^d \end{cases}$$

$$= \sum_{k=0}^{d-1} b^{\frac{p-1}{d}k} = 1 + b^{\frac{q-1}{d}} + \cdots + b^{\frac{q-1}{d}(d-1)}.$$

Note that if $b \notin c^d$, then the last equation is indeed $= \frac{b^{p-1}-1}{b^{\frac{p-1}{d}}-1} = 0$.

Now

$$N_d = \sum_{x_1,\dots,x_{d-1}} \sum_{k=0}^{d-1} (-x_1^d - \cdots - x_{d-1}^d)^{\frac{p-1}{d}k}.$$

$$\sum_{x_1,\ldots,x_{d-1}\in\mathbb{F}_p} x_1^{u_1}\cdots x_{d-1}^{u_{d-1}} = (\sum_{x_1\in\mathbb{F}_p} {x_1}^{u_1})\cdots(\sum_{x_{d-1}\in\mathbb{F}_p} x_{d-1}^{u_{d-1}}).$$

This sum is zero if $(p-1)\nmid u_i$ or $u_i = 0$ for some i. Thus the above expression for N_d is nonzero implies that $u_i \geq p-1,\ \forall i$. Hence

$$\sum_{i=1}^{d-1} u_i \geq (p-1)(d-1).$$

If $k < d-1$, then

$$\deg\ (x_1^d + \cdots + x_{d-1}^d)^{\frac{p-1}{d}k} = (p-1)k < (p-1)(d-1).$$

$\Rightarrow$

$$\begin{aligned} N_d &= \sum_{x_1,\ldots,x_{d-1}\in\mathbb{F}_p} (-x_1^d - \cdots - x_{d-1}^d)^{\frac{p-1}{d}(d-1)} \\ &= (-1)^{\frac{p-1}{d}(d-1)} \sum_{x_1,\ldots,x_{d-1}\in\mathbb{F}_p} \binom{\frac{p-1}{d}(d-1)}{\frac{p-1}{d},\ldots,\frac{p-1}{d}} x_1^{p-1}\cdots x_{d-1}^{p-1} \\ &= (-1)^{\frac{p-1}{d}(p-1)} \binom{\frac{p-1}{d}(d-1)}{\frac{p-1}{d},\ldots,\frac{p-1}{d}} (\sum_{x\in\mathbb{F}_p} x^{p-1})^{d-1} \\ &= (-1)^{d-1}(-1)^{\frac{p-1}{d}(d-1)} \binom{\frac{p-1}{d}(d-1)}{\frac{p-1}{d},\ldots,\frac{p-1}{d}} \end{aligned}$$

which is not congruent to 0 (mod p). This implies that $p\nmid N_d$ and hence that $p\nmid b_d$. The theorem is proved.

Remark 1.17. If $d \mid (p-1)$, the Stickelberger theorem (or a direct calculation) implies that $v_p(S_p(ax^d)) = \frac{1}{d}$, $a \neq 0$. Write

$$\begin{aligned} F(x) &= \prod_{a\in\mathbb{F}_p^*/(\mathbb{F}_p^*)^d} (x - S_p(ax^d)) \\ &= x^d + b_1 x^{d-1} + \cdots + b_d. \end{aligned}$$

Then

$$p \mid b_i,\ v_p(b_d) = 1.$$

Thus $F(x)$ is p-Eisenstein and deg $(S_p(ax^d)) = d$. This gives a short p-adic proof. We shall introduce p-adic numbers and the Stickelberger theorem in the appendices.

Remark 1.18. For $d = 3$, Heath-Brown and Patterson [HP] proved that the real number $S_p(x^3)/2\sqrt{p}$ is equally distributed in the interval $[-1, 1]$

as p tends to infinity, disproving an old conjecture of Kummer (1846). Patterson [Pa] further conjectured that as t tends to ∞,

$$\sum_{p\le t}\frac{S_p(x^3)}{2\sqrt{p}}\sim\frac{(2\pi)^{2/3}t^{5/6}}{5\Gamma(2/3)\log t}.$$

Remark 1.19. The same method can be used to prove the Chevalley-Warning theorem: If $f(x_1,....,x_n)\in\mathbb{F}_p[x_1,....,x_n]$, $n>d=\deg(f)$, then

$$N(f):=\#\{(x_1,...,x_n)\in\mathbb{F}_p^n\mid f(x_1,...,x_n)=0\}\equiv 0\ (\mod p).$$

If $n=d$, this is a Calabi-Yau hypersurface. One can get a congruence formula instead of p-divisibility, see[W5].

Remark 1.20. Proof of Newton's formula

$$\begin{aligned}1+b_1x+\cdots+b_dx^d&=\prod_{i=1}^{d}(1-x_ix)\\ \frac{1}{1+b_1x+\cdots+b_dx^d}&=\frac{1}{\prod_{i=1}^{d}(1-x_ix)}\\ \frac{1}{1-x_ix}&=\exp\ (\sum_{k=1}^{\infty}x_i^k\frac{x^k}{k})\\ \frac{1}{1+b_1x+\cdots+b_dx^d}&=\exp\ (\sum_{k=1}^{\infty}(\sum_{i=1}^{d}x_i^k)\frac{x^k}{k})\\ &=\exp\ (\sum_{k=1}^{\infty}M_k\frac{x^k}{k}).\end{aligned}$$

Example 1.21. For $A\in M_{d\times d}(\mathbb{C})$, the above equation implies

$$\frac{1}{\det(I-AX)}=\exp\ (\sum_{k=1}^{\infty}Tr(A^k)\frac{A^k}{k}).$$

Take logarithmic derivative, we obtain

$$\sum_{k=1}^{\infty}M_kx^{k-1}=-\frac{b_1+2b_2x+\cdots+db_dx^{d-1}}{1+b_1x+\cdots+b_dx^d},$$

$$(1+b_1x+\cdots+b_dx^d)(\sum_{k=1}^{\infty}M_kx^{k-1})+(b_1+2b_2x+\cdots+db_dx^{d-1})=0.$$

Comparing the coefficients, one gets the Newton formula.

Recall

$$\begin{array}{ccc} \mathbb{Q}(\zeta_p) & \text{---} & 1 \\ | \ \frac{p-1}{d} & & | \ \frac{p-1}{d} \\ K_d & \text{---} & H_d = (\mathbb{F}_p^*)^d \\ | \ d & & | \ d \\ \mathbb{Q} & \text{---} & | \ \mathbb{F}_p^* \end{array}$$

Gauss (1804):

$$K_d = \mathbb{Q}(S_p(x^d)).$$

1.4. **Construction of K_d via Kloosterman Sums.** For $\lambda \in \mathbb{F}_p^*$, $n \in \mathbb{N}$, define the n-dimensional Kloosterman sum

$$Kl_{n,p}(\lambda) = \sum_{x_1,\dots,x_n \in \mathbb{F}_p^*} \zeta_p^{(x_1+\cdots+x_n+\frac{\lambda}{x_1\cdots x_n})} \in \mathbb{Z}[\zeta_p].$$

Theorem 1.22. As a complex number,

$$|Kl_{n,p}(\lambda)| \leq (n+1)\sqrt{p^n} \text{ (Deligne, 1980).}$$

Theorem 1.23. ([W3], 1995) As an algebraic number,

$$\deg Kl_{n,p}(\lambda) = \frac{p-1}{(n+1,p-1)}.$$

Idea: The minimal polynomial of $Kl_{n,p}(\lambda)$ is not p-Eisenstein. Using the Stickelberger theorem, one can show that

$$v_p(Kl_{n,p}(\lambda) - (-1)^n) = \frac{n+1}{p-1}.$$

This implies that the minimal polynomial of $Kl_{n,p}(\lambda) - (-1)^n$ is a generalised p-Eisenstein polynomial of degree $(p-1)/(n+1,p-1)$.

As a consequence, we deduce

$$K_d = \mathbb{Q}(Kl_{n,p}(\lambda)),$$

where $n = \frac{p-1}{d} - 1$.

□

1.5. **Low degree cases.** Suppose $f(x) \in \mathbb{F}_p[x]$. Recall the exponential sum

$$S_p(f) = \sum_{x \in \mathbb{F}_p} \zeta_p^{f(x)} \in \mathbb{Z}[\zeta_p].$$

We ask

$$\deg S_p(f) =?$$

Notice that

$$\forall a \in \mathbb{F}_p^* \Rightarrow \sigma_a(S_p(f)) = S_p(af),\ \deg S_p(f) = \deg S_p(af),\ \forall a \in \mathbb{F}_p^*.$$

Without loss of generality, we can assume that $f(x)$ is monic. Since $x^p = x,\ \forall x \in \mathbb{F}_p$, we can also assume $\deg(f) < p$.

Taken together, we can assume $1 \leq d = \deg(f) \leq p-1$,

$$f(x) = x^d + a_{d-2}x^{d-2} + \cdots + a_d.$$

- $d = 1,\ f(x) = x,\ S_p(x) = 0,\ \deg S_p(x) = 1.$
- $d = 2,\ f(x) = x^2 + c.$ In this case, we have

$$S_p(x^2+c) = S_p(x^2) \cdot \zeta_p^c = \sqrt{(-1)^{\frac{p-1}{2}} p} \cdot \zeta_p^c.$$

$$\deg S_p(x^2+c) = \begin{cases} 2, \text{if } c = 0 \\ p-1, \text{if } c \in \mathbb{F}_p^*. \end{cases}$$

$$S_p(x^2+c)^2 = (-1)^{\frac{p-1}{2}} p \zeta_p^{2c},\ 2c \neq 0.$$

$$\mathbb{Q} \subseteq \mathbb{Q}(S_p(x^2+c)^2) \subseteq \mathbb{Q}(S_p(x^2+c)) \subseteq \mathbb{Q}(\zeta_p).$$

$$\deg S_p(x^2+c) = (p-1) \cdot 1 = p-1.$$

- $d = 3,\ f(x) = x^3 + ax + b \in \mathbb{F}_p[x],\ (p > 3)$. In this case, $\deg S_p(f)$ can be completely classified (a future research project).

1.6. **Permutation polynomials.**

Definition 1.24. $f(x) \in \mathbb{F}_p[x]$ is called PP (permutation polynomial) if $f(x) :\ \mathbb{F}_p \to \mathbb{F}_p$ is bijective.

Theorem 1.25. Let $1 \leq d = \deg(f) \leq p-1$. Then

$$\deg S_p(f) = 1 \Leftrightarrow\ f(x)\ \textit{is a PP over}\ \mathbb{F}_p.$$

Proof. " $\Leftarrow$ " Suppose $f(x)$ is PP, then

$$S_p(f) = \sum_{x \in \mathbb{F}_p} \zeta_p^{f(x)} = \sum_{y \in \mathbb{F}_p} \zeta_p^y = 0$$

which implies $\deg S_p(f) = 1$.
" $\Rightarrow$ ". Suppose $m := S_p(f) \in \mathbb{Z}$. Define

$$n_k = \#\{a \in \mathbb{F}_p \mid f(a) = k\ \} \in \mathbb{Z}_{\geq 0},\ k \in \{0, 1, ..., p-1\} = \mathbb{F}_p.$$

Then

$$S_p(f) = \sum_{k=0}^{p-1} n_k \zeta_p^k = \ m \in \mathbb{Z}.$$

This implies that ζ_p is a root of the polynomial

$$F(x) := (\sum_{k=0}^{p-1} n_k x^k) - m \in \mathbb{Z}[x].$$

Hence ζ_p is a common root of $F(x)$ and $\phi_p(x)$. Since $\phi_p(x)$ is irreducible over $\mathbb{Q}$, we have

$$\phi_p(x) \mid F(x),\ \deg\ (F) \leq p - 1 = \ \deg \phi_p(x).$$

Then $F(x) = c \cdot \phi_p(x)$ for some constant $c \in \mathbb{Q}$. The fact that $1 \leq \deg f \leq p - 1$ implies that $f(x)$ is a non constant function, hence $c \neq 0$. Note that

$$\phi_p(x) = x^{p-1} + \cdots + x + 1.$$

We obtain

- $n_1 = \cdots = n_{p-1} = c$,
- $n_0 - m = c$,
- $n_0 + n_1 + \cdots + n_{p-1} = p$.

The fact that $f(x)$ is non constant implies that

$$n_1 = \cdots = n_{p-1} \geq 1.$$

Since

$$n_0 + n_1 + \cdots n_{p-1} = p,$$

if

$$n_1 = \cdots = n_{p-1} \geq 2,$$

then $p \geq 2(p-1)$, a contradiction. Hence

$$n_1 = \cdots = n_{p-1} = 1$$

and

$$n_0 = 1.$$

We conclude that $f(x)$ is a PP.

□

Corollary 1.26. Classification of $f(x) \in \mathbb{F}_p[x]$ with $\deg S_p(f) = 1$ is equivalent to the classification of PP's over $\mathbb{F}_p$.

Example 1.27.

(1) $f(x) = ax + b$ $(a \neq 0)$ is PP.
(2) $f(x) = x^d$ is PP over $\mathbb{F}_p$ iff $(d, p-1) = 1$.

Definition 1.28. For $1 \leq d \leq p-1$, let

$$M_d(p) = \#\{f(x) \in \mathbb{F}_p[x] \mid f(x) \textit{ is PP over } \mathbb{F}_p, \deg(f) = d\}.$$

The number of permutations in $\mathbb{F}_p$ is $p!$. By Lagrange interpolation, every map from $\mathbb{F}_p$ to itself is uniquely represented by a non-constant polynomial in $\mathbb{F}_p[x]$ of degree at most $p-1$. It follows that

$$\sum_{d=1}^{p-1} M_d(p) = p!.$$

Question 1.29. For $1 \leq d \leq p-1$, $M_d(p) = ?$

It is clear that

$$M_1(p) = (p-1)p.$$

If $(d, p-1) = 1$, then $M_d(p) > 0$ since then x^d is PP.

Theorem 1.30. If $1 < d \mid (p-1)$, then $M_d(p) = 0$.

Proof. Without loss of generality, let

$$f(x) = x^d + a_1 x^{d-1} + \cdots + a_d \in \mathbb{F}_p[x].$$

If $f(x)$ is a PP, we compute the power sum

$$\begin{aligned} 0 = \sum_{y \in \mathbb{F}_p} y^{\frac{p-1}{d}} &= \sum_{x \in \mathbb{F}_p} f(x)^{\frac{p-1}{d}} \\ &= \sum_{x \in \mathbb{F}_p} (x^d + a_1 x^{d-1} + \cdots + a_d)^{\frac{p-1}{d}} \\ &= \sum_{x \in \mathbb{F}_p} x^{p-1} = p - 1 \neq 0 \textit{ in } \mathbb{F}_p. \end{aligned}$$

This is a contradiction. □

Corollary 1.31. If $2 \leq d \mid (p-1)$, $d = \deg f$, then $\deg S_p(f) \geq 2$.

Theorem 1.32. If $(d, p-1) > 1$ and $p > d^4$, then $M_d(p) = 0$, i.e. there is no PP of degree d.

This is the consequence of the Carlitz-Wan conjecture as proved by Lenstra [CF](1995) for general finite fields. In this easier prime field case, it also follows directly from the fact that the projective plane curve defined by the affine equation

$$F(x,y) = \frac{f(x) - f(y)}{x - y}$$

has a non-singular $\mathbb{F}_p$-rational point at infinity and hence the polynomial is not exceptional, see below. In the easier prime field case, a much stronger result is the classification of exceptional polynomials, as given by Fried's solution (1974) of the Schur conjecture, see also Turnwald(1995), Mueller(1997).

Theorem 1.33 (**Schur Conjecture over $\mathbb{F}_p$**)**.** Suppose $p > d^4$, then $f(x)$ is PP over $\mathbb{F}_p$ iff $f(x)$ is a composition of monomials

$$x^n,\ (n, p-1) = 1$$

and Dickson Polynomials ($b \neq 0$)

$$D_n(x,b),\ (n, p^2-1) = 1.$$

Definition 1.34. The **Dickson polynomial** is defined by

$$\begin{aligned} D_n(x,b) &= (\frac{x + \sqrt{x^2 - 4b}}{2})^n + (\frac{x - \sqrt{x^2 - 4b}}{2})^n \\ &= \sum_{j=0}^{\lfloor n/2 \rfloor} \frac{n}{n-j} \binom{n-j}{j} (-b)^j x^{n-2j},\ b \neq 0. \end{aligned}$$

If $b = 0$, then $D_n(x,0) = x^n$.

Theorem 1.35. For $b \in \mathbb{F}_p^*$, $D_n(x,b)$ is PP over $\mathbb{F}_p$ iff $(n, p^2-1) = 1$.

Example 1.36. Let $n = 3$, then

$$D_n(x,b) = x^3 + 3bx\ (3b \neq 0)$$

is PP over $\mathbb{F}_p$ iff $(3, p^2-1) = 1$. But $3 \mid (p^2-1)$, hence $D_n(x,b)$ is not a PP over $\mathbb{F}_p$. In this case $2 \leq \deg S_p(D_3(x,b)) \mid \frac{p-1}{2}$. One can show that $\deg S_p(D_3(x,b)) = \frac{p-1}{2}$.

Open Problem

$$\deg S_p(D_n(x,b)) = ?$$

If $b = 0$, Gauss showed that $\deg S_p(x^n) = (n, p-1)$. If $b \neq 0$, it is an open problem to determine $\deg S_p(D_n(x,b))$.

1.7. **Exceptional polynomials.** If $f(x)$ with $1 < d = \deg f < p$ is PP over $\mathbb{F}_p$, then $f(x) - f(y) \neq 0$ for all $x \neq y$ in $\mathbb{F}_p$. This means that the plane curve $F(x,y) := \frac{f(x)-f(y)}{x-y}$ has no $\mathbb{F}_p$-rational points off the diagonal. Thus,

$$\#\{(x,y) \in \mathbb{F}_p^2 \mid F(x,y) = 0\} \leq d-1.$$

If $F(x,y)$ has an absolutely irreducible factor over $\mathbb{F}_p$, the Weil bound implies that

$$d-1 \geq \#\{(x,y) \in \mathbb{F}_p^2 \mid F(x,y) = 0\} \geq p - (d-1)^2\sqrt{p}.$$

This is a contradiction if $p > d^4$.

Definition 1.37. $f(x) \in \mathbb{F}_p[x]$ is exceptional (E.P) if

$$F(x,y) := \frac{f(x) - f(y)}{x-y}$$

has no absolutely irreducible factor over $\mathbb{F}_p$.

Theorem 1.38.

(1) If $f(x) \in \mathbb{F}_p[x]$ is E.P, then $f(x)$ is PP over $\mathbb{F}_p$.
(2) If $f(x)$ is PP over $\mathbb{F}_p$ and $p > d^4$, then $f(x)$ is E.P.

This means that if $p > d^4$, then EP is equivalent to PP.

Conjecture 1.39. (Carlitz-Wan) There is an E.P over $\mathbb{F}_p$ of degree d iff $(d, p-1) = 1$.

As indicated before, this conjecture was proved by Lenstra [CF] (1995) for general finite fields. In this much easier prime field case, it follows directly from the fact that the projective curve defined by the affine equation

$$F(x,y) = \frac{f(x) - f(y)}{x-y}$$

has a non-singular $\mathbb{F}_p$-rational point at infinity and hence the polynomial is not exceptional. This is the geometric approach in [W2] and the motivation behand the Carlitz-Wan conjecture for general finite fields.

1.8. **General results.**

Definition 1.40. For $k \in \mathbb{F}_p$, let

$$n_0(f) = \#\{a \in \mathbb{F}_p \mid f(a) = 0\},$$
$$n_k(f) = \#\{a \in \mathbb{F}_p \mid f(a) = k\} = n_0(f(x) - k).$$

Theorem 1.41. (W, 2019) If $1 \le d = \deg f \le p-1$, then

$$\frac{p-1}{(p-1, n_0(f)-1)} \mid \deg\ S_p(f) \mid (p-1).$$

Proof. Let $f(x) \in \mathbb{F}_p[x]$. For $k \ge 1$, we define

$$N_k(f) = \#\{(x_1, \dots, x_k) \in \mathbb{F}_p^k \mid f(x_1) + \cdots + f(x_k) = 0\}.$$

Write

$$F(x) = \prod_{a \in \mathbb{F}_p^*} (x - S_p(af)) = x^{p-1} + F_1 x^{p-1} + \cdots + F_{p-1}.$$

Let

$$H = \{t \in \mathbb{F}_p^* \mid \sigma_t(S_p(f)) = S_p(f)\} = \textit{Stablizer of } S_p(f) \textit{ in } \mathbb{F}_p^*.$$

One checks that

$$F(x) = \prod_{a \in \mathbb{F}_p^*/H} (x - S_p(af))^{|H|} = M(x)^{|H|},$$

where

$$M(x) = \prod_{a \in \mathbb{F}_p^*/H} (x - S_p(af)) \in \mathbb{Q}(\zeta_p)^{\mathbb{F}_p^*}[x] = \mathbb{Q}[x]$$

is the minimal polymonial of $S_p(f)$. It follows that

$$\deg S_p(f) = \deg M(x) = \frac{p-1}{|H|}.$$

Let

$$\begin{aligned} P_k &= \sum_{a \in \mathbb{F}_p^*} S_p(af)^k \\ &= \sum_{a \in \mathbb{F}_p^*} (\sum_{x_1 \in \mathbb{F}_p} \zeta_p^{af(x_1)}) \cdots (\sum_{x_k \in \mathbb{F}_p} \zeta_p^{af(x_k)}) \\ &= \sum_{x_1, \dots, x_k \in \mathbb{F}_p} \sum_{a \in \mathbb{F}_p^*} \zeta_p^{a(f(x_1) + \cdots + f(x_k))} \\ &= \sum_{x_1, \dots, x_k \in \mathbb{F}_p} (\sum_{a \in \mathbb{F}_p} \zeta_p^{a(f(x_1) + \cdots + f(x_k))} - 1). \end{aligned}$$

Notice that

$$\sum_{a \in \mathbb{F}_p} \zeta_p^{ab} = \begin{cases} p, & b = 0 \\ 0, & b \ne 0 \end{cases}$$

then

$$P_k = pN_k(f) - p^k.$$

Recall that

$$F(x) = x^{p-1} + F_1 x^{p-2} + \cdots + F_{p-1} = M(x)^{|H|}.$$

Take derivative, we get

$$(p-1)x^{p-1} + (p-2)F_1 x^{p-3} + \cdots + F_{p-2} = |H|M(x)^{|H|-1}M(x)'.$$

Hence

$$(p-1, (p-2)F_1, \cdots, 2F_{p-3}, F_{p-2}) \equiv 0 \ (\mod |H|).$$

Namely,

$$(p-1, F_1, 2F_2, \cdots, (p-3)F_{p-3}, (p-2)F_{p-2}) \equiv 0 \ (\mod |H|).$$

By Newton formula,

$$\begin{cases} 0 = P_1 + F_1, \\ 0 = P_2 + P_1F_1 + 2F_2, \\ \cdots \\ 0 = P_{p-1} + P_{p-2}F_1 + \cdots + P_1F_{p-2} + (p-1)F_{p-1}. \end{cases}$$

We have shown above that $jF_j \equiv 0 \ (\mod |H|), \forall\ 1 \leq j \leq p-1$. Hence by Newton formula, one recursively finds

$$\begin{cases} P_1 \equiv 0 \quad (\mod |H|), \\ P_2 \equiv 0 \quad (\mod |H|), \\ \quad \cdots \\ P_{p-1} \equiv 0 \quad (\mod |H|). \end{cases}$$

$$0 \equiv P_k = pN_k(f) - p^k \equiv N_k(f) - 1 \ (\mod |H|).$$

Hence

$$(p-1, N_1(f)-1, \cdots, N_{p-1}(f)-1) \equiv 0 \ (\mod |H|).$$

Then

$$|H| \mid (p-1, N_1(f)-1, \cdots, N_{p-1}(f)-1).$$

$$\deg S_p(f) = \frac{p-1}{|H|}$$

$$= \frac{p-1}{(p-1, N_1(f)-1, \cdots, N_{p-1}(f)-1)} \frac{(p-1, N_1(f)-1, \cdots, N_{p-1}(f)-1)}{|H|}.$$

Therefore

$$\frac{p-1}{(p-1, N_1(f)-1, \cdots, N_{p-1}(f)-1)} \mid \deg S_p(f).$$

Since $N_1(f) = n_0(f)$, the theorem is proved. □

Corollary 1.42. If $(p-1, n_0(f)-1) = 1$, then $\deg\ S_p(f) = p-1$.

Example 1.43. If $n_0(f) = 0,\ 2\ or\ p-1$, then $\deg\ S_p(f) = p-1$.

Remark 1.44. If $n_0(f) \neq 1$, then $(p-1, n_0(f)-1) \leq \frac{p-1}{2}$, which implies that $\deg S_p(f) \geq 2$. This also follows directly from the fact that $f(x)$ is not a PP when $n_0(f) \neq 1$.

Example 1.45. If $f(x) = x^d + bx^{d-1} = x^{d-1}(x+b),\ (b \neq 0)$, then $n_0(f) = 2$. Therefore $\deg S_p(f) = p-1$.

Example 1.46. If $f(x)$ is odd, i.e. $f(x) = f(-x)$, then

$$\overline{S_p(f)} = \overline{\sum_{x\in\mathbb{F}_p} \zeta_p^{f(x)}} = \sum_{x\in\mathbb{F}_p} \zeta_p^{-f(x)} = \sum_{x\in\mathbb{F}_p} \zeta_p^{f(-x)} = S_p(f).$$

Then $S_p(f) \in \mathbb{Q}(\zeta_p + \zeta_p^{-1}) = \mathbb{Q}(\zeta_p)^{\{\pm 1\}}$.

$$\deg S_p(f) \mid [\mathbb{Q}(\zeta_p)^{\{\pm 1\}} : \mathbb{Q}] = \frac{p-1}{|\{\pm 1\}|} = \frac{p-1}{2}.$$

Corollary 1.47. If $f(x)$ is odd, i.e. $f(x) = f(-x)$, then

$$\frac{p-1}{(p-1, n_0(f)-1)} \mid \deg S_p(f) \mid \frac{p-1}{2}.$$

Corollary 1.48. If $f(x)$ is odd and $n_0(f) = 3$, then $\deg S_p(f) = \frac{p-1}{2}$.

Example 1.49. $f(x) = x^3 - b^2x = x(x-b)(x+b),\ (b \neq 0)$, is odd, then $\deg S_p(f) = \frac{p-1}{2}$. More generally, $f(x) = x^{2k+1}(x-b)(x+b)(b \neq 0)$ is odd, then $n_0(f) = 3$, $\deg S_p(f) = \frac{p-1}{2}$.

Notice that $f(x)$ is odd iff $f(x) = xg(x^2)$ for some nonzero polynomial $g(x)$. Let $e \mid (p-1)$, $f(x) = xg(x^e)$,

$$H(e) = \{t \in \mathbb{F}_p \mid t^e = 1\},\ |H(e)| = (e, p-1) = e.$$

For all $t \in H(e)$,

$$\sigma_t(S_p(f)) = S_p(tf) = S_p(txg(x^e)) = S_p(txg((tx)^e)) = S_p(f(tx)) = S_p(f).$$

Therefore $S_p(f) \in \mathbb{Q}(\zeta_p)^{H(e)}$ and

$$\deg S_p(f) \mid [\mathbb{Q}(\zeta_p)^{H(e)} : \mathbb{Q}] = \frac{p-1}{|H(e)|} = \frac{p-1}{e}.$$

Corollary 1.50. If $f(x) = xg(x^e)$ for some $e \mid (p-1)$, then

$$\frac{p-1}{(p-1, n_0(f)-1)} \mid \deg S_p(f) \mid \frac{p-1}{e}.$$

Corollary 1.51. If $f(x) = xg(x^e)$ for some $e \mid (p-1)$ and $(p-1, n_0(f)-1) = e$ then $\deg S_p(f) = \frac{p-1}{e}$.

Example 1.52. Let $f(x) = x(x^e - b^e),\ (b \neq 0),\ e|(p-1)$. Then

$$n_0(f) = e+1,\ (p-1, (e+1)-1) = (p-1, e) = e.$$

Hence $\deg S_p(f) = \frac{p-1}{e}$.

§ 2. Finite Fields

Definition 2.1. A field F is finite if $|F| < \infty$.

Example 2.2. Let p be a prime, then $\mathbb{F}_p = \mathbb{Z}/p\mathbb{Z}$ is a finite field. For $n \in \mathbb{Z}_{>0}$, then $\mathbb{Z}/n\mathbb{Z}$ is a finite field iff n is a prime. This is because $\mathbb{Z}/n\mathbb{Z}$ is a field iff (n) is a maximal ideal iff n is a prime.

Definition 2.3. The characteristic of a field F is the smallest positive integer k (if it exists) such that $k \cdot 1 = 0$. Otherwise, we define $char(F) = 0$.

Proposition 2.4. If $charF \neq 0$, then $charF = p$ where p is a prime number.

Proof. If $k > 0$, then $k \cdot 1 = 0$ in F, hence $k \geq 2$. Suppose $k = k_1k_2, k_1, k_2 \geq 2$, then $0 = k = k_1k_2$ in F. Since F is a field, we have k_1 *or* k_2 is 0 in F. Contradict to the definition of characteristic. Therefore k is a prime. Furthermore, suppose there exists different prime numbers p_1, p_2 such that $p_1 = p_2 = 0$ in F. Since p_1 and p_2 are coprime, we can deduce that $1 = 0$ in F, a contradiction. □

If $char(F) = 0$, then $F \supseteq \mathbb{Z} \cdot 1 \supseteq \mathbb{Z}$. Therefore $F \supseteq \mathbb{Q}$. If $char(F) = p > 0$, then $F \supseteq \mathbb{Z}/p\mathbb{Z} \simeq \mathbb{F}_p$. Denote prime fields by

$$\{\mathbb{Q},\ \mathbb{F}_2,,\ \mathbb{F}_3,\ \mathbb{F}_5, \ldots,\ \mathbb{F}_p, \ldots\}$$

All the finite fields F are finite extensions of finite prime fields. And if $char(F) = p$, then F is a finite extension of $\mathbb{F}_p$. We denote $[F : \mathbb{F}_p] = r$, then $r = dim_{\mathbb{F}_p} F$. Let $\alpha_1, \ldots, \alpha_r$ be a basis of $F/\mathbb{F}_p$, then

$$F = \mathbb{F}_p\alpha_1 + \cdots + \mathbb{F}_p\alpha_r.$$

Therefore $|F| = p^r < \infty$.

Proposition 2.5. If F is a finite field, then $|F| = p^r$ for the unique prime $p = char(F)$ and $r = [F : \mathbb{F}_p]$.

Theorem 2.6. For every prime number $q = p^r$, there is a finite field F with q elements, unique up to isomorphism. Denote this field by $\mathbb{F}_q = \mathbb{F}_{p^r}$.

For $\alpha \in \mathbb{F}_q$, let $f(x) \in \mathbb{F}_q$ be the minimal polynomial of α over $\mathbb{F}_p$. Then the ring homomorphism

$$\phi : \mathbb{F}_p[x] \to \mathbb{F}_p[\alpha]$$

is surjective and $ker(\phi) = (f(x))$. Since $(f(x))$ is a maximal ideal in $\mathbb{F}_p[x]$, $\mathbb{F}_p[\alpha] \simeq \mathbb{F}_p[x]/(f(x))$ is a field and $\mid \mathbb{F}_p[\alpha] \mid = p^{\deg f}$.

Definition 2.7. For positive integers d, let

$$\begin{aligned}\pi_d(p) &= \#\{\textit{monic irreducible polynomials } f(x) \in \mathbb{F}_p[x] \textit{ of degree } d\} \\ &= \#\{x^d + a_1x^{d-1} + \cdots + a_d, \textit{ irreducible in } \mathbb{F}_p[x]\}.\end{aligned}$$

We want to give an explicit formula for $\pi_d(p)$ which implies that $\pi_d(p) > 0$ for every degree d.

Definition 2.8. The *Möbius* function $\mu(n)$ on $\mathbb{N}$ is defined by

$$\mu(n) = \begin{cases} 1, & n = 1 \\ 0, & p^2 \mid n \textit{ for some prime number } p \\ (-1)^r, & \textit{if } n = p_1 \cdots p_r \textit{ for distinct prime numbers } p_1, \ldots, p_r. \end{cases}$$

Remark 2.9. RH holds iff $\sum\limits_{n \le X} \mu(n) = O(X^{\frac{1}{2}+\varepsilon}),\ \forall \varepsilon > 0.$

Proposition 2.10. (*Möbius* inversion) Let $f(n),\ g(n)$ be two functions on $\mathbb{N}$, then

$$f(n) = \sum_{d \mid n} g(n),\ \forall n \Leftrightarrow g(n) = \sum_{d \mid n} \mu(\frac{n}{d}) f(d).$$

2.1. **Prime number theorem in $\mathbb{F}_p[x]$.**

Definition 2.11. For $d \in \mathbb{N}$, let

$$\pi_d := \#\{\ \textit{monic irreducible } x^d + a_1x^{d-1} + \cdots + a_d\ \in \mathbb{F}_p[x]\ \}.$$

Theorem 2.12.

$$\mid \pi_d - \frac{p^d}{d} \mid \le 2 \cdot \sqrt{p^d}.$$

Definition 2.13.

$$\begin{aligned} Z(T) :&= \sum_{monic\ f(x)\in\mathbb{F}_p[x]} T^{\deg(f)} \\ &= \sum_{d=0}^{\infty} T^d \cdot \#\{monic\ f(x) \in \mathbb{F}_p[x]\ of\ degree\ d\ \} \\ &= \sum_{d=0}^{\infty} T^d \cdot p^d = \frac{1}{1-pT}. \end{aligned}$$

Since $\mathbb{F}_p[x]$ is a UFD,

$$f(x) = x^d + a_1 x^{d-1} + \cdots + a_d = g_1(x)^{k_1} \cdots g_l(x)^{k_l}$$

where $g_i(x)$ is monic irreducible, i.e. the standard factorization.

$$\begin{aligned} Z(T) &= \sum_{g_1(x),g_2(x),\ldots monic,\ irred} \ \sum_{k_1,k_2,\cdots=0}^{\infty} T^{\deg(g_1(x)^{k_1} g_2(x)^{k_2}\cdots)} \\ &= (\sum_{k_1=0}^{\infty} T^{k_1 \deg(g_1)})(\sum_{k_2=0}^{\infty} T^{k_2 \deg(g_2)}) \cdots \\ &= \frac{1}{1-T^{\deg(g_1)}} \frac{1}{1-T^{\deg(g_2)}} \cdots \\ &= \prod_{monic,\ irred\ g(x)\in\mathbb{F}_p[x]} \frac{1}{1-T^{\deg(g)}} \\ &= \prod_{d=1}^{\infty} (\frac{1}{1-T^d})^{\pi_d} = \prod_{d=1}^{\infty} \exp(\sum_{k=1}^{\infty} \frac{T^{dk}}{k} \pi_d) \\ &= \exp(\sum_{d=1}^{\infty} \frac{T^d}{d} N_d), \end{aligned}$$

where $N_d = \sum_{k|d} k \cdot \pi_k$. Hence

$$\exp(\sum_{d=1}^{\infty} \frac{T^d}{d} N_d) = \frac{1}{1-pT}.$$

Take logarithm,

$$\sum_{d=1}^{\infty} \frac{T^d}{d} N_d = -\log(1-pT) = \sum_{d=1}^{\infty} \frac{T^d}{d} p^d.$$

Then $N_d = p^d = \sum_{k|d} k\pi_k,\ \forall\ d$. By *Möbius* inversion, we get

$$d\pi_d = \sum_{k|d} \mu(\frac{d}{k})p^k = \sum_{k|d} \mu(k)p^{\frac{d}{k}} = p^d + O(dp^{\frac{d}{2}}).$$

Hence

$$\pi_d = \frac{1}{d}\sum_{k|d} \mu(k)p^{\frac{d}{k}} = \frac{p^d}{d} + O(p^{\frac{d}{2}}).$$

Write $d = p_1^{r_1}\cdots p_l^{r_l}$, where $p_1 < \cdots < p_l$ are primes, $r_i \geq 1$. If $k \mid d$, then $k = p_1^{s_1}\cdots p_l^{s_l}$, $0 \leq s_i \leq r_i$. If some $s_i \geq 2$, then $\mu(k) = 0$. If $k = p_1^{s_1}\cdots p_l^{s_l}$, $s_i \in \{0,1\}$, $\mu(k) = (-1)^{s_1+\cdots+s_l}$. Then

$$\begin{aligned}
\pi_d &= \frac{1}{d}\sum_{s_1,\ldots,s_l\in\{0,1\}} (-1)^{s_1+\cdots+s_l} p^{p_1^{r_1-s_1}\cdots p_l^{r_l-s_l}} \\
&= \frac{1}{d}(\sum_{s_1\in\{0,1\}} (-1)^{s_1}\cdot p^{p_1^{r_1-s_1}})\cdots(\sum_{s_l\in\{0,1\}} (-1)^{s_l}\cdot p^{p_l^{r_l-s_l}}) \\
&= \frac{1}{d}(p^{p_1^{r_1}} - p^{p_1^{r_1-1}})\cdots(p^{p_l^{r_l}} - p^{p_l^{r_l-1}}) > 0.
\end{aligned}$$

Hence $\pi_d > 0, \forall d = 1, 2, \ldots$ and

$$\pi_d - \frac{p^d}{d} = O(p^{\frac{d}{2}}).$$

2.2. **Structure of $\mathbb{F}_q = \mathbb{F}_{p^r}$.**

Example 2.14. If $r = 1$, then

$$(\mathbb{F}_p, +) \simeq \mathbb{Z}/p\mathbb{Z},\ (\mathbb{F}_p^*, \cdot) \simeq \mathbb{Z}/(p-1)\mathbb{Z}.$$

Theorem 2.15. (Structure of finitely generated abelian groups) Let A be a finitely generated abelian group, i.e.

$$A = \mathbb{Z}\cdot g_1 + \cdots + \mathbb{Z}\cdot g_n =< g_1, \ldots, g_n > .$$

Then

$$A \simeq \mathbb{Z}^h \oplus \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z},\ d_1|\cdots|d_s,$$

where the non-negative integer h and the positive integers d_i ($d_i \geq 2$) are uniquely determined by A.

Theorem 2.16.

(1)

$$(\mathbb{F}_{p^r}, +) \cong \mathbb{Z}/p\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/p\mathbb{Z} \cong (\mathbb{Z}/p\mathbb{Z})^r.$$

Let $\{\alpha_1, \ldots, \alpha_r\}$ be a basis of $\mathbb{F}_{p^r}$ over $\mathbb{F}_p$, then

$$\mathbb{F}_{p^r} = \mathbb{F}_p\alpha_1 + \cdots + \mathbb{F}_p\alpha_r.$$

(2)

$$(\mathbb{F}_{p^r}, \times) \simeq \mathbb{Z}/(q-1)\mathbb{Z} \simeq \mathbb{Z}/(p^r-1)\mathbb{Z}.$$

Proof. Since $\mathbb{F}_{p^r}^*$ is a finite abelian group,

$$\mathbb{F}_{p^r}^* \simeq \mathbb{Z}/d_1\mathbb{Z} \oplus \cdots \oplus \mathbb{Z}/d_s\mathbb{Z},\ d_1|\cdots|d_s.$$

with $(p^r-1) = d_1 \cdots d_s$. We need to prove

$$d_1 = \cdots = d_{s-1} = 1, d_s = (p^r-1).$$

If $\alpha \in \mathbb{F}_q^*$, then $\alpha^{q-1} = 1$. Therefore $\alpha^q = \alpha,\ \forall \alpha \in \mathbb{F}_q$. We deduce that

$$x^q - x = \prod_{\alpha \in \mathbb{F}_q} (x - \alpha)$$

By the structure theorem, $\alpha^{d_s} = 1,\ \forall \alpha \in \mathbb{F}_q^*$. Therefore the polynomial $x^{d_s} - 1$ has at least $(q-1)$ distinct roots. This implies that $d_s \geq q-1$. Hence $d_s = q-1$. □

Remark 2.17.

(1) If $f(x) = x^d + a_1x^{d-1} + \cdots + a_d \in F[x]$, where F is a field, then $f(x)$ has at most d roots in F.
(2) This is false over a ring. For example, take $f(x) = x^2$, $R = \mathbb{Z}/p^2\mathbb{Z}$, then

$$\{\alpha \in R \mid \alpha^2 = 0 \ in\ R\} = \{p\mathbb{Z}/p^2\mathbb{Z}\}.$$

$(\mathbb{F}_q, +) \simeq (\mathbb{Z}/p\mathbb{Z})^r$ as $\mathbb{Z}-$module. $(\mathbb{F}_q^*, \times) \simeq \mathbb{Z}/(q-1)\mathbb{Z}$ as $\mathbb{Z}-$module.

Definition 2.18. Let $Frob_p \in Aut(\mathbb{F}_q/\mathbb{F}_p)$:

$\mathbb{F}_{p^r} \to \mathbb{F}_{p^r} : \alpha \mapsto \alpha^p, \alpha + \beta \mapsto (\alpha+\beta)^p = \alpha^p + \beta^p, (\alpha\beta) \mapsto (\alpha\beta)^p = \alpha^p\beta^p.$

Hence $Frob_p$ is a ring homomorphism, and

$$Ker(Frob_p) = \{\alpha \in \mathbb{F}_q \mid \alpha^p = 0\} = \{0\}$$

Therefore $Frob_p$ is injective, surjective, bijective.

Notice that

$$Frob_p^{-1}(\alpha) = \alpha^{\frac{1}{p}} = (\alpha^q)^{\frac{1}{p}} = \alpha^{p^{r-1}}.$$

$$Frob_p^i(\alpha) = \alpha^{p^i}.$$

Hence $Frob_p^r(\alpha) = 1$, $Gal(\mathbb{F}_{p^r}/\mathbb{F}_p) =< Frob_p > \simeq \mathbb{Z}/r\mathbb{Z}$. And $Frob_p$ is an $\mathbb{F}_p$-linear automorphism from $\mathbb{F}_q$ to $\mathbb{F}_q$.

Definition 2.19. An $\mathbb{F}_p[T]-$module structure on $\mathbb{F}_q$: For $\alpha \in \mathbb{F}_q$,

$$f(T) = a_d T^d + \cdots + a_1 T + a_0 \in \mathbb{F}_p[T],$$

we define

$$f(T) \circ \alpha = a_d \cdot Forb_p(\alpha)^d + \cdots + a_1 Forb_p(\alpha) + a_0.$$

$$= a_d \cdot \alpha^{p^d} + \cdots + a_1 \cdot \alpha^p + a_0 \in \mathbb{F}_q.$$

Theorem 2.20. As $\mathbb{F}_p[T]-$modules, $\mathbb{F}_q \cong \mathbb{F}_p[T]/(T^r - 1)$.

It follows that $\mathbb{F}_q$ is a cyclic torsion $\mathbb{F}_p[T]-$module, i.e.

$$\mathbb{F}_q = \mathbb{F}_p[T] \cdot \alpha \cong \mathbb{F}_p[T]/(T^r - 1) \cdot \alpha$$

for some $\alpha \in \mathbb{F}_q$. Hence

$$\{\alpha, T\alpha, \ldots, T^{r-1}\alpha\} = \{\alpha, \ldots, \alpha^{p^{r-1}}\}$$

is a basis of $\mathbb{F}_q/\mathbb{F}_p$, called a normal basis.

Definition 2.21. The trace map $Tr : \mathbb{F}_q \to \mathbb{F}_p$:

$$\alpha \mapsto Tr(\alpha) = \sum_{\sigma \in Gal(\mathbb{F}_q/\mathbb{F}_p)} \sigma(\alpha) = \alpha + \alpha^2 + \cdots + \alpha^{p^{r-1}} \in \mathbb{F}_q^{Gal(\mathbb{F}_q/\mathbb{F}_p)} = \mathbb{F}_p.$$

Tr is $\mathbb{F}_p-$linear and surjective.

We have

$$Ker(Tr) = \{x \in \mathbb{F}_q \mid Tr(x) = 0\} = \{y^p - y \mid y \in \mathbb{F}_q\}.$$

Notice that

$y_1^p - y_1 = y_2^p - y_2 \Leftrightarrow y_1^p - y_2^p = y_1 - y_2 \Leftrightarrow (y_1 - y_2)^p = y_1 - y_2 \Leftrightarrow y_1 - y_2 \in \mathbb{F}_p$

Hence

$$|Ker(Tr)| = \frac{q}{p}.$$

Similarly, for $a \in \mathbb{F}_p$,

$$\#\{x \in \mathbb{F}_q \mid Tr(x) = a\} = \frac{q}{p}.$$

Definition 2.22. The norm map $Norm : \mathbb{F}_q^* \to \mathbb{F}_p^*$:

$$Norm(\alpha) = \alpha \cdot \alpha^2 \cdot \alpha^{p^{r-1}} = \alpha^{1+p+\cdots+p^{r-1}} = \alpha^{\frac{q-1}{p-1}}.$$

Norm is a surjective group homomorphism.

More generally, for $\alpha \in \mathbb{F}_q$, we have

$$\mathbb{F}_p[x] \ni Norm(x-\alpha) = x^r - Tr(\alpha)x^{r-1} + \cdots + (-1)^r Norm(\alpha).$$

A fact about finite fields:

$$\mathbb{F}_{p^{d_1}} \subseteq \mathbb{F}_{p^{d_2}} \Leftrightarrow d_1 \mid d_2.$$

This is because $[\mathbb{F}_{p^{d_2}} : \mathbb{F}_{p^{d_1}}][\mathbb{F}_{p^{d_1}} : \mathbb{F}_p] = [\mathbb{F}_{p^{d_2}} : \mathbb{F}_p] = p^{d_2}$.

§ 3. Exponential sums over finite field $\mathbb{F}_q$

Let p be a prime and $q = p^r$, $[\mathbb{F}_q : \mathbb{F}_p] = r$. More precisely,

$$\mathbb{F}_q = \mathbb{F}_{p^r} = \mathbb{F}_p[x]/(g(x))$$

where $g(x) \in \mathbb{F}_p[x]$ is an irreducible polynomial of degree r.

Definition 3.1. For $f(x) \in \mathbb{F}_q[x]$, we define

$$S_q(f) = \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr(f(x))} \in \mathbb{Z}[\zeta_p].$$

As an algebraic integer in $\mathbb{Q}(\zeta_p)$, clearly $\deg S_q(f) | (p-1)$.

Question 3.2. $\deg S_q(f) = ?$

As we shall see, this question for general finite field $\mathbb{F}_q$ is significantly more complicated than the case of prime finite field $\mathbb{F}_p$. In fact, this problem is not completely solved, even for the simplest monomial $f(x) = x^d$ for general finite field $\mathbb{F}_q$.

Without loss of generality, we can assume that

$$1 \le d = \deg f \le q-1.$$

Since

$$Tr(x^{pk}) = Tr(x^k), \ \forall x \in \mathbb{F}_q$$

we can also assume that $p \nmid d$.

Example 3.3. Suppose $f(x) = ax + b \in \mathbb{F}_q[x],\ (a \neq 0)$, then

$$\begin{aligned} S_q(f) &= \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr(ax+b)} = \sum_{y \in \mathbb{F}_q} \zeta_p^{Tr(y)} \\ &= \sum_{a \in \mathbb{F}_p} \#\{x \in \mathbb{F}_q \mid Tr(x) = a\} \cdot \zeta_p^a \\ &= \frac{q}{p} \sum_{a \in \mathbb{F}_p} \zeta_p^a = 0. \end{aligned}$$

3.1. **Gauss sums over $\mathbb{F}_q$.** Assume now that $2 \leq d \leq q-1,\ p > 2$.

Example 3.4. Let $f(x) = x^2$, $q = p$ $(r = 1)$. Then

$$S_p(x^2) \overset{Gauss}{=} \sqrt{(-1)^{\frac{p-1}{2}} p},\ \deg S_p(x^2) = 2.$$

If $q = p^r$, then

$$-S_{p^r}(x^2) \overset{Hasse-Davenport}{=} (-S_p(x^2))^r = \left(-\sqrt{(-1)^{\frac{p-1}{2}} p}\right)^r.$$

Corollary 3.5.

$$\deg S_{p^r}(x^2) = \begin{cases} 2, & 2 \nmid r \\ 1, & 2 \mid r. \end{cases}$$

Example 3.6. Let $f(x) = ax^2 + bx + c \in \mathbb{F}_q[x]$, $a \neq 0$. By a linear transformation, we can assume that $f(x) = ax^2 + c$.

$$S_q(ax^2 + c) = S_q(ax^2) \cdot \zeta_p^{Tr(c)} = \eta(a) \cdot S_q(x^2) \cdot \zeta_p^{Tr(c)}$$

where $\eta(a) = \pm 1$, then

$$S_q(ax^2 + c) = \pm \left(-\sqrt{(-1)^{\frac{p-1}{2}} p}\right)^r \cdot \zeta_p^{Tr(c)}.$$

Corollary 3.7.

$$\deg S_q(ax^2 + c) = \begin{cases} 2, & 2 \nmid r,\ Tr(c) = 0 \\ 1, & 2 \mid r,\ Tr(c) = 0 \\ p-1, & Tr(c) \neq 0 \end{cases}$$

Example 3.8. $d = 3$, $p > 3$, $f(x) = ax^3 + bx + c \in \mathbb{F}_q[x]$, $a \neq 0$

$$\deg S_q(f) = ?$$

Classification is not yet complete.

Example 3.9. $f(x) = x^d,\ d \mid (q-1)$, $\deg S_q(x^d) =?$ (open problem)

- $q = p$ $(r = 1)$, $d \mid (p-1)$, then $\deg S_q(x^d) \overset{Gauss}{=} d$.
- Theorem (Myerson[My], 1981) Let $q = p^r$. If $d \mid (p-1)$ and $(d, r) = 1$, then $\deg S_q(x^d) = d$.
- Theorem (Wan, 2019) Let $q = p^r$. If $d \mid (p-1)$, then

$$\deg S_q(x^d) = \frac{d}{(d, r)}.$$

Idea: $\forall t \in \mathbb{F}_p^*$, $\sigma_t(\zeta_p) = \zeta_p^t$,

$$\sigma_t(S_q(x^d)) = \sum_{x \in \mathbb{F}_q} \zeta_p^{tTr(x^d)} = \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr(tx^d)} = S_q(x^d),\ \forall t \in (\mathbb{F}_q^*)^d \cap \mathbb{F}_p^* := H.$$

Then $H \subset \mathbb{F}_p^*$ and

$$H = \{t \in \mathbb{F}_q^* \mid t^{(p-1, \frac{q-1}{d})} = 1\},\ |H| = (p-1, \frac{q-1}{d}).$$

Hence $S_q(x^d) \in \mathbb{Q}(\zeta_p)^H$, therefore

$$\deg S_q(x^d) \mid [\mathbb{Q}(\zeta_p)^H : \mathbb{Q}] = \frac{p-1}{|H|} = \frac{p-1}{(p-1, \frac{q-1}{d})}.$$

If $d \mid (p-1)$, we have

$$\begin{aligned}
\frac{p-1}{(p-1, \frac{q-1}{d})} &= \frac{p-1}{(p-1, \frac{p-1}{d}\frac{q-1}{p-1})} \\
&= \frac{p-1}{\frac{p-1}{d}(d, \frac{q-1}{p-1})} \\
&= \frac{d}{(d, \frac{q-1}{p-1})} \\
&= \frac{d}{(d, r + (p-1)*)} \\
&= \frac{d}{(d, r)}.
\end{aligned}$$

Define

$$F(x) = \prod_{\sigma \in \mathbb{F}_p^*/H} (x - \sigma(S_q(x^d))) \in \mathbb{Q}[x].$$

This is a polynomial in $\mathbb{Q}[x]$ of degree $d/(d,r)$ with $S_q(x^d)$ as a root. It is enough to show that $F(x)$ is irreducible over $\mathbb{Q}$. The Stickelberger theorem implies that $v_p(S_q(ax^d)) = r/d$ for all $a \in \mathbb{F}_p^*$. Thus, the constant term of $F(x)$ has p-adic valuation given by

$$\frac{d}{(d,r)}\frac{r}{d} = \frac{r}{(d,r)}.$$

This integer is relatively prime to the degree $d/(d,r)$ of $F(x)$. It follows that $F(x)$ is a generalized p-Eisenstein [W3] and hence irreducible over $\mathbb{Q}$.

Corollary 3.10. Assume $d \mid (q-1)$ and $a \in \mathbb{F}_q^*$. Then

$$\deg S_q(ax^d) \mid \frac{p-1}{(p-1, \frac{q-1}{d})}.$$

If $d \mid (p-1)$, then

$$\deg S_q(ax^d) \;=\; \frac{p-1}{(p-1, \frac{q-1}{d})}.$$

If $d \mid \frac{q-1}{p-1}$, then

$$\deg S_q(ax^d) \;= \frac{p-1}{(p-1)(1, \frac{q-1}{(p-1)d})} = 1.$$

If d is a prime, then $\deg S_q(ax^d)$ is completely determined.

Problem 1. For general $d|(q-1)$ and $a \in \mathbb{F}_q^*$, $\deg S_q(ax^d)$ is unknown. It depends on $a \in \mathbb{F}_q^*/\mathbb{F}_p^*(\mathbb{F}_q^*)^d$.

3.2. **Kloosterman sums over $\mathbb{F}_q$.**

Definition 3.11. For $\lambda \in \mathbb{F}_q^*$, $n \in \mathbb{N}$, define the Kloosterman sum

$$Kl_{n,q}(\lambda) = \sum_{x_1,\ldots,x_n \in \mathbb{F}_q^*} \zeta_p^{Tr(x_1+\cdots+x_n+\frac{\lambda}{x_1\cdots x_n})} \in \mathbb{Z}[\zeta_p].$$

Question 3.12. $\deg Kl_{n,q}(\lambda) =?$

Idea: $\forall t \in \mathbb{F}_p^*$,

$$\begin{aligned}\sigma_t(Kl_{n,q}(\lambda)) &= \sum_{x_1,\ldots,x_n \in \mathbb{F}_q^*} \zeta_p^{Tr(tx_1+\cdots+tx_n+\frac{t^{n+1}\lambda}{tx_1\cdots tx_n})} \\ &= Kl_{n,q}(t^{n+1}\lambda).\end{aligned}$$

This is equal to $Kl_{n,q}(\lambda)$ if $t^{n+1}=1$. Let

$$H=\{t\in\mathbb{F}_p^* \mid t^{n+1}=1\}=\{t\in\mathbb{F}_p^* \mid t^{(n+1,p-1)}=1\},$$

then $|H|=(n+1,p-1)$. Hence $Kl_{n,q}(\lambda)\in\mathbb{Q}(\zeta_p)^H$ and

$$\deg Kl_{n,q}(\lambda) \mid [\mathbb{Q}(\zeta_p)^H:\mathbb{Q}]=\frac{p-1}{|H|}=\frac{p-1}{(n+1,p-1)}.$$

Theorem 3.13. ([W3], 1995) Let $q=p^r$. If $Tr(\lambda)\neq 0$, then

$$\deg Kl_{n,q}(\lambda)=\frac{p-1}{(n+1,p-1)}.$$

In the case $q=p$ ($r=1$), the condition $Tr(\lambda)=\lambda\neq 0$ is automatically satisfied and hence we recover the previous theorem in the prime field case.

Corollary 3.14. For $q=p^r$, we have

$$\#\{\lambda\in\mathbb{F}_q^* | \deg Kl_{n,q}(\lambda)=\frac{p-1}{(n+1,p-1)}\}\geq(1-\frac{1}{p})(q-1).$$

Let $\mu_p(r)$ denote the proportion of $\lambda\in\mathbb{F}_q^*$ such that $\deg Kl_{n,q}(\lambda)$ reaches its maximun value $\frac{p-1}{(n+1,p-1)}$. The above corollary implies that $\mu_p(r)\geq(p-1)/p$ for all r. One can ask if the limit of $\mu_p(r)$ exists r goes to infinity, and if so, what is the limit?

Problem 2. If $Tr(\lambda)=0$, then

$$\deg Kl_{n,q}(\lambda)=?$$

If $p>C_r$ for some explicit constant C_r, then this problem is theoretically solved by the work in [Fi] and [W3], but no simpe formula is known for $\deg Kl_{n,q}(\lambda)$, see [KRV] for an attempt.

3.3. **General results.**

Definition 3.15. Let

$$N(f)=\#\{(x,y)\in\mathbb{F}_q^2 \mid y^p-y=f(x)\}.$$

It is the number of $\mathbb{F}_q$-rational points on the affine Artin-Schveier curve $y^p-y=f(x)$. The same proof as in the prime field case gives

Theorem 3.16.

$$\frac{p-1}{(p-1,N(f)-1)} \mid \deg S_q(f) \mid (p-1).$$

Corollary 3.17. If $(p-1, N(f)-1) = 1$, then $\deg S_q(f) = p-1$.

Remark 3.18. If $q = p$, then

$$N(f) = p\#\{x \in \mathbb{F}_p \mid f(x) = 0\} \equiv \#\{x \in \mathbb{F}_p \mid f(x) = 0\} \mod (p-1).$$

This reduces to the previous result in the prime field case.

Example 3.19. If $f(x) = xg(x^e)$ for some $e|(p-1)$, then

$$\deg S_q(f) \mid \frac{p-1}{e}.$$

Corollary 3.20. If $f(x) = xg(x^e)$ for some positive integer $e|(p-1)$ and $(p-1, N(f)-1) = e$, then

$$\deg S_q(f) = \frac{p-1}{e}.$$

Question 3.21. Classification of $f(x)$ with $\deg S_q(f) = 1$?

Theorem 3.22. Let $f(x) \in \mathbb{F}_q[x]$ and $1 \le d = \deg f \le q-1$.

- If $q = p$, then
$$\deg S_q(f) = 1 \Leftrightarrow f \textit{ is PP over } \mathbb{F}_p.$$
- If $q = p^r$, then
$$\deg S_q(f) = 1 \Leftrightarrow f \textit{ is charming.}$$

Definition 3.23. $f(x) \in \mathbb{F}_q[x]$ is called charming if

$$\#\{x \in \mathbb{F}_q \mid Tr(f(x)) = k\},\ k \in \mathbb{F}_p$$

is independent of $k \in \mathbb{F}_p^*$.

Proof.

$$S_q(f) = \sum_{x \in \mathbb{F}_q} \zeta_p^{Tr(f(x))}.$$

Let

$$n_k = \#\{x \in \mathbb{F}_q \mid Tr(f(x)) = k\} \in \mathbb{Z}_{\ge 0},\ 0 \le k \le p-1.$$

Then

$$S_q(f) = \sum_{k=0}^{p-1} n_k \zeta_p^k.$$

If $m = S_q(f) \in \mathbb{Z}$, then ζ_p is a root of the polynomial

$$F(x) = (\sum_{k=0}^{p-1} n_k x^k) - m \in \mathbb{Z}[x].$$

Since $\deg F(x) \leq p-1$ and the minimal polynomial of ζ_p is

$$\phi_p(x) = x^{p-1} + x^{p-2} + \cdots x + 1,$$

we have

$$\phi_p(x) \mid F(x).$$

Hence $F(x) = c \cdot \phi_p(x)$ for some $c \in \mathbb{Q}$. Therefore

$$n_{p-1} = n_{p-2} = \cdots = n_1 = n_0 - m = c.$$

i.e. n_k is independent of $k \in \mathbb{F}_p^*$. Then $f(x)$ is charming.
Conversely, if $f(x)$ is charming, then

$$n_{p-1} = n_{p-2} = \cdots = n_1 = c \in \mathbb{Z}.$$

Hence

$$\begin{aligned} S_q(f) &= \sum_{k=0}^{p-1} n_k \zeta_p^k = (\sum_{k=1}^{p-1} n_k \zeta_p^k) + n_0 \\ &= c \cdot (\sum_{k=1}^{p-1} \zeta_p^k) + n_0 = n_0 - c \in \mathbb{Z}. \end{aligned}$$

Therefore $\deg S_q(f) = 1$. □

Example 3.24. If $f(x)$ is PP over $\mathbb{F}_q$, then

$$\#\{x \in \mathbb{F}_q \mid Tr(f(x)) = k\} = \#\{x \in \mathbb{F}_q \mid Tr(x) = k\} = \frac{q}{p}$$

for all $k \in \mathbb{F}_p$. Hence $f(x)$ is charming. The converse is not true in general. If $1 < d \mid \frac{q-1}{p-1}$, then $\deg S_q(x^d) = 1$. Hence x^d is a charming polynomial. But x^d is not a PP over $\mathbb{F}_p$. This is because

$$\#\{x \in \mathbb{F}_q \mid x^d = 1\} = d > 1.$$

Problem 3. Classify all charming polynomials over $\mathbb{F}_q$. This should be an interesting new subject, but it would be more difficult than the classification of permutation polynomials.

Definition 3.25. For $1 \leq d \leq q-1$, let

$$M_d(q) := \#\{charming\ polynomials\ of\ degree\ d\ over\ \mathbb{F}_q\}$$

Problem 4. $M_d(q) =?$ When $M_d(q) > 0$?

§ 4. Degree variations

A further basic question is how the degree of the exponential sum $S_q(f)$ varies as f varies. There are many ways that one can vary f. For example, the coefficients of f can vary in $\mathbb{F}_q$. An important example we have discussed is the variation of the degree for the Kloosterman sum $KL_n(q,\lambda)$ when the coefficient λ varies in $\mathbb{F}_q^*$. In another direction, we can fix f and let q varies. Let $f(x) \in \mathbb{F}_q[x]$ be a polynomial of degree d not divisible by p. We can ask how the degree of $S_{q^k}(f)$ varies as k varies in the set of positive integers. In this direction, we propose the following periodicity conjecture.

Conjecture 4.1 (Degree Periodicity Conjecture)**.** For any polynomial $f(x) \in \mathbb{F}_q[x]$, the degree function $\deg S_{q^k}(f)$ in k is a periodic function of k for all large k. In particular, the degree generating function

$$D(f,T) = \sum_{k=1}^{\infty} \deg S_{q^k}(f) T^k$$

is a rational function in T.

This can be easily checked to be true if $d \leq 2$. It is also true for the monomial $f(x) = ax^d$ ($a \in \mathbb{F}_q^*$) when either $d|(p-1)$ or $(d, p-1) = 1$. In particular, it is true for $f(x) = ax^d$ when d is a prime.

More generally, one can ask how the degree of exponential sums varies in a p-adic tower, in the framework of the Davis-Wan-Xiao paper [DWX].

Another variation problem is the stability of the p-adic valuation for the sequence of exponential sums $S_{q^k}(f)$ as k varies. In this direction, we propose.

Conjecture 4.2 (Valuation Stability Conjecture)**.** For any polynomial $f(x) \in \mathbb{F}_q[x]$, the p-adic valuation $v_p(\deg S_{q^k}(f))$ is periodically given by in a finite number of polynomials (possibility infinity) in p^k and k for all large k. This should also be true when one considers ℓ-adic valuation for each prime $\ell \neq p$.

§ 5. Appendices

5.1. **p-Adic numbers.** Integers $\mathbb{Z} = \{\cdots -2, -1, 0, 1, 2, \cdots\}$, we have binary operations $+, -, \times$. Given non-zero $n \in \mathbb{Z}$, $|n| =$? By unique

factorization, we can write

$$n = \pm \prod_{p \ prime} p^{a_p}, \ a_p = ?$$

$$\begin{aligned} \mathbb{Z} &\overset{\text{mod } 2}{\to} \mathbb{Z}/2\mathbb{Z} := \mathbb{F}_2 \to \cdots \to \overline{\mathbb{F}_2}, \\ &\overset{\text{mod } 3}{\to} \mathbb{Z}/3\mathbb{Z} := \mathbb{F}_3 \to \cdots \to \overline{\mathbb{F}_3}, \\ &\vdots \\ &\overset{\text{mod } p}{\to} \mathbb{Z}/p\mathbb{Z} := \mathbb{F}_p \to \mathbb{F}_{p^r} \to \overline{\mathbb{F}_p} = \bigcup_{r=1}^{\infty} \mathbb{F}_{p^r}. \end{aligned}$$

$$\mathbb{Z} \hookrightarrow \mathbb{Q} \to K \ (number \ fields) \to \overline{\mathbb{Q}} \ (algebraic \ numbers).$$

Real numbers is the completion of rational numbers

$$\mathbb{Q} \underset{completion}{\overset{|\cdot|_\infty}{\to}} \mathbb{R} \overset{algebraic \ closure}{\to} \mathbb{C} = \mathbb{R}(i).$$

There are other absolute values on $\mathbb{Q}$.
For example, take p to be a prime,

$$\mathbb{Q} \overset{|\cdot|_p}{\to} \mathbb{Q}_p \overset{algebraic \ closure}{\to} \overline{\mathbb{Q}_p} \underset{completion}{\overset{|\cdot|_p}{\to}} \mathbb{C}_p.$$

$\mathbb{C}_p$ is also algebraically closed. $(p = 2, 3, 5, \cdots)$

Definition 5.1. An absolute value $||\cdot||$ on $\mathbb{Q}$ is a non-trivial function

$$||\cdot|| : \mathbb{Q} \to \mathbb{R}_{\geq 0}$$

such that

(1) $||1|| = 1$,
(2) $||ab|| = ||a|| \cdot ||b||$,
(3) $||a + b|| \leq ||a|| + ||b||$.

Example 5.2. $|\cdot|$ is an absolute value on $\mathbb{Q}$. The trivial absolute value is defined by $|0| = 0$ and $|x| = 1$ for $x \neq 0$. We will consider non-trivial absolute values.

Definition 5.3. Let p be a prime. The $p-$adic valuation

$$v_p : \mathbb{Q} \to \mathbb{Z}.$$

If $r \in \mathbb{Q}^*$, then $r = \pm \prod_{prime} p^{a_p},\ a_p \in \mathbb{Z}$ and

$$v_p(r) = \begin{cases} a_p, & if\ r \neq 0 \\ \infty, & if\ r = 0. \end{cases}$$

(1) $v_p(1) = 0$,
(2) $v_p(r_1 r_2) = v_p(r_1) + v_p(r_2)$,
(3) $v_p(r_1 + r_2) \geq \min\{v_p(r_1),\ v_p(r_2)\}$.

Definition 5.4. The $p-$adic absolute value is defined by

$$|r|_p = (\frac{1}{p})^{v_p(r)}.$$

- $|1|_p = (\frac{1}{p})^{v_p(1)} = (\frac{1}{p})^0 = 1,\ |0|_p = (\frac{1}{p})^{v_p(0)} = (\frac{1}{p})^\infty = 0.$
- $|r_1 r_2|_p = (\frac{1}{p})^{v_p(r_1 r_2)} = (\frac{1}{p})^{v_p(r_1)+v_p(r_2)} = |r_1|_p |r_2|_p.$
- We have

$$\begin{aligned} |r_1 + r_2|_p &= (\frac{1}{p})^{v_p(r_1+r_2)} \leq (\frac{1}{p})^{\min\{v_p(r_1),\ v_p(r_2)\}} \\ &\leq \max\{(\frac{1}{p})^{v_p(r_1)},\ (\frac{1}{p})^{v_p(r_2)}\} \\ &= \max\{|r_1|_p,\ |r_2|_p\} \leq |r_1|_p + |r_2|_p. \end{aligned}$$

Hence $|\cdot|_p$ is an absolute value on $\mathbb{Q}$.

Theorem 5.5. (Ostowski) Up to equivalence of topology,

$$\{|\cdot|,\ |\cdot|_p,\ p\ primes\}$$

are all the non-trivial absolute values on $\mathbb{Q}$.

Example 5.6.

$|100|_\infty = 100,\ |100|_2 = (\frac{1}{2})^2 = \frac{1}{4},\ |100|_3 = (\frac{1}{3})^0 = 1,\ |100|_5 = (\frac{1}{5})^2 = \frac{1}{25}.$

The multiplications of these terms are just equal to 1.

Proposition 5.7. If $r \in \mathbb{Q}^*$, then $\prod_p |r|_p = 1$.

Let $r = \pm \prod_{finite\ primes} p^{a_p}$, then

$$|r|_\infty = \prod_{finite\ primes} p^{a_p},\ |r|_p = (\frac{1}{p})^{a_p}.$$

Example 5.8. $r_i \in \mathbb{Q}$, $|r_i|_p \to 0 \Leftrightarrow r_i$ is more and more divisible by p. If we write $r_i = p^{a_i} \cdot u_i$, then

$$r_i \to 0 \ p-adically \ \Leftrightarrow a_i \to \infty,$$
$$r_i \to \infty \ p-adically \ \Leftrightarrow a_i \to -\infty.$$

Proposition 5.9. An infinite series $\sum_{i=1}^{\infty} a_i, \ (a_i \in \mathbb{Q})$ converges p-adically iff $|a_i|_p \to 0$.

Reason:

$$|\sum_{i=n}^{m} a_i|_p \leq \max_{n \leq i \leq m} |a_i|_p \to 0 \ (n \to \infty).$$

Example 5.10.

$$1 + p + p^2 + p^3 + \cdots = \begin{cases} \infty & in \ \mathbb{R} \\ \frac{1}{1-p} & in \ p-adic \end{cases}$$

$$1 + (\frac{1}{p}) + (\frac{1}{p})^2 + (\frac{1}{p})^3 + \cdots = \begin{cases} \infty & in \ p-adic \\ \frac{1}{1-\frac{1}{p}} & in \ \mathbb{R} \end{cases}$$

Definition 5.11.

$$\mathbb{Q}_p = the \ limits \ of \ Cauchy \ sequences \ in \ \mathbb{Q} \ with \ p-adic \ |\cdot|_p$$
$$= the \ completion \ of \ \mathbb{Q} \ with \ respect \ to \ |\cdot|_p.$$

Real number $r \in \mathbb{R}$,

$$r = \pm a_m \cdots a_0 . a_{-1} a_{-2} \cdots (decimal \ expansion)$$

where $a_i \in \{0, 1, , \ldots, 9\}$. The expression is essentially unique, for example $1 = 0.9999 \cdots$.

$r = \pm a_m \cdot (10^m) + a_{m-1} \cdot (10^{m-1}) + \cdots + a_0 + a_{-1}(10)^{-1} + a_{-2}(10)^{-2} + \cdots$

$p-$adic numbers.

$$r = a_{-m} \cdots a_{-1} \cdot a_0 \cdot a_1 a_2 \cdots, \ a_i \in \{0, 1, \cdots, p-1\}$$
$$r = a_{-m}(\frac{1}{p})^m + \cdots a_{-1}(\frac{1}{p})^1 + a_0 + a_1 p^1 + a_2 p^2 + \cdots$$
$$|r|_p = (\frac{1}{p})^{-m} = p^m, \ a_m \neq 0.$$

Unlike the case in real numbers, $|r_1 + r_2|_p = \max\{|r_1|_p, \ |r_2|_p\}$ if $|r_1|_p \neq |r_2|_p$.

Definition 5.12.

$$\begin{aligned}\mathbb{Z}_p &= \ p-adic\ completion\ of\ \mathbb{Z}\\ &= a_0+a_1p+a_2p^2+\cdots,\ a_i\in\{0,1,\ldots,p-1\}\ (\ p-adic\ integers\ )\\ &= \{r\in\mathbb{Q}_p\mid |r|_p\le 1\}.\end{aligned}$$

Proposition 5.13.

(1) $\mathbb{Z}_p$ is a subring of $\mathbb{Q}_p$.
(2) $\mathbb{Q}_p$ is a field.
(3) $\mathbb{Q}_p$ is complete under $|\cdot|_p$.

Example 5.14. $x^2-p=(x-\sqrt{p})(x+\sqrt{p})$ is irreducible in $\mathbb{Q}_p$.

Since $|\sqrt{p}|_p=(\frac{1}{p})^{\frac{1}{2}}$, if $\sqrt{p}\in\mathbb{Q}_p$, then $|\sqrt{p}|=(\frac{1}{p})^m,\ m\in\mathbb{Z}$, which is a contradiction. Hence $\sqrt{p}\notin\mathbb{Q}_p$.

$$\mathbb{Q}_p \overset{finite\ extension}{\to} K\ (p\text{–}adic\,number\ fields)\to \overline{\mathbb{Q}_p}(alg\ closure\ of\ \mathbb{Q}_p)\overset{|\cdot|_p}{\to}\mathbb{C}_p.$$

If $z\in\mathbb{C}$, $\mathbb{Q}\to\mathbb{R}\to\mathbb{C}$, then $|z|=\sqrt{z\overline{z}}=\sqrt{\prod_{\sigma\in Gal(\mathbb{C}/\mathbb{R})}\sigma(z)}$.

If $z\in\overline{\mathbb{Q}_p}$, let

$$f(x)=x^d+a_1x^{d-1}+\cdots+a_d\in\mathbb{Q}_p[x]$$

be the minimal polynomial of z over $\mathbb{Q}_p$. Then $|z|_p=(|a_d|_p)^{\frac{1}{d}}$.

$$|\sqrt{p}|_p=(|\sqrt{p}(-\sqrt{p})|_p)^{\frac{1}{2}}=(|-p|_p)^{\frac{1}{2}}=(\frac{1}{p})^{\frac{1}{2}}.$$

Example 5.15. $\frac{x^p-1}{x-1}=\prod_{k=1}^{p}(x-\zeta_p^k),\ \zeta_p\in\overline{\mathbb{Q}_p}$. Let $\pi=\zeta_p-1$, then $\mathbb{Q}(\zeta_p)=\mathbb{Q}(\pi)$. $|\zeta_p|_p=1$, $|\pi|_p=\ (\frac{1}{p})^{\frac{1}{p-1}}$:

$$\prod_{k=1}^{p-1}(x-\zeta_p^k)=x^{p-1}+x^{p-2}+\cdots+x+1.$$

Take $x = 1$, then $\prod_{k=1}^{p-1}(1-\zeta_p^k) = p$. For $kh = 1$ in $\mathbb{F}_p^*$, we have

$$\frac{1-\zeta_p^k}{1-\zeta_p} = \zeta_p^{k-1} + \zeta_p^{k-2} + \cdots + \zeta_p + 1 \in \mathbb{Z}[\zeta_p],$$
$$\frac{1-\zeta_p}{1-\zeta_p^k} = \frac{1-\zeta_p^{k\cdot h}}{1-\zeta_p^k} = 1 + \zeta_p^k + \cdots + (\zeta_p^k)^{h-1} \in \mathbb{Z}[\zeta_p].$$

Hence

$$p = \prod_{k=1}^{p-1}(1-\zeta_p^k) = \pi^{p-1} \cdot u$$

where $u \in \mathbb{Z}[\zeta_p]^* \hookrightarrow u \in \mathbb{Z}_p[\zeta_p]^*$.

Example 5.16. The logarithim function

$$\log(1+x) = x - \frac{x^2}{2} + \cdots + (-1)^{n-1}\frac{x}{n} + \cdots = \sum_{n=1}^{\infty}(-1)^{n-1}\frac{x}{n}$$

converges for $|x| < 1$ in $\mathbb{C}$ and converges for $|x|_p < 1$ in $\mathbb{C}_p$.

$$\sum_{n=0}^{\infty} n^{n^n} x^n$$

converges for $x = 0$ in $\mathbb{C}$, but converges for $|x|_p < 1$ in $\mathbb{C}_p$.

Example 5.17. The exponential function

$$e^x = \sum_{n=0}^{\infty}\frac{x^n}{n!} = 1 + x + \frac{x^2}{2!} + \frac{x^3}{3!} + \cdots$$

converges in $|x| < \infty$ in $\mathbb{C}$ (entire function). But e^x converges in $|x|_p < (\frac{1}{p})^{\frac{1}{p-1}}$ in $\mathbb{C}_p$. Indeed, this is because $v_p(n!) = \frac{n-\sigma(n)}{p-1}$, where $\sigma(p)$ is the sum of p-digits of n. Write

$$n = n_0 + n_1 p + n_2 p^2 + \cdots + n_k p^k,\ 0 \le n_i < p.$$

Then $\sigma(n) = n_0 + n_1 + n_2 + \cdots + n_k$. Hence e^x converges

$$\Leftrightarrow \frac{|x|_p^n}{|n!|_p} \to 0 \Leftrightarrow |x|_p^n \cdot p^{\frac{n}{p-1}} \to 0 \Leftrightarrow |x|_p \cdot p^{\frac{1}{p-1}} \to 0 \Leftrightarrow |x|_p < (\frac{1}{p})^{\frac{1}{p-1}}.$$

5.2. **Zeta functions and L-functions over $\mathbb{F}_q$.** Let p be a prime and $q = p^r$, $r \in \mathbb{N}$.

$$f(x_1, \ldots, x_n) \in \mathbb{F}_q[x_1, \ldots, x_n],$$
$$\mathbb{F}_q \to \mathbb{F}_{q^k} \to \overline{\mathbb{F}_q}.$$

Definition 5.18.

(1)

$$N_k(f) := \#\{(x_1, \ldots, x_n) \in \mathbb{F}_{q^k}^n \mid f(x_1, \ldots, x_n) = 0\},\ k = 1, 2, ...$$

(2)

$$S_k(f) := \sum_{x_1, \ldots, x_n \in \mathbb{F}_{q^k}} \zeta_p^{Tr_{\mathbb{F}_{q^k}/\mathbb{F}_p}(f(x_1, \ldots, x_n))} \in \mathbb{Z}[\zeta_p],\ k = 1, 2, ...$$

Then

$$q^k N_k(f) = S_k(x_0 f(x_1, \ldots, x_n)) = \sum_{x_0 \in \mathbb{F}_{q^k}} \sum_{x_1, \ldots, x_n \in \mathbb{F}_{q^k}} \zeta_p^{Tr_{\mathbb{F}_{q^k}/\mathbb{F}_p}(x_0 f(x_1, \ldots, x_n))}.$$

Definition 5.19. The zeta function is

$$Z(f, T) = \exp(\sum_{k=1}^{\infty} \frac{T^k}{k} N_k(f)) \in \mathbb{Q}[[T]].$$

The L-function is

$$L(f, T) = \exp(\sum_{k=1}^{\infty} \frac{T^k}{k} S_k(f)) \in \mathbb{Q}[\zeta_p][[T]].$$

Theorem 5.20. (Dwork, 1960)

$$Z(f, T) \in \mathbb{Q}(T),\ L(f, T) \in \mathbb{Q}(\zeta_p)(T).$$

Write

$$Z(f, T) = \frac{\prod_{i=1}^{\rho_1}(1 - \alpha_i T)}{\prod_{j=1}^{\rho_2}(1 - \beta_j T)} \ in\ \overline{\mathbb{Q}}.$$

Then

$$N_k(f) = \beta_1^k + \cdots + \beta_{\rho_2}^k - \alpha_1^k - \cdots - \alpha_{\rho_1}^k,\ k = 1, 2, \cdots$$

Proof. (Dwork)

(1) $Z(f, T)$ is a p-adic mereomorphic function in T.

(2) $Z(f, T)$ converges in $|T| < s,\ (s > 0)$ in $\mathbb{C}$.

(3) The coefficients are integers in $\mathbb{Z}$ (or in a fixed number field).

□

Theorem 5.21. (Deligne, 1980) As complex numbers,

$$|\alpha_i| = \sqrt{q}^{n_i},\ |\beta_j| = \sqrt{q}^{m_j},$$

where $n_i,\ m_j \in \mathbb{Z} \cap [0, n]$

As ℓ-adic numbers ($\ell \neq p$), $|\alpha_i|_l = |\beta_i|_l = 1$.

Problem 5. As p-adic numbers, $|\alpha_i|_q = |\alpha_i|_p^r =?$, $|\beta_j|_q = |\beta_j|_p^r =?$

$$-\log_q |\alpha_i|_q = v_q(\alpha_i) = \frac{1}{r} v_p(\alpha_i) =?,\ v_q(\beta_j) = \frac{1}{r} v_p(\beta_j) =?$$

For a systematic study of this slope problem for L-functions of exponential sums, see the exposition in [W4].

Example 5.22. (Kloosterman sums over $\mathbb{F}_q$) Let $\lambda \in \mathbb{F}_q^*$, $n \in \mathbb{N}$,

$$Kl_{n,q^k}(\lambda) = \sum_{x_1,\dots,x_n \in \mathbb{F}_{q^k}} \zeta_p^{Tr_{\mathbb{F}_{q^k}/\mathbb{F}_p}(x_1+\cdots+x_n+\frac{\lambda}{x_1\cdots x_n})}.$$

$$\begin{aligned} L(Kl_n(\lambda), T)^{(-1)^{n-1}} &= \exp(\sum_{k=1}^{\infty} \frac{T^k}{k} Kl_{n,q^k}(\lambda))^{(-1)^{n-1}} \\ &= \prod_{i=1}^{n+1} (1 - \alpha_i T). \end{aligned}$$

Hence

$$Kl_{n,q^k}(\lambda) = (-1)^n(\alpha_1^k + \cdots + \alpha_{n+1}^k).$$

In $\mathbb{C}$, $\Rightarrow (Deligne, 1980)$ $|\alpha_i| = \sqrt{q}^n$. Hence

$$|\ Kl_{n,q^k}(\lambda)\ | \leq (n+1)\sqrt{q}^{nk},\ k = 1, 2, \dots$$

In $\mathbb{C}_p$, $\Rightarrow (Sperber, 1986)$ $v_q(\alpha_i) = i,\ i = 0, 1, \dots, n,\ |\alpha_i|_q = (\frac{1}{q})^i$.

Example 5.23. (Gauss sums) $f(x) = x^d$, $d \mid (q-1)$,

$$S_{q^k}(x^d) = \sum_{x \in \mathbb{F}_{q^k}} \zeta_p^{Tr_{\mathbb{F}_{q^k}/\mathbb{F}_p}(x^d)}, \ k = 1, 2, 3, \ldots$$

$$\begin{aligned} L_d(T) :&= \exp(\sum_{k=1}^{\infty} \frac{T^k}{k} S_{q^k}(x^d)) \\ &= \prod_{i=1}^{d-1} (1 - \alpha_i T), \ |\alpha_i| = \sqrt{q}. \end{aligned}$$

The Hasse-Davenport relation implies that the α_i's are the standard Gauss sums:

$$\alpha_i = -\sum_{x \in \mathbb{F}_q} \chi_i(x) \zeta_p^{Tr(x)},$$

where $\chi_i = \omega^{(1-q)i/d}$ and ω is the Teichmuller character of $\mathbb{F}_q^*$.

As complex numbers, it is easy to check that $|\alpha_i| = \sqrt{q}$.

Problem 6. In $\mathbb{C}_p$, $|\alpha_i|_q =?$, $v_q(\alpha_i) =?$

The answer is given by the following classical result.

Theorem 5.24. (Stickelbeger, 1890). For $1 \leq i \leq d-1$, write

$$\frac{q-1}{d} i = k_0(i) + k_1(i)p + \cdots + k_{r-1}(i)p^{r-1}$$

in base p-expansion, where the $k_j(i) \in \{0, 1, \ldots, p-1\}$ are the p-digits. Then

$$v_q(\alpha_i) = \frac{1}{r(p-1)} \left(\sum_{j=0}^{r-1} k_j(i) \right).$$

Question 5.25. For $a \in \mathbb{F}_q^*$ and $d|(q-1)$,

$$v_q(S_q(ax^d)) =?$$

No simple formula is known in general. But if $d|(p-1)$, then $k_j(i) = i(p-1)/d$ for all $1 \leq d-1$ and $0 \leq j \leq r-1$, and thus the Stickelberger theorem gives

$$v_q(\alpha_i) = \frac{i}{d}, \ 1 \leq i \leq d-1,$$

and

$$v_q(S_q(x^d)) = v_q(-\alpha_1 - \cdots - \alpha_{d-1}) = \frac{1}{d}.$$

§ References

[BE] D. C. Berdt and R. J. Evans, The determination of Gauss sums, Bull. Amer. Math. Soc. (N.S.) 5 (1981), 107-121.

[CF] S.D. Cohen and M.D. Fried, Lenstra's proof of the Carlitz-Wan conjecture on exceptional polynomials: an elementary version, Finite Fields & Appl., Vol. 1, 3(1995), 372-375.

[DWX] C. Davis, D. Wan and L. Xiao, Newton slopes for Artin-Schreier-Witt towers, Math. Ann., 364 (2016), no. 3, 1451-1468.

[Fi] B. Fisher, Kloosterman sums as algebraic integers, Math. Ann., Vol 301, 1(1995), 485-505.

[HP] D.R. Heath-Brown and S. J. Patterson, The distribution of Kummer sums at prime arguments, J. Reine Angew. Math., 310 (1979), 111-130.

[KRV] K. Kononen, M. Rinta-aho, K. Väänänen, On the degree of a Kloosterman sum as an algebraic integer, https://arxiv.org/abs/1107.0188.

[My] G. Myerson, Period polynomials and Gauss sums for finite fields, Acta Arith., 39 (1981), 251-264.

[Pa] S. J. Patterson, On the distribution of Kummer sums, J. Reine Angew. Math., 303/304 (1978), 126-143.

[W1] D. Wan, Some arithmetic properties of the minimal polynomials of Gauss sums, Proc. Amer. Math. Soc., Vol 100, 2(1987), 225-228.

[W2] D. Wan, Permutation polynomials and resolution of singularities over finite fields, Proc. Amer. Math. Soc., 110(1990), 303-309.

[W3] D. Wan, Minimal polynomials and distinctness of Kloosterman sums, Finite Fields & Appl., 1(1995), 189-203.

[W4] D. Wan, Variation of p-adic Newton polygons for L-functions of exponential sums, Asian J. Math. Vol 8, 3(2004), 427-474.

[W5] D. Wan, Mirror symmetry for zeta functions, In Mirrror Symmetry V, AMS/IP Studies in Advanced Mathematics, Vol.38, 2006, 159-184.