Character sums and their applications

Ta The Anh
Mathematics BSc

May 2014

Supervisor: Gyarmati Katalin

Faculty of Science, Institute of Mathematics
Eötvös Loránd University

Contents

Acknowledgment

I would like to thank my supervisor Gyarmati Katalin for her time, her helps and encouragements. She has introduced to me many interesting problems, results and papers. She also had read carefullly through my manuscripts several times, pointed out and corrected quite a lot of errors. For all of that I will always be grateful.

Ta The Anh

Notations

$\mathbb{N}, \mathbb{Z}, \mathbb{C}$ are the sets of natural numbers, integers, complex numbers respectively.

$\mathbb{Z}_n$ is the group of residue classes modulo n.

$\mathbb{F}_q$ is the finite field of q elements.

$\overline{\mathbb{F}_q}$ is the algebraic closure of $\mathbb{F}_q$.

$\mathbb{Z}_n^*$ is the multiplicative group of $\mathbb{Z}_n$.

C_n is the cyclic group of order n.

$\mathbb{S}^1 = \{z \in \mathbb{C} : |z| = 1\}$.

$e(x) := e^{2i\pi x}$.

$\phi(n)$ is the Euler phi function at n.

$\mu(n)$ is the Möbius function at n.

$(\frac{\cdot}{p})$ is the Legendre symbol modulo p.

$\omega(n)$ is the number of distinct prime divisors of n.

$g(x) = O(f(x))$ means that there is a constant $C > 0$ such that $|g(x)| < C \cdot f(x)$ as $x \to \infty$.

$g(x) \ll f(x)$ also means $g(x) = O(f(x))$.

$g(x) = o(f(x))$ means that $\lim\limits_{x\to\infty} \frac{g(x)}{|f(x)|} = 0$ as $x \to \infty$.

$g(x) \sim f(x), x \to \infty$ means that $\frac{g(x)}{f(x)} \to 1$ as $x \to \infty$.

1 Introduction

In the present thesis, I study the distribution of primitive roots, quadratic residues and quadratic non-residues modulo a prime. In Sections 1 and 2, I will recall some of the most important earlier results, which I will use to solve some problems in Sections 3 and 4. These two sections contain my own results: Theorems 2.3.5, 3.1.1, 3.1.2, 3.2.1, 3.2.2, 4.1.5, 4.2.1 and 4.2.2. Section 5 introduces famous open questions about primitive roots. An Appendix is a summary of an elementary proof for a weaker version of Weil's theorem from [1].

1.1 Order and primitive root

Let n and a be positive integers with $(n, a) = 1$. By Euler theorem we have: $a^{\phi(n)} \equiv 1 \pmod{n}$. We recall the definitions of the *multiplicative order* and the *primitive root* modulo n as

Definition 1.1.1 The *multiplicative order* of a modulo n, denoted by $\mathrm{ord}_n(a)$, is the smallest positive integer which satisfies $a^{\mathrm{ord}_n(a)} \equiv 1 \,(\bmod\ n)$. We obtain that $\mathrm{ord}_n(a)$ divides $\phi(n)$. If $\mathrm{ord}_n(a) = \phi(n)$, then a is called a *primitive root* modulo n.

In other words, a is a primitive root modulo n if and only if the residue class of a modulo n is a generator of $\mathbb{Z}_n^*$. In general, primitive roots modulo n exist iff $\mathbb{Z}_n^*$ is a cyclic group. We have

Theorem 1.1.2 (*Classification of the multiplicative group of residue classes*)

i) $\mathbb{Z}_1^* \cong C_1$.

ii) $\mathbb{Z}_2^* \cong C_1$, $\mathbb{Z}_4^* \cong C_2$ and $\mathbb{Z}_{2^k}^* \cong C_2 \times C_{2^{k-2}}$, when $k > 2$.

iii) $\mathbb{Z}_{p^k}^* \cong C_{\phi(p^k)} = C_{p^{k-1}(p-1)}$, if p is an odd prime.

iv) In general, if $n = p_1^{k_1} p_2^{k_2} p_3^{k_3} \dots p_r^{k_r}$, then using the Chinese remainder theorem, we get

$$\mathbb{Z}_n^* \cong \mathbb{Z}_{p_1^{k_1}}^* \times \mathbb{Z}_{p_2^{k_2}}^* \times \ldots \times \mathbb{Z}_{p_r^{k_r}}^*.$$

Thus $\mathbb{Z}_n^*$ is a cyclic group iff $n = 2,\ 4,\ p^k$ or $2p^k$, where p is an odd prime. As a consequence, we see that primitive roots modulo n exist only for these values of n. The number of primitive roots modulo n is $\phi(\phi(n))$ ([2, Theorem 10.9]).

Definition 1.1.3 Let g be a primitive root modulo n. For every integer x with $(x, n) = 1$, the *discrete logarithm* of x denotes the unique integer $\mathrm{ind}_g(x)$ which satisfies $0 \leq \mathrm{ind}_g(x) \leq \phi(n) - 1$ and

$$x \equiv g^{\mathrm{ind}_g(x)} \pmod{n}.$$

1.2 Multiplicative character.

Definition 1.2.1 We call a function $\chi : \mathbb{Z} \to \mathbb{C}$ is a *multiplicative charater* modulo n if it has the following properties:

i) $\chi(k + n) = \chi(k)$ for all integer k,

ii) $\chi(k) = 0$ if and only if $(k, n) > 1$,

iii) $\chi(kh) = \chi(k)\chi(h)$ for all integers k and h.

Remarks. i) We call a multiplicative character modulo n is *principal* and we denote it by χ_0, if $\chi(k) = 1$ for all k with $(k, n) = 1$ and $\chi(k) = 0$ for all k with $(k, n) > 1$.

ii) A multiplicative character χ is of *order* d if d is the smallest positive integer with $\chi^d = \chi_0$. We write $\mathrm{ord}(\chi) = d$.

iii) We write $\bar{\chi}(k) = \overline{\chi(k)}$.

Let n be a positive integer. Consider its prime factorization: $n = 2^\alpha p_1^{\alpha_1} p_2^{\alpha_2} \dots p_r^{\alpha_r}$, where p_i's are distinct odd primes. Then every multiplicative character modulo n is of the form $\chi = \chi' \chi_1 \chi_2 \dots \chi_r$, where χ' is a character modulo 2^α, χ_i is a character modulo $p_i^{\alpha_i}$ for $i = 1, 2, \dots, r$.

All multiplicative characters modulo p^α where p is an odd prime and $\alpha \geq 1$, or $p = 2$ and $\alpha \in \{1, 2\}$, are of the form:

$$\chi(k) = \begin{cases} e(\frac{\mathrm{ind}_g(k) \cdot l}{\phi(p^\alpha)}) \text{ if } p \nmid k, \\ 0 \text{ if } p \mid k. \end{cases}$$

where g is a primitive root modulo p^α and $l = 0, 1, 2, \dots, \phi(p^\alpha) - 1$.

The case of modulo 2^α when $\alpha \geq 3$ is different. For every odd integer k, we denote by $b(k)$ the unique integer such that $1 \leq b(k) \leq \frac{\phi(p^\alpha)}{2}$ and

$$k \equiv (-1)^{\frac{k-1}{2}} \cdot 5^{b(k)} \pmod{2^\alpha}.$$

All multiplicative characters modulo 2^α are of the form:

$$\chi'(k) = \begin{cases} (-1)^{\frac{k-1}{2} \cdot a} \cdot e(\frac{b(k)}{2^{\alpha-2}} \cdot c) \text{ if } b(k) \text{ is odd}, \\ 0 \text{ if } b(k) \text{ is even}. \end{cases}$$

where $a = 1, 2$ and $c = 1, 2, \dots, \frac{\phi(2^\alpha)}{2}$.

We just have described all multiplicative characters modulo n. The following propositions are basic properties of multiplicative characters:

Proposition 1.2.3 We have

$$\sum_{\chi \pmod n} \chi(x) = \begin{cases} \phi(n) \text{ if } x \equiv 1 \pmod n, \\ 0 \text{ if } x \not\equiv 1 \pmod n. \end{cases} \tag{1.2.1}$$

Proposition 1.2.4 We have

$$\sum_{x=1}^{n} \chi(x) = \begin{cases} \phi(n) \text{ if } \chi = \chi_0, \\ 0 \text{ if } \chi \neq \chi_0. \end{cases} \tag{1.2.2}$$

Proposition 1.2.5 Let x be an integer and n be a positive integer with $(x, n) = 1$. For given integers $m_1, m_2, \dots, m_r$, we have:

$$\#\{i : m_i \equiv x \pmod n\} = \frac{1}{\phi(n)} \cdot \sum_{\chi \pmod n} \chi(x) \sum_{i=1}^{r} \overline{\chi}(m_i). \tag{1.2.3}$$

Proposition 1.2.6 For a given charater χ of order d modulo n, we have

$$1 + \chi(x) + \chi(x)^2 + \dots + \chi(x)^{d-1} = \begin{cases} d \text{ if } x = y^d \text{ for some } y \in \mathbb{Z}_n^*, \\ 1 \text{ if } (x, n) > 1, \\ 0 \text{ otherwise.} \end{cases} \tag{1.2.4}$$

We will use these propositions in the next sections.

1.3 Additive character.

Definition 1.3.1 Let $(G, +)$ be a finite abelian group. We define an *additive character* of G as a homomorphism $\psi : G \to \mathbb{S}^1$. Thus $\psi(x + y) = \psi(x) \cdot \psi(y)$ for all $x, y \in G$.

Remark. We will only consider the cases when $G = \mathbb{Z}_p$, $G = \mathbb{Z}_p \times \mathbb{Z}_p$ and $G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$, where p is a prime.

If $G = \mathbb{Z}_p$, then all additive characters of G are of the form

$$\psi_r(x) = e(\frac{rx}{p}) \text{ for all } x \in G,$$

where $r \in \{0, 1, 2, \dots, p - 1\}$.

If $G = \mathbb{Z}_p \times \mathbb{Z}_p$, then all additive characters of G are of the form

$$\psi_{r,s}((x,y)) = e(\frac{rx+sy}{p}) \text{ for all } (x,y) \in G,$$

where $r, s \in \{0, 1, 2, \ldots, p-1\}$.

If $G = \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1} \times \mathbb{Z}_{p-1}$, then all additive characters of G are of the form

$$\psi_{r,s,t}((x,y,z)) = e(\frac{rx+sy+tz}{p-1}) \text{ for all } (x,y,z) \in G,$$

where $r, s, t \in \{0, 1, 2, \ldots, p-2\}$.

We recall some basic properties of additive characters:

Proposition 1.3.2 For a given $x \in G$, we have

$$\sum_{\psi} \psi(x) = \begin{cases} |G| \text{ if } x = 0, \\ 0 \text{ if } x \neq 0. \end{cases} \tag{1.3.1}$$

Proposition 1.3.3 For a given additive character ψ of G, we have

$$\sum_{x \in G} \psi(x) = \begin{cases} |G| \text{ if } \psi = \psi_0, \\ 0 \text{ if } \psi \neq \psi_0. \end{cases} \tag{1.3.2}$$

1.4 Estimates for character sums.

In order to solve certain counting problems we will use character and exponential sums. The next step is to estimate them. In Propositions 1.2.4 and 1.3.3, character sums over the whole groups are well studied. We recall some bounds for character sums over subsets of groups.

Character sums over intervals of the form $\sum\limits_{x=m+1}^{m+n} \chi(x)$ are called *incomplete sums*. Pólya and Vinogradov proved the following famous estimate:

Theorem 1.4.1 (*Pólya-Vinogradov Inequality*) Let χ be a nonprincipal multiplicative character modulo q, $q > 2$ and m, n be two integers with $n > 0$. Then we have

$$\left| \sum_{x=m+1}^{m+n} \chi(x) \right| \ll \sqrt{q} \cdot \log q. \tag{1.4.1}$$

At the present time, the best bound for incomplete sums is due to Burgess in [3]:

Theorem 1.4.2 (*Burgess' bound*, [3]) Let p be a prime and χ be a non-principal multiplicative character modulo p. For any integers m, n, r with $n, r > 0$, we have

$$\left|\sum_{x=m+1}^{m+n} \chi(x)\right| \ll n^{1-\frac{1}{r+1}} \cdot p^{\frac{1}{4r}} \cdot \log p. \tag{1.4.2}$$

The following result which is due to Gyarmati and Sárközy studies multiplicative character sums over arbitrary subsets:

Theorem 1.4.3 (*The dual of Vinogradov's lemma*) [4, Theorem 2] If $\alpha(x), \beta(x)$ are complex valued functions over the finite field $\mathbb{F}_q$ and χ is a nonprincipal multiplicative character modulo q, then writing

$$\mathcal{S} = \sum_{x\in\mathbb{F}_q}\sum_{y\in\mathbb{F}_q}\alpha(x)\beta(y)\chi(x+y),$$

and

$$X = \sum_{x\in\mathbb{F}_q}|\alpha(x)|^2 \ , \ Y = \sum_{y\in\mathbb{F}_q}|\beta(y)|^2$$

we have

$$|\mathcal{S}| \leq (XYq)^{1/2}. \tag{1.4.3}$$

The proof uses Weil's theorem and Vinogradov's lemma.

In [4], Gyarmati and Sárközy proved the following generalization of Vinogradov's lemma for two variable polynomials over a finite field:

First, we give the definition of the *primitive kernel* in [4]. Let $f(x,y) \in \mathbb{F}_q[x,y]$ be a two variable polynomial. Write

$$f(x,y) = \sum_{i=0}^{n} r_i(y)x^i = \sum_{j=0}^{m} s_j(x)y^j \text{ where } r_i(y) \in \mathbb{F}_q[y] \ , \ s_j(x) \in \mathbb{F}_q[x].$$

Then $f(x,y)$ is said to be *primitive in x* if $\gcd(r_1(y), r_2(y), \cdots, r_n(y)) = 1$ and *primitive in y* if $\gcd(s_1(x), s_2(x), \cdots, s_m(x)) = 1$.

We write $f(x,y)$ in the following form

$$f(x,y) = R(y)S(x)H(x,y),$$

where the polynomial $H(x,y)$ is primitive both in x and y. $H(x,y)$, which is well defined up to a constant factor, is called the *primitive kernel* of $f(x,y)$.

Theorem 1.4.4 (*Gyarmati, Sárközy*) [4, Theorem 5] Assume that $\alpha(x)$,$\beta(x)$ are complex valued functions on $\mathbb{F}_p$, χ is a nonprincipal multiplicative character of order d of $\mathbb{F}_p$, and $f(x,y)$ is a two variable polynomial over $\mathbb{F}_p$ such that its primitive kernel $H(x,y)$ is not of the form $cK(x,y)^d$. Let n,m be the degree of $f(x,y)$ in variables x,y respectively. Writing

$$\mathcal{S} = \sum_{x\in\mathbb{F}_p}\sum_{y\in\mathbb{F}_p}\alpha(x)\beta(y)\chi(f(x,y)),$$

$$X = \sum_{x\in\mathbb{F}_p}|\alpha(x)|^2\ ,\ Y = \sum_{y\in\mathbb{F}_p}|\beta(y)|^2$$

and

$$b = \max_{y\in\mathbb{F}_p}|\beta(y)|,$$

we have

$$|S| < \left(X(2nYp^{3/2} + 5b^2nmp^2)\right)^{1/2}. \tag{1.4.4}$$

For problems of counting special values of polynomial over finite fields, we will use the following theorem of Weil:

Theorem 1.4.5 (*Weil's bound*) Let $h(x) \in \mathbb{F}_p[x]$ be a polynomial and χ be a nonprincipal multiplicative character of order k modulo p. Suppose that $h(x)$ is not of the form $ch_1(x)^k$. Denote by s the number of distinct roots of $h(x)$ in $\overline{\mathbb{F}_p}$. We have:

$$\left|\sum_{x=0}^{p-1}\chi(h(x))\right| \le (s-1)\cdot\sqrt{p} \le (\deg(h)-1)\cdot\sqrt{p}. \tag{1.4.5}$$

In Appendix, we give an elementary proof of a weaker version of Weil's bound from [1].

For additive characters, we have the following estimates:

Lemma 1.4.6 ([2, Theorem 8.21]) Let p be a prime and M be a natural number with $1 < M < p$. Then for any natural number r with $1 < r < p$, we have

$$\left|\sum_{1\le x\le M} e(\frac{rx}{p})\right| \le \frac{p}{2r}. \tag{1.4.6}$$

The sums of the form $\mathrm{Kl}(r, s; p) = \sum\limits_{0<t<p} e(\frac{rt+s\cdot\frac{1}{t}}{p})$ are called the *Kloosteman sums*. We have

Theorem 1.4.7 (*Weil's bound for Kloosterman sum*)

$$|\mathrm{Kl}(r, s; p)| \leq 2\sqrt{p}. \tag{1.4.7}$$

(See for example [5, Chapter 11]).

Conditional bounds for character sums are also obtained under the assumption of the generalised Riemann hypothesis.

Conjecture 1.4.8 (*The Generalised Riemann hypothesis - GRH*) For a given multiplicative character χ modulo q, define the corresponding *Dirichlet L-function* of χ by

$$L(\chi, s) = \sum_{n=1}^{\infty} \frac{\chi(n)}{n^s} \text{ for all } s \in \mathbb{C} \text{ with } Re(s) > 1.$$

Then $L(\chi, s)$ has an analytic continuation to a meromorphic function over $\mathbb{C}$. GRH states that if $L(\chi, s) = 0$ and $0 < Re(s) < 1$, then $Im(s) = 1/2$.

The case $q = 1$ and $\chi(n) = 1$ for all n is the original *Riemann hypothesis*.

Assuming GRH, Montgomery and Vaughan showed the following estimate for character sum, which improves the Pólya-Vinogradov's inequality:

Corollary 1.4.9 ([6]) Under the assumption of GRH, we have

$$\left|\sum_{x=m+1}^{m+n} \chi(x)\right| \ll \sqrt{q} \cdot \log \log q. \tag{1.4.8}$$

2 Extremal values

2.1 The least primitive root.

Let p be a prime. There are $\phi(p-1)$ distinct primitive roots modulo p. We will give an upper bound for the smallest primitive root modulo p. Denote by $g(p)$ the least primitive root modulo p. We will use estimates of character sums in order to give an upper bound for $g(p)$.

Let m, n be integers, with $0 < m < m+n < p$. Denote by $\mathcal{N}_{m,n}$ the number of primitive roots modulo p between $m+1$ and $m+n$. Write $p-1 = \prod\limits_{i=1}^{r} q_i^{\alpha_i}$, and $Q = \prod\limits_{i=1}^{r} q_i$, where q_i's are distinct primes. We prove the following well known identity:

Lemma 2.1.1 ([6, 9.20])

$$\mathcal{N}_{m,n} = \frac{1}{Q}\sum_{d|Q}\phi(\frac{Q}{d})\mu(d)\sum_{\chi:\ \mathrm{ord}(\chi)=d}\ \sum_{x=m+1}^{m+n}\chi(x). \tag{2.1.1}$$

Proof of Lemma 2.1.1 Using formula (1.2.4) for every charater χ_i of order q_i and $x \not\equiv 0 \,(\mathrm{mod}\ p)$, we have

$$1 + \chi_i(x) + \chi_i(x)^2 + \ldots + \chi_i(x)^{q_i-1} = \begin{cases} q_i \text{ if } q_i \mid \mathrm{ind}_g(x), \\ 0 \text{ otherwise.} \end{cases}$$

Since an integer x is a primitive root modulo p iff $\mathrm{ord}_p(x) = p-1$, which is equivalent to $(\mathrm{ind}_g(x), Q) = 1$, we have:

$$\prod_{i=1}^{r}(1 - \frac{1 + \chi_i(x) + \ldots + \chi_i(x)^{q_i-1}}{q_i}) = \begin{cases} 1 \text{ if } x \text{ is a primitive root modulo } p \\ 0 \text{ otherwise.} \end{cases} \tag{2.1.2}$$

Summing up formulas (2.1.2) for all $x \in \{m+1, m+2, \ldots, m+n\}$, we obtain:

$$\mathcal{N}_{m,n} = \sum_{x=m+1}^{m+n}\ \prod_{i=1}^{r}(1 - \frac{1 + \chi_i(x) + \chi_i(x)^2 + \ldots + \chi_i(x)^{q_i-1}}{q_i})$$

It is sufficient to show that:

$$\prod_{i=1}^{r}(1-\frac{1+\chi_i(x)+\chi_i(x)^2+\ldots+\chi_i(x)^{q_i-1}}{q_i})=\frac{1}{Q}\sum_{d|Q}\phi(\frac{Q}{d})\mu(d)\sum_{\chi\colon\,\mathrm{ord}(\chi)=d}\chi(x).$$

For $d \mid Q$, note that

$$\prod_{q_i\nmid d}(1-\frac{1}{q_i})=\prod_{q_i\nmid d}(\frac{\phi(q_i)}{q_i})=\phi(\frac{Q}{d})\cdot\frac{d}{Q}$$

and

$$\begin{aligned}\prod_{q_i|d}(-\frac{\chi_i(x)+\chi_i(x)^2+\ldots+\chi_i(x)^{q_i-1}}{q_i}) &= \prod_{q_i|d}\frac{-1}{q_i}\cdot\prod_{q_i|d}\sum_{j=1}^{q_i-1}\chi_i(x)^j\\ &= \frac{\mu(d)}{d}\cdot\sum_{\chi\colon\,\mathrm{ord}(\chi)=d}\chi(x)\end{aligned}$$

Hence

$$\begin{aligned}&\prod_{i=1}^{r}(1-\frac{1+\chi_i(x)+\chi_i(x)^2+\ldots+\chi_i(x)^{q_i-1}}{q_i})\\ &=\prod_{i=1}^{r}(1-\frac{1}{q_i}-\frac{\chi_i(x)+\chi_i(x)^2+\ldots+\chi_i(x)^{q_i-1}}{q_i})\\ &=\sum_{d|Q}\prod_{q_i\nmid d}(1-\frac{1}{q_i})\cdot\prod_{q_i|d}(-\frac{\chi_i(x)+\chi_i(x)^2+\ldots+\chi_i(x)^{q_i-1}}{q_i})\\ &=\sum_{d|Q}\phi(\frac{Q}{d})\cdot\frac{d}{Q}\cdot\frac{\mu(d)}{d}\cdot\sum_{\chi\colon\,\mathrm{ord}(\chi)=d}\chi(x)\\ &=\frac{1}{Q}\sum_{d|Q}\phi(\frac{Q}{d})\mu(d)\sum_{\chi\colon\,\mathrm{ord}(\chi)=d}\chi(x).\blacksquare\end{aligned}$$

We will use Burgess' bound (1.4.2) to obtain the following estimate of $g(p)$:

Theorem 2.1.2 We have

$$g(p)=O(p^{\frac{1}{4}+\epsilon})\text{ for all }\epsilon>0,\text{ as }p\to\infty. \tag{2.1.3}$$

Proof of Theorem 2.1.2 By formula (2.1.1), we have

$$\mathcal{N}_{m,n}=\frac{1}{Q}\sum_{d|Q}\phi(\frac{Q}{d})\mu(d)\sum_{\chi\colon\,\mathrm{ord}(\chi)=d}\sum_{x=m+1}^{m+n}\chi(x).$$

If $d = 1$, then χ is the principal charater and the corresponding term in the sum is

$$\frac{1}{Q} \cdot \phi(Q) \cdot n = \frac{\phi(Q)}{Q} \cdot ((1 - \frac{1}{p})n + O(1)) = \frac{\phi(p-1)}{p}n + O(1).$$

If $\mathrm{ord}(\chi) = d > 1$, then χ is not the principal character. Using (1.4.2), we have:

$$\begin{aligned}
\mathcal{N}_{m,n} &\leq \frac{\phi(p-1)}{p}n + O(1) + \frac{1}{Q}\sum_{d|Q,d>1}\phi(\frac{Q}{d})\sum_{\chi\colon \mathrm{ord}(\chi)=d}\left|\sum_{x=m+1}^{m+n}\chi(x)\right| \\
&\leq \frac{\phi(p-1)}{p}n + O(1) + \frac{1}{Q}\sum_{d|Q,d>1}\phi(\frac{Q}{d})\sum_{\chi\colon \mathrm{ord}(\chi)=d} n^{\frac{1}{2}} \cdot p^{\frac{1}{4}} \cdot \log p \\
&= \frac{\phi(p-1)}{p}n + O(1) + \frac{1}{Q}\sum_{d|Q,d>1}\phi(\frac{Q}{d})\phi(d)n^{\frac{1}{2}} \cdot p^{\frac{1}{4}} \cdot \log p \\
&= \frac{\phi(p-1)}{p}n + O(1) + \frac{1}{Q}\sum_{d|Q,d>1}\phi(\frac{Q}{d})\phi(d)n^{\frac{1}{2}} \cdot p^{\frac{1}{4}} \cdot \log p \\
&= \frac{\phi(p-1)}{p}n + O(1) + \frac{\phi(Q)}{Q}.(2^{\omega(p-1)} - 1)n^{\frac{1}{2}} \cdot p^{\frac{1}{4}} \cdot \log p \\
&= \frac{\phi(p-1)}{p}n + O(p^{\frac{1}{4}+\epsilon}) \text{ for all } \epsilon > 0.
\end{aligned}$$

By taking $m = 0$ and let $p \to \infty$, we see that if $n = O(p^{\frac{1}{4}+\epsilon})$, then $\mathcal{N}_{m,n} > 0$. Thus there exists at least one primitive root modulo p between 0 and $O(p^{\frac{1}{4}+\epsilon})$.

We conclude that $g(p) = O(p^{\frac{1}{4}+\epsilon})$ for all $\epsilon > 0$ as $p \to \infty$. ■

Shoup showed in [7] that under the assumption of GRH, we have $g(p) = O((\log p)^6)$.

2.2 The least quadratic nonresidue.

Let p be a prime. Then the first quadratic residue modulo p is 1. Denote by n_p the first quadratic nonresidue modulo p. Vinogradov conjectured that $n_p = O_\epsilon(p^\epsilon)$ for all $\epsilon > 0$ as $p \to \infty$.

First, there is an elemetary bound for n_p as follows:

Theorem 2.2.1 [8, Exercise 4.1.14,b] We have

$$n_p < \sqrt{p} + 1. \tag{2.2.1}$$

Proof of Theorem 2.2.1 Since $1 < n_p < p$, we may choose a positive integer m such that $(m-1)n_p < p < mn_p$. Thus $0 < mn_p - p < n_p$. So $mn_p - p$ must be a quadratic residue modulo p as n_p is the least quadratic nonresidue modulo p.

We have $(\frac{mn_p - p}{p}) = (\frac{mn_p}{p}) = (\frac{m}{p})(\frac{n_p}{p}) = -(\frac{m}{p}) = 1$. So m is also a quadratic nonresidue modulo p and $m \geq n_p$.

It implies that $(n_p - 1)n_p < p \Rightarrow n_p < \sqrt{p} + 1$. ■

By combining a sieve theory argument of Vinogradov and Burgess' bound (1.4.2), we give a sharper bound for n_p.

Theorem 2.2.2 [9] We have

$$n_p = O_\epsilon(p^{\frac{1}{4\sqrt{e}}+\epsilon}) \text{ for all } \epsilon > 0, p \to \infty. \tag{2.2.2}$$

Proof of Theorem 2.2.2 Applying (1.4.2) for Legendre symbol, we have

$$n_p = \left| \sum_{x=1}^{n_p} (\frac{x}{p}) \right| \ll n_p^{1-\frac{1}{r+1}} \cdot p^{\frac{1}{4r}} \cdot \log p.$$

$\Rightarrow n_p \ll p^{\frac{r+1}{4r}} \cdot (\log p)^{r+1}$. Let $r \to \infty$, we obtain that $n_p \ll_\epsilon p^{\frac{1}{4}+\epsilon}$.

Vinogradov's method is the following:

$$\left| \sum_{x=1}^{M} (\frac{x}{p}) \right| = \left| \sum_{x=1}^{M} ((\frac{x}{p}) - 1) + M \right| \geq M - 2 \cdot \#\{n : 1 \leq n \leq M, (\frac{n}{p}) = -1\}$$

If $(\frac{n}{p}) = -1$, then there is a prime r such that $r|n$ and $(\frac{r}{p}) = -1$. In the case $n = n_p$, we obtain that n_p is a prime. Hence

$$\begin{aligned} \left| \sum_{x=1}^{M} (\frac{x}{p}) \right| &\geq M - 2 \cdot \#\{n : 1 \leq n \leq M, (\frac{n}{p}) = -1\} \\ &\geq M - 2 \cdot \sum_{\substack{n_p \leq r \leq M \\ r:prime}} \#\{n : 1 \leq n \leq M, r|n\} \\ &\geq M - 2 \cdot \sum_{\substack{n_p \leq r \leq M \\ r:prime}} \frac{M}{r} \\ &\geq M - 2 \left(\sum_{\substack{r \leq M \\ r:prime}} \frac{M}{r} - \sum_{\substack{r \leq n_p \\ r:prime}} \frac{M}{r} \right). \end{aligned}$$

By Mertens' theorem, we have $\sum\limits_{\substack{r \leq y \\ r:prime}} \frac{1}{r} = \log\log y + O(1)$ as $y \to \infty$. It implies that

$$\left|\sum_{x=1}^{M}(\tfrac{x}{p})\right| \geq M - 2M(\log\log M - \log\log n_p + O(1)) = 2M(\tfrac{1}{2} - \log\tfrac{\log M}{\log n_p} + O(1))$$

Let $M = p^{1/4+\epsilon}$. Since $\log p = o(p^{\epsilon})$ for all $\epsilon > 0$, let $r \to \infty$ we have

$$\left|\sum_{x=1}^{M}(\tfrac{x}{p})\right| \ll M^{1-\frac{1}{r+1}} \cdot p^{\frac{1}{4r}} \cdot \log p = p^{1/4+\frac{1}{4r}+\epsilon(1-\frac{1}{r+1})} \cdot \log p = o(M)$$

If we assume that $n_p \geq M^{\frac{1}{\sqrt{e}}+\epsilon}$, then we get

$$o(M) = \left|\sum_{x=1}^{M}(\tfrac{x}{p})\right| \geq 2M(\tfrac{1}{2} - \log\frac{\log M}{\log M^{\frac{1}{\sqrt{e}}+\epsilon}} + O(1)) = 2M(\log\epsilon + O(1)),$$

which is a contradiction.

So $n_p < M^{\frac{1}{\sqrt{e}}+\epsilon} = O_{\epsilon}(p^{\frac{1}{4\sqrt{e}}+\epsilon})$.■

Ankeny showed in [10] that under the assumption of GRH, we have $n_p = O((\log p)^2)$.

2.3 The consecutive values.

In the previous sections, we were looking for estimates for the least primitive root and the first quadratic nonresidue modulo prime p. Our method was to find a sort interval, which contains a primitive root or a quadratic nonresidue. Conversely, it is natural to ask questions about intervals which contain only primitive roots, quadratic residues and quadratic nonresidues.

More precisely, we ask that for a given positive integer $n \geq 2$, for which prime p there exists a number x with $0 < x < p$ such that $x+1, x+2, \ldots, x+n$ are all primitive roots, or are all quadratic residues modulo p ? Does there exist a positive constant $C(n)$ depending only on n such that for all prime p with $p > C(n)$, there is always an interval of length n of primitive roots and quadratic residues?

In [11], Jagmohan Tanti and Thangadurai gave explicit values for $C(n)$'s. In fact, they proved that

Theorem 2.3.1 ([11, Theorem 1.2]) For a positive integer $n \geq 3$, we write $C(n) = (n-2)^2 4^n$. Then for all primes p with $p > C(n)$, there exist an interval of length n of quadratic residues modulo p.

Theorem 2.3.2 ([11, Theorem 1.3]) For a positive integer $n \geq 2$, we write $C(n) = \exp(2^{5.54n})$. Then for all primes p with $p > C(n)$, there exist an interval of length n of primitive roots modulo p.

Let d be a divisor of $p-1$ with $d|(p-1)$. Generalizing Theorem 2.3.1, we ask for the existence of intervals of length n of d-th powers in $\mathbb{F}_p$.

Lemma 2.3.3 Given positive integers n and d. For r with $0 \leq r \leq (d-1)n$, denote by $\mathcal{S}(r)$ the number of tuples of integers of the form $(k_1, k_2, \ldots, k_n)$ which satisfies $0 \leq k_i \leq d-1$ and $\sum\limits_{i=1}^{n} k_i = r$. Then we have

$$\sum_{r=0}^{(d-1)n} \mathcal{S}(r) = d^n. \tag{2.3.1}$$

Proof of Lemma 2.3.3 We have

$$(1 + x + x^2 + \ldots + x^{d-1})^n = \sum_{r=0}^{(d-1)n} \mathcal{S}(r) x^r.$$

By taking $x = 1$ we get formula (2.3.1).■

Let $P(d, n, p)$ be the number of intervals of d-th powers in $\mathbb{F}_p$ and χ be a nonprincipal multiplicative character of order d modulo p. Using formula (1.2.4) for $0 \leq x \leq p-n-1$, we have

$$\prod_{i=1}^{n} \frac{1 + \chi(x+i) + \chi^2(x+i) + \ldots + \chi^{d-1}(x+i)}{d} = \begin{cases} 1 \text{ if } x+i \text{ is a } d\text{-th power for all } i, \\ 0 \text{ otherwise.} \end{cases}$$

Thus

$$\begin{aligned}
P(d,n,p) &= \sum_{x=0}^{p-n-1} \prod_{i=1}^{n} \frac{1 + \chi(x+i) + \chi^2(x+i) + \ldots + \chi^{d-1}(x+i)}{d} \\
&= \frac{1}{d^n} \sum_{x=0}^{p-n-1} \sum_{\substack{0 \leq k_i \leq d-1 \\ i=1,\cdots,n}} \chi^{k_1}(x+1)\chi^{k_2}(x+2)\ldots\chi^{k_n}(x+n) \\
&= \frac{1}{d^n} \sum_{x=0}^{p-1} \sum_{\substack{0 \leq k_i \leq d-1 \\ i=1,\cdots,n}} \chi((x+1)^{k_1}(x+2)^{k_2}\ldots(x+n)^{k_n}) \\
&= \frac{1}{d^n} \sum_{x=0}^{p-1} \sum_{r=0}^{(d-1)n} \sum_{\sum\limits_{i=1}^{n} k_i = r} \chi((x+1)^{k_1}(x+2)^{k_2}\ldots(x+n)^{k_n}) \\
&= \frac{p}{d^n} + \frac{1}{d^n} \sum_{x=0}^{p-1} \sum_{r=1}^{(d-1)n} \sum_{\sum\limits_{i=1}^{n} k_i = r} \chi((x+1)^{k_1}(x+2)^{k_2}\ldots(x+n)^{k_n}).
\end{aligned}$$

It follows that

$$\left|P(d,n,p)-\frac{p}{d^n}\right| \leq \frac{1}{d^n}\sum_{x=0}^{p-1}\sum_{r=1}^{(d-1)n}\sum_{\sum k_i=r}\left|\chi((x+1)^{k_1}(x+2)^{k_2}\dots(x+n)^{k_n})\right|.$$

By Weil's bound (1.4.6), we have

$$\sum_{x=0}^{p-1}\left|\chi((x+1)^{k_1}(x+2)^{k_2}\dots(x+n)^{k_n})\right| \leq (n-1)\sqrt{p}.$$

Hence

$$\left|P(d,n,p)-\frac{p}{d^n}\right| \leq \frac{1}{d^n}\sum_{r=1}^{(d-1)n}\sum_{\sum k_i=r}(n-1)\sqrt{p} = \frac{(n-1)\sqrt{p}}{d^n}(\sum_{r=0}^{(d-1)n}\mathcal{S}(r)-\mathcal{S}(0)).$$

By $\mathcal{S}(0)=0$ and formula (2.3.1), we have

Lemma 2.3.4

$$\left|P(d,n,p)-\frac{p}{d^n}\right| \leq (n-1)\sqrt{p}(1-\frac{1}{d^n}). \tag{2.3.2}$$

There is an interval of length n of d-th powers in $\mathbb{F}_p$ iff $P(d,n,p)>0$. By (2.3.2), we see that $P(d,n,p)>0$ if

$$\frac{p}{d^n}-(n-1)\sqrt{p}(1-\frac{1}{d^n})>0 \Leftrightarrow \sqrt{p}>(n-1)(d^n-1).$$

We conclude that

Theorem 2.3.5 Given positive integers $n \geq 2$ and $d \geq 2$. Then for all primes p with $d|(p-1)$ and $p>(n-1)^2(d^n-1)^2$, there exists an interval of length n of d-th powers in $\mathbb{F}_p$.

Remarks. *i*) By Dirichlet theorem, for a given $d \geq 2$ there exist infinitely many primes p with $d|(p-1)$. So there exist infinitely many primes p with $d|(p-1)$ and $p>(n-1)^2(d^n-1)^2$ in Theorem 2.3.4.

ii) If d is too large to compared with p, then intervals of length n of d-th powers in $\mathbb{F}_p$ might not exist. For example, when $d=\frac{p-1}{2}$ there are at most three d-th powers in $\mathbb{F}_p$ are $1,0$ and -1.

3 Special values of polynomials over finite fields

Let p be a prime. Carlitz, in his paper [12], studied the following questions:

Let $f_1(x), f_2(x), \ldots, f_r(x)$ and $g_1(x), g_2(x), \ldots, g_s(x)$ be non constant polynomials over $\mathbb{F}_p$. Assume that $f_i(x)$'s are pairwise relatively prime and squarefree polynomials, and also that $g_i(x)$'s are pairwise relatively prime and squarefree polynomials.

We would like to estimate

$\mathcal{N}_r = \#\{x \in \mathbb{F}_p :$ all $f_i(x)$'s are primitive roots$\}$;

$\mathcal{M}_s = \#\{x \in \mathbb{F}_p : (\frac{g_j(x)}{p}) = \epsilon_i$ for all $i = 1, 2, \ldots, s\}$, where $\epsilon_i \in \{+1, -1\}$'s are given;

and $\mathcal{N}_{r,s} = \#\{x \in \mathbb{F}_p : f_i(x)$'s and $g_j(x)$'s satisfy the previous conditions simultaneously$\}$.

In fact, he showed that:

$$\mathcal{N}_r \sim \frac{\phi^r(p-1)}{p^{r-1}} \text{ ; } 2^s\mathcal{M}_s \sim p \text{ ; and } 2^r\mathcal{N}_{r,s} \sim \frac{\phi^r(p-1)}{p^{r-1}} \text{ as } p \to \infty.$$

After rewriting $\mathcal{N}_r$, $\mathcal{M}_s$, $\mathcal{N}_{r,s}$ in terms of character sums [12, Lemma 3], his main argument is to use estimate for character sums of the form: $\left|\sum_{x=0}^{p-1} \chi(f(x))\right|$. In fact, he used an estimate of Davenport and mentioned that a better result could be obtained by applying Weil's bound (1.4.5).

Using (1.4.5), we will give the explicit error terms for $\mathcal{N}_r$ and $\mathcal{M}_s$. For simplicity, we only consider the case of one polynomial.

3.1 Primitive roots.

Let $f(x)$ be a polynomial over $\mathbb{F}_p$. Denote by $\mathcal{N}(f)$ the number of x's in $\mathbb{F}_p$ such that $f(x)$ is a primitive root modulo p. Then we have

Theorem 3.1.1(Carlitz, [12]) If $f(x)$ is not of the form $cg(x)^k$ where $k > 1$ and $k \mid p-1$, then

$$\mathcal{N}(f) = \phi(p-1) + O(\frac{\phi(p-1) \cdot 2^{\omega(p-1)}}{\sqrt{p}}) \text{ as } p \to \infty. \tag{3.1.1}$$

Remark. Hardy and Ramanujan proved that for almost all integers n, we have $\omega(n) \sim \log\log n$. But there is not an asymptotic formula for $\omega(n)$ as $n \to \infty$. However, for all primes $p \geq 5$, we have $\omega(p-1) \leq 1.385 \cdot \frac{\log p}{\log\log p}$ ([13, page 167]).

In another direction, we will study the problem in the case of two variable polynomials over subsets of $\mathbb{F}_p \times \mathbb{F}_p$.

In [14], I extend this problem for arbitrary subsets of $\mathbb{F}_p \times \mathbb{F}_p$: Let $\mathcal{A}$, $\mathcal{B}$ be two subsets of $\mathbb{F}_p$ and $f(x,y)$ be a two variable polynomial over $\mathbb{F}_p$. The degrees of $f(x,y)$ in variables x, y are n, m respectively. Denote by $\mathcal{N}_{\mathcal{A},\mathcal{B}}(f)$ the number of pairs $(x,y) \in \mathcal{A} \times \mathcal{B}$ such that $f(x,y)$ is a primitive root modulo p. We have

Theorem 3.1.2 If the primitive kernel $H(x,y)$ of $f(x,y)$ is not of the form $cK(x,y)^k$ where $k > 1$ and $k \mid p-1$, then

$$\mathcal{N}_{\mathcal{A},\mathcal{B}}(f) = \frac{\phi(p-1)}{p-1} \cdot |\mathcal{A}||\mathcal{B}| + O(\phi(p-1) 2^{\omega(p-1)} \cdot n^{1/2} (\frac{|\mathcal{A}|^{1/2}|\mathcal{B}|^{1/2}}{p^{1/4}} + m^{1/2}|\mathcal{A}|)^{1/2}) \text{ as } p \to \infty. \tag{3.1.2}$$

In order to rewrite $\mathcal{N}_r$ in terms of character sums we use Lemma 2.2 in Carlitz's paper [12] and sum up over $\mathbb{F}_p$.

Lemma 3.1.3 (Carlitz, [12, Lemma 2.2]) We have

$$\mathcal{N}(f) = \frac{\phi(p-1)}{p-1} \cdot \left(p + \sum_{\substack{d \mid p-1 \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\text{ord}(\chi)=d} \sum_{x=0}^{p-1} \chi(f(x)) \right). \tag{3.1.3}$$

Extending Lemma 2.2 of Carlitz in [12] for two variable polynomials and summing up over the subset $\mathcal{A} \times \mathcal{B}$, we have

Lemma 3.1.5

$$\mathcal{N}_{\mathcal{A},\mathcal{B}}(f) = \frac{\phi(p-1)}{p-1} \cdot \left(|\mathcal{A}||\mathcal{B}| + \sum_{\substack{d \mid p-1 \\ d>1}} \frac{\mu(d)}{\phi(d)} \sum_{\text{ord}(\chi)=d} \sum_{\substack{x \in \mathcal{A} \\ y \in \mathcal{B}}} \chi(f(x,y)) \right). \tag{3.1.4}$$

Then we will use (1.4.5) to estimate the character sum

$$\left|\sum_{x\in\mathcal{A}}\sum_{y\in\mathcal{B}}\chi(f(x,y))\right|$$

For the detailed proofs of Theorems 3.1.1 and 3.1.2, see [14]

Remark. From (3.1.2), we see that for large a prime p if $|\mathcal{A}||\mathcal{B}| \geq np^{3/2}$, then we have $\mathcal{N}_{\mathcal{A},\mathcal{B}}(f) > 0$.

For certain polynomials $f(x,y)$ and sets $\mathcal{A},\mathcal{B}$, we obtain the following corollaries of Theorem 3.1.2 :

Corollary 3.1.6 Let M be a positive integer and $\mathcal{A} = \mathcal{B} = \{1, 2, ..., M\}$. Let p be a large prime.

i) For $f(x,y) = ax + by$; $p \nmid a, p \nmid b$ and $M \geq p^{3/4}$, we get that there exists a primitive root modulo p of the linear form $ax + by$ where $1 \leq x, y \leq p^{3/4}$.

ii) For $f(x,y) = xy$ and $M \geq p^{3/4}$, there exists a primitive root modulo p of the form xy where $1 \leq x, y \leq p^{3/4}$.

ii) For $f(x,y) = x^2 + y^2$ and $M \geq 2p^{3/4}$, there exists a primitive root modulo p of the form $x^2 + y^2$ where $1 \leq x, y \leq 2p^{3/4}$.

Corollary 3.1.7 Let $\mathcal{A}$ be the set of quadratic residues modulo p and take $f(x,y) = x + y$. Since $|\mathcal{A}| = \frac{p-1}{2}$, we have $\mathcal{N}_{\mathcal{A},\mathcal{B}}(f) > 0$ when $|\mathcal{B}| \geq \frac{1}{2}p^{1/2}$ and p large enough. That means there is a primitive modulo p of the form x^2+y with $1 \leq y \leq \frac{1}{2}p^{1/2}$.

3.2 Quadratic residues.

Let $f(x)$ be a polynomial over $\mathbb{F}_p$. Denote by $\mathcal{Q}(f)$ the number of x's in $\mathbb{F}_p$ such that $f(x)$ is a quadratic residue modulo p. We have

Theorem 3.2.1 (Carlitz, [12])

i) If $f(x) \in \mathbb{F}_p[x]$ is not of the form $cg(x)^2$ with $c \in \mathbb{F}_p,\ g(x) \in \mathbb{F}_p[x]$, then we have

$$\left|\mathcal{Q}(f) - \frac{p}{2}\right| \leq \frac{\deg(f) - 1}{2} \cdot \sqrt{p} + \frac{\deg(f)}{2}. \tag{3.2.1}$$

ii) Let $r_p(f)$ be the number of x's with $1 \leq x \leq p$ for which $f(x) \equiv 0 \pmod{p}$. If $f(x) \in \mathbb{F}_p[x]$ is of the form $cg(x)^2$ with $c \in \mathbb{F}_p,\ g(x) \in \mathbb{F}_p[x]$, then we have

$$\mathcal{Q}(f) = \begin{cases} p - r_p(f) \text{ if } c \text{ is a quadratic residue modulo } p, \\ 0 \text{ if } c \text{ is a quadratic nonresidue modulo } p. \end{cases} \tag{3.2.2}$$

For the proof of Theorem 3.2.1, see [14].

Remark. (3.2.1) tells us that for all, but very special form of $cg(x)^2$, of polynomial $f(x)$, the number of x's such that $f(x)$ is a quadratic residue modulo p is of average size $\frac{1}{2}p + O(\sqrt{p})$ as $p \to \infty$.

In [14], I study the extended version of this problem: Let $\mathcal{A}$, $\mathcal{B}$ be two subsets of $\mathbb{F}_p$, and $f(x, y)$ be a two variable polynomial over $\mathbb{F}_p$. The degrees of $f(x, y)$ in variables x, y are n, m respectively. Denote by $\mathcal{Q}_{\mathcal{A},\mathcal{B}}(f)$ the number of pairs $(x, y) \in \mathcal{A} \times \mathcal{B}$ such that $f(x, y)$ is a quadratic residue modulo p. Using estimate (1.4.5) of Gyarmati and Sárközy for Legendre symbol in the same way in Theorem 3.2.1, we get

Theorem 3.2.2 If the primitive kernel $H(x, y)$ of $f(x, y)$ is not of the form $cK(x, y)^2$, then

$$|\mathcal{Q}_{\mathcal{A},\mathcal{B}}(f) - |\mathcal{A}||\mathcal{B}|| \leq |\mathcal{A}|^{1/2}|\mathcal{B}|^{1/2}p^{3/4} \cdot n^{1/2}(2 + 5mp^{1/2})^{1/2} + mn. \qquad (3.2.3)$$

4 Covering finite fields

4.1 Exponents of primitive root.

Let p be a large prime and a be an arbitrary element in $\mathbb{F}_p^*$. Let M be a positive integer with $1 < M < p$. The set $\{a^x : 1 \leq x \leq M\}$ represents every element of $\mathbb{F}_p^*$ if and only if a is a primitive root modulo p and $M = p - 1$.

Let a_1, a_2 be two elements of $\mathbb{F}_p^*$ and M_1, M_2 be two positive integers with $1 < M_1, M_2 < p$. The following question was asked in [15]:

What conditions are needed on M_1 and M_2 such that the set $\{a_1^x + a_2^y : 1 \leq x \leq M_1, 1 \leq y \leq M_2\}$, or the set $\{a_1^x - a_2^y : 1 \leq x \leq M_1, 1 \leq y \leq M_2\}$ represents every element of $\mathbb{F}_p^*$, or in other words, covers $\mathbb{F}_p^*$?

Andrew Odlyzko conjectured that when $a_1 = a_2 = g$ is a primitive root modulo p, the set $\{g^x - g^y : 1 \leq x, y \leq M\}$ covers $\mathbb{F}_p$ when $M = O(p^{\frac{1}{2}+\epsilon})$ for any fixed $\epsilon > 0$ and for any p large enough with respect to ϵ .

So far, the only known method to solve these problems is based on charater sums. Rudnik and Zaharescu [16] showed that for $M = O(p^{\frac{3}{4}} \log p)$ the set $\{a_1^x - a_2^y : 1 \leq x \leq M_1, 1 \leq y \leq M_2\}$ covers $\mathbb{F}_p^*$. Recently, Cilleruelo and Zumalacárregui in [15] improved the bound to $\sqrt{2}p^{\frac{3}{4}}$. In fact, they proved that:

Theorem 4.1.1([15, Theorem 1]) If $\min(\text{ord}_p(a), M) \geq \sqrt{2}p^{\frac{3}{4}}$, then

$$\{a^x - a^y : 1 \leq x, y \leq M\} = \mathbb{F}_p.$$

Theorem 4.1.2([15, Theorem 2]) If $\min(\text{ord}_p(a_1), M_1) \cdot \min(\text{ord}_p(a_2), M_2) \geq p^{\frac{3}{2}}$, then

$$\{a_1^x + a_2^y : 1 \leq x \leq M_1, 1 \leq y \leq M_2\} \supseteq \mathbb{F}_p^*,$$
$$\{a_1^x - a_2^y : 1 \leq x \leq M_1, 1 \leq y \leq M_2\} \supseteq \mathbb{F}_p^*.$$

Here we only consider the primitive roots' case:

Corollary 4.1.3 Let g be a primitive modulo p, i.e $\text{ord}_p(g) = p - 1$. If $M \geq \sqrt{2}p^{\frac{3}{4}}$, then

$$\{g^x - g^y : 1 \leq x, y \leq M\} = \mathbb{F}_p.$$

Corollary 4.1.4 Let g_1, g_2 be two primitive roots modulo p, i.e $\mathrm{ord}_p(g_1) = \mathrm{ord}_p(g_2) = p-1$. If $M_1 \cdot M_2 \geq p^{\frac{3}{2}}$, then

$$\{g_1^x + g_2^y : 1 \leq x \leq M_1, 1 \leq y \leq M_2\} \supseteq \mathbb{F}_p^*,$$
$$\{g_1^x - g_2^y : 1 \leq x \leq M_1, 1 \leq y \leq M_2\} = \mathbb{F}_p.$$

In [17], I extend these results to the case of three primitive roots. Let g_1, g_2, g_3 be primitive roots modulo p. We also expect that $\{g_1^x + g_2^y + g_3^z : 1 \leq x, y, z \leq M\} \supseteq \mathbb{F}_p^*$ when $M = O(p^{\frac{1}{3}+\epsilon})$ for any fixed $\epsilon > 0$ and for any p large enough with respect to ϵ. Using the method of Cilleruelo and Zumalacárregui in [15], we prove that

Theorem 4.1.5 If $M \geq 2p^{\frac{2}{3}}$, then

$$\{g_1^x + g_2^y + g_3^z : 1 \leq x, y, z \leq M\} \supseteq \mathbb{F}_p^*.$$

4.2 Products.

Let p be a prime. For an integer M with $1 < M < p-1$, denote by $\mathcal{S}_M$ the set $\{xy \bmod p : 1 \leq x, y \leq M\}$. The natural question is for which values of M the set $\mathcal{S}_M$ contains all nonzero residues modulo p? From [18], it is conjectured that M can be as small as $p^{1/2+\epsilon}$. Garaev also suggested in [18] that M can be taken as small as $p^{3/4+\epsilon}$ and one can improve it to $p^{3/4}$. However, he did not publish his proof of these facts. In the present thesis, I will prove them. More precisely, we have

Theorem 4.2.1 ([18]) If $M \geq \frac{1}{\sqrt{2}} p^{\frac{3}{4}} \log p$, then

$$\mathcal{S}_M = \mathbb{F}_p^*. \tag{4.2.1}$$

After that, we will use the ideas of Cilleruello and Zumalacárregui in [15] to improve the bound to

Theorem 4.2.2 ([18])For any $\epsilon > 0$ and any large enough prime p, if $M \geq 2\sqrt{2+\epsilon} \cdot p^{\frac{3}{4}}$, then we have

$$\mathcal{S}_M = \mathbb{F}_p^*. \tag{4.2.2}$$

Proof of Theorem 4.2.1 The idea is that if there is an element α of $\mathbb{F}_p^*$ such that $\alpha \notin \mathcal{S}_M$, then we can deduce from this an upper bound for M: $M < C$. Conversely, if $M \geq C$, then there does not exist such an element α in $\mathbb{F}_p^*$, or in other words: $\mathcal{S}_M \supseteq \mathbb{F}_p^*$. Since p is a prime, we obtain that $\mathcal{S}_M = \mathbb{F}_p^*$.

Recall that all additive characters of $\mathbb{Z}_p \times \mathbb{Z}_p$ are of the form $\psi_{r,s}((x,y)) = e(\frac{rx+sy}{p})$ with $0 \leq s, t \leq p-1$. Thus we have

$$\sum_{\psi}\sum_{1\leq x,y\leq M}\sum_{0<t<p}\psi((x,\frac{y}{\alpha})+(t,\frac{1}{t})) = M^2\cdot(p+1)+\sum_{0<r,s<p}\sum_{0<t<p}\psi_{r,s}((t,\frac{1}{t}))\sum_{1\leq x,y\leq M}\psi_{r,s}((x,\frac{y}{\alpha})).$$

Suppose that $\alpha \notin \mathcal{S}_M$, which means $xy \neq \alpha$ for all $1 \leq x, y \leq M$. Then the left handside of the previous equation is equal to 0. Hence

$$M^2\cdot(p+1) = \left|\sum_{0<r,s<p}\sum_{0<t<p}e(\frac{rt+s\cdot\frac{1}{t}}{p})\sum_{1\leq x\leq M}e(\frac{rx}{p})\sum_{1\leq y\leq M}e(\frac{s\frac{y}{\alpha}}{p})\right|. \quad (4.2.3)$$

We need the following lemma

Lemma 4.2.3 ([2, Theorem 8.21]) Let p be a prime and M be a natural number such that $1 < M < p$. Then for any natural number r with $1 < r < p$, we have

$$\left|\sum_{1\leq x\leq M}e(\frac{rx}{p})\right| \leq \frac{p}{2r}. \quad (4.2.4)$$

From (4.2.3) and (4.2.4), we obtain that

$$M^2\cdot(p+1) \leq \max_{0<r,s<p}\left|\sum_{0<t<p}e(\frac{rt+s\cdot\frac{1}{t}}{p})\right|\cdot\frac{p}{2}\sum_{r=1}^{p-1}\frac{1}{r}\cdot\frac{p}{2}\sum_{s=1}^{p-1}\frac{1}{s}.$$

By applying (1.4.7), we get that

$$M^2\cdot(p+1) \leq 2\sqrt{p}\cdot\frac{p}{2}\sum_{r=1}^{p-1}\frac{1}{r}\cdot\frac{p}{2}\sum_{s=1}^{p-1}\frac{1}{s}.$$

Since $(1+\frac{1}{2}+\frac{1}{3}+\ldots+\frac{1}{p}) \sim \log p$ as $p \to \infty$, for p large enough we have:

$$M^2 \leq \frac{p^2\sqrt{p}}{2(p+1)}\cdot(\log p)^2 < \frac{p\sqrt{p}}{2}\cdot(\log p)^2.$$

So we obtain (4.2.1): $M < \frac{1}{\sqrt{2}}p^{\frac{3}{4}}\cdot\log p.$■

Proof of Theorem 4.2.2 For $\alpha \in \mathbb{F}_p^*$, we denote by $U(\alpha)$ the set $\{(x,y) : xy = \alpha\}$. Let $V = \{(x,y) : 1 \leq x, y \leq \frac{M}{2}\}$. Thus $V + V = \mathcal{S}_M$ and $\sum_{\psi\neq\psi_{0,0}}\left|\sum_{v\in V}\psi(v)\right|^2 = p^2\cdot|V| - |V|^2$.

Suppose that $\alpha \notin \mathcal{S}_M$, which means $xy \neq \alpha$ for all $1 \leq x, y \leq M$, or equivalently $(V+V) \cap U(\alpha) = \emptyset$, we have

$$0 = \sum_{\psi} \sum_{v,v' \in V} \sum_{u \in U(\alpha)} \psi(v+v'-u) = |V|^2 \cdot |U(\alpha)| + \sum_{\psi \neq \psi_{0,0}} \sum_{v,v' \in V} \sum_{u \in U(\alpha)} \psi(v+v'-u).$$

Hence

$$\begin{aligned} |V|^2 \cdot |U(\alpha)| &= \left| \sum_{\psi \neq \psi_{0,0}} \sum_{v,v' \in V} \psi(v+v') \sum_{u \in U(\alpha)} \psi(-u) \right| \\ &\leq \sum_{\psi \neq \psi_{0,0}} \left| \sum_{u \in U(\alpha)} \psi(-u) \right| \left| \sum_{v \in V} \psi(v) \right|^2 . \end{aligned} \tag{4.2.5}$$

Since $U(\alpha)$ is the set of solutions of the equation $xy = \alpha$, we have $|U(\alpha)| = p-1$. By applying (1.4.7), we get

$$\begin{aligned} \left| \sum_{u \in U(\alpha)} \psi(-u) \right| &= \left| \sum_{xy=\alpha} \psi((x,y)) \right| = \left| \sum_{0<x<p} \psi((x, \frac{\alpha}{x})) \right| = \left| \sum_{0<x<p} e(\frac{rx + s \cdot \frac{\alpha}{x}}{p}) \right| \\ &\leq 2\sqrt{p}. \end{aligned} \tag{4.2.6}$$

Combining (4.2.5) and (4.2.6), we have

$$|V|^2 \cdot (p-1) \leq 2\sqrt{p} \cdot \sum_{\psi \neq \psi_{0,0}} \left| \sum_{v \in V} \psi(v) \right|^2 = 2\sqrt{p}(p^2|V| - |V|^2).$$

Hence

$$|V| = \left(\frac{M}{2}\right)^2 \leq \frac{2p^2\sqrt{p}}{p + 2\sqrt{p} - 1}.$$

Since $\frac{2p^2\sqrt{p}}{p+2\sqrt{p}-1} < (2+\epsilon)p^{\frac{3}{2}}$ for any $\epsilon > 0$ and large enought p, we get

$$\left(\frac{M}{2}\right)^2 < (2+\epsilon) \cdot p^{\frac{3}{2}}.$$

So we obtain $M < 2\sqrt{2+\epsilon} \cdot p^{\frac{3}{4}}$ for any $\epsilon > 0$ and large enought p, which proves (4.2.2).■

5 Open problems and questions

5.1 Artin's conjecture.

One of the most famous unsolved problems about primitive root is the so called Artin's conjecture, due to Emil Artin:

Conjecture 5.1.1 (*Artin's conjecture*) A given integer a which is neither -1 and nor a square of an integer, is a primitive root modulo p for infinitely many prime p.

More precisely, Artin's conjecture also predicts the asymptotic density for these primes in the set of prime numbers. The Artin'constant C is

$$C = \prod_{p:prime} (1 - \frac{1}{p(p-1)}) = 0.3739...$$

Let $P(a)$ be the set of primes p such that a is a primitive root modulo p. Then the density $C(a) = \lim\limits_{n\to\infty} \frac{\#\{p\in P(a):p\leq n\}}{\pi(n)}$ is conjectured to be exist, and:

i) $P(a) = \begin{cases} \{2\}, & \text{when } a = -1 \text{ or } a \text{ is an odd square,} \\ \varnothing, & \text{when } a \text{ is an even square.} \end{cases}$

We have $C(a) = 0$.

ii) If $a = b^k$, where $k \neq 2$, then $C(a) = v(k)C(b)$, where $v(k)$ is a multiplicative arithmetic function defining at prime powers as $v(q^n) = \frac{q(q-2)}{q^2-q-1}$ for prime q.

iii) Writing $a = sf(a) \cdot r^2$ with $sf(a)$ is squarefree integer. If $sf(a) \equiv 1 \pmod 4$, then

$$C(a) = (1 - \prod_{\substack{q|sf(a)\\ q:prime}} \frac{1}{q^2-q-1})C.$$

iv) For all other values of a: $C(a) = C$.

In 1967, Hooley showed under the assumption of GRH that this conjecture is true. In 1984, R.Gupta and Ram Murty proved the conjecture is true for infinitely manny values of a, but their sieve theory argument does not give any precise value of a. After that, Roger Heath-Brown improved their result and showed that there are at most two prime numbers a for which the conjecture fails. Heath-Brown's result lead to a dramatic claim that there is an integer between arbitrary three primes for which Artin's conjecture is true. However, we do not know which one is it.

5.2 Sequence of primitive roots.

Let p be an odd prime. Recall that primitive roots modulo p^n exist for all positive integer n. Denote by $lg_p(n)$ the least primitive root modulo p^n. Thus $lg_p(1) = g(p)$. Jacobi proved that $lg_p(n) = lg_p(2)$, for all $n \geq 2$, see [19]. We are interested in relations between $lg_p(1)$ and $lg_p(2)$. There is an elementary criterion:

Proposition 5.2.1 ([19]) A primitive root g modulo p is also a primitive root modulo p^2 if and only if

$$g^{p-1} \neq 1 \,(\text{mod } p^2). \tag{5.2.1}$$

Following A.Paszkiewicz in [19], there are only two odd primes less than 10^{12} is 41487 and 6692367337 for which $lg_p(1) \neq lg_p(2)$. He also raised two problems:

Conjecture 5.2.2([19]) For almost all prime p, we have $lg_p(1) = lg_p(2)$.

Question 5.2.3([19]) Is it true that there are infinitely manny primes p for which $lg_p(1) \neq lg_p(2)$?

As a consequence of (5.2.1), we have $lg_p(1) \leq lg_p(2)$. So the question is for which prime p, we have $lg_p(2) \geq lg_p(1)$?

6 Appendix

We give a summary of Part I of the book [1]: *Equations Over Finite Fields: An Elementary Approach* of Wolfgang M. Schmidt, sketching an elementary proof for a weaker version of Weil's bound. All theorems and lemmas are indexed as in [1].

6.1 Equations $y^d = f(x)$ and $y^d - y = f(x)$.

6.1.1 Finite fields.

Let $\mathbb{F}_q$ be a finite field of order q, where $q = p^k$, p prime. $\mathbb{F}_q$ is the splitting field of $X^q - X$ over $\mathbb{F}_p$ and all of its elements are roots of $X^q - X$. The multiplicative group $\mathbb{F}_q^*$ is a cyclic group of order $q - 1$.

Let $\mathbb{F}_r/\mathbb{F}_q$ be a finite extension with $r = q^h$. Then

$$Gal(\mathbb{F}_r/\mathbb{F}_q) = Hom_{\mathbb{F}_q}(\mathbb{F}_r, \mathbb{F}_r) = \{id, Frob_q, Frob_q^2, \cdots, Frob_q^{h-1}\},$$

where $Frob_q : \mathbb{F}_r \to \mathbb{F}_r$ is the Frobenius automorphism $Frob_q(x) = x^q$. The elements of $\mathbb{F}_q$ are exactly the fixed points of $Frob_q$. The trace function of $\mathbb{F}_r/\mathbb{F}_q$ is $Tr(x) = x + x^q + x^{q^2} + \cdots + x^{q^{h-1}}$.

Lemma1F For every $x \in \mathbb{F}_q$, the following statements are equivalents:

(i) $Tr(x) = 0$.

(ii) $\exists y \in \mathbb{F}_r : x = y^q - y$.

(iii) There are exactly q elements $y \in \mathbb{F}_r$ such that $x = y^q - y$.

Denote by D the differential operator on $k[X]$. Then we have

Theorem 1G Let k be a finite field of characteristic p. M is an integer with $M \leq p$ (this is an essential condition). If we have $P(X) \in k[X]$ and $x \in k$ such that

$$0 = P(x) = DP(x) = D^2P(x) = \cdots = D^{M-1}P(x),$$

then $(X - x)^M | P(X)$.

6.1.2 Equations $y^d = f(x)$.

Consider the equation $y^d = f(x)$ in $\mathbb{F}_q$ with $d|q-1$. An elliptic equation is an equation of the form $y^2 = f(x)$, where $\deg f(X) = 3, 4$ and $f(X)$ has distinct roots. A hyperelliptic equation is an equation of the form $y^2 = f(x)$, where $f(X)$ is arbitrary.

Let N be the number of solutions of $y^d = f(x)$ with $x, y \in \mathbb{F}_q$;

N_0 be the number of solutions of $f(x) = 0$ with $x \in \mathbb{F}_q$;

N_1 be the number of solutions of $f(x)^{(q-1)/d} - 1 = 0$ with $x \in \mathbb{F}_q$;

N_2 be the number of solutions of $f(x)^{(d-1)(q-1)/d} + f(x)^{(d-2)(q-1)/d} + \cdots + f(x)^{(q-1)/d} + 1 = 0$ with $x \in \mathbb{F}_q$.

We have $q = N_0 + N_1 + N_2$, because for all $x \in \mathbb{F}_q$ the equation $f(x)^q - f(x) = 0$ implies that

$$f(x) \cdot (f(x)^{(q-1)/d} - 1) \cdot (f(x)^{(d-1)(q-1)/d} + f(x)^{(d-2)(q-1)/d} + \cdots + 1) = 0.$$

We also have $N = N_0 + dN_1$, because $0 = y^d = f(x)$ or $0 \neq y^d = f(x)$ implies that $f(x)^{(q-1)/d} - 1 = 0$ (the number of y's is $(q-1, d) = d$ from Lemma 2D).

It has been shown that if $Y^d - f(X)$ is not absolutely irreducible (reducible over $\mathbb{F}_q$ or become reducible over $\mathbb{F}_{q^2}$), then the number of solutions is not approximate to q. So we need to assume that $Y^d - f(X)$ is absolutely irreducible in order to be able to prove that $|N - q| = O(\sqrt{q})$. Absolute irreducibility is analized by the following lemmas

Lemma 2B Absolute irreducibility is invariant under non-singular linear substitution,i.e if $ae - bd \neq 0$, then $f(X, Y)$ is irreducible over k iff $f(aX + bY + c, dX + eY + f)$ is irreducible over k.

Lemma 2C For $Y^d - f(X) \in k[X, Y]$, the following statements are equivalents:

(i) $Y^d - f(X)$ is absolutely irreducible.

(ii) $Y^d - cf(X)$ is absolutely irreducible $\forall c \in k, c \neq 0$.

(iii) If $f(X) = a(X - x_1)^{d_1}(X - x_2)^{d_2} \cdots (X - x_s)^{d_s}$ is the factorization of f in $\bar{k}$, then $(d, d_1, d_2, \cdots, d_s) = 1$.

Corollary (Stepanov's condition) Writing $\deg f = m$. If $(m, d) = 1$, then $Y^d - f(X)$ is absolutely irreducible.

Lemma 2D C_n is the cyclic group of order n. C_n^d is the subgroup of d-th powers in C_n. Then for every $x \in C_n^d$, there are exactly (n, d) elements $y \in C_n$ such that $y^d = x$.

6.1.3 Construction of auxiliary polinomials.

For an absolutely irreducible polynomial $Y^d - f(X)$, we write deg $f = m$ and assume that: $m > 1, d > 1$; $d|q-1$; $(m,d) = 1$; $q = p$ or p^2. We write $g(X) = f(X)^{(q-1)/d}$.

Lemma 3A Suppose that $h_i(X) = k_{i0}(X) + X^q k_{i1}(X) + \cdots + X^{ql} k_{il}(X)$, $0 \le i \le d-1$, and deg $k_{ij} \le q/d - m$.

If $h_0(x) + g(X)h_1(X) + \cdots + g(X)^{d-1}h_{d-1}(X) \equiv 0$, then $k_{ij}(X) \equiv 0,$ for all i, j.

Proof of Lemma 3A We have

$$h_0(x) + g(X)h_1(X) + \cdots + g(X)^{d-1}h_{d-1}(X) = \sum_{j=0}^{l} g(X)^i X^{qj} k_{ij}(X) \equiv 0$$

If the degrees of $g(X)^i X^{qj} k_{ij}(X)$ are different for all i, j, then $g(X)^i X^{qj} k_{ij}(X) \equiv 0$, which implies that $k_{ij} \equiv 0$

The degree of $g(X)^i X^{qj} k_{ij}(X)$ is

$$i.\text{deg } g + qj + \text{deg } k_{ij} = (q/d)(dj + im) + \text{deg } k_{ij} - (i/d)m.$$

Hence

$$(q/d)(dj + im) - m < \text{deg } g(X)^i X^{qj} k_{ij}(X) \le (q/d)(dj + im) + (q/d) - m.$$

(Since deg $k_{ij} \le q/d - m$).

So we need to show that the intervals

$$[(q/d)(dj + im) - m; (q/d)(dj + im) + (q/d) - m]$$

are disjoint, which is true because for $(i,j) \neq (i',j')$, we have $dj + im \neq dj' + i'm$ from $(m,d) = 1$ (by considering modulo d). ■

Lemma 3B(*Fundamental lemma*)(The existence of auxiliary polynomial with zeros of high order) Let $a(Z)$ be a polinomial of degree ϵ, where $1 \le \epsilon \le d-1$. $\mathcal{S}$ is the set of $x \in \mathbb{F}_q$ such that either $a(g(x)) = 0$ or $f(x) = 0$. An integer M satisfies: $m + 1 \le M$ and $(M+3)^2 \le (2q)/d$.

Then there exists a nonzero polynomial $r(X)$ which has a zero of order at least M for every $x \in \mathcal{S}$ and

$$\text{deg } r \le \epsilon \cdot (q/d) \cdot M + 4mq.$$

Proof of Lemma 3B

We will find $r(X)$ in the form $f(X)^M \cdot \sum\limits_{i=0}^{d-1}\sum\limits_{j=0}^{K} k_{ij}(X)g(X)^iX^{qj}$, where $k_{ij}(X)$ (its coefficients) are to be determined, deg $k_{ij} \leq (q/d) - m$, $K = \lfloor(\epsilon/d)(M+m+1)\rfloor$.

First, we check that

$$\begin{aligned}
\deg r(X) &\leq \deg f(X)^M + \deg \sum_{i=0}^{d-1}\sum_{j=0}^{K} k_{ij}(X)g(X)^iX^{qj} \\
&\leq \deg f(X)\cdot M + \max \deg k_{ij}(X)g(X)^iX^{qj} \\
&\leq \deg f(X)\cdot M + \max \deg k_{ij}(X) + \max \deg g(X)^i + \max \deg X^{qj} \\
&\leq mM + (q/d - M) + (d-1)m((q-1)/d) + qK \\
&\leq \epsilon\cdot(q/d)\cdot M + 4mq \text{ (by substituting the value of } K).
\end{aligned}$$

Since $r(X)$ has a factor $f(X)^M$, we only need to choose $r(X)$ such that it has a zero of order at least M for every x satisfying $a(g(x)) = 0$.

The point is that we can use Theorem 1G to choose $r(X)$ so $D^lr(x) = 0$ for all $0 \leq l \leq M-1$ for each x with $a(g(x)) = 0$. Note that $q = p$ or p^2, therefore $M < p$. We have the essential condition of 1G. Denote by $\mathcal{B}$ the number of polynomials of this form.

Denote by $\mathcal{A}$ the number of polynomials we obtain from possible $k_{ij}(X)$'s. $\mathcal{A}$ can be caculated by the number of possible coefficients of polynomials $k_{ij}(X)$.

All we have to do is to show that $\mathcal{A} > \mathcal{B}$ by counting $\mathcal{B}$ and $\mathcal{A}$.

To count $\mathcal{B}$ we need to analize $D^lr(X)$. By induction on $l : 0 \leq l \leq M-1$, we get that

$$D^lr(X) = f(X)^{M-l}.\sum_{i=0}^{d-1}\sum_{j=0}^{K} k_{ij}^{(l)}(X)g(X)^iX^{qj},$$

where $k_{ij}^{(l+1)}(X) = f(X).(Dk_{ij}^{(l)}(X)) + (Df(X)).(M - l + i((q-1)/d)).k_{ij}^{(l)}(X)$.

We see that $k_{ij}^{(l+1)}(X)$ is a polynomial, and deg $k_{ij}^{(l+1)}(X) \leq$ deg $k_{ij}^{(l)}(X) + m - 1$. Thus deg $k_{ij}^{(l)}(X) \leq (q/d) - m + l(m-1)$ (by descending to deg $k_{ij}(X)$).

Since deg $a(Z) = \epsilon$, we have

$$a(z) = 0 \Rightarrow z^\epsilon = c_0 + c_1z + \cdots + c_{\epsilon-1}z^{\epsilon-1}$$

Writing

$$z^i = c_0^{(i)} + c_1^{(i)}z + \cdots + c_{\epsilon-1}^{(i)}z^{\epsilon-1}, \forall i \geq 0$$

Considering $x \in \mathbb{F}_q$ such that $a(g(x)) = 0 \Rightarrow g(x) = z \Rightarrow$

$$g(x)^i = c_0^{(i)} + c_1^{(i)} g(x) + \cdots + c_{\epsilon-1}^{(i)} g(x)^{\epsilon-1}$$

Therefore, if $x \in \mathbb{F}_q$ with $a(g(x)) = 0$, we can rewrite

$$D^l r(X) = f(X)^{M-l} \cdot \sum_{t=0}^{\epsilon-1} s_t^{(l)}(X) g(X)^t,$$

where

$$s_t^{(l)}(X) = \sum_{i=0}^{d-1} \sum_{j=0}^{K} c_t^{(i)} k_{ij}^{(l)}(X) X^j (\text{ note that} X^{qj} = X^j).$$

and deg $s_t^{(l)}(X) < q/d + l(m-1) - 1 + K$.

We need that $s_t^{(l)}(X) \equiv 0$ for all $0 \leq t \leq \epsilon - 1$, which implies a homogeneuos linear equations of coefficients of $k_{ij}(X)$'s. Then if the number of equations is less then number of variables (number of coefficients of $k_{ij}(X)$'s), i.e $\mathcal{B} < \mathcal{A}$, then there exist a nontrivial solution and we obtain a good choice of $k_{ij}(X)$'s.

The number of coefficients of $s_t^{(l)}(X)$'s, which we want all of them to be 0 with $0 \leq t \leq \epsilon - 1$ and $0 \leq l \leq M - 1$ is

$$\begin{aligned} \mathcal{B} &\leq \sum_{t=0}^{\epsilon-1} \sum_{l=0}^{M-1} \text{deg } s_t^{(l)}(X) \\ &\leq \sum_{t=0}^{\epsilon-1} \sum_{l=0}^{M-1} (q/d + l(m-1) - 1 + K) \\ &< \epsilon M((q/d) + K) + (M^2/2)(m-1)\epsilon \end{aligned}$$

and $\mathcal{A} = \sum_{i=0}^{d-1} \sum_{j=0}^{K} \text{deg } k_{ij}(X)$.

Choose deg $k_{ij}(X)$ as maximal as possible: deg $k_{ij}(X) = (q/d) - m$, we have $\mathcal{A} = ((q/d) - m)d(K+1)$

Then $\mathcal{B} < \mathcal{A}$ follows from conditions of M, K.

To show that $r(X) \not\equiv 0$, we use Lemma 3A: since there is a polynomial $k_{ij}(X) \not\equiv 0$, we obtain $r(X) \not\equiv 0$. ■

6.1.4 Proof of the main theorem.

Theorem 2A(*Main theorem:* $|N-q| = O(\sqrt{q})$) Let $Y^d - f(X)$ be an absolutely irreducible polynomial with $m = \deg f$ and $q > 100dm^2$. N is the number of zeros of $Y^d - f(X)$. Then we have

$$|N-q| \leq 4d^{3/2}m\sqrt{q}.$$

Proof of Theorem 2A (Under conditions in Fundamental lemma)

Since the number of zeros of $r(X)$, counting with multiplicities, can not exceed $\deg r(X)$, we have

$$|\mathcal{S}| \cdot M \leq \ \deg r \leq \epsilon \cdot (q/d) \cdot M + 4qm.$$

Choose $M = \lfloor \sqrt{2q/d} \rfloor - 3$. As $q > 100dm^2$, we have $m+1 \leq \sqrt{q/d} \leq M \leq \sqrt{2q/d} - 3$. Thus

$$|\mathcal{S}| \leq \epsilon \cdot (q/d) + 4qm/M \leq \epsilon \cdot (q/d) + 4m\sqrt{dq}.$$

i) Choose $a(Z) = Z - 1$: So S is the set of $x \in \mathbb{F}_q$ such that $g(x) = 1$ or $f(x) = 0$, and $\epsilon = 1$.

Hence $|\mathcal{S}| = N_0 + N_1 \leq (q/d) + 4m\sqrt{dq}$, which implies that

$$N = dN_1 + N_0 \leq d \cdot |\mathcal{S}| \leq q + 4d^{3/2}m\sqrt{q}.$$

ii) Choose $a(Z) = Z^{d-1} + \cdots + Z + 1$: So S is the set of $x \in \mathbb{F}_q$ such that $g(x)^{d-1} + \cdots + g(x) + 1 = 0$ or $f(x) = 0$, and $\epsilon = d - 1$.

Hence $|\mathcal{S}| = N_0 + N_2 \leq (d-1)(q/d) + 4m\sqrt{dq}$

$\Rightarrow N_1 = q - N_0 - N_2 \geq (q/d) - 4m\sqrt{dq}$

$\Rightarrow N = dN_1 + N_0 \geq d \cdot N_1 \geq q - 4d^{3/2}m\sqrt{q}$.

We obtain that

$$q - 4d^{3/2}m\sqrt{q} \leq N \leq q + 4d^{3/2}m\sqrt{q}$$

with conditions $(m, d) = 1$ and $q = p$ or p^2, which can be removed by technical arguments. ■

6.1.5 A weaker version of Weil's bound.

Theorem 2B ($\left|\sum\limits_{x\in\mathbb{F}_q}\chi(f(x))\right| = O(q^{1/2})$)

Let $\chi \neq \chi_0$ be a multiplicative of exponent d with $d|p-1$. $f(X) \in \mathbb{F}_q[X]$ is a polynomial of degree m such that $Y^d - f(X)$ is absolutely irreducible. If $q > 100dm^2$, then

$$\left|\sum_{x\in\mathbb{F}_q}\chi(f(x))\right| < 5md^{3/2}q^{1/2}.$$

Proof of Theorem 2B (Deducing from 2A) Let g be a primitive root modulo q. Write $N_k = \#\{(x,y) : y^d - f(x)g^{-k} = 0\}$ to be the number of zeros of $Y^d - f(X)g^{-k}$.

From Lemma 2C, we have $Y^d - f(X)g^{-k}$ is also absolutely irreducible. Thus by Theorem 2A we have $|N_k - q| < 4md^{3/2}q^{1/2}$.

Write $N'_k = \#\{(x,y) : y^d - f(x)g^{-k} = 0, y \neq 0\}$ to be the number of zeros of $Y^d - f(X)g^{-k}$ with $Y \neq 0$.

If $y = 0$, then $f(x) = 0$. Thus we have

$$\#\{(x,y) : y^d - f(x)g^{-k} = 0, y = 0\} \leq \#\{x : f(x) = 0\} \leq \deg f = m.$$

So we obtain $|N_k - N'_k| \leq m$. It follows that $|N'_k - q| < 5md^{3/2}q^{1/2}$.

Rewrite $\sum\limits_{x\in\mathbb{F}_q}\chi(f(x)) = \sum\limits_{k=0}^{d-1} Z_k \cdot \chi(g^k)$ with $Z_k = \#\{x : f(x)\cdot g^{-k} \in (\mathbb{F}_q^*)^d$, i.e $f(x)\cdot g^{-k} = y^d$ for some $y \neq 0\}$.

Note that $Z_k = N'_k/d$, so by writing $Z_k = (q/d) + R_k$, we have $|R_k| < 5md^{1/2}q^{1/2}$.

As $\sum\limits_{k=0}^{d-1}\chi(g^k) = 0$ (since χ is of exponent d), we have

$$\begin{aligned}\left|\sum_{x\in\mathbb{F}_q}\chi(f(x))\right| &= \left|\sum_{k=0}^{d-1} Z_k\cdot\chi(g^k)\right| = \left|\sum_{k=0}^{d-1}((q/d)+R_k)\cdot\chi(g^k)\right| = \left|\sum_{k=0}^{d-1} R_k\cdot\chi(g^k)\right| \\ &\leq \sum_{k=0}^{d-1}|R_k| \leq d\cdot 5md^{1/2}q^{1/2} = 5md^{3/2}q^{1/2}.\end{aligned}$$

■

Theorem 2B' (*Weil type conditions*) Let χ be a multiplicative character of order $d > 1$. $f(X) \in \mathbb{F}_q[X]$ is a polynomial of degree m and is not of the form $c \cdot l(X)^d$ with $c \in \mathbb{F}_q$ and $l(X) \in \mathbb{F}_q[X]$. If $q > 100dm^2$, then we have

$$\left|\sum_{x\in\mathbb{F}_q}\chi(f(x))\right| < 5md^{3/2}q^{1/2}.$$

Lemma 4B (*Analizing* $f(X) = c \cdot l(X)^d$ *condition*) For $f(X) \in \mathbb{F}_q[X]$ and $d|q-1$, the following statements are equivalents:

(i) $f(X) = c \cdot k(X)^d$ with $c \in \mathbb{F}_q$ and $k(X) \in \mathbb{F}_q[X]$.

(ii) $f(X) = h(X)^d$ with $h(X) \in \overline{\mathbb{F}}_q[X]$.

(iii) $f(X) = c \cdot (X - x_1)^{e_1} \cdot (X - x_2)^{e_2} \cdots (X - x_s)^{e_s}$ with $x_i \in \overline{\mathbb{F}}_q$ and $d|e_i$.

Proof of Lemma 4B *(iii)* $\Rightarrow$ *(i)*: Suppose *(iii)*, and let $k(X) = (X - x_1)^{e_1}.(X - x_2)^{e_2} \cdots (X - x_s)^{e_s} \in \overline{\mathbb{F}}_q[X]$. Then we need to show that $k(X) \in \mathbb{F}_q[X]$.

Since $k(X)^d = f(X)/c \in \mathbb{F}_q[X]$, by writing $k(X) = X^u + c_1X^{d-1} + \cdots + c_u$, we will show that $c_i \in \mathbb{F}_q$.

Considering $k(X)^d = (X^u + c_1X^{d-1} + \cdots + c_u)^d \in \mathbb{F}_q$, the coefficient of X^{du-i} in $k(X)^d$ is $d \cdot c_i+$ (a polynomial in $c_1, ..., c_{i-1}$). Since $dc_1 \in \mathbb{F}_q$, we obtrain $c_1 \in \mathbb{F}_q$. Thus we have $c_i \in \mathbb{F}_q$ for all i by induction. $\blacksquare$

Proof of Theorem 2B'

Write $f(X) = c \cdot (X - x_1)^{e_1} \cdot (X - x_2)^{e_2} \cdots (X - x_s)^{e_s}$ with x_i's are distinct in $\overline{\mathbb{F}}_q$.

Since $f(X) \neq c{\cdot}l(X)^d$, we have $e = \gcd(e_1, \cdots, c_s, d)$ is a proper divisor of d, i.e $e < d$.

Let $k(X) = (X - x_1)^{e_1/e} \cdot (X - x_2)^{e_2/e} \cdots (X - x_s)^{e_s/e}$, then $k(X) \in \mathbb{F}_q[X]$ by Lemma 4B.

From $f(X) = c \cdot k(X)^e$ and Corollary of Lemma 2C with $\gcd(e_1/e, \cdots, c_s/e, d/e) = 1$, we have $Y^{d/e} - k(X)$ is absolutely irreducible and deg $k = m/e$. As $e|d$ and $e < d$, χ^e is of exponent $d/e > 1$. By using Themrem 2B, we have

$$\left|\sum_{x\in\mathbb{F}_q}\chi(f(x))\right| = \left|\chi(c).\sum_{x\in\mathbb{F}_q}\chi^e(k(x))\right| < 5(m/e)(d/e)^{3/2}q^{1/2} \le 5md^{3/2}q^{1/2}.\blacksquare$$

References

[1] W.M. Schmidt, *Equations Over Finite Fields: An Elementary Approach.* Kendrick Press, 2004.

[2] Tom M. Apostol, *Introduction to Analitic Number Theory.* Springer-Verlag, 1976.

[3] D. Burgess, "On character sums and primitive roots," *Proc. London math. Soc.(3)*, no. 12, pp. 179–192, 1962.

[4] K.Gyarmati, A.Sárközy, "Equations in finite fields with restricted solution sets, I.(Charactersums)," *Acta Math. Hungar.*, no. 118, pp. 129–148, 2008.

[5] Henryk Iwaniec, Emmanuel Kowalski, *Analytic Number Theory.* American Mathematical Society, Providence, RI, 2004.

[6] Hugh L. Montgomery, Robert Vaughan, *Multiplicative Number Theory I. Classical Theory.* Cambridge Univesity Press, 2006.

[7] Victor Shoup, "Searching for primitive roots in finite fields," *Math. Comp.*, no. 58, pp. 369–380, 1992.

[8] Freud Róbert, Gyarmati Edit, *Számelmélet.* Nemzeti Tankönyvkiadó, Budapest, 2006.

[9] D.A.Burgess, "The distribution of quadratic residues and non-residues," *Mathematika*, no. 4, pp. 106–112, 1957.

[10] N.C. Ankeny, "The least quadratic non residue," *Annals of Mathematics*, no. 55, pp. 65–72, 1952.

[11] Jagmohan Tanti, R.Thangadurai, "Distribution of residues and primitive roots," *Proc. Indian Acad. Sci. (Math. Sci.)*, no. 123, pp. 203–211, 2013.

[12] L. Carlitz, "Sets of primitive roots," *Compositio Mathematica*, no. tome 13, pp. 65–70, 1956-1958.

[13] Sándor J, Mitrinovic D S, Crstici B, *Handbook on Number Theory I.* The Netherlands: Springer, 1994.

[14] Ta The Anh, "On the distribution of quadratic residues and primitive roots over finite fields,"

[15] J.Cilleruelo, A.Zumalacárregui, "An additive problem in finite fields with powers of elements of large multiplicative order," *Rev. Mat. Complut.*, 2013.

[16] Z.Rudnik, A.Zaharescu, "The distribution of spacings between small powers of a primitive root.," *Israel J. Math.*, no. 120, pp. 271–287, 2000.

[17] Ta The Anh, "A remark on an additive problem of primitive roots over finite fields,"

[18] M.Z. Garaev, "Character sums in short intervals and the multiplication table modulo a large prime," *Monasth. Math.*, no. 148, pp. 127–138, 2006.

[19] A.Paszkiewicz, "A new prime p for which the least primitive root mod p and the least primitive root mod p2 are not equal," *Math.Comput.*, no. 266, pp. 1193–1195, 2009.