UNIVERSITY OF CALIFORNIA
RIVERSIDE

Multiplicative Character Sums and the Applications to Problems in Analytic Number Theory

A Dissertation submitted in partial satisfaction
of the requirements for the degree of

Doctor of Philosophy

in

Mathematics

by

Kyle Castro

June 2017

Dissertation Committee:

Dr. Mei-Chu Chang, Chairperson
Dr. Kevin Costello
Dr. Qi Zhang

The Dissertation of Kyle Castro is approved:

Committee Chairperson

University of California, Riverside

Acknowledgments

I would like to thank my advisor, Mei-Chu Chang, for her commitment to my success and the amount of support she has given me; without it I could not have completed this process. I would also like to thank my committee members, Kevin Costello and Qi Zhang, for their time and feedback.

This process has been a great opportunity for me to grow and mature as a mathematician and I am happy to have shared the experience with the graduate students at the University of California Riverside. Thank you for participating in the talks I have given in the Graduate Student Seminar as well as the Combinatorial Number Theory Seminar.

Lastly, I owe a huge amount of gratitude to everyone in my personal life for more than can be described here. My family has provided been an amazing support system me at all times, good or bad. Thank you for always putting an emphasis on education; it has been a driving factor in my pursuit of this degree. To my girlfriend Amanda, thank you for your patience and understanding in this process; I love you and I always will. I would also like to thank my friends Miguel and Luca for the inspiration they provided every time I needed it; we are the three best friends that anyone could have.

To my parents and siblings: Mom, Dad, Derek, Ryan, Riane, and Devin.

ABSTRACT OF THE DISSERTATION

Multiplicative Character Sums and the Applications to Problems in Analytic Number Theory

by

Kyle Castro

Doctor of Philosophy, Graduate Program in Mathematics
University of California, Riverside, June 2017
Dr. Mei-Chu Chang, Chairperson

In this thesis, the reader is provided with a self-contained study of multiplicative characters modulo composite integers. The results found here are primarily upper bounds on Dirichlet characters, including those with polynomial arguments. Moreover, the applications of these character sum bounds will also be discussed; in particular the direct impact on the lower bound on the size of a subgroup of a finite field containing the image of an interval of consecutive integers under a polynomial function is discussed in Chapter 4. My main goals are to extend existing bounds on Dirichlet character sums to characters with composite moduli and create new generalizations of character sums bounds while also providing the reader with an understanding of the various applications.

Contents

Table of Contents **vii**

1 Introduction **1**
1.1 Notation and Introductory Theorems 2

2 Background Material **6**
2.1 Characters 6

3 Character Sums **17**
3.1 Various Bounds 18
3.2 Character Sums Over Shifted Intervals 21
3.3 Graham-Ringrose 24

4 Multiplicative Energy of Polynomial Images of Intervals Modulo q **35**
4.1 Preparations 39
4.2 Proofs 42

5 Summary and Future Work **48**

Bibliography **51**

Chapter 1

Introduction

Analytic number theory is a vast topic which stems from the inability to solve problems in number theory without the complex tools of analysis. Because of the interest in the upper and lower bounds of complicated expressions, many combinatorial techniques can be applied to improve the results of early analytic number theorists. The focus of this dissertation will mirror its motivation which revolves around the notion of a Dirichlet character.

Definition 1 *Let G be a finite abelian group. A multiplicative character is a function $f : G \to \mathbb{C}$ which preserves multiplication; that is, $f(ab) = f(a)f(b)$ for all $a, b \in G$. If G is the group of units in the ring of integers modulo q, we will say $f : \mathbb{Z}_q^* \to \mathbb{C}$ is a multiplicative character modulo q.*

It follows from the multiplicative property of characters that $f(1) = 1$. Moreover, if $m = |G|$, we have $[f(a)]^m = f(a^m) = 1$; hence $f(a)$ is a complex m^{th} root of unity. We are specifically interested in multiplicative characters modulo q. In fact, we can define a

Dirichlet character as follows.

Definition 2 *Let $\bar{n}$ denote the equivalence class of integers n modulo q. A Dirichlet character is the extension of the character f on $\mathbb{Z}_q^t imes$ to $\chi : \mathbb{Z} \to \mathbb{C}$ via $\chi(n) = f(\bar{n})$ with $\chi(n) = 0$ whenever $(\bar{n}, q) > 1$.*

Dirichlet Characters are named after Peter Gustav Lejeune Dirichlet who is considered to be the original analytic number theorist because of the methods he used to prove the existence of primes in an arithmetic progression. His proof relied on the use of Dirichlet characters and they still common tools in number theory almost 200 years later. Although the study of multiplicative characters can be quite extensive, readers with little to no background in the topic are welcome to read this entire work as it is completely self-contained. Many proofs of background material will be offered throughout this chapter as they appear in various texts.

1.1 Notation and Introductory Theorems

The following notation will be used throughout the dissertation:

1. $\omega(q)$ is the number of distinct prime divisors of the integer q.
2. $d(q)$ is the number of divisors of the integer q.
3. $V(J)$ represents the variety, or common zero set, of a set of functions J.
4. $\pi_q(\cdot)$ will be used as an operator with functional arguments which evaluates the function modulo q.

5. $E(A_1, \ldots, A_m) = |\{(a_1, a_1', \ldots, a_m, a_m') \in A_1^2 \times \cdots \times A_m^2 : a_1 \cdots a_m = a_1' \cdots a_m'\}|$ is the multiplicative energy of m sets.

6. The logarithmic height of a polynomial is the maximum logarithm of the modulus of the coefficients of the polynomial.

7. δ, ϵ, c, and c' are various constants with δ, $\epsilon > 0$. Furthermore, the constant p will always be considered as prime and the constant q will be a composite integer with any added conditions stated as needed.

8. $A = o(B)$ is equivalent to the statement that $|A| \leq \epsilon |B|$ for any $\epsilon > 0$ as the given parameter tends to infinity.

9. $A \ll B$ is equivalent to the statement $|A| \leq c|B|$ for some constant c.

10. $A(\cdot)$ is the indicator function for a given set A; that is, $A(a) = 1$ for all a in A and 0 otherwise.

11. Given a real number $q \geq 1$ and $x = (x_1, \ldots, x_n)$, the q-norm is given by $\|x\|_q := \left(\sum_{i=1}^{n} |x_i|^q \right)^{1/q}$

The following theorems will be useful at various points in the future. The first is the discrete version of Holder's Inequality [Fol84].

Theorem 3 *(Holder) Suppose* $1 < p < \infty$ *and* $p^{-1} + q^{-1} = 1$ *(that is,* $q = p/(p-1)$*). Given complex valued functions* f *and* g*, then*

$$\|fg\|_1 \leq \|f\|_p \|g\|_q$$

In the case that $p = q = 2$, Theorem 3 is known as the Cauchy-Schwarz Inequality; since it will be used most throughout this dissertation, it is stated here as well.

Corollary 4 *(Cauchy-Schwarz) Given $a_i, b_i \in \mathbb{C}$,*

$$\left|\sum_{i=1}^{n} a_i b_i\right| \leq \left(\sum_{j=1}^{n} |a_j|^2\right)^{1/2} \left(\sum_{k=1}^{n} |b_k|^2\right)^{1/2}.$$

To conclude this chapter, we present a useful upper bound on the number of divisors of a natural number.

Proposition 5 *Given a positive integer n,*

$$d(n) < e^{\frac{3 \log n}{\log \log n}}.$$

Proof. Suppose

$$n = p_1^{k_1 - 1} p_2^{k_2 - 1} \cdots p_r^{k_r - 1}$$

where we use $k_i - 1$ and assume $k_i \geq 2$ for ease of notation. Then clearly $d(n) = k_1 k_2 \cdots k_r$. However, we can group the powers according to the size of its corresponding prime divisor as follows,

$$d(n) = \prod_{\substack{p_i | n \\ p_i < \sqrt{\log n}}} k_i \prod_{\substack{p_i | n \\ p_i \geq \sqrt{\log n}}} k_i.$$

Note that for all i, $k_i \leq \log n$. Now we have

$$\prod_{\substack{p_i | n \\ p_i < \sqrt{\log n}}} k_i \leq \prod_{\substack{p_i | n \\ p_i < \sqrt{\log n}}} \log n < (\log n)^{\sqrt{\log n}} = e^{\sqrt{\log n} \log \log n}.$$

Moreover since $\log \log n < \frac{\sqrt{\log n}}{\log \log n}$, we have

$$\prod_{\substack{p_i | n \\ p_i < \sqrt{\log n}}} k_i \leq e^{\sqrt{\log n} \frac{\sqrt{\log n}}{\log \log n}} = e^{\frac{\log n}{\log \log n}}.$$

On the other hand if $p_i \geq \sqrt{\log n}$, then $p_i^2 \geq \log n$ and

$$p_i^{\frac{2(k_i-1)}{\log\log n}} \geq (\log n)^{\frac{k_i-1}{\log\log n}} = e^{k_i-1}$$

giving

$$p_i^{\frac{2k_i}{\log\log n}} \geq k_i.$$

Therefore

$$\prod_{\substack{p_i|n \\ p_i \geq \sqrt{\log n}}} k_i \leq \prod_{\substack{p_i|n \\ p_i \geq \sqrt{\log n}}} p_i^{\frac{2(k_i-1)}{\log\log n}} \leq n^{\frac{2}{\log\log n}} = e^{\frac{2\log n}{\log\log n}}.$$

where the last inequality holds since $\prod_{\substack{p_i|n \\ p_i \geq \sqrt{\log n}}} p_i^{k_i-1} \leq n$. Finally putting both cases together gives

$$d(n) < e^{\frac{\log n}{\log\log n}} e^{\frac{2\log n}{\log\log n}}$$

as desired. ■

It is important to note that Proposition 5 gives two bounds on the number of divisors of an integer based on the "smoothness" of the integer. In particular, the fact that for a positive integer n with $p_i < \sqrt{\log n}$ for all $p_i|n$, $d(n) < e^{\frac{\log n}{\log\log n}}$ will be especially useful in the later chapters.

Chapter 2

Background Material

The reader will now be provided with an in-depth background on the theory of multiplicative characters by discussing the theorems needed for the main results of this thesis. The theorems and proofs discussed in this chapter are primarily found in [Apo76] and [IK04].

2.1 Characters

Lemma 6 *Given G, a subgroup of $\mathbb{Z}_q^*$, any multiplicative character on G can be extended to a character on $\mathbb{Z}_q^*$ in $\frac{\varphi(q)}{|G|}$ different ways.*

Proof. Given a subgroup $G \subsetneq \mathbb{Z}_q^*$, let $\chi : G \to \mathbb{C}$ be a multiplicative character on G. Let $a \in \mathbb{Z}_q^*/G$, then there exists an integer k such that $a^k \in G$. Now, consider the subgroup of $\mathbb{Z}_q^*$ generated by $G \cup a$; call it G'. Taking m to be the minimal k such that $a^k \in G$, we can extend χ to $\chi' : G' \to \mathbb{C}$ by first setting $\chi'(a) = z$ where z is a $\frac{\varphi(q)}{m}$-th root of unity such that $z^m = \chi(a^m) = \chi'(a^m)$. Recall, every element in G' can be written in the form ga^i for

some $g \in G$ and some integer i; therefore, defining $\chi'(ga^i) = \chi(g)\chi'(a)^i$ we have a character on G'.

To show the extension is well-defined, suppose $g_1 a^{i_1} = g_2 a^{i_2}$. It follows that $a^{i_1 - i_2} \in G$ which means that $i_1 \equiv i_2 \pmod{m}$ since m is the order of a in $\mathbb{Z}_q^*/G$. Then for some integer b, $i_1 = i_2 + mb$ which gives $g_2 = g_1 a^{mb}$. Thus

$$\begin{aligned}
\chi'(g_1 a^{i_1}) &= \chi(g_1)\chi'(a)^{i_1} = \chi(g_1)\chi'(a)^{i_2+mb} \\
&= \chi(g_1)\chi'(a)^{i_2}\chi'(a)^{mb} \\
&= \chi(g_1)\chi'(a)^{i_2}\chi'(a^m)^b \\
&= \chi(g_1)\chi'(a)^{i_2}\chi(a^{mb}) \\
&= \chi(g_1 a^{mb})\chi'(a)^{i_2} \\
&= \chi(g_2)\chi'(a)^{i_2} = \chi'(g_2 a^{i_2}).
\end{aligned}$$

Notice, there are $\dfrac{|G'|}{|G|}$ choices for $\chi'(a)$ and inducting on the index gives $\dfrac{\varphi(q)}{|G'|}$ extensions of each χ' to a character on $\mathbb{Z}_q^*$; thus there are $\dfrac{\varphi(q)}{|G'|}\dfrac{|G'|}{|G|}$ extensions of χ to a character on $\mathbb{Z}_q^*$ as desired. ■

The previous lemma gives us the following proposition.

Proposition 7 *There are exactly $\varphi(q)$ distinct multiplicative characters modulo q.*

Proof. This is an immediate corollary of Lemma 6. Taking $G = \{1\}$, we have that the character χ on G extends to a character on $\mathbb{Z}_q^*$, and therefore to $\mathbb{Z}_q$, $\varphi(q)$ different ways. ■

We denote each distinct multiplicative character as χ_i for $i = 0, 1, \ldots, \varphi(q) - 1$ where the *principal character* is defined to be $\chi_0(a) = 1$ for any $a \in \mathbb{Z}_q^*$. The following are some examples of Dirichlet characters for the readers intuition.

Example 8 *If χ is a Dirichlet character modulo 2,*

χ / n	0	1
$\chi_0(n)$	0	1

Example 9 *If χ is a Dirichlet character modulo 3,*

χ / n	0	1	2
$\chi_0(n)$	0	1	1
$\chi_1(n)$	0	1	-1

Example 10 *If χ is a Dirichlet character modulo 4,*

χ / n	0	1	2	3
$\chi_0(n)$	0	1	0	1
$\chi_1(n)$	0	1	0	-1

Example 11 *If χ is a Dirichlet character modulo 5,*

χ / n	0	1	2	3	4
$\chi_0(n)$	0	1	1	1	1
$\chi_1(n)$	0	1	i	-i	-1
$\chi_2(n)$	0	1	-1	-1	1
$\chi_3(n)$	0	1	-i	i	-1

Example 12 *If χ is a Dirichlet character modulo 6,*

χ / n	0	1	2	3	4	5
$\chi_0(n)$	0	1	0	0	0	1
$\chi_1(n)$	0	1	0	0	0	-1

Do you notice any similarities between Examples 9 and 12? They have more in common than one might think.

Definition 13 *Given χ a multiplicative character modulo q and d a divisor of q, we say d is an induced modulus for q if $\chi(a) = 1$ whenever $(a, q) = 1$ and $a \equiv 1 \pmod{d}$. If there are no induced moduli for q, the character is called primitive.*

Theorem 14 *Given χ a Dirichlet character modulo q, d a divisor of q, and integers a and b, d is an induced modulus for q if and only if $\chi(a) = \chi(b)$ whenever $a \equiv b \pmod{d}$, $(a, q) = 1$, and $(b, q) = 1$.*

Proof. Assuming $\chi(a) = \chi(b)$ whenever $a \equiv b \pmod{d}$ and $(a, q) = (b, q) = 1$, letting $b = 1$ satisfies the definition of an induced modulus.

On the other hand, assume d is an induced modulus for q and choose a and b such that $(a, q) = (b, q) = 1$ and $a \equiv b \pmod{d}$. Let a' be the inverse of a in $\mathbb{Z}_q^*$, then $aa' \equiv 1 \pmod{d}$ and $aa' \equiv ba' \equiv 1 \pmod{d}$ with $\chi(aa') = 1$. Thus $\chi(aa') = \chi(ba')$ which gives $\chi(a) = \chi(b)$. ■

Using the examples above, we see that the character χ_1 mod 4 is a primitive character since the only possible induced modulus is $d = 2$; however, $3 \equiv 1 \pmod{2}$, but $\chi_1(3) \neq 1$.

On the other hand, consider the character χ_1 modulo 6; the possible induced moduli are $d = 2$ or $d = 3$. If $d = 2$, we have $5 \equiv 1 \pmod{2}$, but $\chi_1(5) \neq 1$ so $d = 2$ is not an induced modulus for 6. If $d = 3$, then for all $a \equiv 1 \pmod{3}$, $\chi_1(a) = 1$ so 3 is an induced modulus. In the language of Theorem 14 we see that 3 is an induced modulus for 6 since $\chi_1(1) = \chi_1(7) = \chi_1(13)\ldots$ with $1 \equiv 7 \equiv 13\ldots \pmod{3}$ and $\chi_1(5) = \chi_1(11) = \chi_1(17)\ldots$ with $5 \equiv 11 \equiv 17\ldots \pmod{3}$. Notice that the same argument holds for χ_0 mod 6. In fact there is an interesting result on the existence of primitive characters.

Theorem 15 *Given $q \equiv 2$ (mod 4), there do not exist any primitive characters mod q.*

Proof. Given $q \equiv 2 \pmod{4}$, let χ be any multiplicative character modulo q. Note, we have that $q = 2d$ for some odd integer d. Take $a, b \in \mathbb{Z}$ relatively prime to q such that $a \equiv b \pmod{d}$. Then, by Theorem 14 it suffices to show $\chi(a) = \chi(b)$.

Since $a \equiv b \pmod{d}$, $a = b + md$ for some integer m; however, m must be even as follows. If $a = b + md$ for m odd, then for some $k \in \mathbb{Z}$

$$a = b + md = b + (2k+1)d = b + k(2d) + d = b + kq + d$$

which gives that $a \equiv b + d \pmod{q}$. However b and d are odd so we have that $(b + d, q) > 1$ contradicting $(a, q) = 1$. Now, since $a = b + md$ for m even

$$a = b + (2k)d = b + k(2d) = b + kq$$

so that $a \equiv b \pmod{q}$. Hence $\chi(a) = \chi(b)$ for every multiplicative character modulo q. ■

Notice that Theorem 15 actually proves that for $q = 2d \equiv 2 \pmod{4}$, d is an induced modulus for every character modulo q. We can finally show the direct relationship between Examples 9 and 12 using the following theorem.

Theorem 16 *Given an integer n and a non-primitive multiplicative character χ modulo q, there exists an induced modulus $q_1|q$ such that $\chi(n) = \chi_0(n)\psi(n)$ where ψ is a primitive character mod q_1 and χ_0 is the principle character modulo q.*

Proof. Take q_1 to be the smallest induced modulus for q. We can construct ψ modulo q_1 as follows. For any $(n, q_1) = 1$, let d be the product of all the primes which divide q but not n. Taking $m = n + q_1 d$ gives $(m, q) = 1$ and $m \equiv n \pmod{q_1}$. So defining

$$\psi(n) = \begin{cases} \chi(m) & \text{if } n \in \mathbb{Z}_{q_1}^* \\ 0 & \text{otherwise} \end{cases}$$

gives a character modulo q_1. For all $(n, q) = 1$, Theorem 14 gives $\chi(n) = \chi(m)$ so that

$$\chi(n) = \chi(m) = \psi(n) = \chi_0(n)\psi(n).$$

Moreover, if $(n, q) \neq 1$,

$$\chi(n) = 0 = \chi_0(n)\psi(n).$$

Lastly, ψ must be primitive modulo q_1. If not, there exists an induced modulus k for q_1 with $k < q_1$; however k (which also divides q) must also be an induced modulus for q. That is, for $n \equiv 1 \pmod{k}$ with $(n, q) = 1$

$$\chi(n) = \chi_0(n)\psi(n) = \psi(n) = 1$$

where the last equality holds since k is an induced modulus for q_1. Since q_1 was assumed to be the smallest induced modulus of q, we have a contradiction. ■

Consider the following definition,

Definition 17 *Given any integer q and χ a Dirichlet character modulo q,*

$$\sum_{n=1}^{q} \chi(n)$$

is called complete since it the sum over all values of $\mathbb{Z}_q$.

We are primarily interested in incomplete sums of multiplicative characters because complete character sums can be rather uninteresting as the following proposition demonstrates.

Proposition 18 *If χ is a Dirichlet character modulo q,*

$$\sum_{n=1}^{q} \chi(n) = \begin{cases} \varphi(q) & \chi = \chi_0 \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. If $\chi = \chi_0$, $\chi(n) = 1$ for all $n \in \mathbb{Z}_q^*$, thus $\sum_{n=1}^{q} \chi(n) = \varphi(q)$. Now suppose $\chi \neq \chi_0$; then there is an element $a \in \mathbb{Z}_q^*$ such that $\chi(a) \neq 1$. Note,

$$\sum_{n=1}^{q} \chi(n) = \sum_{n=1}^{q} \chi(an) = \chi(a) \sum_{n=1}^{q} \chi(n)$$

so that

$$(1 - \chi(a)) \sum_{n=1}^{q} \chi(n) = 0;$$

however, since $\chi(a) \neq 1$ we have that $\sum_{n=1}^{q} \chi(n) = 0$. ■

Note, the set of characters on a group G form a group $\hat{G}$ under multiplication; that is, for all characters $\chi_i, \chi_j \in \hat{G}$ and $a \in G$, we define character multiplication by $(\chi_i \chi_j)(a) = \chi_i(a)\chi_j(a)$. $\hat{G}$ is the dual group of G with identity χ_0 and inverses $\bar{\chi}(a) = \chi(a^{-1})$. Moreover, Given $n \in \mathbb{Z}_q^*$, characters have the orthogonality relation that $\chi_i(n)\bar{\chi_j}(n) = 1$ if and only if $i = j$. Therefore, we have the following fact.

Proposition 19 *Given q a positive integer and the Dirichlet characters χ_i, χ_j modulo q*

$$\sum_{n=1}^{q} \chi_i(n)\bar{\chi_j}(n) = \begin{cases} \varphi(q) & i = j \\ 0 & \textit{otherwise.} \end{cases}$$

Proof. Notice if $i = j$, $\chi_i(n)\bar{\chi_j}(n) = 1$ for all $n \in \mathbb{Z}_q^*$. Thus,

$$\sum_{n=1}^{q} \chi_i(n)\bar{\chi_j}(n) = \varphi(q).$$

On the other hand, for $i \neq j$ $\chi_i(n)\bar{\chi_j}(n) = \chi'(n)$ for some nontrivial character χ' in the dual of $\mathbb{Z}_q^*$. Thus by Proposition 18, the complete character sum is zero. ■

Consider the following definition and lemma.

Definition 20 *Given an integer m and χ a multiplicative character mod q,*

$$\sum_{n=1}^{q} \chi(n) e^{2\pi imn/q}$$

is called a Gauss sum and is denoted $G(m, \chi)$.

Lemma 21 *Given an integer n and χ a multiplicative character mod q,*

$$\chi(n) = \sum_{m=1}^{q} a_q(m) e^{2\pi imn/q}$$

where

$$a_q(m) = \frac{1}{q} \sum_{n=1}^{q} \chi(n) e^{-2\pi imn/q}.$$

In the language of Definition 20 have $a_q(m) = \frac{1}{q} G(-m, \chi)$.

Proof. Consider

$$\sum_{m=1}^{q} a_q(m) e^{2\pi imn/q} = \frac{1}{q} \sum_{m=1}^{q} \sum_{r=1}^{q} \chi(r) e^{-2\pi imr/q} e^{2\pi imn/q} = \frac{1}{q} \sum_{m=1}^{q} \sum_{r=1}^{q} \chi(r) e^{2\pi im(n-r)/q}.$$

However,

$$\sum_{m=1}^{q} e^{2\pi im(n-r)/q} = 0$$

unless $r = n$; therefore

$$\sum_{m=1}^{q} a_q(m) e^{2\pi imn/q} = \frac{1}{q} \sum_{m=1}^{q} \chi(n) = \chi(n)$$

as desired ■

We can now discuss the notion of a separable Gauss sum.

Definition 22 *Given an integer m and χ a multiplicative character mod q, $G(m, \chi)$ is said to be separable if $G(m, \chi) = \bar{\chi}(m) G(1, \chi)$.*

Theorem 23 *Given an integer m and χ a multiplicative character mod q, $G(m,\chi)$ is separable if and only if $G(m,\chi) = 0$ for $(m,q) > 1$.*

Proof. If $(m,q) = 1$, then

$$G(m,\chi) = \sum_{n=1}^{q} \chi(n) e^{2\pi imn/q} = \bar{\chi}(m) \sum_{n=1}^{q} \chi(mn) e^{2\pi imn/q} = \bar{\chi}(m) \sum_{a=1}^{q} \chi(a) e^{2\pi ia/q}$$

$$= \bar{\chi}(m) G(1,\chi)$$

On the other hand if $(m,q) > 1$, then $\bar{\chi}(m) = 0$ and so $G(m,\chi) = \bar{\chi}(m)G(1,\chi)$ if and only if $G(m,\chi) = 0$. ■

Theorem 24 *Given a multiplicative character mod q, assume $G(m,\chi) \neq 0$ for some integer m with $(m,q) > 1$. Then there exists a proper divisor d of q, such that $\chi(a) = 1$ whenever $(a,q) = 1$ and $a \equiv 1 \pmod{d}$.*

Proof. Given m with $(m,q) > 1$, let $k = (m,q)$ and $d = \frac{q}{k}$; moreover, choose a such that $(a,q) = 1$ and $a \equiv 1 \pmod{d}$. Then

$$G(m,\chi) = \sum_{n=1}^{q} \chi(n) e^{2\pi imn/q} = \sum_{n=1}^{q} \chi(an) e^{2\pi iman/q} = \chi(a) \sum_{n=1}^{q} \chi(n) e^{2\pi iman/q}.$$

However, $a = 1 + bd = 1 + b(\frac{q}{k})$ for some integer b. So $\frac{mna}{q} = \frac{mn}{q} + \frac{mnbq}{qk} = \frac{mn}{q} + \frac{mnb}{k}$. Since $k|m$ we have that $\frac{mnb}{k} \in \mathbb{Z}$ which gives us that $e^{2\pi iman/q} = e^{2\pi imn/q}$. Thus $G(m,\chi) = \chi(a)G(m,\chi)$ and since $G(m,\chi) \neq 0$, we have $\chi(a) = 1$. ■

The conclusion of theorem 23 should look familiar (see definition 13). Hence we have the following corollary.

Corollary 25 *The Gauss sum of a primitive character is separable.*

Proof. Suppose that χ is a primitive character modulo q and the Gauss sum $G(m,\chi)$ is not separable. Then by Theorem 23, $G(m,\chi) \neq 0$ for some m with $(m,q) > 1$. However, Theorem 24 gives that there exists an induced modulus for q which contradicts the fact that χ is a primitive character. ■

Theorem 26 *Given an integer n and χ a primitive Dirichlet character modulo q,*

$$\chi(n) = \frac{\tau_q(\chi)}{\sqrt{q}} \sum_{m=1}^{q} \bar{\chi}(m) e^{-2\pi i m n/q}$$

where $\tau_q(\chi) = \dfrac{G(1,\chi)}{\sqrt{q}}$.

Proof. Since χ is a primitive character, its corresponding Gauss sum is separable. Thus, the Fourier coefficients are $a_q(m) = \dfrac{1}{q}\bar{\chi}(-m)G(1,\chi)$ so that using Lemma 21 we have

$$\chi(n) = \frac{G(1,\chi)}{q} \sum_{m=1}^{q} \bar{\chi}(-m) e^{2\pi i m n/q} = \frac{G(1,\chi)}{q} \sum_{m=1}^{q} \bar{\chi}(m) e^{-2\pi i m n/q}.$$

Letting $\tau_q(\chi) = \dfrac{G(1,\chi)}{\sqrt{q}}$ yields the desired result. ■

In the previous theorem $|\tau_q(\chi)| = 1$ which follows from bounding $|G(m,\chi)|^2$ as follows.

Theorem 27 *Given an integer m and χ a primitive character mod q, $|G(m,\chi)| = \sqrt{q}$.*

Proof. Since χ is a primitive character, its corresponding Gauss sum is separable giving

$$|G(m,\chi)|^2 = G(m,\chi)\bar{G}(m,\chi) = \bar{\chi}(m)\chi(m)G(1,\chi)\bar{G}(1,\chi) = G(1,\chi)\bar{G}(1,\chi).$$

From the definition of the Gauss sum, we have

$$G(1,\chi)\bar{G}(1,\chi) = G(1,\chi) \sum_{n=1}^{q} \bar{\chi}(n) e^{-2\pi i n/q}.$$

Finally, applying the definition again yields

$$|G(m,\chi)|^2 = \sum_{n=1}^{q} G(n,\chi)e^{-2\pi in/q} = \sum_{l=1}^{q} \chi(l) \sum_{n=1}^{q} e^{2\pi in(l-1)/q}.$$

However $\sum_{n=1}^{q} e^{2\pi in(l-1)/q} = 0$ unless $l = 1$, so $|G(m,\chi)|^2 = q\chi(1) = q$. ■

Chapter 3

Character Sums

In this chapter we would like to examine incomplete character sums more closely. As mentioned earlier, Dirichlet used nontrivial upper bounds on these character sums to give the existence of quadratic non-residues modulo an integer q; that is, the Legendre (Jacobi) symbol

$$\left(\frac{n}{q}\right) = \begin{cases} 0 & \text{if } (n,q) \neq 1 \\ 1 & \text{if } (n,q) = 1 \text{ and } x^2 \equiv n \pmod{q} \\ -1 & otherwise \end{cases}$$

is a quadratic character. Thus the bounds described in this chapter will not only give the existence of quadratic non-residues, but also give lower bounds on the number of non-residues.

3.1 Various Bounds

There have a been a number of substantial results on the upper bounds of incomplete character sums for both prime and composite moduli; in this section we will discuss the most notable of the existing bounds. We start with the Polya-Vinogradov ineuality [Apo76, Theorem 8.21].

Theorem 28 *(Polya-Vinogradov) Given χ a primitive character modulo q, for all $N \geq 1$ we have*

$$\left| \sum_{n \leq N} \chi(n) \right| < \sqrt{q} \log q.$$

Proof. First, note that this bound holds trivially for all intervals of size $N < \sqrt{q} \log q$ since, by the triangle inequality,

$$\left| \sum_{n \leq N} \chi(n) \right| \leq \sum_{n \leq N} |\chi(n)| \leq N.$$

Now, suppose $N \geq \sqrt{q} \log q$. Using Theorem 26 we have

$$\chi(n) = \frac{\tau_q(\chi)}{\sqrt{q}} \sum_{m=1}^{q-1} \bar{\chi}(m) e^{-2\pi i m n/q}$$

where we sum $1 \leq m \leq q-1$ since $\bar{\chi}(q) = 0$. Summing over all $n \leq N$ gives

$$\sum_{n \leq N} \chi(n) = \sum_{1 \leq n \leq N} \chi(n) \frac{\tau_q(\chi)}{\sqrt{q}} \sum_{m=1}^{q} \bar{\chi}(m) \sum_{1 \leq n \leq N} e^{-2\pi i m n/q}$$

where the first equality holds since $\chi(0) = 0$. Taking the absolute value of both sides, applying the triangle inequality, and using the trivial bound on $\bar{\chi}(m)$, we have

$$\left| \sum_{1 \leq n \leq N} \chi(n) \right| = \frac{1}{\sqrt{q}} \left| \sum_{m=1}^{q-1} \bar{\chi}(m) \sum_{1 \leq n \leq N} e^{-2\pi i m n/q} \right| \leq \frac{1}{\sqrt{q}} \sum_{m=1}^{q-1} \left| \sum_{1 \leq n \leq N} e^{-2\pi i m n/q} \right|.$$

Moreover,

$$\sum_{1 \leq n \leq N} e^{-2\pi i (q-m) n/q} = \sum_{1 \leq n \leq N} e^{2\pi i m n/q} \text{ and } \left| \sum_{1 \leq n \leq N} e^{-2\pi i m n/q} \right| = \left| \sum_{1 \leq n \leq N} e^{2\pi i m n/q} \right|$$

hence

$$\left|\sum_{1\le n\le N} e^{-2\pi i(q-m)n/q}\right| = \left|\sum_{1\le n\le N} e^{2\pi imn/q}\right|.$$

So we have

$$\left|\sum_{1\le n\le N}\chi(n)\right| \le \frac{2}{\sqrt{q}}\sum_{m<\frac{q}{2}}\left|\sum_{1\le n\le N} e^{-2\pi imn/q}\right|.$$

In fact

$$\sum_{1\le n\le N} e^{-2\pi imn/q} = \sum_{1\le n\le N}(e^{-2\pi im/q})^n,$$

so we can consider the geometric series

$$\left|\sum_{1\le n\le N} e^{-2\pi imn/q}\right| = \left|e^{-2\pi im/q}\frac{1-e^{-2\pi imN/q}}{1-e^{-2\pi im/q}}\right| = \left|\frac{e^{\pi imN/q}-e^{-\pi imN/q}}{e^{\pi im/q}-e^{-\pi im/q}}\right|$$

$$= \left|\frac{\sin(\frac{\pi mN}{q})}{\sin(\frac{\pi m}{q})}\right| \le \frac{1}{\sin(\frac{\pi m}{q})} \le \frac{1}{\frac{2(\frac{\pi m}{q})}{\pi}} = \frac{q}{2m}.$$

Notice that the last inequality holds since $\sin\theta \ge \frac{2\theta}{\pi}$ for $0 \le \theta \le \frac{\pi}{2}$. Putting everything back together, we have

$$\left|\sum_{n\le N}\chi(n)\right| \le \frac{2}{\sqrt{q}}\sum_{m<\frac{q}{2}}\frac{q}{2m} < \sqrt{q}\log q$$

as desired. ■

While the Polya-Vinogradov inequality is a well known upper bound, the best unconditional bound for over 50 years is due to Burgess [Bur63, Theorem 12.6].

Theorem 29 *Given χ a primitive character mod q, $r \ge 2$, and $\epsilon > 0$,*

$$\left|\sum_{n\le N}\chi(n)\right| \ll N^{1-\frac{1}{r}}q^{\frac{r+1}{4r^2}+\epsilon}$$

provided that q is cube-free or $r \le 3$.

Assuming the Generalized Riemann Hypothesis, Montgomery and Vaughan established the bound of $\sqrt{q}\log\log q$ [MV77, Theorem 2].

Theorem 30 *(Montgomery-Vaughan) Given χ a primitive character mod q, for any $N \geq 1$ we have*

$$\left|\sum_{n\leq N}\chi(n)\right| \ll \sqrt{q}\log\log q$$

Another useful bound on character sums is result of Graham and Ringrose [IK04, Corollary 12.15].

Theorem 31 *Given a square-free integer $q \geq 3$ and $N < q$, assume $N \geq q^{4/\sqrt{\log\log q}} + P^9$ where P is the largest prime divisor of q.*

Then,

$$\left|\sum_{n=1}^{N}\chi(n)\right| \ll Ne^{-\sqrt{\log q}}.$$

While the previous results involve character sums taken over an interval, we can also consider character sums with polynomial arguments; that is, for some interval of consecutive integers I, some function $f(x)$, and a multiplicative character modulo q we want to find bounds on the more general character sum

$$\left|\sum_{x\in I}\chi(f(x))\right|.$$

An extremely useful bound on complete character sums with polynomial arguments is Weil's bound [IK04, Theorem 11.23].

Theorem 32 *(Weil's Theorem) Let p be a prime, $f \in \mathbb{Z}[x]$ be a polynomial of degree d and χ be a multiplicative character mod p of order $r > 1$. Suppose f mod p is not an r^{th}, then*

we have

$$\left|\sum_{x=1}^{p} \chi(f(x))\right| \leq d\sqrt{p}.$$

Note, the version stated in Theorem 32 is the case specific to our needs in the subsequent chapters. In fact, the more general version of Weil's Theorem holds for arbitrary finite fields.

3.2 Character Sums Over Shifted Intervals

As mentioned earlier, we wish to consider sums of multiplicative characters with polynomial arguments. In this section we discuss the most natural first step in the generalization process, shifted intervals. The following question has recently been posed,

Problem 33 *(J. Bourgain) Given a multiplicative character χ and a prime p, obtain a nontrivial bound on $\sum_{x\in H} \chi(x+a)$ for $H < \mathbb{F}_p^*$, $|H| \sim \sqrt{p}$, and $a \in \mathbb{F}_p^*$.*

Similarly, the question has been posed for quadratic arguments because of its significance to polynomial factorizations over a finite field.

Problem 34 *(I. E. Shparlinski) Given a multiplicative character χ and a prime p, estimate non-trivially*

$$\sum_{x\in H} \chi((x+a)(x+b)), \qquad ab(a-b) \in \mathbb{F}_p^*$$

for $H < \mathbb{F}_p^*$ and $|H| \sim \sqrt{p}$

In [Gon], lies a solution to the first question as an immediate application of Vinogradov's Bilinear Estimate as found in [Vin85].

Theorem 35 *(I. M. Vinogradov) Let p be an odd prime, $a \in \mathbb{F}_p^*$, and χ be a non-principal character modulo p. Take*

$$S = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \xi(x)\eta(y)\chi(xy+a)$$

and

$$S' = \sum_{x=0}^{p-1} \sum_{y=0}^{p-1} \xi(x)\eta(y)\chi(xy(xy+a))$$

for any complex valued functions ξ and η with

$$\sum_{x\in X} |\eta(x)|^2 \leq X, \qquad \sum_{y\in Y} |\eta(y)|^2 \leq Y, \qquad\qquad X, Y \subset \mathbb{F}_p^*$$

Then

$$|S| \leq \sqrt{pXY}, \qquad |S'| \leq \sqrt{pXY}.$$

Taking $\xi(x)$ and $\eta(y)$ to be indicator functions in [Gon, Theorem 2], Ke Gong arrives at the following bound for the character sum over a shifted interval.

Theorem 36 *For any $H < \mathbb{F}_p^*$ and multiplicative character modulo p, we have*

$$\max_{a\in\mathbb{F}_p^*} \left| \sum_{x\in H} \chi(x+a) \right| < \sqrt{p}.$$

In the proof of [Gon, Theorem 2], the bound is actually found as

$$\left| \sum_{x\in H} \chi(x+a) \right| \leq \left(p - \frac{1}{|H|} \left| \sum_{x\in H} \chi(x) \right|^2 \right)^{\frac{1}{2}}.$$

Moreover, the following bound on a nonlinear character sum is stated as a remark at the end of [Gon]; it uses Vinogradov's bilinear estimate on S' in the same exact way.

Theorem 37 *For any $H < \mathbb{F}_p^*$ and multiplicative character modulo p, we have*

$$\left| \sum_{x\in H} \chi(x(x+a)) \right| < \sqrt{p}$$

While these results hold for a prime modulus, one of the mean-value estimates that Gong presents in [Gon] can be immediately extended.

Theorem 38 *(Gong) For $a \in \mathbb{F}_p^*$, we have*

$$\frac{1}{p-1} \sum_{\chi \pmod p} \left| \sum_{n \in H} \chi(n+a) \right| \leq \sqrt{|H|}.$$

In general, the previous theorem can be extended to $\mathbb{Z}_q$ for a composite modulus as well.

Theorem 39 *Given a composite integer q, $a \in \mathbb{Z}_q$, and $H \subset \mathbb{Z}_q$, we have*

$$\frac{1}{\varphi(q)} \sum_{\chi \pmod q} \left| \sum_{n \in H} \chi(n+a) \right| \leq \sqrt{|H|}.$$

Proof. Using the Cauchy-Schwarz inequality

$$\left(\sum_{\chi \pmod q} \left| \sum_{n \in H} \chi(n+a) \right| \right)^2 \leq \varphi(q) \sum_{\chi \pmod q} \left| \sum_{n \in H} \chi(n+a) \right|^2;$$

however

$$\sum_{\chi \pmod q} \left| \sum_{n \in H} \chi(n+a) \right|^2 = \sum_{n \in H} \sum_{m \in H} \sum_{\chi \pmod q} \chi(n+a)\bar{\chi}(m+a).$$

Note that for each m (or n) in H such that $(m+a)$ (or $n+a$ respectively) does not belong to $\mathbb{Z}_q^*$, $\chi(n+a)\bar{\chi}(m+a) = 0$; therefore we only need to consider

$$\sum_{\substack{n,m \in H \\ n+a, m+a \in \mathbb{Z}_q^*}} \sum_{\chi \pmod q} \chi\left(\frac{n+a}{m+a}\right) = \sum_{n=m} \sum_{\chi \pmod q} \chi\left(\frac{n+a}{m+a}\right) + \sum_{n \neq m} \sum_{\chi \pmod q} \chi\left(\frac{n+a}{m+a}\right)$$

$$= \varphi(q)|H| + 0$$

yielding the desired result. ■

3.3 Graham-Ringrose

In [Cha14], M-C. Chang improves Theorem 31 for large intervals by assuming the modulus is a smooth composite integer; this leads to an improvement on the saving discovered in Theorem 31 by carefully counting a "bad" set. This section will cover [Cha14, Theorem 3] as well as a proof of the most generalized version of the result.

Theorem 40 *(Chang) Let q be a square-free integer, χ be a primitive multiplicative character (mod q), and $N < q$. Assume*

(1) for all $p|q$, $p < N^{1/10}$;

(2) $\log N > C\frac{\log q}{\log\log q}$.

Then

$$\left|\sum_{x=1}^{N}\chi(x)\right| \ll Ne^{-(\log N/5)^{3/4}}.$$

As you can see by (2) of Theorem 40, the size of the interval is no longer dependent on the size of the largest prime divisor of the modulus as was the case in Theorem 31; however, the modulus is said to be smooth because of condition (1). Lastly, we point out that the saving in Theorem 40 is an improvement from that of Theorem 31 for large N, but it was stated in [Cha14] that the saving of Theorem 40 was not optimized. Theorem 40 was proven using a more technical, yet stronger, version of the theorem [Cha14, Theorem 3′].

Theorem 41 *(Chang) Assume $q = q_1\cdots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$ and q_r is square-free. Factor*

$$\chi = \chi_1\cdots\chi_r,$$

where χ_i (mod q_i) is arbitrary for $i < r$ and primitive for $i = r$. Assume further,

(i) for all $p|q_r$, $p > \sqrt{\log q_r}$;

(ii) for all i, $q_i < N^{1/3}$;

(iii) $r < c \log\log q$ for some $c < \frac{1}{4} - \epsilon$.

Then

$$\left|\sum_{x=1}^{N} \chi(x)\right| \ll N e^{-(\log q_r)^{1-c}/\log\log q_r}.$$

At first glance, it is not apparent why Theorem 41 implies Theorem 40. Theorem 41 does not assume that the modulus q is square-free, but weakens the assumption to q having a square-free factor; moreover, (ii) maintains the smoothness of q. To show how Theorem 40 holds under these weaker assumptions we state [Cha14, Remark 3.1].

Remark 42 *Writing $q = \bar{p_1} \cdots \bar{p_l} \cdot p_1 \cdot p_2 \cdots$ where*

$$\bar{p_1}, \ldots, \bar{p_l} < \sqrt{\log q} \text{ and } p_1 > p_2 \ldots \geq \sqrt{\log q}.$$

Then

$$\prod_{i=1}^{l} \bar{p_i} < (\sqrt{\log q})^l < e^{2\sqrt{\log q}} < q^{\frac{1}{10}}$$

where the second inequality holds since $l < \pi(\sqrt{\log q}) \sim \dfrac{\sqrt{\log q}}{\log\sqrt{\log q}}$ and the last inequality holds since $2\sqrt{\log q} < \frac{1}{10}\log q$ for q sufficiently large. Thus the prime factors which are smaller than $\sqrt{\log q}$ can be omitted.

Let $q_1 = \prod_{i=1}^{k} p_i$, where k is maximal so that $q_1 < N^{\frac{1}{3}}$. Then, $p_{k+1}q_1 > N^{\frac{1}{3}}$ and by Theorem 40 (1), $q_1 > N^{\frac{1}{3}-\frac{1}{10}} > N^{\frac{1}{5}}$. Repeat this process on $\frac{q}{q_1}$ to get q_2 with $N^{\frac{1}{3}} > q_2 > N^{\frac{1}{5}}$. Then, repeat the process on $\frac{q}{q_1 q_2}$ and so on. After re-indexing, we have

$$q_r > q_{r-1} > \ldots > q_2 > q_1 > N^{\frac{1}{5}}.$$

Hence $q > (N^{\frac{1}{5}})^r$, which together with (2) gives (iii) so that Theorem 41 can be applied.

After the proof of [Cha14, Theorem 3′] a more general version of the theorem is stated with a comment on the changes necessary to prove it. However, before it can be stated we need the following definition.

Definition 43 *Given a prime p and $f \in \mathbb{Z}[x]$, we say p is good (and f is p-good) if f mod p has a simple root or a simple pole. Otherwise, p is called bad and f is called p-bad. Moreover, given $\bar{q}|q_r$ such that $\bar{q} > \sqrt{q_r}$, the pair $(f, \bar{q})$ is called q_r-admissible (or just admissible when there is no ambiguity) if*

$$p > \sqrt{\log q_r} \text{ for all } p|\bar{q}$$

and

$$\prod_{\substack{p|\bar{q} \\ p \text{ is good}}} p > \frac{\bar{q}}{q_r^{\tau}}, \text{ where } \tau = \frac{10}{\log\log q_r}.$$

Given the definition of an admissible pair, we are now able to state [Cha14, Theorem 3″].

Theorem 44 *(Chang) Assume $q = q_1 \cdots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$ and q_r is square-free. Factor $\chi = \chi_1 \cdots \chi_r$, where $\chi_i \pmod{q_i}$ is arbitrary for $i < r$ and primitive for $i = r$. Assume further,*

(i) for all $p|q_r$, $p > \sqrt{\log q_r}$;

(ii) for all i, $q_i < N^{1/3}$;

(iii) $r < c \log\log q$ for some $c < \frac{1}{4} - \epsilon$.

Let

$$f(x) = \prod_j (x - b_j)^{c_j},\ c_j \in \{-1, 1\},\ d = \deg f = \sum |c_j|.$$

Suppose that (f, q_r) is admissible. Furthermore assume

(iv) $d = \deg f < (\log q_r)^{\frac{1}{8}}$.

Then,

$$\left|\sum_{x=1}^{N} \chi(f(x))\right| \ll N e^{-(\log q_r)^{1-c}/\log\log q_r}.$$

While the changes needed to prove Theorem 44 are laid out in [Cha14, Remark 3.5], we will prove a slightly more general version. From here on, we will change the definition of a *good* prime as follows.

Definition 45 *Given a character of order $k > 1$ and $f \in \mathbb{Z}[x]$, the prime p is good (or f is p-good) if f mod p is not a k^{th} power. In other words, f mod p cannot be written as $g(x)^k$ for some polynomial $g(x)$.*

Using this new definition of a good prime and keeping the definition of an admissible pair the same, the following Corollary to Theorem 32 as stated and proven in [Cha14] still holds.

Corollary 46 *(Weil's Theorem′)*

Let $q = p_1 \dots p_l$ be square-free, $f \in \mathbb{Z}[x]$ be a polymonial of degree d, and $\chi \pmod q$ be a multiplicative character of order k. Let $q_1 | q$ be such that for every prime p which divides q_1, f mod p is not an k^{th} power. Then

$$\left|\sum_{x=1}^{q} \chi(f(x))\right| \leq d^{\omega(q_1)} \frac{q}{\sqrt{q_1}}.$$

Proof. Let $\chi = \chi_1 \cdots \chi_l$, where χ_i is a multiplicative character mod p_i for $i = 1, \dots, l$. Then

$$\left|\sum_{x=1}^{q} \chi(f(x))\right| \leq \prod_{i=1}^{l} \left|\sum_{x=1}^{p_i} \chi_i(f(x))\right| \leq \prod_{p_i | q_1} d\sqrt{p_i} \prod_{p_i \nmid q_1} p_i = d^{\omega(q_1)} \frac{q}{\sqrt{q_1}}$$

using Theorem 32 on the $p_i | q_1$ and the trivial bound on those $p_i \nmid q_1$. ■

Remark 47 *In Definition 43, the function is required to have a simple root or pole to ensure that $f \pmod p$ is not an k^{th} power of a polynomial; this assumption allows for the use of Weil's estimate on the complete character sum $\left|\sum_{x=1}^{p} \chi(f(x))\right|$ where χ is a multiplicative character of order $k > 1$. Using Definition 45 we can now remove the assumption that $c_i \in \{-1, 1\}$ for some i in Theorem 44 since its primary purpose is also to ensure $f(x)$ is not an k^{th} power of a polynomial.*

Theorem 44 can now be generalized as follows.

Theorem 48 *Assume $q = q_1 \cdots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$ and q_r square-free. Let $\chi \pmod q$ be a multiplicative character of order k and factor $\chi = \chi_1 \cdots \chi_r$, where $\chi_i \pmod{q_i}$ is arbitrary for $i < r$ and primitive for $i = r$. Let $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree d such that for all $p|q$ f is p-good. Assume further that*

(i) for all $p|q_r$, $p > \sqrt{\log q_r}$;

(ii) for all i, $q_i < N^{1/3}$;

(iii) $r < c \log\log q$ for some $c < \frac{1}{4} - \epsilon$;

and

(iv) $d = \deg f < (\log q_r)^{\frac{1}{8}}$.

Then,

$$\left|\sum_{x=1}^{N} \chi(f(x))\right| \ll N e^{-(\log q_r)^{1-c}/\log\log q_r}.$$

We will prove Theorem 48 in its entirety using the same methods of [Cha14, Theorem 3'] and the necessary changes. To start is [Cha14, Remark 3.3] which will be stated as a proposition.

Proposition 49 *(Chang) Assume $q = q_1 \cdots q_r$ with $(q_i, q_j) = 1$ for $i \neq j$ and q_r square-free such that for all $p|q_r$, $p > \sqrt{\log q_r}$. Let $(f, \bar{q})$ be an admissible pair and let χ be a primitive*

multiplicative character modulo $\tilde{\tilde{q}}$, where $\tilde{\tilde{q}}$ is a square-free multiple of $\bar{q}$. Assume

$$\log d < \frac{1}{\tau} = \frac{\log\log q_r}{10}, \text{ where } d = \deg f.$$

Then,

$$\left|\sum_{x=1}^{\tilde{\tilde{q}}} \chi(f(x))\right| < \tilde{\tilde{q}}(\hat{q})^{-3/10} < \tilde{\tilde{q}}(\bar{q})^{-3/10} q_r^{3\tau/10},$$

where $\hat{q}$ is the product of good primes p which divide $\bar{q}$.

Notice that the previous bound contains a complete character sum, but since the character has polynomial argument the complete sum may be non-zero.

Proof. For $p|\bar{q}|q_r$, the assumptions on p and d give

$$p^{1/5} > (\log q_r)^{1/10} > d. \tag{3.1}$$

Factoring $\chi = \chi_1\chi_2$, where χ_1 is a character mod $\bar{q}$ and χ_2 is a character mod $\frac{\tilde{\tilde{q}}}{\bar{q}}$, we use the trivial bound on χ_2 and Corollary 46 on χ_1 to obtain

$$\left|\sum_{x=1}^{\tilde{\tilde{q}}} \chi(f(x))\right| \leq \left|\sum_{x=1}^{\bar{q}} \chi_1(f(x))\right| \left|\sum_{x=1}^{\tilde{\tilde{q}}/\bar{q}} \chi_2(f(x))\right| \leq \frac{\bar{q}}{\sqrt{\hat{q}}} d^{\omega(\hat{q})} \frac{\tilde{\tilde{q}}}{\bar{q}} = \frac{\tilde{\tilde{q}}}{\sqrt{\hat{q}}} d^{\omega(\hat{q})}.$$

Using (3.1) we have

$$\frac{\tilde{\tilde{q}}}{\sqrt{\hat{q}}} d^{\omega(\hat{q})} = \tilde{\tilde{q}} \prod_{p|\hat{q}} \frac{d}{\sqrt{p}} < \tilde{\tilde{q}} \prod_{p|\hat{q}} p^{-3/10} = \tilde{\tilde{q}}\hat{q}^{-3/10}.$$

Since $(f, \bar{q})$ is admissible, we have $\hat{q} > \bar{q}q_r^{-\tau}$ so that

$$\left|\sum_{x=1}^{\tilde{\tilde{q}}} \chi(f(x))\right| < \tilde{\tilde{q}}(\hat{q})^{-3/10} < \tilde{\tilde{q}}(\bar{q})^{-3/10} q_r^{3\tau/10}$$

as desired. ■

We can now prove Theorem 48 using the techniques/suggestions given in [Cha14].

Proof. To start, consider $\sum_{x=1}^{N} \chi(f(x))$ and use Weyl differencing. Take $M = [\sqrt{N}]$ and shift the interval $[1, N]$ by yq_1 for any $1 \leq y \leq M$. Then

$$\left| \sum_{x=1}^{N} \chi(f(x)) - \sum_{x=1}^{N} \chi(f(x + yq_1)) \right| \leq 2yq_1 \ll Mq_1.$$

Taking the average over the shift yields

$$\frac{1}{N} \left| \sum_{x=1}^{N} \chi(f(x)) \right| \leq \frac{1}{NM} \sum_{x=1}^{N} \left| \sum_{y=1}^{M} \chi(f(x + yq_1)) \right| + O\left(\frac{Mq_1}{N} \right).$$

Define $\chi_1' = \chi_2 \cdots \chi_r$ and use the periodicity of χ_1 as follows

$$\begin{aligned} \frac{1}{NM} \sum_{x=1}^{N} \left| \sum_{y=1}^{M} \chi(f(x + yq_1)) \right| &= \frac{1}{NM} \sum_{x=1}^{N} \left| \sum_{y=1}^{M} \chi_1(f(x + yq_1)) \chi_1'(f(x + yq_1)) \right| \\ &= \frac{1}{NM} \sum_{x=1}^{N} \left| \sum_{y=1}^{M} \chi_1(f(x)) \chi_1'(f(x + yq_1)) \right|. \end{aligned}$$

So applying the Cauchy-Schwarz inequality we have

$$\frac{1}{NM} \sum_{x=1}^{N} \left| \sum_{y=1}^{M} \chi(f(x + yq_1)) \right| \leq \left[\frac{1}{NM^2} \sum_{x=1}^{N} \left| \sum_{y=1}^{M} \chi_1'(f(x + yq_1)) \right|^2 \right]^{1/2}. \tag{3.2}$$

Note,

$$\sum_{x=1}^{N} \left| \sum_{y=1}^{M} \chi_1'(f(x + yq_1)) \right|^2 = \sum_{x=1}^{N} \sum_{y,y'=1}^{M} \chi_1'(f(x + yq_1)) \overline{\chi_1'}(f(x + y'q_1))$$

which, after swapping the sums and taking the absolute value, gives that

$$\frac{1}{NM} \sum_{x=1}^{N} \left| \sum_{y=1}^{M} \chi(f(x + yq_1)) \right| \leq \left[\frac{1}{NM^2} \sum_{y,y'=1}^{M} \left| \sum_{x=1}^{N} \chi_1' \left(\frac{f(x + yq_1)}{f(x + y'q_1)} \right) \right| \right]^{1/2}. \tag{3.3}$$

Now, given (y, y') define $g_{y,y'}(x) = \dfrac{f(x + yq_1)}{f(x + y'q_1)}$ and separate the pairs $(g_{y,y'}, q_r)$ according to whether or not they are q_r-admissible. We use the same counting method as is used in [Cha14, Theorem 3′] on the set of bad primes (as given in Definition 45); that is, if $(g_{y,y'}, q_r)$ is not admissible then the product of the bad primes which divide q_r is at least q_r^{τ}

and must divide $y - y'$ for each factor of f. Letting Q be the product of these bad primes which divide q_r, we have

$$\begin{aligned}
&|\{(y, y') \in [1, M]^2 : (g_{y,y'}, q_r) \text{ is not admissible}\}| \\
&\leq \sum_{\substack{Q|q_r \\ Q \geq q_r^\tau}} |\{(y, y') \in [1, M]^2 : \text{ for all } p|Q,\ g_{y,y'} \text{ is } p\text{-bad}\}| \\
&\leq \sum_{\substack{Q|q_r \\ Q \geq q_r^\tau}} M\big(\frac{M}{Q}\big) d^{\omega(Q)} \text{ (note } M > Q)
\end{aligned}$$

However,

$$\frac{d^{\omega(Q)}}{Q} = \prod_{p|Q} \frac{d}{p} < \prod_{p|Q} \frac{(\log q_r)^{1/8}}{p} < \prod_{p|Q} \frac{p^{1/4}}{p} = Q^{-3/4} \leq q_r^{-3\tau/4}.$$

Then, we have

$$\sum_{\substack{Q|q_r \\ Q \geq q_r^\tau}} M^2\big(\frac{d^{\omega(Q)}}{Q}\big) \leq \sum_{\substack{Q|q_r \\ Q \geq q_r^\tau}} M^2 q_r^{-3\tau/4} \leq 2^{\omega(q_r)} M^2 q_r^{-3\tau/4} \leq M^2 q_r^{-9\tau/20}$$

where the last inequality follows from Proposition 5. So

$$\frac{1}{NM^2} \sum_{y,y'=1}^{M} \left| \sum_{x=1}^{N} \chi_1'(g_{y,y'}) \right| = \frac{1}{NM^2} \Bigg(\sum_{\substack{y,y'=1 \\ \text{non-admissible}}}^{M} \left| \sum_{x=1}^{N} \chi_1'(g_{y,y'}) \right| + \sum_{\substack{y,y'=1 \\ \text{admissible}}}^{M} \left| \sum_{x=1}^{N} \chi_1'(g_{y,y'}) \right| \Bigg).$$

Then using the trivial bound on the non-admissible sum gives

$$\frac{1}{NM^2} \sum_{y,y'=1}^{M} \left| \sum_{x=1}^{N} \chi_1'(g_{y,y'}) \right| \leq q_r^{-9\tau/20} + \frac{1}{N} \left| \sum_{x=1}^{N} \chi_1'(g_1(x)) \right|$$

where

$$\left| \sum_{x=1}^{N} \chi_1'(g_1(x)) \right| = \max_{\substack{g_{y,y'} \\ (g_{y,y'}, q_r) \text{ is admissible}}} \left| \sum_{x=1}^{N} \chi_1'(g_{y,y'}(x)) \right|. \tag{3.4}$$

Hence we have

$$\frac{1}{NM} \sum_{x=1}^{N} \left| \sum_{y=1}^{M} \chi(f(x + yq_1)) \right| \leq q_r^{-9\tau/40} + \left(\frac{1}{N} \left| \sum_{x=1}^{N} \chi_1'(g_1(x)) \right| \right)^{1/2}.$$

Thus there exists $\bar{q}_1|q_r$ such that $\bar{q}_1 > q_r^{1-\tau}$ and for every $p|\bar{q}_1$, g_1 is p-good. Now, we want to continue bounding the remaining sum using induction on each of the characters in the factorization of χ; we do so using the following proposition.

Proposition 50 *For $s = 1, 2, \ldots, r-1$ define $\chi'_s = \chi_{s+1} \cdots \chi_r$. Let $g_s(x) = \prod_j [f(x - b_j)]^{c_j}$ where $b_j, c_j \in \mathbb{Z}$ and $\deg g_s \leq 2^s d$. Let $\bar{q}_0 = q_r$. Suppose there exists $\bar{q}_{s-1}|q_r$ such that $\bar{q}_{s-1} \geq q_r^{1-(s-1)\tau}$ and $(g_s, \bar{q}_{s-1})$ is admissible, then*

$$\frac{1}{N}\left|\sum_{x=1}^{N} \chi'_s(g_s(x))\right| \leq q_r^{\frac{-\tau}{20}\cdot\frac{1}{2}} + \left(\frac{1}{N}\left|\sum_{x=1}^{N} \chi'_{s+1}(g_{s+1}(x))\right|\right)^{1/2}$$

where g_{s+1} is of the same form as g_s with $\deg g_{s+1} \leq 2^{s+1} d$ and there exists $\bar{q}_s|q_r$ such that $\bar{q}_s > q_r^{1-s\tau}$ and $(g_{s+1}, \bar{q}_s)$ is admissible.

Proof. We use Cauchy-Schwarz and the q_{s+1} periodicity of χ_{s+1} in the same manner as before to obtain

$$\frac{1}{N}\left|\sum_{x=1}^{N} \chi'_s(g_s(x))\right| \leq \left[\frac{1}{NM^2}\sum_{y,y'=1}^{M}\left|\sum_{x=1}^{N} \chi'_{s+1}\left(\frac{g_s(x+yq_{s+1})}{g_s(x+y'q_{s+1})}\right)\right|\right]^{1/2}.$$

Let $g_{s+1}(x) = \frac{g_s(x+yq_{s+1})}{g_s(x+y'q_{s+1})}$ where (y, y') is chosen so that the previous character sum is maximal among all good pairs as in (3.4). Then we can bound the size of the bad set of (y, y') exactly as before.

$$\begin{aligned}
&|\{(y, y') \in [1, M]^2 : (g_{s+1}, \bar{q}_s) \text{ is not admissible}\}| \\
&\leq \sum_{\substack{Q|\bar{q}_s \\ Q \geq q_r^{\tau}}} |\{(y, y') \in [1, M]^2 : \text{ for all } p|Q,\ g_{s+1} \text{ is p-bad}\}| \\
&\leq \sum_{\substack{Q|\bar{q}_s \\ Q \geq q_r^{\tau}}} \frac{M^2}{Q}(2^s d)^{\omega(Q)}
\end{aligned}$$

However, applying the same argument as before and using (iii) to bound the 2^s term gives

$$M^2\frac{(2^s d)^{\omega(Q)}}{Q} \leq M^2\prod_{p|Q}\frac{2^r d}{p} < M^2\prod_{p|Q}\frac{(\log q_r)^{3/8}}{p} < M^2 Q^{-1/4} \leq M^2 q_r^{-\tau/4}.$$

Hence the bad set can be bounded by $2^{\omega(q_r)}M^2 q_r^{-\tau/4} > M^2 q_r^{-\tau/20}$ using Proposition 5 with $p_i > \sqrt{\log q_r}$. ■

At the final stage of the inductive process we have

$$\left|\sum_{x=1}^{N}\chi_r(g_{r-1}(x))\right|$$

with $\deg g_{r-1} \leq 2^{r-1}d$. Moreover, there exists $\bar{q}_{r-2}|q_r$ with $\bar{q}_{r-2} > q_r^{1-(r-2)\tau} > \sqrt{q_r}$ such that every $p|\bar{q}_{r-2}$ is good; that is, $(g_{r-1}, \bar{q}_{r-2})$ is admissible and Proposition 49 applies. In particular since $N > q_r^{1/5}$ we can apply Proposition 49 to the complete sums and use the trivial bound on the remainder of the interval. Thus

$$\left|\sum_{x=1}^{N}\chi_r(g_{r-1}(x))\right| < N\bar{q}_{r-2}^{-3/10}q_r^{3\tau/10} < Nq_r^{-(\frac{3}{20}-\frac{3\tau}{10})} < Nq_r^{-1/8}.$$

Putting everything together, we have

$$\begin{aligned}
&\frac{1}{N}\left|\sum_{x=1}^{N}\chi(f(x))\right| \\
&\leq q_r^{-9\tau/40} + q_r^{-\tau/40} + \ldots + (q_r^{-\tau/20})^{1/2^{r-1}} + (q_r^{-1/8})^{1/2^{r-1}} + O\left(\frac{Mq_1}{N}\right) \\
&\ll (q_r^{-\tau/20})^{1/2^{r-1}} + (q_r^{-1/8})^{1/2^{r-1}} \\
&\ll (q_r^{-\tau/20})^{1/2^{r-1}} \\
&= q_r^{-\frac{1}{\log\log q_r}\cdot\frac{1}{2^c\log\log q_r}} \\
&< e^{-\frac{(\log q_r)^{1-c}}{\log\log q_r}}
\end{aligned}$$

as desired. ■

Notice that by Remark 42 the following weaker version of Theorem 48 still holds.

Theorem 51 *Let $q = q_1 \cdots q_r \in \mathbb{Z}$ be square-free, $\chi \pmod q$ be a primitive multiplicative character of order k, $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree d such that for all $p|q$ f is p-good, and take $N < q$. Assume further,*

(1) for all $p|q$, $p < N^{1/10}$;

(2) $\log N > C\dfrac{\log q}{\log\log q}$;

and

(3) $d < (\log q_r)^{1/8}$.

Then,

$$\left|\sum_{x=1}^{N} \chi(f(x))\right| \ll Ne^{-(\frac{\log N}{5})^{3/4}}$$

Chapter 4

Multiplicative Energy of Polynomial Images of Intervals Modulo q

Mei-Chu Chang and I give a result in the spirit of Shparlinski's theorem, [Shp, Theorem 7], through the application of the Theorem 44. This chapter is a essentially [CC] with more details filled in for the reader. In [Shp] lies an improvement to an earlier result of Shparlinski and Gómez-Pérez, [GPS15, Theorem 7], which discusses the greatest lower bound for the order of a subgroup of a finite field containing the image of H consecutive integers under a rational function. There are various bounds for the number of images of consecutive polynomial values which belong to a given multiplicative subgroup (see [CCG$^+$14], [CGOS12], and [GPS15]); [Shp, Theorem 7] shows that the size of the intersection discussed above is dependent on the size of the subgroup of the finite field $\mathbb{F}_p$.

Theorem 52 *(Shparlinski) Let $f(X) \in \mathbb{F}_p[X]$ be a square-free quadratic polynomial. For*

any interval I of consecutive integers and a subgroup G of $\mathbb{F}_p^*$, we have

$$|f(I) \cap G| \leq (1 + |I|^{3/4} p^{-1/8}) |G|^{1/2} p^{o(1)}, \tag{4.1}$$

as $|I| \to \infty$.

While the previous theorem uses a fact about the arithmetic p-norm (see [Shp, Lemma 5]) which is found using Minkowski's Second Theorem in [GPG14], we take a different approach to prove our main result. Note that assuming $f(I) \subset G$, (4.1) is only nontrivial if $|I| > p^{1/2}$ since

$$|f(I) \cap G| \ll |I|^{3/4} p^{-1/8} |G|^{1/2}.$$

However, assuming the modulus is smooth, the following theorem is nontrivial for smaller intervals of integers as well.

Theorem 53 *Given an integer m and some $\epsilon > 0$, let $f(X) \in \mathbb{Z}[X]$ be a monic polynomial of degree d. For a sufficiently large square-free integer $q > q(\epsilon)$, take $I \subset \mathbb{Z}_q$ to be an interval of consecutive integers with $d < (\log |I|)^{1/8}$ such that*

(1) for all $p|q$, $p < q^{\frac{1}{160 d^4 m^{2d}}}$

(2) $\log \log q > 16 d^4 m^{2d}$.

If $\pi_q f(I) \subset G$, for G a subgroup of $\mathbb{Z}_q^*$, then $|G| \geq \min\{|I|^{m/2}, q^{1-\epsilon}\}$.

As a quick note to be mentioned again later, we point out that under the extra assumption that $|I| \geq q^{\frac{1}{16 d^4 m^{2d}}}$, Theorem 53 (2) gives Theorem 40 (2) since

$$\log |I| \geq \frac{\log q}{16 d^4 m^{2d}} > \frac{\log q}{\log \log q}.$$

Moreover, under the same assumption on $|I|$, Theorem 53 (1) gives Theorem 40 (1) since $p < (q^{\frac{1}{16 d^4 m^{2d}}})^{1/10} \leq |I|^{1/10}$. Lastly, the assumption $d < (\log |I|)^{1/8}$ gives Theorem 44 (iv)

since $\log q_r \sim \log |I|$ by Remark 42. In summary, Theorem 44 will apply under the above assumptions as discussed in Remark 42.

Under the conditions of Theorem 51 we can quickly prove a version of Theorem 53 in the form of Theorem 52 as an upper bound for the number of images of consecutive values which belong to a multiplicative subgroup of $\mathbb{Z}_q$.

Theorem 54 *Let $q = q_1 \cdots q_r \in \mathbb{Z}$ be square-free, $\chi \pmod q$ be a primitive multiplicative character of order k, $f(x) \in \mathbb{Z}[x]$ be a polynomial of degree d such that for all $p|q$ f is p-good, and take G to be a multiplicative subgroup of $\mathbb{Z}_q^*$ and take $I \subset \mathbb{Z}_q$ to be an interval of consecutive integers. Assuming*

(1) for all $p|q$, $p < |I|^{1/10}$

(2) $\log |I| > C\dfrac{\log q}{\log \log q}$;

(3) $d < (\log q_r)^{1/8}$.

Then,

$$|f(I) \cap G| \leq \frac{|I|}{\varphi(q)}|G| + o(|I|).$$

Proof. Let $S = \{\chi : \chi \text{ is a multiplicative character modulo } q \text{ and } \chi(a) = 1 \text{ for all } a \in G\}$ and $I' = \{x \in I : f(x) \in G\}$. Consider

$$\left|\sum_{x \in I'} \sum_{\chi \in S} \chi(f(x))\right| = |I'||S|. \tag{4.2}$$

On the other hand, using $I'(\cdot)$ as the indicator function for the set I' we have

$$\left|\sum_{x \in I'} \sum_{\chi \in S} \chi(f(x))\right| = \left|\sum_{x \in I} \sum_{\chi \in S} I'(x)\chi(f(x))\right|.$$

Then the Cauchy–Schwarz inequality gives

$$\begin{aligned}\left|\sum_{x\in I}\sum_{\chi\in S} I'(x)\chi(f(x))\right| &\le |I'|^{1/2}\left(\sum_{x\in I}\left|\sum_{\chi\in S}\chi(f(x))\right|^2\right)^{1/2}\\ &= |I'|^{1/2}\left(\sum_{x\in I}\sum_{\chi\in S}\sum_{\chi'\in S}\chi(f(x))\overline{\chi'}(f(x))\right)^{1/2}\\ &= |I'|^{1/2}\left(\sum_{x\in I}\sum_{\chi=\chi'\in S}\chi(f(x))\overline{\chi'}(f(x))+\sum_{x\in I}\sum_{\substack{\chi,\chi'\in S\\ \chi\neq\chi'}}\chi(f(x))\overline{\chi'}(f(x))\right)^{1/2}\\ &\le |I'|^{1/2}[|I||S|+(|S|^2-|S|)o(|I|)]^{1/2}.\end{aligned}$$

So after a substitution of (4.2), we have

$$|I'||S|^2 \le |I||S| + (|S|^2-|S|)o(|I|)$$

which gives

$$|I'| \le \frac{|I|}{|S|} + o(|I|) = \frac{|I|}{\varphi(q)}|G| + o(|I|) \text{ by (4.12)}$$

as desired. ■

These theorems have relevance in polynomial dynamics as well as in the study of Dirichlet characters. More specifically, Theorem 52 is generalized in the study of the frequency of elements in the orbit of iterations of f which belong to a subfield of $\mathbb{F}_{q^r}$ as in [Ost, Corollary 18] and [RNS15, Theorem 6].

Theorem 55 *(Ostafe) Let $\mathbb{K}=\mathbb{F}_q$ and $\mathbb{L}=\mathbb{F}_{q^r}$ with $A\subseteq\mathbb{L}$ an affine subspace of dimension s over $\mathbb{K}$. Given $f\in\mathbb{L}[X]$, if for some $u\in\mathbb{L}$ and integer N with $2\le N\le \#\{f^{(n)}(u): n=0,1,\ldots\}$ we have*

$$f^{(n)}(u)\in A,\ \ n=0,1,\ldots,N-1,$$

then

$$q^s \ge \frac{1}{2}Nq^{r\vartheta},$$

where $\vartheta = \dfrac{.9\epsilon}{2^{2d}}$ *for arbitrary* ϵ *and specific integer* d *as described in [Ost, Theorem 10].*

Theorem 56 *(Roche-Newton and Shparlinski) Given fields* $\mathbb{K} \subseteq \mathbb{F}$*, let* $f \in \mathbb{F}[x]$ *be of degree* $d \geq 1$ *and let* $u \in \mathbb{F}$*. Assume that for an integer* $N \leq \#\{f^{(n)}(u) : n = 0, 1, \ldots\}$ *we have*

$$\#\{0 \leq n < N : f^n(u) \in \mathbb{K}\} \geq c(d)\frac{N}{\log N} + 1$$

where $c(d) = 2\log(4d)$*. Then for some integer* k *we have* $f^{(k)}(X) \in \mathbb{K}[X]$*.*

Moreover, the bounds of Theorems 52 and 53 give nontrivial bounds on the modulus of a character sum of a polynomial,

$$\left|\sum_{x \in I} \chi(f(x))\right|$$

as discussed in [CS14]. While incomplete character sums over an interval are being studied thoroughly, the notion of character sums with polynomial arguments can be improved with results such as these.

4.1 Preparations

We will need some preparations which will be called on in the proof of Theorem 53. First, we need a sharp arithmetic version of Hilbert's Effective Nullstellensatz Theorem [KPS01, Theorem 1].

Theorem 57 *(Krick-Pardo-Sombra) Let* $P_1, \ldots, P_m \in \mathbb{Z}[X_1, \ldots, X_n]$ *be polynomials of degree at most* D *and logarithmic height at most* H*. If* $V(P_1, \ldots, P_m) = \emptyset$ *in* $\mathbb{C}^n$*, then there exists a positive integer* b *and polynomials* $Q_1, \ldots, Q_m \in \mathbb{Z}[X_1, \ldots, X_n]$ *such that*

$$b = \sum_{i=1}^{m} Q_i P_i \tag{4.3}$$

and

$$\log b \leq 4n(n+1)D^n[H + \log m + (n+7)\log(n+1)D]. \tag{4.4}$$

We will also use the following result on the number of factorizations in a generalized arithmetic progression [Cha03, Proposition 3].

Theorem 58 *(Chang) Given integers $c_0, c_1, \ldots, c_d$ and $J_1, \ldots, J_d \geq 1$ a generalized arithmetic progression P is*

$$P = \{c_0 + \sum_{i=1}^{d} k_i c_i | k_i \in \mathbb{Z}, 0 \leq k_i \leq J_i\}.$$

Let $r_h(n)$ be the number of representations of the integer n as a product of h elements in P. If $J = \max_i J_i$, then for all $n \in \mathbb{Z}$

$$r_h(n) < e^{C_{d.h} \log J / \log\log J}$$

where $C_{d.h}$ is a constant depending on d and h.

Note that the bound above depends on h so to remedy the problems this may cause, we fix m (which plays the role of h) in Theorem 53; this will be discussed again in the proof of Theorem 53. Now, the following lemmas will be also useful; the first is a standard result on the multiplicative energy of sets in the spirit of those proven in [TV06].

Lemma 59 *Given subsets $A_1, \ldots, A_m$ of a multiplicative group,*

$$|A_1 \cdots A_m| \geq \frac{|A_1|^2 \ldots |A_m|^2}{E(A_1, \ldots, A_m)}.$$

Proof. Notice

$$\sum_{x \in A_1 \cdots A_m} \left|\{(x_1, \ldots, x_m) \in A_1 \times A_2 \times \cdots \times A_m : x_1 x_2 \cdots x_m = x\}\right| \geq |A_1||A_2| \cdots |A_m|.$$

However by the Cauchy-Schwarz inequality

$$\Big(\sum_{x\in A_1\cdots A_m}\big|\{(x_1,\dots,x_m)\in A_1\times A_2\times\cdots\times A_m : x_1x_2\cdots x_m=x\}\big|\Big)^2$$

$$\leq |A_1\cdots A_m|\sum_{x\in A_1\cdots A_m}|\{(x_1,\dots,x_m)\in A_1\times A_2\times\cdots\times A_m : x_1x_2\cdots x_m=x\}|^2.$$

However

$$\begin{aligned}\sum_{x\in A_1\cdots A_m}&|\{(x_1,\dots,x_m)\in A_1\times A_2\times\cdots\times A_m : x_1x_2\cdots x_m=x\}|^2\\ &=\sum_{x\in A_1\cdots A_m}|\{(x_1,x_1',\dots,x_m,x_m')\in A_1^2\times\cdots\times A_m^2 : x_1\cdots x_m=x=x_1'\cdots x_m'\}|\\ &=E(A_1,\dots,A_m)\end{aligned}$$

so that

$$|A_1\cdots A_m|\geq\frac{|A_1|^2\dots|A_m|^2}{E(A_1,\dots,A_m)}$$

as desired. ■

Finally, we give a lower bound on the size of the image of an interval I under a polynomial $f \pmod q$.

Lemma 60 *Given a square-free integer q, an interval of consecutive integers $I\subset\mathbb{Z}_q$, and a monic polynomial f of degree d*

$$|\pi_q f(I)|\geq\frac{|I|}{d^{\omega(q)}}. \tag{4.5}$$

Proof. Given $y\in\mathbb{Z}_q$, consider

$$|\{x\in I : f(x)\equiv y \pmod q\}|=\prod_{p|q}|\{x\in I : f(x)\equiv y \pmod p\}|$$

by the Chinese Remainder Theorem. However, the number of solutions to $f(x) \equiv y \pmod{p}$ is less than or equal to the degree of $f(x)$ so that

$$\prod_{p|q} |\{x \in I : f(x) \equiv y \pmod{p}\}| \leq d^{\omega(q)}.$$

Since $|\pi_q f(I)| \geq \frac{|I|}{\max\limits_{y \in \mathbb{Z}_q} |\{x \in I : f(x) \equiv y \pmod{q}\}|}$, we have

$$|\pi_q f(I)| \geq \frac{|I|}{d^{\omega(q)}}$$

as desired. ■

4.2 Proofs

We will prove Theorem 53 using two propositions.

Proposition 61 *Given an integer m, let $f(X) = X^d + C_{d-1}X^{d-1} + \ldots + C_1X + C_0 \in \mathbb{Z}[X]$ be a monic polynomial of degree d. For a square-free integer q and an interval $I \subset \mathbb{Z}_q$ of consecutive integers such that*

(i) $d < (\log |I|)^{1/8}$

(ii) $|I| < q^{1/16d^4m^{2d}}$.

If $\pi_q f(I) \subset G$, for G a subgroup of $\mathbb{Z}_q^*$, then $|G| > |I|^{m/2}$.

Proof. First take $q_1|q$ so that $q_1 > |I|$, but $\frac{q_1}{p} \leq |I|$ for some prime factor p; note, this is always possible for any fixed interval $|I| < q$ since taking q_1 to be the smallest divisor of q greater than $|I|$ gives $\frac{q_1}{p} \leq |I|$ as requested.

For each ordered $2m$-tuple, $\vec{h} = (h_1, \ldots, h_{2m}) \in I^{2m}$, define the polynomial $P_{\vec{h}}(\vec{a}) \in \mathbb{Z}[\vec{a}]$ with indeterminates $\vec{a} = (a_0, \ldots, a_{d-1})$ by

$$P_{\vec{h}}(\vec{a}) := \prod_{i=1}^{m} g(h_i) - \prod_{j=m+1}^{2m} g(h_j)$$

where $g(h_k) = h_k^d + a_{d-1}h_k^{d-1} + \ldots + a_0$ for $1 \leq k \leq 2m$. Let $\vec{C} = (C_0, C_1, \ldots, C_{d-1}) \in \mathbb{Z}^d$ as in the statement of the theorem, then define $E = \{\vec{h} \in I^{2m} : P_{\vec{h}}(\vec{C}) \equiv 0 \pmod{q}\}$ and let J be the ideal generated by $P_{\vec{h}}$ for $\vec{h} \in E$. Then by Lemma 59,

$$|G| \geq \left| \prod_{i=1}^{m} \pi_q f(I) \right| \geq \frac{|\pi_q f(I)|^{2m}}{|E|} \tag{4.6}$$

where the first inequality follows from the fact that since $\pi_q f(I) \subset G$, the product is as well. Notice that Lemma 60 gives, $|\pi_{q_1} f(I)| \geq \frac{|I|}{d^{\omega(q_1)}}$; however since q_1 is square-free and $\frac{q_1}{p} \leq |I|$, for q_1 sufficiently large

$$\omega(q_1) = \omega(\frac{q_1}{p}) + 1 \leq \big(1 + o(1)\big)\frac{\log(\frac{q_1}{p})}{\log\log(\frac{q_1}{p})} + 1 \leq \frac{\log|I|}{\log\log|I|} + 1$$

so that

$$|\pi_{q_1} f(I)| \geq \frac{1}{d}|I|^{1 - \frac{\log d}{\log\log|I|}}.$$

Now assume $|G| \leq |I|^{m/2}$. Then since $|\pi_q f(I)| \geq |\pi_{q_1} f(I)|$, (4.6) gives that

$$|E| \geq \frac{|\pi_{q_1} f(I)|^{2m}}{|G|} \geq d^{-2m}|I|^{\frac{3m}{2} - \frac{2m\log d}{\log\log|I|}} > \frac{|I|^{\frac{5m}{4}}}{\log|I|^{\frac{m}{4}}} \tag{4.7}$$

where the last inequality follows from using (i) to obtain

$$d^{-2m} > [(\log|I|)^{1/8}]^{-2m} = (\log|I|)^{\frac{-m}{4}}$$

and using (i) again to obtain $\log\log|I| > 8\log d$ which gives $\frac{2m\log d}{\log\log|I|} < \frac{m}{4}$ so that

$$(\log|I|)^{\frac{-m}{4}}|I|^{\frac{3m}{2} - \frac{2m\log d}{\log\log|I|}} \geq \frac{|I|^{5m/4}}{\log|I|^{m/4}}.$$

On the other hand, using Theorem 58, for any $\vec{z} = (z_0, \ldots, z_{d-1}) \in \mathbb{C}^d$

$$|\{\vec{h} \in I^{2m} : P_{\vec{h}}(\vec{z}) = 0\}| < |I|^{m+\epsilon_{d,m}} \tag{4.8}$$

for q sufficiently large. So, (4.7) and (4.8) together give that for each $\vec{z} \in \mathbb{C}^d$ there exists $\vec{h} \in E$ such that $P_{\vec{h}}(\vec{C}) \equiv 0 \pmod{q}$, but $P_{\vec{h}}(\vec{z}) \neq 0$. Therefore, $V(J) = \{\emptyset\}$. Thus, by Theorem 57 there exists an integer b with

$$0 < \log b < 4d(d+1)m^d(\log|I|^d + \log|E| + (d+7)\log(d+1)m)$$

and polynomials $Q_{\vec{h}} \in \mathbb{Z}[\vec{a}]$ for all $\vec{h} \in E$ such that

$$b = \sum_{\vec{h} \in E} Q_{\vec{h}} P_{\vec{h}}. \tag{4.9}$$

Note

$$4d(d+1)m^d(\log|I|^d + \log|E| + (d+7)\log(d+1)m) < 4(4d^4m^{2d}\log|I|) \tag{4.10}$$

since $|E| < |I|^{2m}$ and $(d+7)\log(d+1)m < d(d+1)m$ so that

$$\log|I|^d + \log|E| + (d+7)\log(d+1)m < \log|I|^d + \log|I|^{2m} + d(d+1)m$$

so distributing $d(d+1)m^d$ and bounding each term by its coefficient times $d^4m^{2d}\log|I|$ gives (4.10). Now, evaluating (4.9) at $\vec{C}$ gives that $b \equiv 0 \pmod{q}$ and so we have,

$$q \leq b < |I|^{16d^4m^{2d}} \tag{4.11}$$

which contradicts (ii). ■

Contrary to our note immediately after Theorem 53, (ii) of Proposition 61 is the condition for which Theorem 44 does not apply; we discuss the case where $|I| \geq q^{\frac{1}{16d^4m^{2d}}}$ after a brief remark.

Remark 62 *Note that by assuming $\pi_{q_1} f(I) \subset G$ with G a subgroup of $\mathbb{Z}_{q_1}^*$ where q_1 is as above, Proposition 61 holds for wider range of moduli than the smooth q of Theorem 53. Moreover, Proposition 61 is a generalization of [IKS$^+$17, Lemma 6] with explicit constants and a square-free modulus; that is, [IKS$^+$17, Lemma 6] says*

Theorem 63 *(Ivanyos ET AL.) Let $\nu \geq 1$ be a fixed integer. Assume that for some sufficiently large positive integer h and prime p we have*

$$h < p^{(c(d)/\nu)^{2d+1}},$$

where $c(d)$ depends only on d. For any two distinct monic polynomials $f, g \in \mathbb{F}_p[X]$ of degree d, we consider the set

$$A = \left\{ \frac{f(x)}{g(x)} : 1 \leq x \leq h \right\} \subseteq \mathbb{F}_p.$$

Then

$$\#A^{(\nu)} = \{a_1 \dots a_\nu : a_1, \dots, a_\nu \in A\} > e^{(-c(d,\nu)\frac{\log h}{\sqrt{\log\log h}})} h^\nu$$

where $c(d, \nu)$ depends only on ν and d.

So taking $\nu = m$ with $h = |I|$ and assuming $|I| < p^{(c/m)^{2d+1}}$ for some absolute constant c, [IKS$^+$17, Lemma 6] gives that $|G| > |I|^m e^{-c(d,m)\frac{\log|I|}{\sqrt{\log\log|I|}}}$. Note that although $f(x)$ is allowed to be a rational function, Theorem 63 only holds for a prime modulus.

Proposition 64 *Given a sufficiently large square-free integer $q = q_1 \dots q_r$, take $f(X) \in \mathbb{Z}[X]$ to be a monic polynomial of degree d such that the pair (f, q_r) is admissible. Let $I \subset \mathbb{Z}_q$ be an interval of consecutive integers such that*

(i) $\log|I| > \log q / \log\log q$

(ii) for all $p|q$, $p < |I|^{1/10}$.

If $\pi_q f(I) \subset G$, for G a subgroup of $\mathbb{Z}_q^*$, then $|G| \geq q^{1-\epsilon}$ provided $q > q(d, \epsilon)$.

Proof. Let $S = \{\chi : \chi \text{ is a multiplicative character modulo } q \text{ and } \chi(a) = 1 \text{ for all } a \in G\}$. Then,

$$|S| = \frac{\varphi(q)}{|G|} \tag{4.12}$$

by Lemma 6. Moreover, since $\pi_q f(I) \subset G$, we have that $\chi(f(h)) = 1$ for all $h \in I$. Thus,

$$\sum_{h \in I} \chi(f(h)) = |I|. \tag{4.13}$$

Notice that for any character $\chi \in S$ there exists a $q'|q$ such that $\chi = \chi_0\chi_1$ with χ_1 a primitive character mod q' by Theorem 16; moreover, since $\pi_q f(I) \subset G$ it follows that $\chi(f(x)) = \chi_1(f(x))$ for all $x \in I$. Therefore if $|I| \leq q'$, (4.13) is impossible unless assumption (iv) of Theorem 44 is violated; that is $q_r < c(d)$. Up to re-indexing $q_r > q_i$ for all i; this gives a bound for q in terms of d so that $|S| < c'(d)$. Thus (4.12) gives $|G| > \dfrac{\varphi(q)}{c'(d)}$ which gives $|G| > q^{1-\epsilon}$ provided $q > q(d, \epsilon)$.

On the other hand, if $|I| > q'$, we can separate the character sum in (4.13) as follows; let $I' \subset I$ be a complete residue system mod q' so that using [Cha14, Weil's Theorem'] we have

$$\left|\sum_{h \in I} \chi(f(h))\right| = \left|\sum_{h \in I'} \chi_1(f(h)) + \sum_{h \in I \setminus I'} \chi_1(f(h))\right| < d^{\omega(q')}\sqrt{q'} + (|I| - q')$$

which contradicts (4.13) unless $\sqrt{q'} \leq d^{\omega(q')}$. Thus, the characters $\chi \in S$ which are primitive for a small q' can be omitted. That is, if the characters discussed in this case were a significant portion of the set S, then $|S| < c''(d)$ giving a bound on $|G|$ as before. ∎

We can state Proposition 64 without the mention of an admissible pair.

Proposition 65 *Given $f(X) \in \mathbb{Z}[X]$ a monic polynomial of degree d, let q be a square-free integer and $I \subset \mathbb{Z}_q$ be an interval of consecutive integers such that*

(i′) $\log |I| > \log q / \log \log q$

(ii′) for all $p|q$, $p < |I|^{1/10}$

If $\pi_q f(I) \subset G$, for G a subgroup of $\mathbb{Z}_q^*$, then $|G| \geq q^{1-\epsilon}$ provided $q > q(d, \epsilon)$.

Remark 66 *Proposition 65 need not mention that the pair (f, q_r) is admissible as is assumed in Proposition 64. Since*

$$\prod_{\substack{p|q \\ p<\sqrt{\log q}}} p < q^{1/10}$$

as discussed in Remark 42, we can omit the assumption that $p > \sqrt{\log q_r}$. Thus, after the omission of the characters of order k where d is a multiple of k (as discussed in Remark 47), we have that (f, q_r) is admissible so that Proposition 65 follows exactly as in the proof of Proposition 64.

Proof. (of Theorem 53) We have two cases. If $|I| < q^{1/16d^4m^{2d}}$, we can apply Proposition 61 immediately. If $|I| \geq q^{1/16d^4m^{2d}}$, then the assumptions (1) and (2) of Theorem 53 give (i′) and (ii′) of Proposition 65 as in Remark 42 which proves Theorem 53. ■

Chapter 5

Summary and Future Work

The goals at the beginning of this thesis were to extend the result of Theorem 44 to a wider collection of polynomials, to potentially strengthen Theorem 44 by weakening the assumptions, and to optimize the saving found in Theorem 40. Of these three goals, the first two were ultimately accomplished in Chapter 3. By changing the definition of a *good* prime and a *p-good* polynomial in Definition 45, the assumptions of Theorem 48 are instantly (but subtly) weakened. Moreover, the assumptions that $f(x)$ is a product of linear factors and that (f, q_r) is admissible in Theorem 44 were replaced by the assumption that for all $p|q$, f is p-good in Theorem 48. This change allowed for Theorem 48 to hold for a wider range of polynomials rather than those that were q_r-admissible.

Unfortunately, because of the weakened conditions of Theorem 48 the saving cannot be improved using the argument found in the proof. That is, the saving of $\frac{(\log q_r)^{1-c}}{\log\log q_r}$ in Theorem 44 is found using the trivial bound after carefully counting the final "bad" set under Definition 43. Initially, my plan was to apply non-trivial character sum bounds to the

portions of these bad sets for which Weil's bound still applied; however, with Definition 45 the set of bad primes are those such that $f \pmod p$ is a k^{th} power of another polynomial, so the trivial bound is the best possible without the added assumptions. Not only that, but Theorems 44 and 48 are two of the very few existing character sums bounds with polynomial arguments; especially those with composite, non-prime power moduli. As the study of characters with polynomial arguments continues to grow, non-trivial bounds on the bad set of Theorem 44 will allow for the optimization the saving under the weaker assumptions.

In Chapter 4, the reader is given a direct application of Theorems 44 and 48 through the second proposition in the proof of the main theorem. Proposition 64 takes a subset of the set of characters on the group being considered in Theorem 53 and uses Theorem 44 to provide a lower bound on the size of the group G. The main theorem of Chapter 4 is a combination of Propositions 61 and 64. Notice that Proposition 61 uses the majority of the machinery discussed earlier in the chapter including the sharp arithmetic version of Hilbert's arithmetic nullstellensatz theorem and the upper bound on the number of factorizations in a generalized arithmetic progression. The results found in this chapter have been submitted and accepted to *Revista Matemática Iberoamericana*; the same journal in which [Shp] appeared.

As discussed in Remark 62, Proposition 61 is Theorem 63 for a composite modulus and polynomial function. Theorem 63 has immediate applications to polynomial interpolation and identity testing problems as discussed in [IKS$^+$17]. Given a finite field $\mathbb{F}_q$, interpolation from powers refers to the process of recovering a hidden monic polynomial

$f \in \mathbb{F}_q[X]$ given an oracle $\mathfrak{O}_{e,f}$ which for each $x \in \mathbb{F}_q$ outputs $\mathfrak{O}_{e,f}(x) = f(x)^e$ for a positive integer $e|(q-1)$. Identity testing from powers refers to the process of determining whether an unknown polynomial f and a known polynomial g are the same after querying $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$. Theorem 63 gives [IKS+17, Theorem 1] after a clever choice of the necessary constants.

Theorem 67 *(Ivanyos ET AL.) For a prime p and a positive integer $e|(p-1)$ with $e \leq p^\delta$ for some fixed $\delta > 0$, given two oracles $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$ for some unknown monic polynomials $f, g \in \mathbb{F}_p[X]$ of degree d with $f \not\sim_e g$, there is a deterministic algorithm to decide whether $f = g$ in at most $e^{c_0 \delta^{1/(2d)}}$ queries to the oracles, where c_0 is an absolute constant.*

Here $f \sim_e g$ means that f/g is a $(p-1)/e$-th power of a non-constant rational function over $\mathbb{F}_p$ and so it is impossible for the oracles to distinguish f from g. The interested reader might try to extend Proposition 61 to a rational function in hopes of also finding a bound on the number of queries to the oracles $\mathfrak{O}_{e,f}$ and $\mathfrak{O}_{e,g}$ as in Theorem 67.

Bibliography

[Apo76] Tom M Apostol. *Introduction to Analytic Number Theory*. Springer-Verlag, New York, 1976.

[Bur63] David A Burgess. On character sums and l-series ii. *Proceedings of the London Mathematical Society*, 1963.

[CC] Kyle Castro and Mei-Chu Chang. Multiplicative energy of polynomial images of intervals modulo q. *Revista Matematica Iberoamericana*. to appear.

[CCG+14] Mei-Chu Chang, Javier Cilleruelo, Moubariz Z. Garaev, Jose Hernández, Igor E. Shparlinski, and Ana Zumalacárregui. Points on curves in small boxes and applications. *Michigan Mathematical Journal*, 2014.

[CGOS12] Javier Cilleruelo, Moubariz Z. Garaev, Alina Ostafe, and Igor E. Shparlinski. On the concentration of points of polynomial maps and applications. *Mathematische Zeitschrift*, 2012.

[Cha03] Mei-Chu Chang. Factorization in generalized arithmetic progressions and application to the erds-szemerédi sum-product problems. *Geometric and Functional Analysis*, 2003.

[Cha14] Mei-Chu Chang. Short character sums for composite moduli. *Journal d'Analyse Mathematique*, 2014.

[CS14] Mei-Chu Chang and Igor E. Shparlinski. Double character sums over subgroups and intervals. *Bulletin of the Australian Mathematical Society*, 2014.

[Fol84] Gerald B. Folland. *Real Analysis: Modern Techniques and Their Applications*. Wiley, New York, 1984.

[Gon] Ke Gong. An elementary approach to character sums over multiplicative subgroups. Preprint, 2012.

[GPG14] Domingo Gómez-Pérez and Jaime Gutierrez. On the linear complexity and lattice test of nonlinear pseudorandom number generators. In *Applied Algebra and Number Theory*, pages 91–101. Cambridge University Press, Cambridge, 2014.

[GPS15] Domingo Gómez-Pérez and Igor E. Shparlinski. Subgroups generated by rational functions in finite fields. *Monatshefte für Mathematik*, 2015.

[IK04] Henryk Iwaniec and Emmanuel Kowalski. *Analytic Number Theory*. American Mathematical Society, Rhode Island, 2004.

[IKS+17] Gabor Ivanyos, Marek Karpinski, Miklos Santha, Nitin Saxena, and Igor E. Shparlinski. Polynomial interpolation and identity testing from high powers over finite fields. *Algorithmica*, 2017.

[KPS01] Teresa Krick, Luis Miguel Pardo, and Martin Sombra. Sharp arithmetic nullstellensatz. *Duke Mathematical Journal*, 2001.

[MV77] Hugh Lowell Montgomery and Robert C. Vaughan. Exponential sums with multiplicative coefficients. *Inventiones Mathematicae*, 1977.

[Ost] Alina Ostafe. Polynomial values in affine subspaces over finite fields. *Journal d'Analyse Mathematique*. in press.

[RNS15] Oliver Roche-Newton and Igor E. Shparlinski. Polynomial values in subfields and affine subspaces of finite fields. *The Quarterly Journal of Mathematics*, 2015.

[Shp] Igor E. Shparlinski. Polynomial values in small subgroups of finite fields. *Revista Matematica Iberoamericana*. to appear.

[TV06] Terence Tao and Van Vu. *Additive Combinatorics*. Cambridge UP, Cambridge, 2006.

[Vin85] Ivan Vinogradov. *Special Variants of the Method of Trigonometric Sums*. Springer-Verlag, Berlin, 1985.