Sums of p-th Roots of Unity

Wang Yao

Department of Mathematics,

Central European University

May 18, 2015

Chapter 1

Introduction

In this thesis, we discuss the problem of finding the minimum length among certain sums of primitive p-th roots of unity and explore its relation with other pieces of mathematics. This is a well-interconnected problem with many area of mathematics. We will try to cover a few important perspectives.

Through this thesis, our major reference would be T. Tao and Van Vu's book [12] for basic definitions and L. Lev and S. V. Konyagin's paper [7] for research purpose.

Through this thesis, p is a prime and we assume $p \geq 5$ to avoid triviality. Let $S := \{\omega | \omega^p = 1\}$ be the set of roots of $x^p - 1 = 0$. We use X to denote a subset of S. Define $\|X\| = |\sum_{a \in X} a|$. So the central problem we are going to address.

Problem 1.1. *Which subset $X \subset S$ minimizes this function $\|X\|$?*

The above problem was formally asked by G. Myerson in [9]. Let me remark that this problem is far harder than at first glance and open for more than four decades. People tried and failed on this problem many times, although its counterpart for maximizing $\|X\|$ is very easy to solve. The

author also hoped to solve this problem and failed after half year's trial. One chapter will be dedicated to explain why this problem is so hard.

To provide enough background, we recall basic definitions in the following three sections. The first section is for field theory and cyclotomic polynomials. The second section introduces the additive combinatorics and its relation of this problem. The third section focuses on the Fourier transformation on finite Abelian groups and its application in additive combinatorics.

In Chapter 2, we discuss some modifications of Problem 1 and related problems. Informally, we explain why we pick Problem 1 instead of other similar problems.

In Chapter 3, we provide the general result, i.e., the current lower bound and upper bound as well as some partial answers to the related problems. I will provide a simple idea to exclude sets that cannot give the minimum sum.

In Chapter 4, we provide some theoretical and computational evidence on the difficulty from various perspectives.

Chapter 5 is conclusion and discussion of open problems.

1.1 Core Definitions

1.1.1 Notations

In this thesis, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$ denote the ring of integers, the field of rational numbers, the field of real numbers and the field of complex numbers respectively. $i^2 = -1$ and $\exp(x) = e^x$ is the standard exponential function in $\mathbb{C}$. For a prime number p, let $\mathbb{F}_p$ be the finite field of p elements.

1.1.2 The Basics

The p-th unit equation $x^p - 1 = 0$ has p roots in $\mathbb{C}$. They form the set S. To visualize S, we draw these numbers on the complex plane and we let ω denote the first root we meet if we go counterclockwisely from the vector $1 + 0i$. So

$$\omega = \exp\left(\frac{2\pi i}{p}\right) = \cos\left(\frac{2\pi}{p}\right) + i\sin\left(\frac{2\pi}{p}\right).$$

Note $\mathbb{Q}(\omega)$ is a Galois extension of $\mathbb{Q}$. The Galois group is isomorphic to the multiplicative group $\mathbb{F}_p^* \cong \mathbb{Z}_{p-1}$. Define the special exponential function $e(x) = e^{2\pi i x/p}$ in Z_p Let $G := Gal\mathbb{Q}(\omega)/\mathbb{Q}$. Let $g \in G$. Then there exists a $k \in \mathbb{N}$ such that $g(\omega = \omega^k)$. And we denote g_k as g. A group element g can also act on $X \subset S$ by $g(X) = \{g(x)|x \in X|\}$.

1.1.3 Big O and other notations

We adopt the traditional big O notations.

$$f(x) = O(g(x)) := \lim_{x\to\infty} f(x) < Cg(x)$$

for some constant $C > 0$.

$$f(x) = o(g(x)) := \lim_{x\to\infty} \frac{f(x)}{g(x)} = 0.$$

$$f(x) = \Theta(g(x)) := \lim_{x\to\infty} C_1 g(x) \leq f(x) \leq C_2 g(x)$$

for some constants $0 < C_1 < C_2$.

1.2 Additive Combinatorics

Additive combinatorics studies the additive structures in groups and fields.(In this thesis all groups are Abelian). Our main concern in this thesis is about

those in finite groups. Let Z be any cyclic Abelian group and A, B be subsets of G. Define $A+B$ and $A-B$ as follows:

$$A+B := \{a+b | a \in A\, b \in B\}$$
$$A-B := \{a-b | a \in A\, b \in B\}$$

Then the most fundamental problems are estimating the size of $A+B$ and $A-B$. For any $A, B \subset Z$ the following is true.

$$\max(|A|,|B|) \leq |A+B|, |A-B| \quad \leq |A||B|$$
$$|A| \leq |A+A| \leq \frac{|A|(|A|+1)}{2}$$

If A is a subset of Z and $|Z|$ is a prime number, a famous theorem discovered first by Cauchy [1] and later by Davenport [4] gives better bound.

Theorem 1. *Let A, B be subset of Z_p then*

$$|A+B| \geq \min\{|A|+|B|-1, p\} \tag{1.1}$$

To prove Cauchy-Davenport theorem, we need introduce the z-transformation.

Definition 1.2. *Pick $z \in A-B$. Then $B_z = B \cap A-z$ and $A_z = A \cup B+z$.*

The most important properties of the z-transformation are the following

$$|A_z| \geq |A|$$
$$|B_z| \leq |B|$$
$$|A_z|+|B_z| = |A|+|B|$$
$$|A_z+B_z| \leq |A+B|$$

So z-transformation keeps the sum of sizes but shrinks or keeps the size of B and the size of the sum. Also the equalities hold for the first two inequalities if and only if $B+z \subset A$. The proof is straightforward so we omit it.

Proof. [12] We use induction on $|B|$. Suppose the Inequality (1.1) holds for any subset smaller than B. Now take B_z and A_z, if $|B_z| < |B|$, then by the induction hypothesis, we are done. Now, we may assume now $|B_z| = |B|$ for all z. this implies $B + z \subset A$ for all $z \in A - B$. So $B + (A - B) \subset A$. This is just

$$a + b_1 - b_2 \in A \text{ for all } a \in A \text{ and } b_1, b_2 \in B$$

Fixing $b_1 \neq b_2$, we see A has a non trivial translation symmetry. But this cannot happen in Z_p unless $A = Z_p$ for which the theorem holds. So $|B| \leq 1$ and we are done. □

Cauchy-Davenport theorem suggests that $\mathbb{Z}$ and Z_p have different additive properties.

Moreover, Vosper's theorem describes when the equality in the Cauchy-Davenport theorem holds.

Theorem 2. *(Vosper) Let $A, B \subset Z_p$ and p is a prime such that $|A|, |B| \geq 2$ and $|A + B| \leq p - 2$. Then $|A + B| = |A| + |B| - 1$ if and only if A and B are arithmetic progression with the same step*

Proof. [12] We begin with the case that one of A or B is an arithmetic progression. Suppose $A = \{a, a + v, \ldots, a + (n - 1)v\}$, where $n \geq 2$. If

$$|A + B| = |A| + |B| - 1,$$

then

$$B + A = B + (A \backslash (a + (n - 1)v)) + \{0, v\} \text{(by the Cauchy-Davenport theorem)}$$
$$|B + A| = |B + \{0, v\}| + (|A| - 1) - 1$$

So this implies

$$|B + \{0, v\}| = |B| + 1.$$

by Davenport's theorem. So B is an arithmetic progression with step v and so is $A + B$.

Next, we show that if $A + B$ is an arithmetic progression with step v and $|A + B| = |A| + |B| - 1$, then A and B are both arithmetic progression with same step. Consider

$$C = -(Z_p \backslash (A + B))$$

Note C is also an arithmetic progression with the same step v. Now $C + B \subset -(Z_p \backslash A)$ by if $-a \in -A$ is in $C + B$ then this implies $-a - b \in C$ for some $b \in B$ contradicts with $-(A + B) \cap C = \emptyset$ So we have

$$\begin{aligned} |C| &= |Z_p| - |A + B| \\ &= |Z_p| - |A| - |B| + 1 \\ &\geq |2| \\ \text{also } |C + B| &\leq |Z_p| - |A|. \\ \text{But } |C + B| &\geq |C| + |B| - 1 \\ &= |Z_p| - |A|. \end{aligned}$$

So by the conclusion we had in the first case, we have B is an arithmetic progression with step v and for similar reason, so is A.

Finally, we deal with the general case and we prove by induction on $|B|$.

The case $|B| = 2$ is obviously done.

For $|B| > 2$, we use the z-transformation of B. Pick $z \in A - B$ and suppose $1 < |B_z| < |B|$. Then recall

$$\begin{aligned} |A_z| + |B_z| &= |A| + |B|, \\ |A_z| + |B_z| - 1 \leq |A_z + B_z| &\leq |A + B| = |A| + |B| - 1. \end{aligned}$$

The above gives $A + B = A_z + B_z$ by observing $A_z + B_z \subset A + B$. Then by induction hypothesis, have A_z, B_z and $A_z + B_z$ are arithmetic progression with step v and we are done.

It remains to show if for all $z \in A - B$, we have $|B_z| = 1$ or $|B|$. Denote $Z := \{z \in A - B || B_z| = |B|\}$, then by property of z-transform, we have $B + Z \subset A$. So $|Z| \leq |A| - |B| + 1$ by Davenport's theorem. Also $|A - B| \geq |A| + |B| - 1$. So we have

$$|B \backslash Z| \geq 2|B| - 2$$

Recall $B_z = B \cap A - z$. So by pigeon-hole principle, there exist z_1 and z_2 such that $B_{z_1} = B_{z_2} = \{b\}$. This gives

$$A + B = A_{z_1} + b = A_{z_2} + b.$$

Therefore $A_{z_1} = A_{z_2}$. Since $|A \cap B_{z_1}| \leq 1$ and $|A \cap B_{z_2}| \leq 1$. It means $B + z_1$ and $B + z_2$ differs at most in one elements. So B is an arithmetic progression with step $z_1 - z_2$. With the conclusion of the first case, we are done. □

The above two theorems show that arithmetic progressions are very special in additive combinatorics.

1.3 Fourier Analysis method in Additive Combinatorics

1.3.1 Bilinear Form

Note that our general problem origins from finding the minimum Fourier coefficient of a characteristic function χ_A over $\mathbb{Z}_N$. To introduce the full machinery of Fourier Transformation, we borrow the notations and definitions from [12].

To do Fourier transformation on a finite field, we need the definition of the bilinear form. A map from $Z \times Z$ to $\mathbb{R}/\mathbb{Z}$ is a bilinear form if $(\xi, \ )$ and

$(, x)$ are both homomorphism. For $Z = \mathbb{Z}/p\mathbb{Z}$, $(\xi, x) \mapsto \frac{\xi * x}{p}$ is a bilinear form where $*$ is the standard multiplication in $\mathbb{R}$. We usually use $x \cdot \xi$ to denote bilinear form and $x\xi$ to denotes the standard multiplication in $\mathbb{F}_p$.

1.3.2 Fourier Transformation.

The set of all functions from Z to $\mathbb{C}$ forms a inner product space.

The inner product is given by

$$< f, g >= \frac{1}{|Z|} \sum_{x \in Z} f(x)\overline{g(x)}$$

The Fourier transformation of a function f is defined as

$$\widehat{f(\xi)} =< f, e(\xi \cdot x) >= \frac{1}{|Z|} \sum_{x \in Z} f(x) \cdot \overline{e(\xi \cdot x)}$$

where

$$e(x \cdot \xi) = \exp(\frac{x\xi}{|Z|} 2\pi i)$$

The functions $e(\xi x)$ $(\xi \in Z)$ consists a complete basis for $\mathbb{C}^Z$. So we have the Fourier inversion formula

$$f(x) = \sum_{\xi \in Z} \widehat{f(\xi)} e(\xi \cdot x).$$

Let $Z = \mathbb{Z}/p\mathbb{Z}$ be the additive group of order p. We use A and B to denote subsets of Z.

The exponential map induces a bijection from subset of Z to subset of S. Between $A \subset Z$ and $X \subset S$, we write $A \longleftrightarrow X$ for the correspondence. Consider the characteristic function of $A \subset Z$:

$$\chi_A(x) = \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ if } x \notin A \end{cases}$$

We will use characteristic functions and random variable interchangeably.

For random variable we can consider Z as a probability space where for each $x \in Z$, we have $Pr(x) = \frac{1}{|Z|}$. $\chi_A : Z \mapsto \mathbb{R}$ is defined as

$$\chi_A(x) = \begin{cases} 1 \text{ if } x \in A \\ 0 \text{ if } x \notin A \end{cases}$$

And we can have the expectation of χ_A as

$$\mathbf{E}\chi_A = \frac{1}{|Z|}\sum_{x \in Z}\chi_A(x) = \frac{|A|}{|Z|}.$$

Let $A \subset Z$ corresponding to $X \subset S$, the first coefficient of χ_A

$$\widehat{\chi_A(0)} = \frac{1}{|Z|}\sum_{x \in Z}\chi_A(x) = \mathbf{E}_Z(\chi_A).$$

The coefficient

$$\begin{aligned} |\widehat{\chi_A(p-1)}| &= |\frac{1}{|Z|}\sum_{x \in Z}\chi_A(x)\overline{e((p-1)\cdot x)}| \\ &= \frac{1}{|Z|}\sum_{x \in A}\chi_A(x)e^{2\pi i x/p} \\ &= \frac{1}{|Z|}\sum_{x \in A}e^{2\pi i x/p} \\ &= \frac{1}{|Z|}\|X\| \end{aligned}$$

Example: $p = 7$, Let $A = \{0, 1, 2, 5\} \longleftrightarrow X = \{1, \omega,\ \omega^2, \omega^5\}$. Then

$$\begin{aligned} \widehat{\chi_A(0)} &= \mathbf{E}_Z\chi_A = 4/7 \\ \widehat{\chi_A(p-1)} &= \frac{1}{|Z|}\sum_{x \in Z}\chi_A(x)\overline{e(x\cdot p-1)} \\ &= \frac{1}{7}(1 + e(1) + e(2) + e(5)) \\ &= \frac{1}{7}\|X\| \end{aligned}$$

We also introduce the convolution and L_2-norm

Definition 1.3. *If $f, g \in L^2(Z)$ are random variables over the additive group Z, then the convolution of f and g are defined as*

$$f * g(x) = \mathbf{E}_{y \in Z} f(x-y)g(y) = \mathbf{E}_{y \in Z} f(y)g(x-y)$$

We define the *support* of f to be the set $supp(f) = \{f(x) \neq 0 | x \in Z\}$. Now there are several simple to verify properties of the convolution.

$$supp(f * g) \subset supp(f) + supp(g)$$
$$A + B = supp(\chi_A * \chi_B)$$
$$\widehat{fg(\xi)} = \hat{f}\hat{g}$$
$$\mathbf{E}_Z(f * g) = (\mathbf{E}_Z f) \cdot (\mathbf{E}_Z g)$$

where χ_A and χ_B are characteristic functions of $A, B \subset Z$ respectively.

The L_2 norm in the inner product space is simply:

Definition 1.4.

$$\|f\|_2 := \sqrt{< f, f >}$$

The Fourier transformation is intensively used in additive combinatorics We pick on a simple theorem with all the above machinery applied. The proof is very concise in the language of Fourier transformation and no direct combinatorial method is known.

Theorem 3. *[12]Let F be a finite field of order p and $A \subset F \backslash \{0\}$. Then*

$$F \subset A \cdot A + A \cdot A + A \cdot A$$

Proof. [3] We give the non-degenerate bilinear form from $F \times F \mapsto \mathbb{C}$ as $(x, y) \mapsto e(x \cdot y)$. Define

$$f := \mathbf{E}_{y \in A} \chi_{y \cdot A}(x).$$

Here $y \cdot A = \{yx | x \in A|\}$.

Now we can observe $f(x) > 0$ if and only if $x \in A \cdot A$, otherwise $f(x) = 0$. Also:

$$\begin{aligned}
\widehat{f(\xi)} &= \frac{1}{|F|} \sum_{x \in F} f(x) \overline{e(x \cdot \xi)} \\
&= \frac{1}{|F|} \sum_{x \in F} \mathbf{E}_{y \in A} \chi_{y \cdot A}(x) \overline{e(x \cdot \xi)} \\
&= \mathbf{E}_{y \in A} \frac{1}{|F|} \sum_{x \in F} \chi_{y \cdot A}(x) \overline{e(x \cdot \xi)} \\
&= \mathbf{E}_{y \in A} \frac{1}{|F|} \sum_{x \in F} \chi_A(x/y) \overline{e(x/y \cdot y\xi)} \\
&= \mathbf{E}_{y \in A} \widehat{\chi_A(y\xi)}
\end{aligned}$$

Note that formula on page 158 in the book [12] is erroneous, we used the version from the original paper [3]. Now apply Cauchy-Schwartz to $|\widehat{f(\xi)}| = |\mathbf{E}_{y \in A} \widehat{\chi_A(y\xi)}|$ as:

$$\begin{aligned}
|\mathbf{E}_{y \in A} \widehat{\chi_A(y\xi)}| &= |\frac{1}{|A|} \sum_{y \in A} \widehat{\chi_A(y\xi)}| \\
&\leq |\frac{(\sum_{y \in A} |\widehat{\chi_A(y\xi)}|^2)^{1/2}}{|A|^{1/2}}| \\
&\leq |\frac{(\sum_{y \in F} |\widehat{\chi_A(y\xi)}|^2)^{1/2}}{|A|^{1/2}}| \\
&= |\frac{\|\chi_A\|^{1/2}}{|A|^{1/2}}| \\
&= \frac{|A|^{1/2}}{|F|^{1/2}|A|^{1/2}} \\
&= 1/|F|^{1/2}
\end{aligned}$$

For all x,

$$\begin{aligned}
|f*f*f(x) - \frac{1}{|F|}|A|^3| &= |\sum_{\xi\in F} \widehat{f*f*f(\xi)}e(\xi\cdot x) - \frac{1}{|F|}|A|^3| \\
&= |\frac{1}{|F|}\sum_{\xi\in F^*} \widehat{f(\xi)}^3 e(x\xi)| \\
&\leq \frac{1}{|F|}\sum_{\xi\in F^*} |\widehat{f(\xi)}^3| \\
&\leq \frac{1}{\sqrt{|F|}}\sum_{\xi\in F} |\widehat{f(\xi)}|^2 \\
&= \sqrt{|F|}\|f\|_2^2 \\
&= \sqrt{|F|}|A|
\end{aligned}$$

Note $\frac{1}{\sqrt{|F|^3}} > \sqrt{|F|}|A|$. So the above calculations gives $F \subset supp(f*f*f) \subset supp(f)+supp(f)+supp(f) \subset A\cdot A + A\cdot A + A\cdot A$ and we are done.

□

Chapter 2

Related Problems

In this chapter, we discuss some modifications and related problems.

2.1 The Maximum of $\|X\|$

As we stated, the maximum problem is rather easy to answer.

Theorem 4. *For p sufficiently large, $\|X\| \leq \left(\frac{p}{\pi}\right) + o(1)$ and the bound is tight.*

Proof. We claim that we find $U := \{e(j) \in U | j \leq p/4 \text{ or } j \geq 3/4p\}$ that $\|U\|$ is maximum among all subset of S. The computation for the bound is easy

$$\begin{aligned} \|U\| &= |\sum_{-p/2<j<0}^{0\leq j<p/2} e(j)| \\ &= |\sum_{0>j>-p/2}^{0\leq j<p/2} \cos\left(\frac{2\pi j}{p}\right)| \end{aligned}$$

Since every term is positive we obtain:

$$\|U\| = \int_{-p/2}^{p/2} \cos\left(\frac{2\pi x}{p}\right) dx + o(1) = \frac{p}{\pi} + o(1)$$

It remains to show that if X maximizes $\|X\|$, then X must be U, rotation of U or complement of U from S.

We prove the above statement by showing that if X is none of the three possibilities above, then we can find X' such that $\|X'\| > \|X\|$.

Lemma 2.1. *U maximizes $\|U\|$ for subsets of S that is contained in a half plane of $\mathbf{R^2}$.*

Proof. We may assume X is a subset set of U. We show $\|X\| \leq \|U\|$. let $y = \sum_{x \in X} x$. Then assume $\arg(y) = \theta$. If $\theta = 0$, then obviously $\|U\| \geq \|X\|$. Suppose $\theta > 0$, then if we can find $v \in U \backslash X$ and $|\arg(y) - \arg(v)| < \pi/2$, then we are done. If we cannot find such v, it means X contains all $v \in U$ such that $|\arg(v) - \arg(y) < \pi/2|$. So $\arg(y) < \theta - \pi/2 < 0$ contradicts with $arg(y) = \theta > 0$. □

Now we prove the theorem. Let $u = \sum_{x \in X} x$ and $\arg(u) = \theta$. We add all these vectors to X if $< \sum v, u > \geq 0$ and call the modified set X_1 Observe $\|X_1\| \geq \|X\|$ by adding vs. Now X_1 contains a rotation of U.

If X_1 is a rotation of U, then we are done. If not, then take $X_2 = S \backslash X_1$. So $\|X_2\| = \|X_1\|$. Now X_2 is contained in some half plane. So $\|U\| \geq \|X_2\|$ by the lemma and we are done. □

2.2 Derived Problms from Problem 1.1

A more detailed problem would be

Problem 2.2. *For which $X \subset S$ of size k is $\|X\|$ minimal?*

T. Tao asked this on *Mathoverflow.com*[11] (in his question, he asked for p not necessarily a prime number). If we can answer this problem, then

we can easily deduce the answer of Problem 1.1. But even for $k = 5$, the problem is hard.

An important but open problem is to ask whether the following statement is true.

Conjecture 2.3. *For any p, the set X that minimizes $\|\widehat{\ }\|$ is symmetric to the real line on the complex plane or can be rotated to such.*

Experimental data suggest this statement is true for all $p < 81$. But we could not prove it.

From the point of view of Fourier transformation, Problem 1 can be viewed as

Problem 2.4. *For which $A \subset Z$, the Fourier coefficient $\chi_A\widehat{(p-1)})$ is minimum*

2.3 The Littlewood Problem

An imporatant related problem is the "Littlewood's problem"[2]. The L_1-norm of a function from Z to $\mathbb{C}$ is defined as

$$\|f\|_1 := \sum_{\xi \in Z} |\widehat{f(\xi)}|$$

we mainly focus on the characteristic functions of subsets of Z. Littlewood's problem asks:

Problem 2.5. *For each k, what is the minimum of $\|\chi_A\|_1$, if $A \subset Z$ and $|A| = k$?*

This problem is asking the minimum average of Fourier coefficients rather than the single minimum value. Littlewood conjectured that if $\|\chi_A\|_1$ is

minimum among all $|A| = k$, then A must be an arithmetic progression. The strong Littlewould Conjecture remains open for finding the exact value of the minimum and for whether the minimum is obtained when A is an arithmetic progression. But S. V. Konyagin[6] and O. C. Mcgehee et.al [8] independently obtained the following partial result:

Theorem 5. *For $|A| = k$, $\|\chi_A\|_1 \geq C \log k$ for some positive constant C, the lower bound is tight up to constant.*

Estimating the Fourier coefficient of χ_A(historically called trigonometrical sum) is a very useful tool in number theory, especially in counting the numbers of solutions of linear systems in $\mathbb{F}_p$[7][5].

Chapter 3

Existing Bounds

3.1 Bounds for the General Problem

Recall the general problem:

Problem 3.1. *Which subset $X \subset S$ minimizes $\|X\|$?*

We provide a partial answer by Lev and Konyagin

3.1.1 Lower bound

Theorem 6. *(Lev&Konyagin) If $X \subset S$ Then $\|X\| \geq p^{-\frac{p-3}{4}}$.*

Proof. Suppose X has the minimum sum. Let $y = \sum_{j \in A} e(j)$ as an algebraic integer. ($|N(y)| \geq 1$ as $|y| > 0$)

The norm of y would be

$$N(y) = \prod_{g \in Gal(\mathbb{Q}(\omega)/\mathbb{Q})} g(y).$$

Note that for $y = \sum e(j)$, we have $g_k(y) = \sum e(kj)$ for some k. Recall

$|F^*| = p-1$ and $|g_{p-1}(y)| = |y|$, so

$$\begin{aligned} 1 \leq |N(y)|^2 = |y^4|| \prod_{k \neq \pm 1} |g_k(y)|^2 \text{ via Minkowski's inequality} \\ \leq |y^4|(|\frac{1}{p-3} \sum_{k \neq \pm 1} |g_k(y)|)^{p-3} \\ \leq |y^4| p^{p-3}. \end{aligned}$$

By So we we have $\|X\| \geq p^{-\frac{p-3}{4}}$. □

3.1.2 Upper bound.

Theorem 7. *(Lev&Konyagin) For $n = 2^k < \frac{p}{20}$, we can find a set X such that $|X|$=n and $\|X\| \leq n^{\frac{\log p}{\log 4}}$*

Before the proof, we describe the idea behind the proof. Suppose we pick a unit vector u in S and we need a vector that "cancels" u most Then we can choose the two vectors which are closest to $-u$ on the complex plane. For example 1 is the origin vector, then $e(\frac{p-1}{2})$ and $e(\frac{p+1}{2})$ would be two possible choices. Now for $u' = e(\frac{p-1}{2}) + 1$, we can pick two vectors and let their sum cancel u' as much as possible. So at k-th step we consume 2^k vector and we stop when not more vector can be used.

Proof. We provide the best construction so far. Let $p' = \frac{p-1}{2}$ and define A to be the set of all the sumset sums of

$$U = \{p'+1, p'+2, p'+4, \ldots p'+2^{k-1}\} \subset Z_p$$

For the empty set $\emptyset \subset A$, we let the sum be 0.

Claim 3.2. *Take $X \subset S$ and $X \longleftrightarrow A$ then $\|X\| < n^{-\frac{\ln p}{2 \ln 2}}$*

Proof.

$$P\|X\| = |\sum_{B\subset U}\sum_{x\in B} e(x)|$$

By rearranging the terms we have

$$\|X\| = |\prod_{j=0}^{k}(1 + e(\frac{p' + 2^j}{p}))|$$

Expand $e(x)$ to trigonometric functions we have

$$\begin{aligned}
\|X\| &= |2^k \prod_{j=0}^{k-1} \cos\pi\frac{p - 1 + 2^{j+1}}{2p}| \\
&= 2^k \prod_{j=1}^{k} |\sin\frac{\pi}{p}(2^j - 1)| \\
&< \left(\frac{\pi}{p}\right)^k 2^{\frac{k(k+1)}{2}} \\
&= n^{-\frac{\ln(\pi/(\sqrt{2}))}{\ln 2} + \frac{\ln n}{2\ln 2}} \\
&< n^{-\frac{\ln p}{2\ln 2}}
\end{aligned}$$

□

Now, it remains to show the subset sums of U are distinct. Assume

$$\sum_{i\in I}(p' + 2^i) \equiv \sum_{j\in J}(p' + 2^j) \pmod{p} \tag{3.1}$$

for two subset $I, J \subset \{0, \ldots, k-1\}$ and we show $I = J$. Define $\xi = \sum_{i\in I} 2^i$ and $\eta = \sum_{j\in J} 2^j$. Then

$$0 \le \xi, \eta, |I|, |J| \le 2^k < p/20$$

And (3.1) gives

$$\begin{aligned}
2\xi - |I| &\equiv 2\eta - |J| \pmod{p} \\
2\xi - |I| &= 2\eta - |J|
\end{aligned}$$

Write ξ and η in binary form and $|I|$ and $|J|$ are the counter of digits of 1 in their binary form, so either $|I| = |J|$ and $\xi = \eta$ implies $I = J$ or $|I| \neq |J|$ implies $\xi \neq \eta$ hence $I \neq J$. □

3.2 Minimum Cardinality of X

Since it is hard to find the exact answer, we find some partial answers.

Problem 3.3. *What would be the cardinality of X if X is a set with minimum sum.*

Partial answer:

Theorem 8. *Let X be a subset of S. Then $\|X\|$ is not minimum if X has fewer than $\sqrt{\frac{p}{3}}$ elements.*

Proof. Let $I = [\lceil p/3 \rceil, \lfloor 2p/3 \rfloor]$,

Observe that if $A + b = \{x + b | x \in A\}$ $(b \in I)$ does not intersect with A then $||X \cup e(b)X\| < \|X\|$.

Consider $X \longleftrightarrow A$. Recall that if $I \nsubseteq A - A \implies \exists b \in I$ such that $(A + b) \cap A = \emptyset$.

By the estimation of $A - A$, We have $|A - A| \leq n^2 - n + 1 \leq p/3$ .where $n = |A|$. So we have$|A| \leq \sqrt{\frac{p}{3}}$. □

This method cannot give you bound better than $2\sqrt{\frac{p}{3}}$ by the following construction. Pick $J = [0, \lceil \sqrt{p/3} \rceil]$ and $C = [0, \lceil \sqrt{p/3} \rceil]$.Observe $[0, \lceil p/3 \rceil] \subset J-(-C)$. So $A = J+\lceil p/3 \rceil \cup -C$ would be the desired construction. Because $|A| = 2\sqrt{p}$ and $I \subset A - A$.

We might be interested to to ask find A with minimal size and $I \subset A-A$. But even for similar question on $Z = \mathbb{Z}$ and $I = [1, n]$, we don't know the exactly bound. This fact is known via personal communication with Imre Ruzsa.

Problem 3.4. *What is minimum $|A|$ such that $A \subset \mathbb{Z}$ and $[1, n] \subset A + A$*

3.3 Arithmetic Progression

Proposition 3.5. *Let A be an arithmetic progression in Z_p with step k and length m. Then $X \longleftrightarrow A$ and $\|X\|$ is not the minimum.*

Proof. suppose $A = \{0, k, 2k \cdots, (m-1)k\}$. Then

$$\begin{aligned} \|X\| &= \sum_{j=0}^{m-1} \omega^{jk} \\ &= \frac{1-\omega^{(m-1)k}}{1-\omega^k} \\ &> |\frac{sin(1/p)}{2}| \\ &= \Theta\left(\frac{1}{p}\right) \end{aligned}$$

□

The above argument shows the characteristic functions of arithmetic progressions have relatively small Fourier coefficient for every non zero ξ, but not as small the minimum.

3.4 Expectation of $\|X\|^2$

In this section we compute the second moment of $\|X\|$. Recall that the functions from Z to $\mathbb{C}$ form a inner product space. Wwe observe $|\chi_X|^2$ can be expressed with the square sum of its Fourier coefficients and the expectation of $\overline{f(\xi)}$ are the same for $\xi \neq 0$. Let v be a random subset uniformly picked from S. So

$$\chi_v(x) = \sum_{\xi \in Z} \widehat{\chi_v(\xi)} e(\xi \cdot x).$$

Parseval's equality says that if$\{v_i\}$s are complete orthogonal basis, then

$$\|f\|^2 = \sum | < f, v_i > |^2$$

In our case Parseval's equality gives

$$\|\chi_v\|_2^2 = \sum_{\xi \in Z} |\widehat{\chi_v(\xi)}|^2.$$

Now

$$\begin{aligned}
\mathbf{E}(\|\chi_v\|_2^2) &= \frac{1}{2^n} \sum_{A \subset Z} \|\chi_A\|_2^2 \\
&= \frac{1}{2^n} \sum_{A \subset Z} \sum_{\xi \in Z} |\widehat{\chi_A(\xi)}|^2 \\
&= \frac{1}{2^n} \sum_{A \subset Z} \sum_{\xi \in Z} |\frac{1}{|Z|} \sum_{x \in Z} \chi_A(x) \overline{e(\xi \cdot x)}|^2 \\
&= \frac{1}{2^n} \sum_{A \subset Z} \sum_{\xi \in Z} |\frac{1}{|Z|} \sum_{x \in A} \overline{e(\xi \cdot x)}|^2 \\
&= \frac{1}{2^n} \sum_{\xi \in Z} \sum_{A \subset Z} |\frac{1}{|Z|} \sum_{x \in A} \overline{e(\xi \cdot x)}|^2 \\
&= \frac{1}{2^n} \sum_{X \subset S} (\frac{|X|}{|S|})^2 + \frac{1}{|S|^2} \sum_{\substack{\xi \in Z \\ \xi \neq 0 \\ g \in Gal\mathbf{Q}(\omega)/\mathbf{Q}}} \|g_{(p-\xi)}(X)\|^2 \\
&= \mathbf{E}(\mathbb{P}_Z(A)^2) + \frac{1}{2^n} \sum_{\substack{\xi \in Z \\ \xi \neq 0 \\ g \in Gal\mathbf{Q}(\omega)/\mathbf{Q}}} \frac{1}{|S|^2} \sum_{g_{(p-\xi)}(X) \subset S} \|X\|^2 \\
&= \mathbf{E}(\mathbb{P}_Z(A)^2) + \frac{|S|-1}{2^n |S|^2} \|X\|^2 \\
&= \mathbf{E}(\mathbb{P}_Z(A)^2) + \frac{|S|-1}{|S|^2} \mathbf{E}(||X||^2).
\end{aligned}$$

Also note

$$\begin{aligned}
\mathbf{E}(\|\chi_v\|_2^2) &= \frac{1}{2^n} \sum_{A \subset Z} \|\chi_A\|_2^2 \\
&= \frac{1}{2^n} \sum_{A \subset Z} \sum_{x \in Z} |\chi_A(x)|^2 \\
&= \frac{1}{2^n} \sum_{A \subset Z} \sum_{x \in Z} \chi(x) = \frac{1}{2}
\end{aligned}$$

And the first term on the right is

$$\begin{aligned}\mathbf{E}((P_Z A)^2) &= Var(P_Z A) + \mathbf{E}(P_Z(A))^2 \\ &= p \times \frac{1}{2} \times (1 - \frac{1}{2}) \times \frac{1}{p^2} + (\frac{1}{2})^2 \\ &= \frac{1}{4p} + \frac{1}{4}.\end{aligned}$$

So

$$\frac{p-1}{p^2}\mathbf{E}(\|X\|^2) = \frac{1}{4} - \frac{1}{4p}.$$

And we have $\mathbf{E}(\|X\|^2) = (\frac{1}{4} + o(1))p$. So a random $X \subset S$ has $\|X\| \sim \frac{\sqrt{p}}{2}$.

Chapter 4

Difficulties and the Experimental Evidence

In this chapter, we give some evidence on the difficulty of Problem 1.1.

4.1 Difficulty for k is small

One obvious reason is that the number of subset of S is 2^p, which grows exponentially in p. So a brute force method to find the subset X that minimizes $\|X\|$ is infeasible.

Moreover, consider the more detailed problem: recall Problem 2.2

Problem 4.1. *Which $X \subset S$ minimizes $\|X\|$ if $|X| = k$?*

Now we try to answer this problem approximately by asking

Problem 4.2. *For p sufficiently large, what is the order of the difference of minimum $\|X\|$ and 0 if $|X| = k$*

For $k < 5$, these questions can be answered easily, see [9] via geometrical arguments. For $k > 5$, these problem are connected to how to approximate

an arbitrary number via algebraic integer and such problems seem generally hard.

For example, let's consider the next simplest case. Let $k = 5$.

We may assume 1 is in X. Then the problem becomes

Problem 4.3. *For which four elements of S that their sum approximates -1 best and what is the order of the approximation.*

We conjecture the answer is between $\Theta(p^{-1})$ to $\Theta(p^{-2})$ because for $k = 4$, the approximation rate is $\Theta(p^{-1})$.

To find the exact answer, let's begin with checking whether we should pick $e(\frac{p-m}{2})$ where $m = o(1)$. Now we assume Conjecture 2.3 is true. So we find another element in S that the real part of their sum approximate $1/2$ best. It would be $e(\lfloor p/6 \rfloor + l)$ where $l \in Z$ and $l = o(p)$.

$$\mathbf{Re}(e\left(\frac{p-1}{2}\right) + e(\lfloor p/6 \rfloor + l)) = \cos\left(\frac{2\pi(p-m)}{2p}\right) + \cos\left(\frac{2\pi(\lfloor p/6 \rfloor + l)}{p}\right)$$

Write them in their Taylor expansions and let $u = 2\pi/p$:

$$\begin{aligned}
I &= \cos\left(\frac{2\pi(p-m)}{2p}\right) + \cos\left(\frac{2\pi(\lfloor p/6 \rfloor + l)}{p}\right) \\
&= \cos(\frac{-mu}{2})\cos\pi - \sin(\frac{-mu}{2})\sin\pi + \cos(u(l+a))\cos\frac{\pi}{3} - \sin(u(l+a))\sin\frac{\pi}{3} \\
&\text{(where } a = \lfloor p/6 \rfloor - p/6\text{)} \\
&= -\cos(mu/2) + \frac{1}{2}\cos(u(l+a)) - \frac{\sqrt{3}}{2}\sin(u(l+a)) \\
&= -1 + \frac{1}{2}\Big(\frac{mu}{2}\Big)^2 + o(p^{-3}) + \frac{1}{2}\left(1 - \frac{1}{2}(u(l+a))^2 + o(p^{-3})\right) + \frac{\sqrt{3}}{2}\big(u(l+a) + o(p^{-2})\big) \\
&= \frac{1}{2} + u\left(-\frac{\sqrt{3}}{2}(l+a) - \frac{1}{4}u(l+a)^2 + \frac{1}{8}m^2u\right)
\end{aligned}$$

The above calculation implies that we can obtain a $\Theta(p^{-1})$ approximation, but not a $\Theta(p^{-2})$ approximation because we have an $\Theta(1)$ nonzero term in the parenthesis.

Currently, we could not find two vectors that the sum obtained is such. And furthermore, a negative answer for $\Theta(p^{-2})$ approximation is very difficult to obtain because we need disprove approximation of an irrational via algebraic integers, which is generally very difficult.

4.2 Evidence from Empirical data

Here we present the findings of N. D. Noe, for the minimum configuration for all $p < 81$. We list then in Table 4.1, the reader can find brief data in OEIS[10].

(The configuration column in Table 4.1 contais only the upper plane half because all the minimum configurations are symmetric to the real line).

A visualized plot is also made by T. D. Noe in Figure 4.1.

From Table 4.1 and Figure 4.1, we can see that for prime numbers $\min \|X\|$ decreases as p increases and the minimum is close to the existing upper bound. But we cannot make a theory to explain the configuration.

However we can conjecture:

Conjecture 4.4. *For all p prime, The configuration of X such that X minimize $\|X\|$ is symmetric to the real line.*

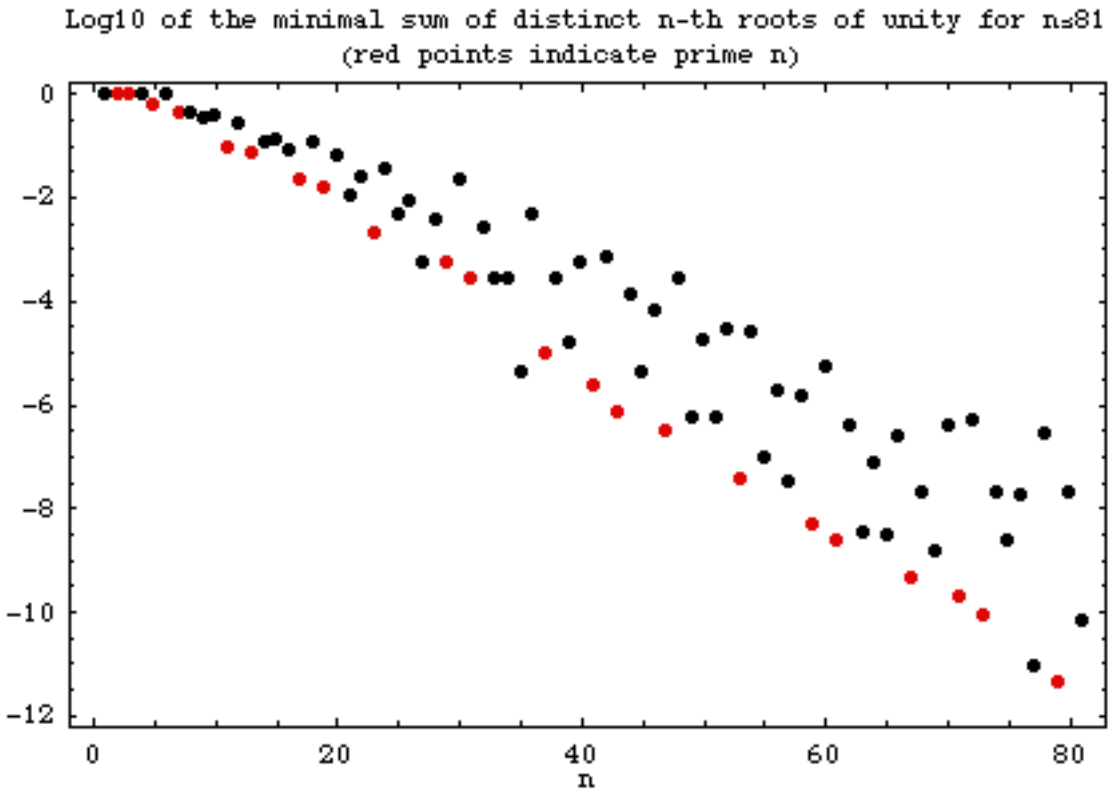
Conjecture 4.5. *For all p, q prime* $\min_p \|X\| < \min_q \|X\|$ *if* $p > q$.

If we allow composite numbers as shown in Figure 4.1, then we don't have the strict monotonicity on the minimum of $\|X\|$. Generally, $\min \|X\|$ is larger

p	$\min \|\|X\|\|$	Cardinality of the minimum	The configuration of $A \longleftrightarrow X$
5	0.618033988750	2	1
7	0.445041867913	2	2
11	0.088155921225	5	0 2 5
13	0.070101776965	6	1 3 6
17	0.020732553832	5	0 4 6
19	0.015942667074	7	0 2 6 8
23	0.002105883604	8	2 5 6 11
29	0.000531288261	14	3 4 5 7 8 12 13
31	0.000285534741	11	0 4 5 7 13 15
37	0.000009249591	18	4 5 6 7 8 10 13 15 18
41	0.000002427733	19	0 1 4 5 6 13 15 16 17 18
43	0.000000710113	17	0 4 5 6 7 14 18 19 20
47	0.000000296426	22	2 4 6 7 11 12 14 15 16 21 22
53	0.000000036964	18	2 3 6 7 15 16 22 24 26
59	0.000000004723	26	2 3 6 8 13 14 15 16 17 18 26 28 29
61	0.000000002376	29	0 1 2 6 8 9 12 15 16 20 21 26 27 29 30
67	0.0000000004402076	30	2 3 7 8 10 13 14 15 20 21 22 25 31 32 33
71	0.0000000002068930	32	2 4 7 8 9 15 17 18 20 21 22 24 26 27 28
73	0.0000000000855482	34	1 3 9 10 11 12 14 16 17 22 23 24 25 28 29 30 33
79	0.0000000000042344	30	2 4 5 6 7 14 17 21 26 28 29 30 32 34 35

Table 4.1: The minimum sum for $p < 81$

Figure 4.1:



for composite numbers but 35 is an exception that $\min_{35} \|X\| < \min_{37} \|X\|$ where 37 is a prime.

A weaker conjecutre compared to Conjecture 4.5 can be made for general n:

Conjecture 4.6. *Conjecture 4.4 is true for all* $n \in \mathbb{N}^+$.

Conjecture 4.7. *Given* $c > 0$*, for* m*,* n *sufficiently large, if* $n > cm$*, then* $\min_m \|X\| > \min_n \|X\|$

We might be interested in finding how "compositeness" of a number n impact on $\min_n \|X\|$. But there is no dicect conjecture that we can made.

Chapter 5

Conclusion

Problem 1.1 remains open and looks inaccessible so far. But rich connections with other pieces of mathematics might suggest broader view and tools are needed to attack it.

Before complete solution, we suggest to prove/disprove those conjectures aforementioned. Conjecture 4.4 looks more hopeful than others but we still do not know.

Bibliography

[1] A.L.Cauchy. Recherches sur les nombres. *Journal. L'école Polyteque 9* (1813), 99–116.

[2] Ben Green, S. K. On the littlewood problem modulo a prime. *Canadian Journal of Mathematics 61* (2009), 141–164.

[3] Bourgain, J. Mordell's exponential sum estimate revisited. *Journal of the American Mathematical Society 18*, 2 (2005), pp. 477–499.

[4] Davenport. On the addition of residuel classes. *Journal of London Mathematics Society 10*, 30-32 (1935).

[5] Green, B. Generalising the hardy-littlewood method for primes. In *IN: PROCEEDINGS OF THE INTERNATIONAL CONGRESS OF MATHEMATICIANS* (2007), pp. 373–399.

[6] Konyagin, S. V. On a problem of littlewood. *Izv. Akad. Nauk SSSR Ser. Mat. 45*, 2 (1981), 243–265.

[7] Konyagin, S. V., and Lev, V. F. On the distribution of exponential sums. *INTEGERS (The Electronic Journal of Combinatorial Number Theory) 0*, A01 (2000).

[8] McGehee, O. C., Pigno, L., and Smith, B. Hardy's inequality and the l1 norm of exponential sums. *Annals of Mathematics 113*, 3 (1981), pp. 613–618.

[9] Myerson, G. How small can a sum of roots of unity be? *American Math. Monthly 93* (1986), 457–459.

[10] Noe, T. D. Oeis-a108380. http://oeis.org/A108380, June 2005.

[11] Tao, T. How small can a sum of a few roots of unity be http://mathoverflow.net/questions/46068/how-small-can-a-sum-of-a-few-roots-of-unity-be, November 2010.

[12] Tao, T., and Vu, V. *Additive Combinatorics*. No. 105. Cambridge Univeristy Press, 2010.