WARING'S NUMBER IN FINITE FIELDS

by

JAMES ARTHUR CIPRA

B.S., Kansas State University, 2000
M.S., Kansas State University, 2004

AN ABSTRACT OF A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas
2010

Abstract

This thesis establishes bounds (primarily upper bounds) on Waring's number in finite fields. Let p be a prime, $q = p^n$, $\mathbb{F}_q$ be the finite field in q elements, k be a positive integer with $k|(q-1)$ and $t = (q-1)/k$. Let A_k denote the set of k-th powers in $\mathbb{F}_q$ and $A'_k = A_k \cap \mathbb{F}_p$. Waring's number $\gamma(k,q)$ is the smallest positive integer s such that every element of $\mathbb{F}_q$ can be expressed as a sum of s k-th powers. For prime fields $\mathbb{F}_p$ we prove that for any positive integer r there is a constant $C(r)$ such that $\gamma(k,p) \leq C(r)k^{1/r}$ provided that $\phi(t) \geq r$. We also obtain the lower bound $\gamma(k,p) \geq \frac{(t-1)}{e}k^{1/(t-1)} - t + 1$ for t prime. For general finite fields we establish the following upper bounds whenever $\gamma(k,q)$ exists:

$$\gamma(k,q) \leq 7.3n \left\lceil \frac{(2k)^{1/n}}{|A'_k| - 1} \right\rceil \log(k),$$

$$\gamma(k,q) \leq 8n \left\lceil \frac{(k+1)^{1/n} - 1}{|A'_k| - 1} \right\rceil,$$

and

$$\gamma(k,q) \ll n(k+1)^{\frac{\log(4)}{n \log |A'_k|}} \log\log(k).$$

We also establish the following versions of the Heilbronn conjectures for general finite fields. For any $\varepsilon > 0$ there is a constant, $c(\varepsilon)$, such that if $|A'_k| \geq 4^{\frac{2}{\varepsilon n}}$, then $\gamma(k,q) \leq c(\varepsilon)k^{\varepsilon}$. Next, if $n \geq 3$ and $\gamma(k,q)$ exists, then $\gamma(k,q) \leq 10\sqrt{k+1}$. For $n = 2$, we have $\gamma(k,p^2) \leq 16\sqrt{k+1}$.

WARING'S NUMBER IN FINITE FIELDS

by

JAMES ARTHUR CIPRA

B.S., Kansas State University, 2000
M.S., Kansas State University, 2004

A DISSERTATION

submitted in partial fulfillment of the
requirements for the degree

DOCTOR OF PHILOSOPHY

Department of Mathematics
College of Arts and Sciences

KANSAS STATE UNIVERSITY
Manhattan, Kansas
2010

Approved by:

Major Professor
Todd Cochrane

Copyleft ↄ

James Arthur Cipra

2010

Abstract

This thesis establishes bounds (primarily upper bounds) on Waring's number in finite fields. Let p be a prime, $q = p^n$, $\mathbb{F}_q$ be the finite field in q elements, k be a positive integer with $k|(q-1)$ and $t = (q-1)/k$. Let A_k denote the set of k-th powers in $\mathbb{F}_q$ and $A'_k = A_k \cap \mathbb{F}_p$. Waring's number $\gamma(k,q)$ is the smallest positive integer s such that every element of $\mathbb{F}_q$ can be expressed as a sum of s k-th powers. For prime fields $\mathbb{F}_p$ we prove that for any positive integer r there is a constant $C(r)$ such that $\gamma(k,p) \leq C(r)k^{1/r}$ provided that $\phi(t) \geq r$. We also obtain the lower bound $\gamma(k,p) \geq \frac{(t-1)}{e}k^{1/(t-1)} - t + 1$ for t prime. For general finite fields we establish the following upper bounds whenever $\gamma(k,q)$ exists:

$$\gamma(k,q) \leq 7.3n \left\lceil \frac{(2k)^{1/n}}{|A'_k| - 1} \right\rceil \log(k),$$

$$\gamma(k,q) \leq 8n \left\lceil \frac{(k+1)^{1/n} - 1}{|A'_k| - 1} \right\rceil,$$

and

$$\gamma(k,q) \ll n(k+1)^{\frac{\log(4)}{n \log |A'_k|}} \log\log(k).$$

We also establish the following versions of the Heilbronn conjectures for general finite fields. For any $\varepsilon > 0$ there is a constant, $c(\varepsilon)$, such that if $|A'_k| \geq 4^{\frac{2}{\varepsilon n}}$, then $\gamma(k,q) \leq c(\varepsilon)k^{\varepsilon}$. Next, if $n \geq 3$ and $\gamma(k,q)$ exists, then $\gamma(k,q) \leq 10\sqrt{k+1}$. For $n = 2$, we have $\gamma(k,p^2) \leq 16\sqrt{k+1}$.

Table of Contents

Table of Contents vi

Acknowledgements vii

Dedication viii

1 Introduction 1
- 1.1 Waring's problem over $\mathbb{F}_p$ . . . 2
- 1.2 Statement of results for Waring's Number over $\mathbb{F}_p$ . . . 6
- 1.3 Waring's problem over $\mathbb{F}_q$ . . . 6
- 1.4 Statement of Results for Waring's Number over $\mathbb{F}_q$ . . . 7

2 Sum and Difference Sets 9

3 Exponential Sums 14
- 3.1 Exponential Sums applied to Sum Sets . . . 17

4 Waring's Number over $\mathbb{F}_p$ 20

5 Further Sum–Set Results for $\mathbb{F}_q$ 25

6 Waring's Number over $\mathbb{F}_q$ 31
- 6.1 Preliminaries . . . 31
- 6.2 Winterhof-Type Bounds for $\gamma(k, q)$. . . . 34
- 6.3 Proofs of Heilbronn-Type Results . . . 38

Bibliography 40

Acknowledgments

I would like to thank Taryn Cipra for her continuing support, Todd Cochrane without whom none of this would have been finished, Chris Pinner for finding my errors, and Bob Burckel for his grammatical corrections.

Dedication

To Freyja, because this really is a love poem. And to Tómas V. Albertsson, because he showed me some galdrabækur.

Chapter 1

Introduction

Waring's problem asks the question: Given a positive integer k does there exist a positive integer s such that every element in a given ring can be represented as a sum of at most s k-th powers? This was originally posed in 1770 for positive integers and answered in the affirmative for integers by Hilbert in 1909. The next obvious question once we know every element can be represented is: What is the least number of summands needed? While these two questions are essentially answered for the integers [28], in the finite field setting the second question is far from settled.

Let p be a prime, n be a positive integer, $q = p^n$ and $\mathbb{F}_q$ be the field of q elements. The smallest s (should it exist) such that

$$x_1^k + x_2^k + \cdots + x_s^k = \alpha \tag{1.1}$$

has a solution for all $\alpha \in \mathbb{F}_q$ is called Waring's number, denoted $\gamma(k, q)$. Similarly we define $\delta(k, q)$ to be the smallest s (should it exist) such that every element of $\mathbb{F}_q$ can be represented as sums or differences of s k-th powers, that is, such that

$$\pm x_1^k \pm x_2^k \pm \cdots \pm x_s^k = \alpha$$

is solvable for all $\alpha \in \mathbb{F}_q$. We will assume throughout that k is such that Waring's number exists for $\mathbb{F}_q$; see Theorem 6.1 below for necessary and sufficient conditions for the existence of $\gamma(k, q)$. It is also plain from this theorem that $\delta(k, q)$ exists if and only if $\gamma(k, q)$ exists.

It is easy to show that $\gamma(k,q) = \gamma(\gcd(k,q-1),q)$ since the set of k-th powers in $\mathbb{F}_q$ is the same as the set of ℓ-th powers, where $\ell = \gcd(k,q-1)$. Thus we may assume $k|(q-1)$. Let A_k denote the set of all k-th powers in $\mathbb{F}_q$, and let A_k^* denote the multiplicative subgroup of nonzero k-th powers,

$$A_k := \{x^k : x \in \mathbb{F}_q\}, \qquad A_k^* := A_k \setminus \{0\}.$$

Tornheim showed [30, Lemma 1] that the collection L of all possible sums of k-th powers in $\mathbb{F}_q$ forms a subfield of $\mathbb{F}_q$. To prove this, first note that L is obviously closed under addition and multiplication. Also, for a nonzero element $l \in L$ we have $-l = (p-1)l \in L$ and $1/l = (1/l)^k l^{k-1} \in L$. Bhaskaran showed [2, Theorem G] that this subfield is proper if and only if there is a $d|n$, $d \neq n$ such that $\frac{p^n-1}{p^d-1}|k$. The work of Tornheim and Bhaskaran can be stated more precisely as follows:

Theorem (6.1)**.** *The following are equivalent for any $q = p^n$ and $k|(q-1)$.*

(i) $\gamma(k,q)$ exists, that is, every element of $\mathbb{F}_q$ is a sum of k-th powers.

(ii) A_k is not contained in any proper subfield of $\mathbb{F}_q$, that is, A_k contains a set of n linearly independent points over $\mathbb{F}_p$.

(iii) $|A_k^*|$ does not divide $p^j - 1$ for any $j|n$, $j < n$, that is, $\frac{p^n-1}{p^j-1}$ does not divide k for any $j|n$, $j < n$.

Note that throughout the Introduction, theorems are numbered according to where they appear in the thesis together with proofs. Thus the complete proof of the preceding theorem is given in Chapter 6.

1.1 Waring's problem over $\mathbb{F}_p$

The earliest result on Waring's problem over a finite field is due to Cauchy [7] who showed that $\gamma(k,p) \leq k$ for any prime p; see Theorem 6.2. The result was discovered again by Hardy and Littlewood [19]. Clearly $\gamma(p-1,p) = p-1$ and $\gamma(\frac{p-1}{2},p) = \frac{p-1}{2}$ for any odd prime p, since $a^{p-1} = 1$ for any $a \in \mathbb{F}_p$ and $a^{\frac{p-1}{2}} = \pm 1$ for any $a \in \mathbb{F}_p$. Thus the bound $\gamma(k,p) \leq k$ is

optimal for arbitrary k. To make any improvement, we must restrict our attention to values of k not divisible by $(p-1)/2$. Under this assumption the Cauchy bound was refined by S. Chowla, Mann and Straus [9] to

$$\gamma(k,p) \leq [k/2] + 1. \tag{1.2}$$

Let t denote the number of nonzero k-th powers,

$$t := \frac{p-1}{k}.$$

Then the bound (1.2) holds provided that $t > 2$. In the work of Cipra, Cochrane and Pinner [10, Theorem 2] it is shown for $t = 3, 4$ or 6 that

$$\sqrt{2k} - 1 \leq \gamma(k,p) \leq 2\sqrt{k}. \tag{1.3}$$

Indeed, the exact value of $\gamma(k,p)$ is given in these three cases.

Heilbronn [21], in his Cal Tech Lecture Notes, made the following conjectures:

$$\text{I: For any } \varepsilon > 0, \text{ there exists a constant } t_\varepsilon \text{ such that } \gamma(k,p) \ll_\varepsilon k^\varepsilon \text{ for } t > t_\varepsilon. \tag{1.4}$$

$$\text{II: For } t > 2,\ \gamma(k,p) \ll k^{1/2}. \tag{1.5}$$

Where $f(x) \ll g(x)$ means there is a constant c such that $f(x) \leq cg(x)$ for all x, and $f(x) \ll_\varepsilon g(x)$ means given ε there is a constant $c(\varepsilon)$ such that $f(x) \leq c(\varepsilon)g(x)$ for all x.

In view of the estimate (1.3) it is plain that the exponent $\frac{1}{2}$ in the second Heilbronn conjecture is best possible for arbitrary $t > 2$.

I. Chowla [8] proved $\gamma(k,p) \ll k^{0.8771}$; Dodson [13], $\gamma(k,p) \leq k^{7/8}$, for k sufficiently large; Tietäväinen [29], $\gamma(k,p) \ll_\varepsilon k^{\frac{3}{5}+\varepsilon}$; Dodson and Tietäväinen [14],

$$\gamma(k,p) < 68(\log k)^2 k^{1/2}. \tag{1.6}$$

Bovey [6] also obtained the similar but slightly weaker bound $\gamma(k,p) \ll_\varepsilon k^{\frac{1}{2}+\varepsilon}$. The latter bounds fall just short of the second Heilbronn conjecture.

From the classical estimate of Weil [31], and Hua and Vandiver [22], on the number of solutions of (1.1) (see (3.2)) one obtains a very small value for $\gamma(k,p)$ for p sufficiently large relative to k:

$$\gamma(k,p) \le s \qquad \text{for} \quad p > (k-1)^{\frac{2s}{s-1}}. \tag{1.7}$$

In particular $\gamma(k,p) \le 2$ for $p > k^4$, $\gamma(k,p) \le 3$ for $p > k^3$ and $\gamma(k,p) \le 1 + \log(k)/\log(\varepsilon)$ for $p > (1+\varepsilon)k^2$. Note that as p approaches k^2 this bound tends to infinity. Dodson [13] obtained a similar bound

$$\gamma(k,p) \le [32 \log k] + 1 \quad \text{for} \quad p > k^2. \tag{1.8}$$

Exponential sums have proven to be a very valuable tool in the estimation of Waring's number. Let $e_p(\cdot)$ denote the additive character on $\mathbb{F}_p$,

$$e_p(\cdot) = e^{2\pi i \cdot/p}.$$

It is well known that a uniform bound on a Gauss sum of the type

$$\left| \sum_{x=1}^{p} e_p(ax^k) \right| \le \Phi, \tag{1.9}$$

for $p \nmid a$, leads immediately to the estimate

$$\gamma(k,p) \le s \quad \text{for} \quad p > \Phi^{\frac{s}{s-1}}, \tag{1.10}$$

and so we define

$$\Phi = \Phi(k) := \max_{p \nmid a} \left| \sum_{x=1}^{p} e_p(ax^k) \right|. \tag{1.11}$$

We readily obtain,

$$\gamma(k,p) \le \left\lceil \frac{\log p}{\log(p/\Phi)} \right\rceil. \tag{1.12}$$

A generalization of (1.12) to any finite field is given in Corollary 3.1; inequality (1.10) corresponding to (3.4).

From the bounds of Heath-Brown and Konyagin [20], $\Phi \ll k^{\frac{5}{8}} p^{\frac{5}{8}}$, $\Phi \ll k^{\frac{3}{8}} p^{\frac{3}{4}}$, one obtains respectively,

$$\gamma(k,p) \le s \quad \text{for} \quad p \gg k^{\frac{5s}{3s-8}}, \quad p \gg k^{\frac{3s}{2s-8}}. \tag{1.13}$$

Further estimates along these lines can be gleaned from Konyagin's [24] refinement of his joint work with Heath-Brown [20], in which he obtains a nontrivial estimate for Φ for $p > k^{\frac{4}{3}+\varepsilon}$.

Bourgain and Konyagin [5] and Bourgain, Glibichuk and Konyagin [4] introduced a new kind of upper bound for Φ: Given $\varepsilon > 0$ there exists a $\delta > 0$ such that if $k < p^{1-\varepsilon}$ then

$$\Phi(k) \leq p^{1-\delta}, \tag{1.14}$$

for p sufficiently large. It follows that

$$\gamma(k,p) \leq \frac{1}{\delta} \quad \text{for} \quad p \gg k^{1+\varepsilon}, \tag{1.15}$$

for any $\varepsilon > 0$, where δ is the value given in (1.14). Although this bound is stronger than what is asked for in the first Heilbronn conjecture, it requires $t \gg k^{\varepsilon}$ rather than t larger than a constant depending on ε.

Konyagin [23, Theorem 1] was the first to obtain a nontrivial estimate of Φ for values of k very close to p in size, obtaining

$$\Phi(k) \leq p\left(1 - \frac{c_\varepsilon}{(\log k)^{1+\varepsilon}}\right), \tag{1.16}$$

for $k \geq 2$ and $p \geq \frac{k \log k}{(\log(\log k+1))^{1-\varepsilon}}$. Although this bound is very weak, it yields the estimate

$$\gamma(k,p) \ll_\varepsilon (\log k)^{2+\varepsilon} \quad \text{for} \quad p \geq \frac{k \log k}{(\log(\log k+1))^{1-\varepsilon}}, \tag{1.17}$$

which implies, in particular, that $\gamma(k,p) \ll (\log k)^3$ for $t > \log k$. Combining this with the work of Bovey [6], Konyagin was able to establish the validity of the first Heilbronn conjecture. Improvements on (1.16) and (1.17) were made by Cochrane, Pinner and Rosenhouse [12]; see Lemma 3.4 and Lemma 3.2.

Finally we note the estimate of Garcia and Voloch [15],

$$\gamma(k,p) \leq 170\frac{k^{7/3}}{(p-1)^{4/3}} \log p, \quad \text{for} \quad p \leq k^{7/4} + 1, \tag{1.18}$$

and, for historical interest, the result of Sister M. Anne Cathleen Real [27] : For any prime $p \equiv 1 \pmod{22}$ with $p \geq 89$ we have $\gamma(11,p) = 2, 3$ or 4.

1.2 Statement of results for Waring's Number over $\mathbb{F}_p$

In chapter 4 we establish the following results for the case of prime fields.

Theorem (4.1). *Let r be a positive integer and $\phi(t)$ be the Euler ϕ-function. If $\phi(t) \geq r$ then $\gamma(k,p) \leq C(r)\ k^{1/r}$ for some constant $C(r)$.*

Letting $r = 2$ we see that there is an absolute constant $C(2)$ such that for $t > 2$, that is, $(k, p-1) < (p-1)/2$, we have

$$\gamma(k,p) \leq C(2)k^{1/2},$$

establishing the second Heilbronn conjecture. Letting $r = \phi(t)$ we get

$$\gamma(k,p) \leq C'(t)\ k^{1/\phi(t)},$$

for some constant $C'(t) = C(\phi(t))$ depending on t. We also establish the following lower bound, showing that the exponent $1/\phi(t)$ cannot be improved, at least for the case of prime t.

Theorem (4.2). *For t prime,*

$$\gamma(k,p) \geq \frac{(t-1)}{e}k^{1/(t-1)} - t + 1.$$

1.3 Waring's problem over $\mathbb{F}_q$

Let $q = p^n$ and $\mathbb{F}_q$ be the finite field in q elements. The earliest bound for $\gamma(k,q)$ is just the analogue of Cauchy's bound $\gamma(k,p) \leq k$, for prime fields.

Theorem (6.2). *If $\gamma(k,q)$ is defined then $\gamma(k,q) \leq k$.*

As noted for the case of $\mathbb{F}_p$ this bound is sharp if $|A_k^*| = 1$ or 2. For $|A_k^*| > 2$ it was established by Tietäväinen [29, Theorem 1], for odd p, and Winterhof [32, Theorem 3], for $p = 2$, that

$$\gamma(k,q) \leq [k/2] + 1. \tag{1.19}$$

Winterhof showed [33, Theorem 1] that provided $\gamma(k,q)$ exists,

$$\gamma(k,q) \leq 6.2n(2k)^{1/n}\log(k). \tag{1.20}$$

Winterhof and Woestijne [34] proved that for p and r primes with p a primitive root (mod r) we have $\gamma\left(\frac{p^{r-1}-1}{r}, p^{r-1}\right) = \frac{(r-1)(p-1)}{2}$. Thus with $k = \frac{p^{r-1}-1}{r}$ and $n = r-1$ one has the estimate,

$$\frac{n}{2}(k^{1/n}-1) \leq \gamma(k,p^n) \leq n(k+1)^{1/n}. \tag{1.21}$$

In light of inequality (1.21), we see that $nk^{1/n}$ is essentially the best possible order of magnitude for Waring's number without further restrictions. For $\mathbb{F}_p$ the usual restriction to improve upper bounds on Waring's number is to impose a lower bound on the number of k-th powers. However Winterhof and Woestijne's result indicates that such restrictions pose problems for improving a bound of the form $nk^{1/n}$ for a general finite field. Under their conditions, the number of k-th powers is equal to $r+1$, which can be made arbitrarily large for an appropriately chosen p and r.

In the general finite field setting the restriction we use is thus more subtle. Instead of placing constraints on the number of elements of A_k, we restrict the minimum size of the intersection of k-th powers with the subfield of prime order: $A_k \cap \mathbb{F}_p$. In the case of Winterhof and Woestijne, with $r \neq 2$, we have $|A_k \cap \mathbb{F}_p| = (p-1,r)+1 = 2$. Lemma 6.1 provides the first equality and conditions on p and r provide the second equality. This is the smallest such intersection since 0 and 1 are always k-th powers. For $r = 2$ we have the classic result $\gamma(\frac{p-1}{2}, p) = \frac{p-1}{2}$.

1.4 Statement of Results for Waring's Number over $\mathbb{F}_q$

Our first improvement of Winterhof's work comes from just a modest refinement of his method. Let $A'_k = A_k \cap \mathbb{F}_p$, the set of k-th powers of elements in $\mathbb{F}_q$ that belong to $\mathbb{F}_p$. Note that $|A'_k| \geq 2$, since 0 and 1 are always k-th powers.

Theorem (6.3). *If $\gamma(k,q)$ exists then we have*

$$\gamma(k,q) \le 7.3n \left\lceil \frac{(2k)^{1/n}}{(\frac{q-1}{k}, p-1)} \right\rceil \log(k) = 7.3n \left\lceil \frac{(2k)^{1/n}}{|A'_k| - 1} \right\rceil \log(k).$$

By combining Winterhof's methods with results from additive combinatorics we are able to remove the $\log k$ factor, giving the stronger result,

Theorem (6.4). *If $\gamma(k,q)$ exists, then*

$$\gamma(k,q) \le 8n \left\lceil \frac{(k+1)^{1/n} - 1}{|A'_k| - 1} \right\rceil.$$

Furthermore, if $|A'_k| \ge 3$, then

$$\gamma(k,q) \le 4n \left(\frac{(k+1)^{1/n} - 1}{|A'_k| - 1} \right) + 12n.$$

Next we show that the exponent $1/n$ can be improved if we impose extra constraints on the size of A'_k.

Theorem (6.5). *If $\gamma(k,q)$ exists, then*

$$\gamma(k,q) \ll n(k+1)^{\frac{\log(4)}{n \log |A'_k|}} \log\log(k).$$

Furthermore, if $|A'_k|^{\left\lceil \frac{\log(\frac{8}{3}(k+1)^{1/n})}{\log |A'_k|} + 8/7 \right\rceil} \le \frac{p-1}{2}$, then

$$\gamma(k,p) \ll n(k+1)^{\frac{\log 4}{n \log |A'_k|}}.$$

Finally, we address the analogues of the Heilbronn conjectures for general finite fields, proving the following theorems.

Theorem (6.6). *For any $\varepsilon > 0$, if $|A'_k| \ge 4^{\frac{2}{\varepsilon n}}$, then $\gamma(k,q) \ll_\varepsilon k^\varepsilon$.*

Theorem (6.7). *If $n \ge 3$ and $\gamma(k,q)$ exists, then $\gamma(k,q) \le 10\sqrt{k+1}$.*
For $n = 2$, we have $\gamma(k,p^2) \le 16\sqrt{k+1}$.

Theorem 6.6 establishes an analogue of the first Heilbronn conjecture (1.4), and Theorem 6.7 establishes an analogue of the second Heilbronn conjecture (1.5).

Chapter 2

Sum and Difference Sets

We begin with some notation. For any subsets A, B of a group $(G, +)$, and positive integer n we define

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

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

and

$$nA := A + A + \cdots + A, \quad (n \text{ summands}).$$

In particular, Waring's number $\gamma(k, q)$ can be defined as the minimal s such that $sA_k = \mathbb{F}_q$, where A_k is the set of k-th powers in $\mathbb{F}_q$.

For subsets A, B of a ring R and positive integers m, n we define

$$AB := \{ab : a \in A, b \in B\},$$

$$nAB := n(AB) = \left\{ \sum_{i=1}^{n} a_i b_i : a_i \in A, b_i \in B, 1 \le i \le n \right\},$$

$$A^m := \{a_1 a_2 \cdots a_m : a_i \in A, 1 \le i \le m\},$$

and consequently

$$nA^m = \left\{ \sum_{i=1}^{n} a_{i1} a_{i2} \cdots a_{im} : a_{ij} \in A, 1 \le i \le n, 1 \le j \le m \right\}.$$

The following two lemmas have proven quite useful.

Lemma 2.1. *If A and B are subsets of a finite abelian group $(G,+)$, such that $|A|+|B|>|G|$, then $A+B=G$.*

Proof. Let A and B be subsets of G with $|A|+|B|>|G|$. Let $g\in G$ and consider the set $\{g\}-A=\{g-a\ :\ a\in A\}$. Note that $|A|=|\{g\}-A|$, and so $|\{g\}-A|+|B|>|G|$. Thus, by the pigeonhole principle, $(\{g\}-A)\cap B\neq\emptyset$, that is there exists $a\in A$ and $b\in B$ such that $a+b=g$. □

Lemma 2.2 (Rusza)**.** *For A, B, and C finite subsets of an abelian group,*

$$|A||B-C|\leq|A+B||A+C|.$$

Proof. For each element $d\in B-C$ fix $b_d\in B$ and $c_d\in C$ such that $d=b_d-c_d$. Now define $f:A\times(B-C)\to(A+B)\times(A+C)$ by $f(a,d)=(a+b_d,a+c_d)$. We will now show this map is injective thus establishing the required inequality. If $f(a,d)=f(a',d')$, then

$$a+b_d=a'+b_{d'},$$
$$a+c_d=a'+c_{d'}.$$

Subtracting these equations, we have

$$b_d-c_d=b_{d'}-c_{d'},$$

or equivalently

$$d=d'.$$

Hence $a=a'$ and f is injective.

□

Applying Rusza's Lemma with $B=C$ gives the useful reformulation:

$$|A+B|\geq|A|^{1/2}|B-B|^{1/2}. \tag{2.1}$$

Lemma 2.3. *[11, 2.2] For any subset S of an abelian group and any positive integer j,*

$$|jS| \geq |S - S|^{1-\frac{1}{2^j}}.$$

The inequality is strict for $|S| > 1$.

Proof. The proof is by induction on j. The lemma is obvious for $j = 1$ and inequality (2.1) with $A = B = S$ establishes the lemma for $j = 2$.

Assume the lemma holds for $j - 1$. Applying inequality (2.1) with $A = (j-1)S$ and $B = S$ gives

$$|jS| = |(j-1)S + S| \geq |(j-1)S|^{1/2}|S - S|^{1/2}.$$

The induction hypothesis on $|(j-1)S|$ gives

$$|jS| \geq (|S - S|^{1-\frac{1}{2^{(j-1)}}})^{1/2}|S - S|^{1/2} = |S - S|^{1-\frac{1}{2^j}}.$$

□

Lemma 2.4 (Cauchy-Davenport Theorem)**.** *Let A and B be non-empty subsets of $\mathbb{F}_p$. Then*

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

Proof. We follow the proof of Alon, Nathanson, and Ruzsa [1]. Let $|A| = k$, $|B| = l$ and $|A + B| = n$. If $n \geq k + l - 1$, the assertion is true, and so we assume that $n < k + l - 1$. Our goal is to prove that $A + B = \mathbb{F}_p$ in this case, that is, $n = p$.

Form the polynomial $f \in \mathbb{F}_p[x, y]$ by

$$f(x, y) = \prod_{c \in A+B} (x + y - c) = \sum_{i+j \leq n} f_{ij} x^i y^j.$$

The sum is over i, j with $i + j \leq n$, because there are n factors in the product.

Since $\mathbb{F}_p$ is a field, there are polynomials $g_i \in \mathbb{F}_p[x]$ of degree less than k and $h_j \in \mathbb{F}_p[y]$ of degree less than l such that $g_i(x) = x^i$ for all $x \in A$ and $h_j(y) = y^j$ for all $y \in B$. Define a polynomial $p \in \mathbb{F}_p[x, y]$ by

$$p(x, y) = \sum_{i<k,\ j<l} f_{ij} x^i y^j + \sum_{i \geq k,\ j \leq n-i} f_{ij} g_i(x) y^j + \sum_{j \geq l,\ i \leq n-j} f_{ij} x^i h_j(y). \tag{2.2}$$

This polynomial coincides with $f(x,y)$ for all $(x,y) \in A \times B$, but for such (x,y) we have, however, $f(x,y) = 0$. Thus $p(x,y) = 0$ for all $(x,y) \in A \times B$. The polynomial $p(x,y)$ is of degree $< k$ in x and of degree $< l$ in y. Let $x \in A$, then $p(x,y) = \sum p_j(x)y^j$ is zero for all $y \in B$, and so all coefficients must be zero. Finally, since $p_j(x)$ is zero for all $x \in A$ and of degree less than $k = |A|$, all coefficients p_{ij} of $p(x,y) = \sum p_{ij}x^i y^j$ must be zero.

Since $n \leq k + l - 2 = (k-1) + (l-1)$ there exist nonnegative integers u, v with $u < k$, $v < l$ and $u + v = n$. We claim that the monomial $x^u y^v$ cannot appear in the second or third sum of (2.2). To appear in the second sum we must have $j = v$, and so $v \leq n - i$. But then $i \leq n - v = u < k$. To appear in the third sum we must have $i = u$, and so $u \leq n - j$. But then $j \leq n - u = v$. Therefore this monomial can only appear in the first sum, and so $f_{uv} = p_{uv} = 0$. Since $u + v = n$, it is plain from the definition of $f(x,y)$ that $f_{uv} = \binom{n}{v}$. Thus $\binom{n}{v} \equiv 0 \pmod{p}$ and we conclude that $p|n$, that is, to prove that $n = p$. □

This next lemma is a special application of the Cauchy-Davenport Theorem.

Lemma 2.5. *For any $A \subset \mathbb{F}_p$,*

$$|lA| \geq \min\{l(|A| - 1) + 1, p\}.$$

Proof. We use induction on l: For $l = 1$ the result is obvious. For $l = 2$ we use Cauchy-Davenport with $A = B$. Now assume the lemma holds for $l - 1$, namely

$$|(l-1)A| \geq \min\{(l-1)(|A| - 1) + 1, p\}. \tag{2.3}$$

Using Cauchy-Davenport (Lemma 2.4) with $B = (l-1)A$, we have

$$|lA| = |A + (l-1)A| \geq \min\{|A| + |(l-1)A| - 1, p\} \geq \min\{l(|A| - 1) + 1, p\}.$$

The last inequality is due to the induction hypothesis (2.3). □

The next few statements are useful for estimating the growth of additive sets in $\mathbb{F}_p$. The first is a sharpening of the Cauchy-Davenport Theorem for multiplicative groups from Nathanson's book, [26], and the second is a recent lemma due to Glibichuk and Konyagin [17, Lemma 5.2 & 5.3].

Lemma 2.6. *[26, Theorem 2.8] For any k and $l \in \mathbb{N}$ and $A := \{x^k | x \in \mathbb{F}_p\} \subset \mathbb{F}_p$ with $1 < \gcd(k, p-1) < \frac{p-1}{2}$,*

$$|lA| \geq \min\{(2l-1)(|A|-1)+1, p\}.$$

Lemma 2.7. *[17, Lemma 5.2 & 5.3] For $l \in \mathbb{N}$, $l \geq 2$, let $N_l = \frac{5}{24}4^l - \frac{1}{3}$. If $A \subset \mathbb{F}_p$, then*

$$|N_l A^l - N_l A^l| \geq \frac{3}{8}\min\{|A|^l, (p-1)/2\}.$$

Furthermore, if $2 \leq l \leq 1 + \frac{\log((p-1)/2)}{\log|A|}$, then

$$|N_l A^l| \geq \frac{3}{8}|A|^{l-8/7}.$$

Chapter 3

Exponential Sums

Exponential sums are just examples of character sums and so we start with a general discussion of characters over finite groups.

Definition 3.1. *Let G be a group with binary operation $+$. A function $\psi : G \to \mathbb{C} \setminus \{0\}$ is called a character on G if ψ is a group homomorphism, that is, $\psi(x+y) = \psi(x)\psi(y)$ for all $x, y \in G$. The character is called trivial if it is identically* 1.

A fundamental character sum that we make frequent use of is the following.

Lemma 3.1. *If ψ is a nontrivial character on a finite group G then $\sum_{x\in G} \psi(x) = 0$.*

Proof. Since ψ is nontrivial, there exists a $g \in G$ with $\psi(g) \neq 1$. Then

$$\sum_{x\in G} \psi(x) = \sum_{x\in G} \psi(x+g) = \psi(g) \sum_{x\in G} \psi(x),$$

and since $\psi(g) \neq 1$ we conclude that $\sum_{x\in G} \psi(x) = 0$. □

The exponential sums we make use of in our thesis are character sums on finite fields. For prime fields $\mathbb{F}_p$, the additive characters are functions of the type $e_p(\lambda x) = e^{2\pi i \lambda x/p}$ with $\lambda \in \mathbb{F}_p$ fixed, while for a more general finite field $\mathbb{F}_q$ they take the form $\Psi(\lambda x)$, where $\lambda \in \mathbb{F}_q$ and $\Psi(x) = e_p(Tr(x))$. Tr denotes the trace from $\mathbb{F}_q$ to $\mathbb{F}_p$ and is defined by $Tr(\alpha) := \alpha + \alpha^p + \cdots + \alpha^{p^{n-1}}$, for $\alpha \in \mathbb{F}_q$. For these cases, Lemma 3.1 takes the form,

Lemma 3.2. *For any prime p and integer λ,*

$$\sum_{x=1}^{p} e_p(\lambda x) = \begin{cases} 0, & \text{if } p \nmid \lambda, \\ p, & \text{if } p|\lambda. \end{cases}$$

Lemma 3.3. *For any prime power $q = p^n$ and $\lambda \in \mathbb{F}_q$,*

$$\sum_{x \in \mathbb{F}_q} \Psi(\lambda x) = \begin{cases} 0, & \text{if } \lambda \neq 0, \\ q, & \text{if } \lambda = 0. \end{cases}$$

Next we show how exponential sums can be used to count the number of solutions of an equation over a finite field. As in (1.11) we define

$$\Phi(k) = \max_{\lambda \in \mathbb{F}_q^*} \left| \sum_{x \in \mathbb{F}_q} \Psi(\lambda x^k) \right|. \tag{3.1}$$

For $\alpha \in \mathbb{F}_q$ we let $N(\alpha, s)$ denote the number of representations, counting multiplicity, of α as a sum of s k-th powers in $\mathbb{F}_q$,

$$N(\alpha, s) = |\{\mathbf{x} \in \mathbb{F}_q^s : x_1^k + x_2^k + \cdots + x_s^k = \alpha\}|.$$

Theorem 3.1. *For any $\alpha \in \mathbb{F}_q$ we have*

$$\left| N(\alpha, s) - q^{s-1} \right| \leq \left(1 - \frac{1}{q}\right) \Phi(k)^s.$$

In comparison, the classical estimate of Hua and Vandiver [22], and Weil [31] for $N(\alpha, s)$ is

$$|N(\alpha, s) - q^{s-1}| \leq (k-1)^s q^{\frac{s-1}{2}}. \tag{3.2}$$

Note that if one inserts the classical bound for a Gauss sum $\Phi(k) \leq (k-1)\sqrt{q}$ into Theorem 3.1, one obtains the slightly weaker bound $|N(\alpha, s) - q^{s-1}| \leq (k-1)^s q^{\frac{s}{2}}$. Thus, Theorem 3.1 is only of interest when the classical bound can be beaten.

Proof. By Lemma 3.3 we have

$$\begin{aligned} qN(\alpha, s) &= \sum_{\mathbf{x}\in\mathbb{F}_q^s} \sum_{\lambda\in\mathbb{F}_q} \Psi(\lambda(x_1^k + \cdots + x_s^k - \alpha)) \\ &= q^s + \sum_{\lambda\neq 0} \Psi(-\lambda\alpha) \sum_{\mathbf{x}\in\mathbb{F}_q^s} \Psi(\lambda(x_1^k + \cdots + x_s^k)) \\ &= q^s + \sum_{\lambda\neq 0} \Psi(-\lambda\alpha) \prod_{i=1}^{s} \sum_{x_i\in\mathbb{F}_q} \Psi(\lambda x_i^k). \end{aligned}$$

Thus by the triangle inequality,

$$|qN(\alpha, s) - q^s| \leq (q-1)\Phi(k)^s.$$

Dividing by q completes the proof. □

Corollary 3.1. *For any prime power q and positive integer k, we have*

$$\gamma(k, q) \leq \left\lceil \frac{\log q}{\log(q/\Phi(k))} \right\rceil.$$

Proof. By Theorem 3.1 we have $N(\alpha, s) > 0$ provided that

$$q^{s-1} > \left(1 - \frac{1}{q}\right) \Phi(k)^s, \tag{3.3}$$

that is, $(q/\Phi(k))^s > q - 1$. It suffices to have $(q/\Phi(k))^s \geq q$. Thus $\gamma(k, q) \leq s$ provided that

$$q \geq \Phi(k)^{s/(s-1)}, \tag{3.4}$$

or equivalently

$$s \geq \frac{\log q}{\log(q/\Phi(k))}. \tag{3.5}$$

□

In the Introduction we noted a number of established bounds for $\Phi(k)$ and the consequent bounds for $\gamma(k, p)$ for the case of prime fields. Many of these bounds extend to a general finite field, including the Gauss bound $\Phi(k) \leq (k-1)\sqrt{q}$ and the Bourgain, Glibichuk, Konyagin bound [4], $\Phi(k) \leq q^{1-\delta}$, provided $k < q^{1-\varepsilon}$, and q is sufficiently large (see Bourgain and

Chang [3, Theorem 1]). Here δ is a positive constant depending on ε. The latter bound gives

$$\gamma(k,q) \le \frac{1}{\delta} \quad \text{for} \quad q \gg k^{1+\varepsilon}. \tag{3.6}$$

For our purposes we need the Gauss sum estimate of Cochrane, Pinner and Rosenhouse [12, Theorem 1.1] for the case of prime fields.

Lemma 3.4. *There exists an absolute constant p_0 such that for $p \ge p_0$ and any integer a with $p \nmid a$,*

$$\left|\sum_{x=1}^{p} e_p(ax^k)\right| \le p\left(1 - \frac{1}{p^{2/\phi(t)}\log p\,(\log\log p)^5}\right), \tag{3.7}$$

where $t = (p-1)/k$ and $\phi(t)$ is the Euler ϕ-function.

One immediately deduces from Corollary 3.1 and the inequality $|\log(1-x)| > x$ for $0 < x < 1$,

Theorem 3.2. *If $p \ge p_0$ then for any positive integer k we have,*

$$\gamma(k,p) \le p^{2/\phi(t)}(\log p)^2(\log\log p)^5.$$

A bound of this general type, namely $\gamma(k,p) \le c(r)tp^{2/r}\log p$ for $\phi(t) \ge r$, also follows from Theorem 4.2 of Konyagin and Shparlinski's book [25], which gives the exponential sum bound

$$\left|\sum_{x=1}^{p} e_p(ax^k)\right| \le p\left(1 - \frac{c(r)}{tp^{2/r}}\right).$$

This bound on $\gamma(k,p)$ is better when the number of nonzero k-th powers t is very small.

3.1 Exponential Sums applied to Sum Sets

Cochrane and Pinner [11] established the following for $\mathbb{F}_p$, but their result and proof can be extended to $\mathbb{F}_q$:

Theorem 3.3. *Let A, B be subsets of $\mathbb{F}_q$ with $0 \notin A$ and m be a positive integer. If $|B|\,|A|^{1-\frac{2}{m}} \ge q$, then $mAB = \mathbb{F}_q$.*

Proof. Let $a \in \mathbb{F}_q$ and N denote the number of $2m$-tuples $(x_1, \ldots, x_m, y_1, \ldots y_m) \in \mathbb{F}_q^{2m}$ with $x_1y_1 + \cdots + x_my_m = a$. We first note that

$$\sum_{\lambda \in \mathbb{F}_q} \left| \sum_{x \in A} \sum_{y \in B} \Psi\left(\lambda(xy)\right) \right|^2 = \sum_{x_1, x_2 \in A} \sum_{y_1, y_2 \in B} \sum_{\lambda \in \mathbb{F}_q} \Psi\left(\lambda(x_1y_1 - x_2y_2)\right)$$
$$= q|\{(x_1, x_2, y_1, y_2) : x_1, x_2 \in A, y_1, y_2 \in B, x_1y_1 = x_2y_2\}| \leq q|A|^2|B|. \tag{3.8}$$

Then

$$qN = |A|^m|B|^m + \sum_{\lambda \neq 0} \sum_{x_i \in A} \sum_{y_i \in B} \Psi(\lambda(x_1y_1 + \cdots + x_my_m - a))$$
$$= |A|^m|B|^m + \sum_{\lambda \neq 0} \Psi(-\lambda a) \left(\sum_{x \in A} \sum_{y \in B} \Psi(\lambda xy) \right)^m. \tag{3.9}$$

To bound the inner sum we use the triangle inequality and then the Cauchy-Bunyakovskii-Schwarz inequality to obtain (for $\lambda \neq 0$),

$$\left| \sum_{x \in A, y \in B} \Psi(\lambda xy) \right| \leq \sum_{y \in B} |\sum_{x \in A} \Psi(\lambda xy)|$$
$$\leq |B|^{1/2} \left(\sum_{y \in B} |\sum_{x \in A} \Psi(\lambda xy)|^2 \right)^{1/2}$$
$$\leq |B|^{1/2} \left(\sum_{y \in \mathbb{F}_q} |\sum_{x \in A} \Psi(\lambda xy)|^2 \right)^{1/2}$$
$$= |B|^{1/2} \left(\sum_{x_1 \in A} \sum_{x_2 \in A} \sum_{y \in \mathbb{F}_q} \Psi(\lambda y(x_1 - x_2)) \right)^{1/2}$$
$$= |B|^{1/2} (q|A|)^{1/2},$$

the last equality following from Lemma 3.3. Therefore, by the triangle inequality, pulling off $m-2$ factors of $\left|\sum_{x \in A, y \in B} \Psi(\lambda xy)\right|$ and using (3.8), we have

$$\left| \sum_{\lambda \neq 0} \Psi(-\lambda a) \left(\sum_{x \in A} \sum_{y \in B} \Psi(\lambda xy) \right)^m \right| < (q|B||A|)^{\frac{m-2}{2}} \sum_{\lambda \in \mathbb{F}_q} \left| \sum_{x \in A} \sum_{y \in B} \Psi\left(\lambda(xy)\right) \right|^2$$
$$\leq (q|B||A|)^{\frac{m-2}{2}} q|A|^2|B| = q^{\frac{m}{2}}|A|^{\frac{m}{2}+1}|B|^{\frac{m}{2}}.$$

We conclude from (3.9) that N is positive provided that

$$|A|^m|B|^m \geq q^{\frac{m}{2}}|A|^{\frac{m}{2}+1}|B|^{\frac{m}{2}},$$

yielding the result of the theorem. □

Chapter 4

Waring's Number over $\mathbb{F}_p$

Let p be an odd prime, k be a positive integer with $k|(p-1)$, $t = (p-1)/k$, and $\phi(t)$ denote the Euler ϕ-function.

We recall the Heilbronn conjectures stated in the Introduction:

I: For any $\varepsilon > 0$, there exists a constant t_ε such that $\gamma(k,p) \ll_\varepsilon k^\varepsilon$ for $t > t_\varepsilon$.

II: For $t > 2$, $\gamma(k,p) \ll k^{1/2}$.

In this chapter we establish the validity of the second Heilbronn conjecture, proving in fact a more general result.

Theorem 4.1. *Let r be a positive integer. Then there exists a constant $C(r)$ such that if $\phi(t) \geq r$ then $\gamma(k,p) \leq C(r)k^{1/r}$.*

The second Heilbronn conjecture is implied by the case $r = 2$, since $\phi(t) \geq 2$ for $t > 2$. To prove the theorem we need the estimate of Cochrane, Pinner and Rosenhouse [12, Theorem 1.1] given in Lemma 3.2 and the following result of Bovey [6, Theorem 1].

Lemma 4.1. *For any positive integer r, there exist constants $c(r)$ and $t_0(r)$ such that*
i) $\gamma(k,p) \leq c(r)\phi(t)k^{1/r}$ for $t > t_0(r)$, and
ii) $\gamma(k,p) \leq c(r)k^{1/\phi(t)}$ for $t \leq t_0(r)$.

Proof of Theorem 4.1. Let r be a positive integer and suppose $\phi(t) \geq r$. Dodson's result

(1.8),

$$\gamma(k,p) \le [32\log k] + 1 \quad \text{for} \quad p > k^2,$$

lets us restrict our attention to $k^2 \ge p$. (Alternatively, we could use the improvement of Glibichuk [16] which states in fact that $\gamma(k,p) \le 8$ for $p > k^2$; see Corollary 5.1). For $\phi(t) \ge 2(2r+1)$ we use Lemma 3.2: For $p \ge p_0$

$$\begin{aligned}\gamma(k,p) &\le p^{\frac{2}{\phi(t)}}(\log p)^2(\log\log p)^5 \\ &\le p^{\frac{1}{2r+1}}(\log p)^2(\log\log p)^5 \ll p^{\frac{1}{2r}} \le k^{1/r}.\end{aligned}$$

For $p \le p_0$, we have trivially $\gamma(k,p) \le p-1 < p_0$. In the remaining case, $r \le \phi(t) < 2(2r+1)$, Lemma 4.1 immediately gives

$$\gamma(k,p) \le c(r)2(2r+1)k^{1/r}.$$

Taken together we see that $\gamma(k,p) \le C(r)k^{1/r}$ for some constant $C(r)$. □

In particular, taking $r = \phi(t)$, Theorem 4.1 gives the bound

$$\gamma(k,p) \le C(t)k^{1/\phi(t)},$$

for some constant $C(t)$. The exponent $1/\phi(t)$ on k is best possible in general as the following lower bound makes clear. The lower bound also shows that the best order of magnitude one can have for the constant $C(t)$ is $C(t) \sim t$. We are still a long way from obtaining such a tight upper bound.

Theorem 4.2. *For t prime,*

$$\gamma(k,p) \ge \frac{(t-1)}{e}k^{1/(t-1)} - t + 1.$$

Proof. Let R denote a primitive t-th root of 1 (mod p), so that the set A_k^* of nonzero k-th powers is just

$$A_k^* = \{1, R, R^2, \ldots, R^{t-1}\}.$$

Let sA_k denote the set of all sums of s k-th powers. Using the fact that

$$R^{t-1} = -1 - R - R^2 - \cdots - R^{t-2},$$

we have

$$\begin{aligned} sA_k &= \{x_1 + x_2R + \cdots + x_tR^{t-1} : x_i \in \mathbb{Z}, x_i \geq 0, 1 \leq i \leq t, 0 \leq x_1 + \cdots + x_t \leq s\} \\ &= \{(x_1 - x_t) + (x_2 - x_t)R + \cdots + (x_{t-1} - x_t)R^{t-2} : \\ &\qquad x_i \in \mathbb{Z},\ x_i \geq 0,\ 1 \leq i \leq t,\ 0 \leq x_1 + \cdots + x_t \leq s\} \\ &\subset \{y_1 + y_2R + \cdots + y_{t-1}R^{t-2} : \\ &\qquad y_i \in \mathbb{Z},\ 1 \leq i \leq t-1,\ \sum_{j=1}^{t-1} y_j \leq s,\ \left(\sum_{j=1}^{t-1} y_j\right) - ty_k \leq s,\ 1 \leq k \leq t-1\}. \end{aligned}$$

The latter inclusion is seen by letting $y_i = x_i - x_t$ and noting that since $x_t \geq 0$,

$$\sum_{i=1}^{t-1} y_i = \sum_{i=1}^{t-1}(x_i - x_t) \leq \sum_{i=1}^{t-1} x_i \leq s,$$

and

$$\begin{aligned} \left(\sum_{i=1}^{t-1} y_i\right) - ty_k &= \left(\sum_{i=1}^{t-1}(x_i - x_t)\right) - t(x_k - x_t) \\ &= \left(\sum_{i=1}^{t-1} x_i\right) - (t-1)x_t - t(x_k - x_t) = \left(\sum_{i=1}^{t} x_i\right) - tx_k \leq s. \end{aligned}$$

Thus the cardinality of sA_k is no more than the number of integer $(t-1)$-tuples in the pyramid

$$\mathcal{P} := \left\{\mathbf{x} \in \mathbb{R}^{t-1} : \sum_{i=1}^{t-1} x_i \leq s, \left(\sum_{i=1}^{t-1} x_i\right) - tx_k \leq s,\ 1 \leq k \leq t-1\right\}.$$

Intersecting the faces of $\mathcal{P}$, we see that $\mathcal{P}$ has vertices,

$$(s, 0, \ldots, 0), \ldots, (0, \ldots, 0, s), (-s, \ldots, -s).$$

To estimate the number of integer points in $\mathcal{P}$, we place a cube $\mathcal{B}(\mathbf{x})$ of volume 1 centered about each integer point $\mathbf{x} \in \mathcal{P}$ to obtain a new region

$$\bigcup_{\mathbf{x} \in \mathcal{P} \cap \mathbb{Z}^{t-1}} \mathcal{B}(\mathbf{x}),$$

whose volume equals the number of such points. We claim that this new region is contained in the fatter pyramid

$$\tilde{\mathcal{P}} := \left\{ \mathbf{x} \in \mathbb{R}^{t-1} : \sum_{i=1}^{t-1} x_i \le s+t-1, \left(\sum_{i=1}^{t-1} x_i \right) - t x_k \le s+t-1,\ 1 \le k \le t-1 \right\},$$

with vertices

$$(s+t-1, 0, \dots, 0), \dots, (0, \dots, 0, s+t-1), (-s-t+1, \dots, -s-t+1).$$

Indeed, let $\mathbf{x} \in \mathcal{P} \cap \mathbb{Z}^{t-1}$ and $\mathbf{y} = \mathbf{x} + \boldsymbol{\varepsilon}$ with $|\varepsilon_i| \le 1/2$, $1 \le i \le t-1$, so that $\mathbf{y}$ represents a typical element of $\tilde{\mathcal{P}}$. Then,

$$\sum_{i=1}^{t-1} y_i = \sum_{i=1}^{t-1} (x_i + \varepsilon_i) \le s + (t-1)/2 \le s+t-1,$$

and for $1 \le k \le t-1$,

$$\begin{aligned} \left(\sum_{i=1}^{t-1} y_i \right) - t y_k &= \left(\sum_{i=1}^{t-1} (x_i + \varepsilon_i) \right) - t(x_k + \varepsilon_k) = \left(\sum_{i=1}^{t-1} x_i \right) - t x_k + \left(\sum_{i \ne k}^{t-1} \varepsilon_i \right) + (1-t)\varepsilon_k \\ &\le s + \frac{1}{2}(t-2) + \frac{1}{2}(t-1) = s + t - \frac{3}{2} < s+t-1. \end{aligned}$$

Lemma 4.2. *The volume of a pyramid in $\mathbb{R}^n$ with vertices at*

$$(b, 0, \dots 0, 0), \dots, (0, 0, \dots 0, b), (-b, -b \dots, -b, -b)$$

is $b^n(n+1)/n!$.

Proof. The volume is just $\frac{1}{n}BH$ where the B is the area of the base $\sum_{i=1}^{n} x_i = b$, $x_i \ge 0$, $1 \le i \le n$, and H is the distance from the base to the vertex $(-b, -b, \dots, -b)$. Plainly

$$H = d((-b, \dots, -b), (b/n, \dots, b/n)) = b\left(1 + \tfrac{1}{n}\right)\sqrt{n},$$

where $d(\mathbf{P}, \mathbf{Q})$ denotes the Euclidean distance. To calculate the base area, we express the base as the surface

$$x_n = b - x_1 - x_2 - \cdots - x_{n-1}$$

over the region $\mathcal{R}$ with $x_i \geq 0$, $\sum_{i=1}^{n-1} x_i \leq b$. The surface area is then given by

$$\int \cdots \int_{\mathcal{R}} \sqrt{1 + \left(\frac{\partial x_n}{\partial x_1}\right)^2 + \cdots + \left(\frac{\partial x_n}{\partial x_{n-1}}\right)^2} dx_1 ... dx_{n-1} = \sqrt{n} \int \cdots \int_{\mathcal{R}} 1 dx_1 ... dx_{n-1}$$
$$= \frac{\sqrt{n} b^{n-1}}{(n-1)!}.$$

Thus the volume is $\frac{1}{n} \cdot b(1 + \frac{1}{n})\sqrt{n} \cdot \sqrt{n} b^{n-1}/(n-1)! = (n+1)b^n/n!$. □

By the lemma, the volume of $\tilde{P}$ is $(s+t-1)^{t-1}t/(t-1)!$, and consequently this is an upper bound on $|sA_k|$. Therefore if $|sA_k| = p$, that is, if every point is a sum of s k-th powers, we must have

$$(s+t-1)^{t-1}t/(t-1)! \geq p,$$

and so, using $p/t > k$,

$$s \geq \left(\frac{p(t-1)!}{t}\right)^{1/(t-1)} - t + 1 > (k(t-1)!)^{1/(t-1)} - t + 1 > k^{1/(t-1)} \frac{t-1}{e} - t + 1,$$

the latter inequality using $n! > (n/e)^n$. □

Chapter 5

Further Sum–Set Results for $\mathbb{F}_q$

In this chapter we will extend some results of Glibichuk [16] from $\mathbb{F}_p$ to a general finite field $\mathbb{F}_q$. This was also done independently by Glibichuk and Rudnev in [18], although they do not state Corollary 5.1 below. To state our main theorem we need the following definition.

Definition 5.1. *A subset $A \subset \mathbb{F}_q$ is said to be symmetric if $A = -A$, where $-A = \{-a : a \in A\}$, and antisymmetric if $A \cap (-A) = \emptyset$.*

Theorem 5.1. *[16, Theorem 1&2] If $A \subset \mathbb{F}_q$ and $B \subset \mathbb{F}_q$ with B symmetric or antisymmetric and $|A||B| > q$, then $8AB = \mathbb{F}_q$.*

This result should be compared with Theorem 3.3 which obtained $mAB = \mathbb{F}_q$ provided that A, B are subsets of $\mathbb{F}_q$ with $0 \notin A$ and $|B|\,|A|^{1-\frac{2}{m}} \geq q$. The latter result is thus obsolete for values of $m \geq 8$. An immediate application of the theorem yields the following:

Corollary 5.1. *For any positive integer k with $k \leq \sqrt{q}$ we have $\gamma(k, q) \leq 8$.*

Proof. The statement is trivial for $q \leq 5$, and so we may assume that $q \geq 6$. We apply Theorem 5.1 with $A = A_k$, $B = A_k^*$ where A_k is the set of k-th powers in $\mathbb{F}_q$. Note that A_k^* is symmetric or antisymmetric depending on whether -1 is a k-th power or not. If $k \leq \sqrt{q}$, then $|A_k||A_k^*| > q$ provided that $\left(\frac{q-1}{\sqrt{q}} + 1\right)\left(\frac{q-1}{\sqrt{q}}\right) > q$, that is, $q^{3/2} > 2q + \sqrt{q} - 1$. The latter holds for $q \geq 6$. Thus by Theorem 5.1, $8A_kA_k^* = \mathbb{F}_q$. But, $A_kA_k^* = A_k$ so we have $8A_k = \mathbb{F}_q$. □

We note that the hypothesis $k \leq \sqrt{q}$ is tight. Indeed, if k exceeds $\sqrt{q}$ then $\gamma(k,q)$ may not exist. For instance if $q = p^2$ and $k = p+1$, then every k-th power is in $\mathbb{F}_p$ (since $(x^{p+1})^{p-1} = 1$ for $x \in \mathbb{F}_q$), and so any sum of k-th powers is in $\mathbb{F}_p$. On the other hand, if $k = p-1$ then the corollary asserts that every element of $\mathbb{F}_q$ is a sum of at most 8 $(p-1)$-th powers.

The proof of Theorem 5.1 uses methods of additive combinatorics. We start with the following definition.

Definition 5.2. *(i) For any $A \subset \mathbb{F}_q$ and $B \subset \mathbb{F}_q$, set*

$$I(A;B) := \{(b_1 - b_2)a_1 + (a_2 - a_3)b_3 : a_1, a_2, a_3 \in A,\ b_1, b_2, b_3 \in B\}.$$

(ii) For any subset $A \subset \mathbb{F}_q$, set

$$I(A) = I(A;A) = \{(a_1 - a_2)a_3 + (a_4 - a_5)a_6 : a_1, a_2, a_3, a_4, a_5, a_6 \in A\}.$$

The next 3 lemmas are extensions of results in [16] from prime fields to general finite fields.

Lemma 5.1. *[16, Lemma 1] Suppose that A, B are nonempty subsets of $\mathbb{F}_q$ and G is a nonempty subset of $\mathbb{F}_q^*$. Then there exists a $\xi \in G$ such that*

$$|A + \{\xi\}B| \geq \frac{|A||B||G|}{(|A|-1)(|B|-1)+|G|},$$

and

$$|A - \{\xi\}B| \geq \frac{|A||B||G|}{(|A|-1)(|B|-1)+|G|}.$$

We note that in the statement of [16, Lemma 1], for $\mathbb{F}_p$, the value $(|A|-1)(|B|-1)$ in Lemma 5.1 is replaced by the larger value $|A||B|$. The weaker bound this leads to would suffice for our purposes below for the case of odd q, but for $q = 2^n$ we need the stronger bound in our lemma.

Proof. For any $\xi \in G$ and $s \in \mathbb{F}_q$, define the functions $f_\xi^+(s)$ and $f_\xi^-(s)$ as follows:

$$f_\xi^+(s) := |\{(a,b) \in A \times B : a + b\xi = s\}|,$$

$$f_\xi^-(s) := |\{(a,b) \in A \times B : a - b\xi = s\}|.$$

Then

$$\begin{aligned}\sum_{s\in\mathbb{F}_q}(f_\xi^+(s))^2 &= |\{(a_1,b_1,a_2,b_2) \in A \times B \times A \times B : a_1 + b_1\xi = a_2 + b_2\xi\}| \\ &= |A||B| + |\{(a_1,b_1,a_2,b_2) \in A \times B \times A \times B : a_1 \neq a_2, a_1 + b_1\xi = a_2 + b_2\xi\},\end{aligned}$$

$$\begin{aligned}\sum_{s\in\mathbb{F}_q}(f_\xi^-(s))^2 &= |\{(a_1,b_1,a_2,b_2) \in A \times B \times A \times B : a_1 - b_1\xi = a_2 - b_2\xi\}| \\ &= |A||B| + |\{(a_1,b_1,a_2,b_2) \in A \times B \times A \times B : a_1 \neq a_2, a_1 - b_1\xi = a_2 - b_2\xi\}|.\end{aligned}$$

Hence,

$$\sum_{s\in\mathbb{F}_q}(f_\xi^+(s))^2 = \sum_{s\in\mathbb{F}_q}(f_\xi^-(s))^2.$$

Note that for all $a_1, a_2 \in A$ and $b_1, b_2 \in B$ such that $a_1 \neq a_2$, there exists at most one ξ satisfying $a_1 + b_1\xi = a_2 + b_2\xi$. Then the number N of 5-tuples $(a_1, a_2, b_1, b_2, \xi)$ with $a_i \in A$, $b_i \in B$ and $\xi \in G$ satisfies

$$N = \sum_{\xi\in G}\sum_{s\in\mathbb{F}_q}(f_\xi^-(s))^2 \leq |A||B||G| + |A|(|A|-1)|B|(|B|-1).$$

In particular, there exists a $\xi \in G$ such that

$$\sum_{s\in\mathbb{F}_q}(f_\xi^-(s))^2 < |A||B| + \frac{|A|(|A|-1)|B|(|B|-1)}{|G|}.$$

For this value of ξ, we have $f_\xi^+(s) = 0$ for $s \notin A + \{\xi\}B$. Thus, the Cauchy-Bunyakovskii-Schwarz inequality yields

$$\begin{aligned}(|A||B|)^2 = \left(\sum_{s\in\mathbb{F}_q} f_\xi^+(s)\right)^2 &\leq |A + \{\xi\}B| \sum_{s\in\mathbb{F}_q}(f_\xi^+(s))^2 \\ &\leq |A + \{\xi\}B| \left(|A||B| + \frac{|A|(|A|-1)|B|(|B|-1)}{|G|}\right),\end{aligned}$$

and

$$(|A||B|)^2 = \left(\sum_{s\in\mathbb{F}_q} f_\xi^-(s)\right)^2 \le |A-\{\xi\}B| \sum_{s\in\mathbb{F}_q} (f_\xi^-(s))^2$$
$$\le |A-\{\xi\}B| \left(|A||B| + \frac{|A|(|A|-1)|B|(|B|-1)}{|G|}\right).$$

Simple algebra gives the desired result. □

Lemma 5.2. *[16, Lemma 2] Suppose that A, B are nonempty subsets of $\mathbb{F}_q$ such that $|A||B| \ge q$. Then there exists $\xi \in \mathbb{F}_q$ such that*

$$|A+\{\xi\}B| > \frac{q}{2},$$
$$|A-\{\xi\}B| > \frac{q}{2}.$$

Proof. Letting $G = \mathbb{F}_q^*$ in Lemma 5.1 we see that there exists a $\xi \in G$ such that

$$|A+\{\xi\}B| \ge \frac{|A||B|(q-1)}{(|A|-1)(|B|-1)+(q-1)},$$

and

$$|A-\{\xi\}B| \ge \frac{|A||B|(q-1)}{(|A|-1)(|B|-1)+(q-1)}.$$

The latter quantity is greater than $q/2$ provided that

$$|A||B|(q-1) > \frac{q}{2}\left[(|A|-1)(|B|-1)+(q-1)\right],$$

that is, provided that

$$|A||B|(q/2-1) > \frac{q}{2}(q-|A|-|B|).$$

Inserting the hypothesized inequality $|A||B| \ge q$ into the left-hand side, we see that it suffices to have

$$(|A|+|B|)/2 > 1,$$

and this inequality is trivial since $|A||B| \ge 2$.

□

Lemma 5.3. *[16, Lemma 3] Suppose $A, B \subset \mathbb{F}_q$. For any $\xi \in \mathbb{F}_q$ with $|A+\{\xi\}B| < |A||B|$, we have $|I(A;B)| \geq |A+\{\xi\}B|$.*

Proof. This is obvious for $\xi = 0$, so assume $\xi \neq 0$. The hypothesis $|A + \{\xi\}B| < |A||B|$ implies there are $a_1, a_2 \in A$ and $b_1, b_2 \in B$ with $(a_1, b_1) \neq (a_2, b_2)$ such that $a_1+b_1\xi = a_2+b_2\xi$, by the pigeon-hole principle. Since $\xi \neq 0$ we have $b_1 \neq b_2$, else $(a_1, b_1) = (a_2, b_2)$. Set $S := \{b_1-b_2\}(A+\{\xi\}B)$. Note that $|S| = |A+\{\xi\}B|$. Given $s \in S$, there is an $a \in A$ and a $b \in B$ with $s = (b_1-b_2)(a+b\xi)$. Since $(b_1-b_2) = \frac{a_2-a_1}{\xi}$, we have $s = (b_1-b_2)a+(a_2-a_1)b \in I(A;B)$. Hence $S \subset I(A;B)$ and $|I(A;B)| \geq |S| = |A + \{\xi\}B|$. □

The main ingredient in the proof of Theorem 5.1 for symmetric B is the following estimate first proven by Bourgain, Glibichuk and Konyagin [4] for $I(A)$ in prime fields $\mathbb{F}_p$. It is an easy consequence of the preceding three lemmas.

Theorem 5.2. *Let A and B be subsets of $\mathbb{F}_q$ such that $|A||B| > q$. Then $|I(A;B)| > q/2$.*

Proof. Lemma 5.2 supplies $\xi \in \mathbb{F}_q^*$ such that $|A + \{\xi\}B| > q/2$ and by assumption

$$|A + \{\xi\}B| \leq q < |A||B|$$

. Hence by Lemma 5.3, we have

$$|I(A;B)| \geq |A + \{\xi\}B| > q/2.$$

□

Proof of Theorem 5.1. Let $A \subset \mathbb{F}_q$ and $B \subset \mathbb{F}_q$ with B symmetric or antisymmetric and $|A||B| > q$.

Case 1. Assume B is antisymmetric. Since $|A||B| > q$, Lemma 5.2 supplies $\xi \in \mathbb{F}_q^*$ such that $|A + \{\xi\}B| > q/2$ and $|A - \{\xi\}B| > q/2$. In particular, by the pigeon-hole principle, $(A + \{\xi\}B) \cap (-A - \{\xi\}B) \neq \emptyset$. Hence there exist $a_1, a_2 \in A$ and $b_1, b_2 \in B$ such that $(a_1 + b_1\xi) = -(a_2 + b_2\xi)$ or equivalently $\xi = -\frac{a_1+a_2}{b_1+b_2}$. (Note, the denominator is nonzero since B is antisymmetric.)

The second inequality $|A - \{\xi\}B| > q/2$ yields

$$\begin{aligned} q/2 < |A - \{\xi\}B| &= \left| \left\{ a_3 + \left(\frac{a_1 + a_2}{b_1 + b_2} \right) b_3 : a_3 \in A, b_3 \in B \right\} \right| \\ &= |\{a_3(b_1 + b_2) + b_3(a_1 + a_2) : a_3 \in A, b_3 \in B\}|. \end{aligned}$$

Thus $|4AB| > q/2$ and by Lemma 2.1, $8AB = \mathbb{F}_q$.

Case 2. Assume B is symmetric. Theorem 5.2 establishes $|I(A;B)| > q/2$. Since B is symmetric, $I(A;B) \subset 4AB$ and applying Lemma 2.1 gives $8AB = \mathbb{F}_q$. □

Chapter 6

Waring's Number over $\mathbb{F}_q$

In this chapter we obtain new bounds on $\gamma(k,q)$ for arbitrary finite fields $\mathbb{F}_q$. In particular, we show that if $\gamma(k,q)$ exists, then

$$\gamma(k,q) < 7.3n \left\lceil \frac{(2k)^{1/n}}{|A_k'|-1} \right\rceil \log k,$$

where $A_k' = A_k \cap \mathbb{F}_q$. We also get

$$\gamma(k,q) \leq 8n \left\lceil \frac{(k+1)^{1/n}-1}{|A_k'|-1} \right\rceil,$$

and

$$\gamma(k,q) \ll n(k+1)^{\frac{\log(4)}{n\log|A_k'|}} \log\log k.$$

Finally we establish the second Heilbronn conjecture in Theorem 6.7 and prove an analogue of the first Heilbronn conjecture in Theorem 6.6.

6.1 Preliminaries

We begin with proofs of Theorems 6.1 and 6.2 stated in the Introduction. We recall that A_k denotes the set of k-th powers in $\mathbb{F}_q$ and A_k^* the set of nonzero k-th powers.

Theorem 6.1. *The following are equivalent for any $q = p^n$ and $k|(q-1)$.*

(i) $\gamma(k,q)$ exists, that is, every element of $\mathbb{F}_q$ is a sum of k-th powers.

(ii) A_k is not contained in any proper subfield of $\mathbb{F}_q$, that is, A_k contains a set of n linearly independent points over $\mathbb{F}_p$.

(iii) $|A_k^*|$ *does not divide* $p^j - 1$ *for any* $j|n$, $j < n$, *that is,* $\frac{p^n-1}{p^j-1}$ *does not divide* k *for any* $j|n$, $j < n$.

Proof. (i) implies (ii): Suppose that $\gamma(k, q)$ exists. Then A_k cannot be contained in a proper subfield of $\mathbb{F}_q$ else every sum of k-th powers is contained in that subfield.

(ii) implies (i): Let $\{x_1, \ldots, x_n\}$ be a set of n linearly independent k-th powers. Then since every element of $\mathbb{F}_q$ is of the form $k_1x_1 + \cdots + k_nx_n$ with the k_i nonnegative integers, we see that every element is a sum of k-th powers.

(ii) implies (iii): If $|A_k^*|$ divides $(p^j - 1)$ for some $j|n$ with $j < n$, then A_k^* is contained in the cyclic subgroup of $\mathbb{F}_q^*$ of order $p^j - 1$, which is $\mathbb{F}_{p^j}^*$. Thus, every k-th power is contained in the proper subfield $\mathbb{F}_{p^j}$.

(iii) implies (ii): If A_k is contained in a proper subfield $\mathbb{F}_{p^j}$, then A_k^* is a subgroup of $\mathbb{F}_{p^j}^*$ and so $|A_k^*|$ divides $p^j - 1$. □

Theorem 6.2. *For any* k, q *such that* $\gamma(k, q)$ *exists, we have* $\gamma(k, q) \leq k$.

Bounds of this type hold even without the assumption $k|(q-1)$, since $\gamma(k, q) = \gamma((k, q-1), q)$ and $(k, q-1) \leq k$.

Proof. Let $k|(q-1)$ and A_k be the set of k-th powers in $\mathbb{F}_q$. For any positive integer n, nA_k is closed under multiplication by elements in A_k^* and so we can write

$$nA_k = \{0\} \cup A_k^*\{x_1\} \cdots \cup A_k^*\{x_l\},$$

for some distinct cosets $A_k^*\{x_i\}$ of A_k^*, $1 \leq i \leq l$. Thus, if $nA_k \neq \mathbb{F}_q$, then

$$|(n+1)A_k| \geq |nA_k| + |A_k|.$$

By induction we get a Cauchy-Davenport type inequality,

$$|nA_k| \geq \min\{q, 1 + n|A_k^*|\}, \tag{6.1}$$

and see that $nA_k = \mathbb{F}_q$ provided that $1 + n|A_k^*| \geq q$, that is, $n \geq \frac{q-1}{|A_k^*|} = k$. Thus

$$\gamma(k, q) \leq k.$$

□

Next we recall that A'_k denotes the set of k-th powers of elements in $\mathbb{F}_q$ that belong to $\mathbb{F}_p$,

$$A'_k = A_k \cap \mathbb{F}_p.$$

Lemma 6.1. *For any q and $k|(q-1)$, $|A'_k| = (p-1, \frac{q-1}{k}) + 1$.*

Proof. The set of nonzero elements of A'_k is just the intersection of the subgroups A^*_k and $\mathbb{F}^*_p$ of $\mathbb{F}^*_q$. Since the latter group is cyclic, the order of the intersection is just

$$(|A^*_k|, p-1) = ((q-1)/k, p-1).$$

□

The next lemma, generalizing Cochrane and Pinner's result [11, Theorem 4.1c] from $\mathbb{F}_p$ to $\mathbb{F}_q$, deals with the relationship between $\gamma(k,q)$ and $\delta(k,q)$, where (as before) $\delta(k,q)$ is the minimal s such that every element of $\mathbb{F}_q$ can be written in the manner $\pm x_1^k \pm \cdots \pm x_s^k$. One trivially has $\delta(k,q) \leq \gamma(k,q)$. It would be nice if the $\log\log q$ factor in the lemma could be replaced with an absolute constant, but it is an open question whether this is possible.

Lemma 6.2. *For any k, q such that $\gamma(k,q)$ is defined we have*

$$\gamma(k,q) \leq 2\lceil \log_2 \log_2 q \rceil \delta(k,q).$$

Proof. We start by noting that by definition of $\delta(k,q)$, $\delta(k,q)A_k - \delta(k,q)A_k = \mathbb{F}_q$. Let $j \geq \log_2 \log_2 q$ be an integer. By Lemma 2.3 with $S = \delta(k,q)A_k$, we have

$$|j\delta(k,q)A_k| > |\delta(k,q)A_k - \delta(k,q)A_k|^{1-\frac{1}{2^j}} = q^{1-\frac{1}{2^j}} \geq q/2.$$

Hence by Lemma 2.1, $2j\delta(k,q)A_k = \mathbb{F}_q$, that is, $\gamma(k,q) \leq 2j\delta(k,q)$. □

In our application of Lemma 6.2, we will actually use the less precise bound

$$\gamma(k,q) \ll (\log\log q)\delta(k,q).$$

6.2 Winterhof-Type Bounds for $\gamma(k,q)$.

Winterhof showed [33, Theorem 1] that provided $\gamma(k,q)$ exists,

$$\gamma(k,q) \leq 6.2n(2k)^{1/n}\log k. \tag{6.2}$$

The key lemma in his proof is the following result.

Lemma 6.3. *[33, Lemma 4]. Suppose $k|(q-1)$. If $|sA_k| \geq 2k$, then*

$$\gamma(k,q) \leq s\left(1+\lfloor(2\log q/\log 2\rfloor\right).$$

Our first theorem is a mild improvement of Winterhof's result (6.2). The proof follows his original proof quite closely.

Theorem 6.3. *If $\gamma(k,q)$ exists, then we have*

$$\gamma(k,p^n) \leq 7.3n\left\lceil\frac{(2k)^{1/n}}{(\frac{q-1}{k},p-1)}\right\rceil\log k = 7.3n\left\lceil\frac{(2k)^{1/n}}{|A_k'|-1}\right\rceil\log k.$$

Proof. The result is trivial for $k=q-1$, so we assume $k<q/2$. If $k<\sqrt{q}$, then Corollary 5.1 gives the result and so we may assume $k\geq\sqrt{q}$. Since $\gamma(k,q)$ exists, there is a basis $\{b_1,\ldots,b_n\}\subset A_k$ of $\mathbb{F}_q$ over $\mathbb{F}_p$. For a given positive integer r, examine elements of the type $(x_{1,1}+\cdots+x_{1,r})b_1+\cdots+(x_{n,1}+\cdots+x_{n,r})b_n$, where the $x_{i,j}$ are k-th powers of elements in $\mathbb{F}_q$ lying in $\mathbb{F}_p$. These are sums of at most rn k-th powers with each coefficient $x_{i,1}+\cdots+x_{i,r}$ representing at least $\min\{p,r(\frac{q-1}{k},p-1)\}$ distinct elements in $\mathbb{F}_p$, by Lemma 6.1 and the application of the Cauchy-Davenport Theorem, Lemma 2.5. Taking $r\geq\frac{(2k)^{1/n}}{(\frac{q-1}{k},p-1)}$ guarantees that each coefficient represents at least $(2k)^{1/n}$ elements in $\mathbb{F}_p$ and thus that such sums represent at least $2k$ elements in $\mathbb{F}_q$. Using Lemma 6.3 and the assumption $k\geq\sqrt{q}$,

we see that

$$\begin{aligned}\gamma(k,q) &\le nr\left(1+\frac{2\log q}{\log 2}\right) \le n\left\lceil\frac{(2k)^{1/n}}{(\frac{q-1}{k},p-1)}\right\rceil\left(1+\frac{2\log q}{\log 2}\right)\\ &\le n\left\lceil\frac{(2k)^{1/n}}{(\frac{q-1}{k},p-1)}\right\rceil\left(1+\frac{4\log k}{\log 2}\right) \le n\left\lceil\frac{(2k)^{1/n}}{(\frac{q-1}{k},p-1)}\right\rceil\left(\frac{1}{\log k}+\frac{4}{\log 2}\right)\log k\\ &\le \left(\frac{5}{\log 2}\right) n\left\lceil\frac{(2k)^{1/n}}{(\frac{q-1}{k},p-1)}\right\rceil\log k \le 7.3n\left\lceil\frac{(2k)^{1/n}}{(\frac{q-1}{k},p-1)}\right\rceil\log k.\end{aligned}$$

□

Winterhof and Woestijne [34] prove that for p and r primes with p a primitive root (mod r) we have $\gamma\left(\frac{p^{r-1}-1}{r}, p^{r-1}\right) = \frac{(r-1)(p-1)}{2}$. Thus with $k = \frac{p^{r-1}-1}{r}$ and $n = r-1$ one has the estimate,

$$\frac{n}{2}(k^{1/n}-1) \le \gamma(k,p^n) \le n(k+1)^{1/n}. \tag{6.3}$$

In light of inequality (6.3), we see that $nk^{1/n}$ is essentially the best possible order of magnitude for Waring's number without further restrictions. By combining Winterhof's methods with results from additive combinatorics we show that the $\log k$ factor in Winterhof's bound (6.2) can be dropped.

Theorem 6.4. *If $\gamma(k,q)$ exists, then*

$$\gamma(k,q) \le 8n\left\lceil\frac{(k+1)^{1/n}-1}{|A'_k|-1}\right\rceil.$$

Furthermore, if $|A'_k| \ge 3$, then

$$\gamma(k,q) \le 4n\left(\frac{(k+1)^{1/n}-1}{|A'_k|-1}\right)+12n.$$

(We note that A'_k always contains 0 and 1, so $|A'_k| \ge 2$.)

The result from additive combinatorics that we need is the following:

Lemma 6.4. *If $\gamma(k,q)$ exists and $|sA_k| \ge k+1$ for some $s \in \mathbb{N}$, then $\gamma(k,q) \le 8s$.*

Proof. If $k = q-1$, the result is trivial, so we assume $k < q-1$. We use Theorem 5.1, with $A = sA_k$ and $B = A_k^*$. Recall that A_k^* is symmetric or antisymmetric depending on whether -1 is a k-th power or not. Also note:

$$(sA_k)A_k^* = sA_k$$

and

$$|A_k^*||sA_k| \geq \frac{q-1}{k}(k+1) = q-1+\frac{q-1}{k} > q.$$

Thus by Theorem 5.1, $8sA_k = \mathbb{F}_q$, that is, $\gamma(k,q) \leq 8s$. □

Proof of Theorem 6.4. The proof again follows the line of argument in Winterhof's original proof [33, Theorem 1]. Namely, we look at the growth of sum sets formed from linear combinations of a basis of k-th powers and carefully chosen coefficient sets. Let $\{b_1, b_2, ..., b_n\}$ be a basis of $\mathbb{F}_q$ over $\mathbb{F}_p$ consisting of k-th powers of elements of $\mathbb{F}_q$. For any positive integer l the set

$$B_l := \{a_1b_1 + \cdots + a_nb_n | a_j \in lA_k'\}$$

is a subset of nlA_k with $|B_l| \geq |lA_k'|^n$ (since the coefficients a_i belong to $\mathbb{F}_p$,) and so

$$|nlA_k| \geq |lA_k'|^n. \tag{6.4}$$

If we take $l \geq \frac{(k+1)^{1/n}-1}{|A_k'|-1}$, then by the Cauchy-Davenport theorem, Lemma 2.5,

$$|lA_k'| \geq \min\{l(|A_k'|-1)+1, p\} \geq \min\left\{(k+1)^{1/n}, p\right\}.$$

If $|lA_k'| = p$ then $B_l = \mathbb{F}_q$, that is, $\gamma(k,q) \leq nl$. If $|lA_k'| \geq (k+1)^{1/n}$ then by (6.4) $|nlA_k| \geq k+1$ and Lemma 6.4 yields the first result of the theorem.

Next, if we take $l \geq \frac{(k+1)^{1/n}-1}{2(|A_k'|-1)} + \frac{1}{2}$ then by Lemma 2.6,

$$|lA_k'| \geq \min\left\{(k+1)^{1/n}, p\right\}.$$

Again, if $|lA_k'| = p$, then $\gamma(k,q) \leq nl$; while if $|lA_k'| \geq (k+1)^{1/n}$, then $|nlA_k| \geq k+1$ and Lemma 6.4 yields the second result of the theorem.

□

Under more stringent conditions on the number of k-th powers falling in the base field we can improve the exponent $1/n$ at the cost of increasing the constant.

Theorem 6.5. *If $\gamma(k,q)$ exists, then*

$$\gamma(k,q) \ll n(k+1)^{\frac{\log 4}{n \log |A_k'|}} \log\log k.$$

Furthermore, if $|A_k'|^{\left\lceil \frac{\log(\frac{8}{3}(k+1)^{1/n})}{\log |A_k'|} + 8/7 \right\rceil} \leq \frac{p-1}{2}$, then

$$\gamma(k,p) \ll n(k+1)^{\frac{\log 4}{n \log |A_k'|}}.$$

Proof. Corollary 5.1 implies the theorem is trivial for $k \leq \sqrt{q}$. Thus, we assume $k > \sqrt{q}$, and for convenience let $l = \left\lceil \frac{\log(\frac{8}{3}(k+1)^{1/n})}{\log |A_k'|} + 8/7 \right\rceil$.

Case 1: If $|A_k'|^l \geq \frac{p-1}{2}$, then we use the first part of Lemma 2.7 with $A = A_k'$ and noting that $(A_k')^l = A_k'$, to establish $|N_l A_k' - N_l A_k'| \geq \frac{3}{8} \min\{|A_k'|^l, (p-1)/2\} \geq \frac{3}{16}(p-1)$. By Lemma 2.5,

$$\begin{aligned} |48(N_l A_k' - N_l A_k')| &\geq \min\{48(|N_l A_k' - N_l A_k'| - 1) + 1, p\} \\ &\geq \min\left\{48(\frac{3}{16}(p-1) - 1) + 1, p\right\} \geq 9p - 56 \geq p, \end{aligned}$$

for $p \geq 7$. If $p < 7$ we use the facts that $|A_k'| \geq 2 \geq \frac{p-1}{2}$ and

$$p \geq |48(N_l A_k' - N_l A_k')| \geq |4A_k'| = p$$

to establish $|48(N_l A_k' - N_l A_k')| = p$. We now have an upper bound on $\delta(k,q)$ and hence on $\gamma(k,q)$ via Lemma 6.2.

$$\gamma(k,q) \ll (\log\log q)\delta(k,q) \ll (\log\log q) n N_l \ll n(k+1)^{\frac{\log 4}{n \log |A_k'|}} \log\log k.$$

Case 2: If $|A_k'|^l \leq \frac{p-1}{2}$, then we use the second part of Lemma 2.7 with the result that

$|N_l A'_k| \geq (k+1)^{1/n}$ and so $|nN_l A_k| \geq k+1$. Hence by Lemma 6.4

$$\begin{aligned}\gamma(k,q) &\leq 8nN_l = 8n\left(\frac{5}{24}4^l - \frac{1}{3}\right) = 8n\left(\frac{5}{24}4^{\left\lceil \frac{\log(\frac{8}{3}(k+1)^{1/n})}{\log|A'_k|}+8/7\right\rceil} - \frac{1}{3}\right)\\ &\leq 8n\left(\frac{5}{24}4^{\frac{\log(\frac{8}{3}(k+1)^{1/n})}{\log|A'_k|}+15/7} - \frac{1}{3}\right) = 8n\left(\frac{5}{3}2^{\frac{9}{7}}4^{\frac{\log\frac{8}{3}}{\log|A'_k|}}4^{\frac{\log(k+1)}{n\log|A'_k|}} - 1/3\right)\\ &= 8n\left(\frac{5}{3}2^{\frac{9}{7}}4^{\frac{\log\frac{8}{3}}{\log|A'_k|}}(k+1)^{\frac{\log 4}{n\log|A'_k|}} - 1/3\right) \ll n(k+1)^{\frac{\log 4}{n\log|A'_k|}}.\end{aligned}$$

Alone, this case gives the second part of the theorem. Combined with case 1, we have the first part of the theorem. □

6.3 Proofs of Heilbronn-Type Results

In the case when q is prime, Heilbronn conjectured in [21] (and Konyagin proved in [23]) that for any $\varepsilon > 0$, $\gamma(k,p) \ll_\varepsilon k^\varepsilon$ if $|A_k| > c(\varepsilon)$. It is interesting to note that in this case $A_k = A'_k$. By placing the size condition on A'_k instead of A_k, we extend Heilbronn's conjecture to a general finite field, and obtain an explicit value for $c(\varepsilon)$.

Theorem 6.6. *For any $\varepsilon > 0$, if $|A'_k| \geq 4^{\frac{2}{\varepsilon n}}$, then $\gamma(k,q) \ll_\varepsilon k^\varepsilon$.*

Proof. Again, we first note that Corollary 5.1 lets us restrict our attention to $k > \sqrt{q}$, or equivalently $n < \frac{2\log(k)}{\log p}$. We make the further assumption: $|A'_k| \geq 4^{2/n\varepsilon}$. Using Theorem 6.5, we see that

$$\gamma(k,q) \ll n(k+1)^{\frac{\log 4}{n\log|A'_k|}}\log\log k \ll (\log(k))^2 k^{\frac{\log 4}{n\log|A'_k|}} \ll (\log k)^2 k^{\varepsilon/2}.$$

□

Heilbronn further conjectured that for $\frac{p-1}{k} > 2$, $\gamma(k,p) \ll k^{1/2}$. This was established by Cipra, Cochrane and Pinner [10, Theorem 1]. Furthermore, Cochrane and Pinner [11] give an explicit constant: $\gamma(k,p) \leq 83k^{1/2}$. For $n \geq 2$ we obtain here,

Theorem 6.7. *If $n \geq 3$ and $\gamma(k,q)$ exists, then $\gamma(k,q) \leq 10\sqrt{k+1}$.*
For $n = 2$, we have $\gamma(k,p^2) \leq 16\sqrt{k+1}$.

Proof. We first note that for $k \leq 396$ the result follows from the bound, (1.19) $\gamma(k,q) \leq [\frac{k}{2}] + 1$. Thus we may assume $k \geq 396$. Corollary 5.1 lets us also assume $k > \sqrt{q}$. In particular, $k > 2^{n/2}$. By Theorem 6.4, we have for $n \geq 18$,

$$\frac{\gamma(k,q)}{\sqrt{k+1}} \leq 8n(k+1)^{1/n-1/2} \leq 8n2^{\frac{n}{2}(\frac{1}{n}-\frac{1}{2})} = \frac{8\sqrt{2}n}{2^{n/4}} \leq 10.$$

For $2 \leq n \leq 17$, we have

$$\frac{\gamma(k,q)}{\sqrt{k+1}} \leq 8n(k+1)^{1/n-1/2} \leq \frac{8n}{396^{1/2-1/n}} \leq \begin{cases} 10, & \text{if } n > 2, \\ 16, & \text{if } n = 2. \end{cases}$$

□

Bibliography

[1] N. Alon, M. Nathanson, and I. Ruzsa, *Adding distinct congruence classes modulo a prime,* Amer. Math. Monthly 102 (3) (1995), 250-255.

[2] M. Bhaskaran, *Sums of m-th powers in algebraic and abelian number fields,* Arch. Math. (Basel) 17 (1966), 497-504; Correction, ibid. 22 (1972), 370-371.

[3] J. Bourgain, M.-C. Chang, *A Gauss sum estimate in arbitrary finite fields,* C. R. Acad. Sci. Paris, Ser. I 342 (2006), 643-646.

[4] J. Bourgain, A. Glibichuk, and S. Konyagin, *Estimates for the number of sums and products and for exponential sums in fields of prime order*, J. London Math. Soc. 73 (2006), 380-398.

[5] J. Bourgain and S. Konyagin, *Estimates for the number of sums and products and for exponential sums over subgroups in fields of prime order*, C. R. Acad. Sci. Paris. Ser. I 337 (2003), 75-80.

[6] J.D. Bovey, *A new upper bound for Waring's problem (mod p)*, Acta Arith. 32 (1977) 157-162.

[7] A. Cauchy, *Recherches sur les nombres,* J. École Polytechnique 9 (1813), 99-116.

[8] I. Chowla, *On Waring's problem (mod p),* Proc. Indian Nat. Acad. Sci. A 13 (1943), 195-220.

[9] S. Chowla, H.B. Mann and E.G. Straus, *Some applications of the Cauchy-Davenport theorem*, Norske Vid. Selsk. Forh. Trondheim 32 (1959), 74-80.

[10] J.A. Cipra, T. Cochrane, and C. Pinner, *Heilbronn's conjecture on Waring's number (mod p)*, J. Number Theory 125 (2007), 289-297.

[11] T. Cochrane and C. Pinner, *Sum-product estimates applied to Waring's problem mod p*, Integers 8 (2008), A46.

[12] T. Cochrane, C. Pinner, and J. Rosenhouse, *Bounds on exponential sums and the polynomial Waring problem mod p*, J. London Math. Soc. (2) 67 (2003), 319-336.

[13] M.M. Dodson, *On Waring's problem in GF[p],* Acta Arith. 19 (1971), 147-173.

[14] M.M. Dodson and A. Tietäväinen, *A note on Waring's problem in GF(p)*, Acta Arith. 19 (1971), 147-173.

[15] C. Garcia and J.F. Voloch, *Fermat curves over finite fields,* J. Number Theory 30 (1988), 345-356.

[16] A.A. Glibichuk, *Combinational Properties of Sets of Residues Modulo a Prime and the Erdős-Graham Problem*, Mathematical Notes 79, No. 3 (2006), 356-365.

[17] A.A. Glibichuk and S.V. Konyagin, *Additive properties of product sets in fields of prime order,* Additive Combinatorics, CRM Proceedings & Lecture Notes 43 (2007), 279-286.

[18] A.A. Glibichuk and M. Rudnev, *On additive properties of product sets in an arbitrary finite field*, Journal d'Analyse Mathématique 108 (1) (2009), 159-170.

[19] G.H. Hardy and J.E. Littlewood, *Some problems of "Partitio Numerorum", VIII: The number* $\Gamma(k)$ *in Waring's problem,* Proc. London Math. Soc. (2) 28 (1927), 518-542.

[20] D.R. Heath-Brown and S. Konyagin, *New bounds for Gauss sums derived from k-th powers, and for Heilbronn's exponential sum,* Quart. J. Math. 51 (2000), 221-235.

[21] H. Heilbronn, *Lecture Notes on Additive Number Theory mod p*, California Institute of Technology (1964).

[22] L.K. Hua and H.S. Vandiver, *Characters over certain types of rings with applications to the theory of equations in a finite field*, Proc. Nat. Acad. Sci. U.S.A. 35 (1949), 94-99.

[23] S.V. Konyagin, *On estimates of Gaussian sums and Waring's problem for a prime modulus*, Trudy Mat. Inst. Stelov. 198 (1992) 111-124 (Russian); Proc. Steklov Inst. Math. 1 (1994) 105-117 (English trans.).

[24] S.V. Konyagin, *Estimates for trigonometric sums over subgroups and for Gauss sums.* (Russian) IV International Conference "Modern Problems of Number Theory and its Applications": Current Problems, Part III (Russian) (Tula, 2001), 86–114, Mosk. Gos. Univ. im. Lomonosova, Mekh.-Mat. Fak., Moscow, 2002.

[25] S.V. Konyagin and I. Shparlinski, *Character sums with exponential functions and their applications*, Cambridge University Press, 1999.

[26] M.B. Nathanson, *Additive Number Theory*, Springer, 1996.

[27] Sister M.A.C. Real, *Waring's Problem, Modulo p, and the Representation Symbol*, Proc. Iowa Acad. of Sci. 66 (1959), 362-364.

[28] C. Small, *Waring's number mod n,* Amer. Math. Monthly 84 (1)(1977), 12-25.

[29] A. Tietäväinen, *On diagonal forms over finite fields,* Proc. Amer. Math. Soc. 65 (1977), 35-36.

[30] L. Tornheim, *Sums of n-th powers in fields of prime characteristic,* Duke Math. J. (1938), 359-362.

[31] A. Weil, *Number of solutions of equations in finite fields,* Bull. AMS 55 (1949), 497-508.

[32] A. Winterhof, *On Waring's problem in finite fields,* Acta Arith. 87 (1998), 171-177.

[33] A. Winterhof, *A note on Waring's problem in finite fields,* Acta Arith. 96 (2001), 365-368.

[34] A. Winterhof and C. van de Woestijne, *Exact solutions to Waring's problem for finite fields*, arXiv:0810.0485v1 [math.NT] (2007).