Finite Field Waring's Problem

Holden Lee

12/8/10

1 Introduction

In 1770, Waring asked the following question: given $d \in \mathbb{N}$, can every positive integer can be written as a sum of a bounded number of dth powers of positive integers? We call a set A in $\mathbb{N}_0$ a basis of order n if every element of $\mathbb{N}_0$ can be written as a sum of n elements of A, so the question can be rephrased as, is the set of dth powers of positive integers a basis of finite order? This was proved to be true. Rather than trying to prove existence directly, it is helpful to be "greedier" and instead try to estimate the number of solutions $r_{d,n}(b)$ to

$$y_1^d + \cdots + y_n^d = b, \quad y_i \in \mathbb{N}_0 \tag{1}$$

for given b, n, d. If $r_{d,n}(b) > 0$ for all sufficiently large b for some n, then Waring's problem for dth powers is true. (It is sufficient for $r_{d,n}(b) > 0$ for sufficiently large b because then we could always increase n to take care of small numbers.)

As described in [2, Chapter 5], the Hardy-Littlewood Circle Method can be used to estimate $r_{k,n}(b)$. Note that $r_{k,n}(b)$ is the coefficient of $e^{2\pi ibx}$ in

$$\left(\sum_{k\geq 0, k^d\leq b} e^{2\pi ixk^d}\right)^n = \sum_{0\leq k_1,\ldots,k_n\leq b^{\frac{1}{d}}} e^{2\pi ix(k_1^d+\cdots+k_n^d)}. \tag{2}$$

This product expands into a sum of functions of the form $e^{2\pi imx}$. Note that the functions $e^{2\pi imx}$ are orthonormal over $[0,1]$, that is, for $p, q \in \mathbb{Z}$,

$$\int_0^1 e^{2\pi ipx}\overline{e^{2\pi iqx}}\,dx = \begin{cases} 1, & p = q \\ 0, & p \neq q. \end{cases}$$

Then to pick out the coefficient of $e^{2\pi ibx}$, we multiply (2) by $e^{-2\pi ibx}$ and integrate from 0 to 1:

$$r_{d,n}(b) = \int_0^1 \left(\sum_{k\geq 0, k^n\leq b} e^{2\pi ixk^d}\right)^n e^{-2\pi ibx}\,dx. \tag{3}$$

For $s \geq 2^k + 1$, this gives (after a lot of work)

$$r_{d,n}(N) = \mathfrak{S}(N)\Gamma\left(1+\frac{1}{d}\right)^n \Gamma\left(\frac{n}{d}\right)^{-1} N^{\frac{n}{d}-1} + o(N^{\frac{n}{d}-1}) \tag{4}$$

where $\mathfrak{S}(N)$ is the singular series for Waring's Problem; it is defined as an exponential sum and satisfies $c_1 < \mathfrak{S}(N) < c_2$ for some positive constants c_1, c_2. The basic method is to divide the integral (3) into two parts, into an integral over the major arcs and over the minor arcs, which give the main contribution and the error term, respectively. Note that (4) makes sense intuitively: Given (1), if we choose y_i to be any numbers in $[0, N^{\frac{1}{d}}]$, then we get all possible ways of expressing the numbers between 0 and N as a sum of dth powers (as well as some ways to express greater numbers). There are approximately $N^{\frac{n}{d}}$ choices for the n numbers; we can expect on the order of $\frac{1}{N}$ of these to sum to N, giving the estimate up to a constant factor.

We could also ask an analogue of Waring's Problem for finite fields instead of $\mathbb{Z}$; that is, can every number in $\mathbb{F}_q$ can be written as a sum of a bounded number of dth powers of positive integers, and if so, what is the minimum number needed? Note that the first question is less interesting in this case: either the dth powers form a proper subfield of $\mathbb{F}_q$, in which case the answer is no, or the dth powers do not form a proper subfield, and the answer is yes because $\mathbb{F}_q$ is finite. To answer the second question, we use a similar idea to Waring's Problem for $\mathbb{Z}$, namely encapsulate the number of representations as a sum of n dth powers in a sum of orthonormal functions. Instead of $e^{2\pi i m}$, we consider a system of orthonormal functions on $\mathbb{F}_q$ called the additive characters χ. Hence instead of (2), we consider the product

$$\left(\sum_{y\in\mathbb{F}_q} \chi(y^d)\right)^n = \sum_{y_1,\ldots,y_n\in\mathbb{F}_q} \chi(y_1^d + \cdots + y_n^d). \tag{5}$$

(The additive characters have the nice property that $\chi(a+b) = \chi(a)\chi(b)$, like the property of the exponential function $e^{2\pi i m x}$. In fact, as we will see, the characters are given by exponential functions.) $\overline{\text{Note}}$ (5) is true for all characters. To extract out the coefficient of $\chi(b)$, we multiply by $\overline{\chi(b)}$, average over all distinct characters χ, and take advantage of orthonormality to get

$$r_{d,n}(b) = \frac{1}{q}\sum_{\chi}\left\{\left(\sum_{y\in\mathbb{F}_q}\chi(y^d)\right)^n \overline{\chi(b)}\right\}. \tag{6}$$

Compare this to (3), where we multiplied by $e^{-2\pi i b x}$ and integrated over $0 \le x \le 1$. In the next section we will give define and give properties of characters that help us estimate (6).

2 Characters

To evaluate (6) it would be helpful if $\chi(y^d) = \chi(y)^d$. However, this cannot hold as we defined χ so that it would preserve additive structure, not multiplicative structure. Thus to evaluate (6) we would like to rewrite it as a sum of functions ψ such that $\psi(ab) = \psi(a)\psi(b)$, and such that the set of ψ are orthonormal. Thus we will need both the concepts of additive and multiplicative characters. We make this precise below.

Definition 2.1: Let G be an abelian group. A **character** of G is a homomorphism from G to $\mathbb{C}^\times$. A character is trivial if it is identically 1. We denote the trivial character by χ_0 or ψ_0.

Definition 2.2: Let $\mathbb{F}_q$ be a given finite field. An additive character $\chi : \mathbb{F}_q^+ \to \mathbb{C}$ is a character χ with $\mathbb{F}_q$ considered as an additive group. A multiplicative character $\psi : \mathbb{F}_q^\times \to \mathbb{C}$ is a character with $\mathbb{F}_q^\times = \mathbb{F}_q - \{0\}$ considered as a multiplicative group. We extend ψ to $\mathbb{F}_q$ by defining $\psi(0) = 1$ if ψ is trivial, and $\psi(0) = 0$ otherwise. Note that the extended ψ still preserves multiplication.

We proceed to give an explicit description of characters for abelian groups. First, recall the following theorem.

Theorem 2.3 (Structure Theorem for Abelian Groups)**:** Let G be a finite abelian group. Then there exist positive integers $m_1, \ldots, m_k$ so that

$$G \cong \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}.$$

Theorem 2.4: The group $G = \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$ has $|G|$ characters and each is given by an element $(r_1, \ldots, r_k) \in \mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$:

$$\chi_{r_1,\ldots,r_k}(n_1, \ldots, n_k) = \prod_{j=1}^{k} e^{\frac{2\pi i r_j n_j}{m_j}}.$$

Moreover the set of characters $\widehat{G}$ form a multiplicative group isomorphic to G.

Proof. It is easy to check that $\chi = \chi_{r_1,\ldots,r_k}$ is a homomorphism. Let e_j be the element in G with 1 in the jth coordinate and 0's elsewhere. Since $\chi(e_j)^{m_j} = 1$, we must have $\chi(e_j) = e^{\frac{2\pi i r_j}{m_j}}$ for some r_j. Each element of G can be expressed as a combination of the e_j, so this shows all characters are in the above form.

For the second part, note that $(r_1, \ldots, r_k) \mapsto \chi_{r_1,\ldots,r_k}$ is an isomorphism. □

Corollary 2.5: Every finite abelian group G has $|G|$ characters.

Theorem 2.6 (Orthogonality relations)**:** Let G be a finite abelian group and $\chi_j, 1 \le k \le n$ be all characters of G. Then

1. (Row orthogonality) $\langle \chi_j, \chi_k \rangle := \frac{1}{|G|} \sum_{g \in G} \chi_j(g)\overline{\chi_k(g)} = \begin{cases} 0, & j \ne k \\ 1, & j = k \end{cases}.$
2. (Column orthogonality) $\sum_{j=1}^{n} \chi_j(g)\overline{\chi_j(h)} = \begin{cases} 0, & g \ne h \\ |G|, & g = h \end{cases}.$

Proof. Write G as $\mathbb{Z}/m_1\mathbb{Z} \times \cdots \times \mathbb{Z}/m_k\mathbb{Z}$. Let $(r_1, \ldots, r_k)$ and $(s_1, \ldots, s_k)$ be in G. Then

$$\langle \chi_{r_1,\ldots,r_k}, \chi_{s_1,\ldots,s_k} \rangle = \sum_{(p_1,\ldots,p_k) \in G} \prod_{j=1}^{k} e^{\frac{2\pi i (r_j - s_j) p_j}{m_j}} \tag{7}$$

$$= \sum_{(p_1,\ldots,p_{k-1}) \in G} \left[\left(\prod_{j=1}^{k-1} e^{\frac{2\pi i (r_j - s_j) p_j}{m_j}} \right) \sum_{p_k=0}^{m_k-1} e^{2\pi i (r_k - s_k) p_k} \right]. \tag{8}$$

If $(r_1, \dots, r_k) = (s_1, \dots, s_k)$ then (7) evaluates to $|G|$. Otherwise, we may assume without loss of generality that $r_k \neq s_k$; then the inner sum in (8) evaluates to 0 by writing it as a geometric series.

The proof for column orthogonality is similar. □

The most useful case of row orthogonality is when we set $\chi_k = \chi_0$:

Corollary 2.7: If χ is a character of G and $\chi \neq \chi_0$ then

$$\sum_{g \in G} \chi(g) = 0.$$

Next we use these tools to give the additive and multiplicative characters explicitly. We know that $\mathbb{F}_q^\times$ is cyclic; let ξ be a generator.

Theorem 2.8 (Multiplicative characters of $\mathbb{F}_q$)**:** The multiplicative characters of $\mathbb{F}_q$ are given by

$$\psi_j(\xi^n) = e^{\frac{2\pi i j n}{q-1}}$$

for $0 \leq j < q - 1$.

Proof. By identifying $\xi \in \mathbb{F}_q^\times$ with $1 \in \mathbb{Z}/(q-1)\mathbb{Z}$, this follows directly from Theorem 2.4. □

Describing the additive characters takes slightly more creativity, since it is inconvenient to decompose $\mathbb{F}_q^+$ into cyclic groups.

Theorem 2.9 (Additive characters of $\mathbb{F}_q$)**:** Suppose $q = p^r$ with p prime. The additive characters of $\mathbb{F}_q$ are given by

$$\chi_a(g) = e^{\frac{2\pi i}{p} \mathrm{Tr}(ag)} \tag{9}$$

for $a \in \mathbb{F}_q$ where

$$\mathrm{Tr}(g) = g + g^p + \cdots + g^{p^{r-1}}.$$

Proof. The automorphisms of $\mathbb{F}_q$ fixing $\mathbb{F}_p$ are generated by the Frobenius automorphism σ sending g to g^p. Since $\mathrm{Tr}(g)$ is fixed under this operation, it must be in the ground field $\mathbb{F}_p$. This makes (9) well-defined since only the value of $\mathrm{Tr}(ag)$ modulo p matters in (9). The fact that χ_a is a homomorphism comes directly from the fact that σ is a homomorphism.

Since $\chi_1(ag) = \chi_a(g)$, if $\chi_a = \chi_b$ then $\chi_1(ag) = \chi_1(bg)$ and $\chi_1((a-b)g) = 0$. However, χ_1 is not trivial (identically equal to 1) since there are at most p^{r-1} values of g such that $g + \cdots + g^{p^{r-1}} = 0$. Thus $a = b$. This shows all characters in our list are distinct. Since we have found $|G|$ characters we have found all of them. □

Remark 2.10: In general, a n-dimensional complex representation of a group G is a homomorphism ρ from G into $GL_n(\mathbb{C})$, and the character χ of a representation is defined by $\chi(g) = \mathrm{Tr}(\rho(g))$. This coincides with Definition 2.1 for abelian G, if we just consider 1-dimensional representations, since ρ is multiplication by a constant and χ is just that constant.

The general case of Corollary 2.5 is replaced by the following: every finite group has a number of irreducible characters equal to the number of conjugacy classes. The orthogonality relations hold when we consider just irreducible characters, and with $|G|$ replaced by the size of the centralizer of g in the equation for column orthogonality.

3 Gauss Sums

To relate additive characters to multiplicative characters, we need to evaluate sums in the form

$$G(\psi,\chi)=\sum_{y\in\mathbb{F}_q^\times}\psi(y)\chi(y). \tag{10}$$

where ψ is a multiplicative character and χ is an additive character.

Suppose we wanted to write an additive character in terms of multiplicative characters. By row orthogonality, $\frac{1}{q-1}\sum_{\psi\in\widehat{\mathbb{F}_q^\times}}\psi(y)\overline{\psi(g)}$ equals 1 if $y=g$ and is 0 otherwise. This allows us to introduce multiplicative characters as follows: for $y\in\mathbb{F}_q^\times$,

$$\begin{aligned}\chi(y)&=\frac{1}{q-1}\sum_{g\in\mathbb{F}_q^\times}\chi(g)\sum_{\psi\in\widehat{\mathbb{F}_q^\times}}\psi(y)\overline{\psi(g)}\\&=\frac{1}{q-1}\sum_{\psi\in\widehat{\mathbb{F}_q^\times}}\psi(y)\sum_{g\in\mathbb{F}_q^\times}\overline{\psi}(g)\chi(g)\\&=\frac{1}{q-1}\sum_{\psi\in\widehat{\mathbb{F}_q^\times}}G(\overline{\psi},\chi)\psi(y). \qquad (11)\end{aligned}$$

The Gauss sums are the coefficients of the expansion of χ in terms of multiplicative characters. The next theorem tells us how to calculate Gauss sums.

Theorem 3.1: Let ψ_0 and χ_0 denote the trivial multiplicative and additive characters, respectively. Then

$$G(\psi,\chi)=\begin{cases}q-1, & \psi=\psi_0,\chi=\chi_0\\-1, & \psi=\psi_0,\chi\neq\chi_0\\0, & \psi\neq\psi_0,\chi=\chi_0\end{cases}$$

and

$$|G(\psi,\chi)|=\sqrt{q},\ \psi\neq\psi_0,\chi\neq\chi_0$$

Proof. The first case is trivial. For the second case,

$$G(\psi_0,\chi)=\sum_{y\in\mathbb{F}_q^\times}\chi(y)=\left(\sum_{y\in\mathbb{F}_q}\chi(y)\right)-1=-1$$

by Corollary 2.7. The third case directly from Corollary 2.7 with ψ.

For the final case,

$$\begin{aligned}
|G(\psi,\chi)|^2 &= \sum_{g_1,g_2\in\mathbb{F}_q^\times} \overline{\psi(g_1)}\psi(g_2)\overline{\chi(g_1)}\chi(g_2)\\
&= \sum_{g_1,g_2\in\mathbb{F}_q^\times} \psi(g_1^{-1}g_2)\chi(g_2-g_1)\\
&= \sum_{h\in\mathbb{F}_q^\times}\sum_{g_1\in\mathbb{F}_q^\times} \psi(h)\chi(g_1(h-1)) && \text{setting } h=g_1^{-1}g_2\\
&= \sum_{h\in\mathbb{F}_q^\times}\psi(h)\left[\left(\sum_{g_1\in\mathbb{F}_q}\chi(g_1(h-1))\right)-\chi(0)\right]\\
&= \sum_{h\in\mathbb{F}_q^\times}\psi(h)\left(\sum_{g_1\in\mathbb{F}_q}\chi(g_1(h-1))\right) && \text{by Corollary 2.7 with } \psi\\
&= \psi(1)q = q
\end{aligned}$$

In the last step, we used Corollary 2.7, noting that as g_1 ranges over $\mathbb{F}_q$, $g_1(h-1)$ ranges over $\mathbb{F}_q$ for $h\neq 1$, and is constantly 0 for $h=1$. □

We will need the following fact later on.

Proposition 3.2: For $a\in\mathbb{F}_q^\times$ and $b\in\mathbb{F}_q$,

$$G(\psi,\chi_{ab}) = \overline{\psi(a)}G(\psi,\chi_b).$$

Proof. Using the fact that $\chi_c(g)=\chi_1(cg)$,

$$\begin{aligned}
G(\psi,\chi_{ab}) &= \sum_{y\in\mathbb{F}_q^\times}\psi(y)\chi_{ab}(y)\\
&= \sum_{y\in\mathbb{F}_q^\times}\psi(y)\chi_b(ay)\\
&= \sum_{y\in\mathbb{F}_q^\times}\psi(a^{-1}y)\chi_b(y) && \text{replacing } y\to a^{-1}y\\
&= \psi(a)^{-1}\sum_{y\in\mathbb{F}_q^\times}\psi(y)\chi_b(y)\\
&= \overline{\psi(a)}G(\psi,\chi_b)
\end{aligned}$$

□

4 Enumerating Solutions

We return to our original problem. Rather than just work with sums of dth powers, we work with diagonal equations

$$a_1y_1^{d_1}+\cdots+a_ny_n^{d_n}=b \tag{12}$$

where $a_i \in \mathbb{F}_q^\times$ and $d_i \in \mathbb{N}$. First, note that because of the following lemma, we can restrict to case where $d_i | q-1$.

Lemma 4.1: The multisets $\{y^d | y \in \mathbb{F}_q\}$ and $\{y^{\gcd(d,q-1)} | y \in \mathbb{F}_q\}$ are equal.

Proof. Let ξ be a generator for $\mathbb{F}_q^\times$, and write $d = k \gcd(d, q-1)$ where $\gcd(k, q-1) = 1$. Then removing the one occurrence of 0 in the two sets, we get $\{\xi^{jd} | 0 \le j < q-1\}$ and $\{\xi^{j \gcd(d,q-1)} | 0 \le j < q-1\}$. The lemma follows from the fact that as multisets,

$$\{jd \pmod{q-1} | 0 \le j < q-1\} = \{j \gcd(d, q-1) \pmod{q-1} | 0 \le j < q-1\}.$$

Indeed, each multiple of $\gcd(d, q-1)$ appears $\frac{q-1}{\gcd(d,q-1)}$ times on both sides. □

As (12) always has the trivial solution when $b = 0$, we just need to estimate the number of solutions to (12) when $b \ne 0$.

Theorem 4.2: [1, 6.37] Fix $b \ne 0, d_i | q-1$ and let N be the number of solutions to (12) when $b \ne 0$ is fixed. Then

$$|N - q^{n-1}| \le [(d_1 - 1) \cdots (d_n - 1) - (1 - q^{-\frac{1}{2}}) M(d_1, \ldots, d_n)] q^{\frac{n-1}{2}}$$

where $M(d_1, \ldots, d_n)$ is the number of n-tuples in the set

$$S := \left\{ (j_1, \ldots, j_n) \in \mathbb{Z}^n | 1 \le j_i \le d_i - 1 \text{ and } \sum_{i=1}^n \frac{j_i}{d_i} \in \mathbb{Z} \right\}.$$

Note that we would expect N to be close to q^{n-1}, because there are q^n possible choices for $(y_1, \ldots, y_n)$ and q possible values for their sum.

Proof. We use the idea mentioned in the introduction. We have

$$N = \frac{1}{q} \sum_{y_1,\ldots,y_n \in \mathbb{F}_q,\, \chi \in \widehat{\mathbb{F}_q^+}} \chi(a_1 y_1^{d_1} + \cdots + a_n y_n^{d_n}) \overline{\chi}(b) = \frac{1}{q} \sum_{y_1,\ldots,y_n \in \mathbb{F}_q,\, \chi \in \widehat{\mathbb{F}_q^+}} \chi(a_1 y_1^{d_1}) \cdots \chi(a_n y_n^{d_n}) \overline{\chi}(b)$$

since by row orthogonality the inner sum is 1 if $a_1 y_1^{d_1} + \cdots + a_n y_n^{d_n} = b$ and 0 otherwise. Note that χ_0 contributes q^n to the sum. Taking it out and factoring the remaining terms gives

$$N = q^{n-1} + \frac{1}{q} \sum_{\chi \in \widehat{\mathbb{F}_q^+}, \chi \ne \chi_0} \left(\overline{\chi}(b) \prod_{j=1}^n \sum_{y_j \in \mathbb{F}_q} \chi(a_j y_j^{d_j}) \right) \tag{13}$$

We write the sums of additive characters as sums of multiplicative characters using the following lemma.

Lemma 4.3: Let χ be a nontrivial additive character and λ a multiplicative character of order d dividing $q-1$. Then

$$\sum_{y \in \mathbb{F}_q} \chi(ay^d) = \sum_{j=1}^{d-1} \overline{\lambda}(a)^j G(\lambda^j, \chi).$$

Proof. Note that λ exists since the group of multiplicative characters is isomorphic to $\mathbb{Z}/(q-1)\mathbb{Z}$ by Theorem 2.4. Suppose $\chi = \chi_c$. We write χ as a sum of multiplicative characters using (11), get the Gauss sum to be independent of a by using Proposition 3.2, and take out the exponent as we were hoping to do:

$$\begin{aligned}
\sum_{y\in\mathbb{F}_q} \chi(ay^d) &= \sum_{y\in\mathbb{F}_q} \chi_{ac}(y^d) \\
&= 1 + \sum_{y\in\mathbb{F}_q^\times} \chi_{ac}(y^d) \\
&= 1 + \frac{1}{q-1} \sum_{\psi\in\widehat{\mathbb{F}_q^\times}} \sum_{y\in\mathbb{F}_q^\times} G(\overline{\psi}, \chi_{ac})\psi(y^d) \\
&= 1 + \frac{1}{q-1} \sum_{\psi\in\widehat{\mathbb{F}_q^\times}} \overline{\psi}(a)G(\overline{\psi}, \chi_c) \sum_{y\in\mathbb{F}_q} \psi(y)^d && (14) \\
&= 1 + \sum_{j=0}^{d-1} \overline{\lambda}(a)^j G(\lambda^j, \chi) && (15) \\
&= \sum_{j=1}^{d-1} \overline{\lambda}(a)^j G(\lambda^j, \chi) && (16)
\end{aligned}$$

Note (15) follows since by Corollary 2.7, $\sum_{y\in\mathbb{F}_q^\times} \psi(y)^d = 0$ unless ψ^d is the trivial character, which is true iff ψ is a power of λ. In that case, the inner sum in (14) is $q-1$. In (16) we used $G(\psi_0, \chi) = -1$ (Theorem 3.1). □

Using Lemma 4.3 and letting λ_j be the multiplicative character with $\lambda_j(\xi^t) = e^{\frac{2\pi i t}{d_j}}$ we rewrite (13) as

$$\begin{aligned}
N - q^{n-1} &= \frac{1}{q} \sum_{\chi\in\widehat{\mathbb{F}_q^+}, \chi\neq\chi_0} \left(\overline{\chi}(b) \prod_{j=1}^{n} \sum_{k=1}^{d-1} \overline{\lambda_j}(a_j)^k G(\lambda_j^k, \chi) \right) \\
&= \frac{1}{q} \sum_{\chi\in\widehat{\mathbb{F}_q^+}, \chi\neq\chi_0} \sum_{(k_1,\ldots,k_n), 1\le k_i\le d_i-1} \overline{\chi}(b)\overline{\lambda_1}^{k_1}(a_1)\cdots\overline{\lambda_n}^{k_n}(a_n) G({\lambda_1}^{k_1}, \chi)\cdots G({\lambda_n}^{k_n}, \chi) \\
&= \frac{1}{q} \sum_{c\in\mathbb{F}_q^\times} \sum_{(k_1,\ldots,k_n), 1\le k_i\le d_i-1} \overline{\chi_c}(b)\overline{\lambda_1}^{k_1}(a_1)\cdots\overline{\lambda_n}^{k_n}(a_n) G({\lambda_1}^{k_1}, \chi_c)\cdots G({\lambda_n}^{k_n}, \chi_c) \\
&= \frac{1}{q} \sum_{(k_1,\ldots,k_n), 1\le k_i\le d_i-1} G({\lambda_1}^{k_1}, \chi_{a_1})\cdots G({\lambda_n}^{k_n}, \chi_{a_n}) \sum_{c\in\mathbb{F}_q^\times} \overline{\chi_b}(c)\overline{\lambda_1}^{k_1}(c)\cdots\overline{\lambda_n}^{k_n}(c) && (17) \\
&= \frac{1}{q} \sum_{(k_1,\ldots,k_n), 1\le k_i\le d_i-1} G({\lambda_1}^{k_1}, \chi_{a_1})\cdots G({\lambda_n}^{k_n}, \chi_{a_n}) G(\overline{\lambda_1}^{k_1}\cdots\overline{\lambda_n}^{k_n}, \overline{\chi_b}) && (18)
\end{aligned}$$

where in (17) we used Proposition 3.2 twice, to get

$$\overline{\lambda_j}^{k_j}(a_j)G(\lambda_j{}^{k_j},\chi_c)=\overline{\lambda_j}^{k_j}(c)\overline{\lambda_j}^{k_j}(a_j)G(\lambda_j{}^{k_j},\chi_1)=\overline{\lambda_j}^{k_j}(c)G(\lambda_j{}^{k_j},\chi_{a_j}).$$

Now we apply Theorem 3.1 to get that $|G(\lambda_i^{k_i},\chi_{a_i})|=\sqrt{q}$. Note

$$(\overline{\lambda_1}^{k_1}\cdots\overline{\lambda_n}^{k_n})(\xi^t)=e^{(2\pi i)\left(\frac{k_1}{d_1}+\cdots+\frac{k_n}{d_n}\right)t}$$

is the trivial character iff $(k_1,\ldots,k_n)\in S$. Hence $|G(\overline{\lambda_1}^{k_1}\cdots\overline{\lambda_n}^{k_n},\overline{\chi_b})|=1$ if $(k_1,\ldots,k_n)\in S$ and $\sqrt{q}$ otherwise. Using this and the triangle inequality, (18) becomes

$$|N-q^{n-1}|\le\frac{1}{q}[q^{\frac{n}{2}}|S|+q^{\frac{n+1}{2}}((d_1-1)\cdots(d_n-1)-|S|)],$$

proving the theorem. □

5 Applications to Waring's Problem

Now we derive Small's bound [3] for Waring's constant $g(d,q)$, the minimum n such that (12) has a solution with $d_1=\cdots=d_n=d$ for all b. By Lemma 4.1, $g(d,q)=g(\gcd(d,q-1),q)$, so it suffices to consider the case $d|q-1$.

First, note that sufficient condition for Waring's constant to exist is that the set $\{y^d|y\in\mathbb{F}_q\}$ is not contained in a proper subfield of $\mathbb{F}_q$. Since this set is generated multiplicatively by ξ^d, and any subfield is multiplicatively generated by $\xi^{\frac{p^r-1}{p^k-1}}$ for some $k|d$, writing $q=p^r$ with p prime we need

$$\frac{p^r-1}{p^k-1}\nmid d\quad\text{for every proper divisor } k \text{ of } r. \tag{19}$$

Apply Theorem 4.2 (dropping the term with $M(d_1,\ldots,d_n)$) to get

$$N\ge q^{n-1}-(d-1)^n q^{\frac{n-1}{2}} \tag{20}$$

This is positive when

$$q^{\frac{n-1}{2}}>(d-1)^n\iff\frac{n}{2}(\ln q-2\ln(d-1))>\frac{\ln q}{2} \tag{21}$$

Thus we obtain the following bound for $g(d,q)$:

Theorem 5.1: Suppose $d|q-1$ and $q>(d-1)^2$. Then

$$g(d,q)\le\left\lfloor\frac{\ln q}{\ln q-2\ln(d-1)}+1\right\rfloor.$$

Note that in particular, (21) for $n = 2$ allows us to make the "inverse" statement that if $q > (d-1)^4$, then the equation $y_1^d + y_2^d = b$ has a solution for any $b \in \mathbb{F}_q$. That is, for any d, in any sufficiently large finite field every element can be written as a sum of 2 dth powers.

When (19) holds but $q \le (d-1)^2$, we can still get a less exciting estimate for $g(d, q)$ using elementary methods [5]. Suppose $q = p^r$, where p is prime. The dth powers span $\mathbb{F}_q$ over $\mathbb{F}_p$, so a subset, say $a_1, \dots, a_r$, forms a basis. Every element can be written as

$$b = c_1 a_1 + \cdots + c_r a_r, \quad c_i \in \mathbb{F}_p. \tag{22}$$

We claim that each c_i can be written as a sum of at most $g(d', p)$ dth powers, where $d' = \frac{p-1}{\gcd\left(\frac{q-1}{d}, p-1\right)}$. Indeed, the dth powers in $\mathbb{F}_q^\times$ are the $\left(\frac{q-1}{d}\right)$th roots of unity, so the dth powers of $\mathbb{F}_q^\times$ contained in $\mathbb{F}_p^\times$ are the $\gcd\left(\frac{q-1}{d}, p-1\right)$th roots of unity, which are the d'th powers of elements in $\mathbb{F}_q^\times$. Since the product of two dth powers is also a dth power, (22) gives a representation of b as a sum of $rg(d', p)$ kth powers.

$$g(d, q) \le rg(d', p), \quad d' = \frac{p-1}{\gcd\left(\frac{q-1}{d}, p-1\right)}. \tag{23}$$

Now we bound $g(d', p)$. Let A be the set of d'th powers of elements of $\mathbb{F}_p$. Let $nA = \{a_1 + \cdots + a_n, a_i \in A\}$. Note that $A \backslash \{0\}$ is a subgroup of order $\frac{p-1}{d'}$ in $\mathbb{F}_p^\times$. Note that $(mA)\backslash\{0\}$ is a union of cosets of $A\backslash\{0\}$ of the multiplicative group $\mathbb{F}_p^\times$ since if $a = y_1^{d'} + \cdots + y_n^{d'} \in mA$ then for any $c^{d'} \in A$, $c^{d'}a = (cy_1)^{d'} + \cdots + (cy_n)^{d'} \in mA$. For any m, $mA + \{0, 1\} \subseteq (m+1)A$, implying that either $mA = \mathbb{F}_p$ or $mA \subset (m+1)A$. Since $(mA)\backslash\{0\}$ is a union of cosets, by induction it must have at least $\min\left(p-1, m\frac{p-1}{d'}\right)$ elements. Hence $d'A = \mathbb{F}_p$. This shows

$$g(d', p) \le d'. \tag{24}$$

Putting (23) and (24) together gives the following:

Theorem 5.2: Suppose $q = p^r$ satisfies (19). Then

$$g(d, q) \le r \cdot \frac{p-1}{\gcd\left(\frac{q-1}{d}, p-1\right)}.$$

Note that we could have used the Cauchy-Davenport Theorem to conclude (24) immediately. This theorem says that given subsets $A_1, \dots, A_n$ of $\mathbb{F}_p$, the sumset $A_1 + \cdots + A_n$ contains at least $\min(p, |A_1| + \cdots + |A_n| - n + 1)$ elements. However, the above reasoning with cosets is more powerful because it uses the structure of the set A. The argument can be strengthened using Vosper's Theorem, an "inverse" theorem to Cauchy-Davenport which says that if $|A_1| + |A_2| \le p - 2$, then $|A_1 + A_2| = |A_1| + |A_2| - 1$, i.e. equality holds in Cauchy-Davenport, only when A_1, A_2 are arithmetic progressions with the same difference. Using this result, we can show that when $p > 2d' + 1$, in the proof above, $(m+1)A$ contains at least two more cosets then mA (if it is not already equal to $\mathbb{F}_p$), and that $g(d', q) \le \left\lfloor \frac{d'}{2} \right\rfloor + 1$. This approach is more combinatorial, while the proof of Theorem 5.1 is more algebraic. Both approaches can be quite fruitful; for example combintorial arguments have given exact values of Waring's constant for certain values of d and q [6], where $d|q-1$ is large relative to q.

The bound in Theorem 5.1 is strong for q large relatively to d, but weak for q close to $(d-1)^2$. The bound in Theorem 5.2 works for all d, q satisfying (19), but is weak for large q. There are various other bounds for $g(d,q)$ that are effective different ranges of d, q; for example, if $q > d^2$, then $g(d,q) < \lfloor 8 \ln q \rfloor + 1$, which is stronger than the bound in Theorem 5.1 for q close to d^2, and depends only on q. A list of known bounds can be found in [5].

6 Further Explorations

As a corollary of Theorem 5.1, we saw that given d, in every sufficiently large finite field every element can be written as a sum of 2 dth powers. It is natural to ask how small a subset of the dth powers we can choose so that the property above still holds. In other words, we want a subset that is a thin basis. The following theorem, whose proof is modeled after the existence of a thin basis for $\mathbb{N}_0$ [4], gives an answer.

Theorem 6.1: Let $d | q-1$ be fixed and let A be the set of dth powers in $\mathbb{F}_q$. Then there exist constants C_1, C_2 such that for sufficiently large q, there exists a subset $S \subseteq A$ satisfying the following:

1. S is a basis of order 2 for $\mathbb{F}_q$.
2. S has at most $C_1 \sqrt{q \ln q}$ elements.
3. Every nonzero element of $\mathbb{F}_q$ has at most $C_2 \ln q$ representations as a sum of 2 dth powers.

Proof. All implicit constants in our proof depend on d alone.

We rely on the fact that by (20), for large q, the number of representations for each residue as a sum of dth powers is approximately the same. Pick a random subset B of the set of $A \backslash \{0\}$, such that any nonzero element of A is included in B independently with probability $\sqrt{\frac{Cd^2 \ln q}{q}}$, where $C > 8$ is a constant. Let I denote the indicator function, that is, $I(P) = 1$ if P is a true statement, and $I(P) = 0$ otherwise. Then the number of ways to express $b \in \mathbb{F}_q^\times$ as a sum of 2 numbers in B is

$$\begin{aligned} r_{2,B}(b) &= \sum_{i,j \in A,\, i+j=b} I(i \in B) I(j \in B) \\ &= 2 \underbrace{\sum_{\substack{\{i,j\} \in A, i \neq j, \\ i+j=b,\, i,j \neq 0}} I(i \in B) I(j \in B)}_{(*)} + O(1). \end{aligned} \tag{25}$$

where the $O(1)$ term is nonnegative. We made the sum is over all unordered pairs of distinct elements, so that the values of the terms are independent of each other. Let X_b be the sum (*) above. Note that X_b has $\frac{q+O(q^{1/2})}{2d^2}$ summands: Indeed, by (20) with $n = 2$, there are $q + O(q^{1/2})$ solutions to $y_1^d + y_2^d = b$; there are at most $3d = O(1)$ solutions where one of y_1, y_2 is equal to 0 or $y_1^d = y_2^d$; we divide by d^2 since at most d values of y_i give the same value of y_i^d, and divide by 2 since we are considering unordered pairs. Taking the expected value, and noting that the probability that $i \in B$ and $j \in B$ for fixed $i \neq j$ is $\frac{Cd^2 \ln q}{q}$,

$$E(X_b) = \frac{q + O(q^{1/2})}{2d^2} \cdot \frac{Cd^2 \ln q}{q} = \frac{C}{2} \ln q + O(q^{-1/2} \ln q). \tag{26}$$

Now we use the following.

Theorem 6.2 (Chernoff's Inequality)**:** [4, Theorem 1.8] Let $X_b = t_1 + \cdots + t_n$ where the t_i are independent random variables taking the values 0 or 1. Then for any $\varepsilon > 0$,

$$P\left(|X - E(X)| \geq \varepsilon E(X)\right) \leq 2e^{-\min(\varepsilon^2/4, \varepsilon/2)E(X)}.$$

Letting $\varepsilon = 1$ and noting that the terms in the sum X are linearly independent, we get

$$\begin{aligned} P(|X_b - E(X_b)| \geq E(X_b)) &\leq 2e^{-E(X_b)/4} \\ &= 2e^{-\frac{1}{4}\left(\frac{C \ln q}{2} + O(q^{-1/2} \ln q)\right)} \\ &= 2e^{-\frac{C}{8}\ln(q)} e^{O(q^{-1/2} \ln q)} \\ &= 2q^{-\frac{C}{8}} O(1) \end{aligned}$$

Hence

$$P(0 < X_b < 2E(X_b) \text{ for each } b) \geq 1 - \sum_{b \in \mathbb{F}_q^\times} P(|X_b - E(X)| \geq E(X)) \geq 1 - 2q^{1-\frac{C}{8}} O(1).$$

Since $C > 8$, this is positive for any sufficiently large q. Thus there exists a set B such that $0 < X_b < 2E(X_b)$; by (25) and (26) this gives $0 < r_{2,B}(b) \leq C \ln q + O(q^{-1/2} \ln q)$. Let l, m denote the number of pairs (i, j) such that $i, j \in B$ and $i + j$ is nonzero, zero, respectively. Then

$$l = \sum_{b \in \mathbb{F}_q^\times} r_{2,B}(b) \leq Cq \ln q + O(q^{1/2} \ln q), \quad l + m = |B|^2.$$

Note that at most $|B|$ pairs in B sum to 0, so $m \leq |B|$ and $l \geq |B|^2 - |B|$. This gives $|B|^2 \leq \frac{|B|}{|B|-1} l$, and $|B| = O(\sqrt{q \ln q})$. Let $S = B \cup \{0\}$; then S is a basis of order 2 and satisfies the desired conditions. □

Next we find bounds for Waring's constant for $\mathbb{Z}/m\mathbb{Z}$. Let $G(d, m)$ denote the least number n such that for all $b \in \mathbb{Z}/m\mathbb{Z}$, there exist $y_i \in \mathbb{Z}/m\mathbb{Z}$ with

$$y_1^d + \cdots + y_n^d \equiv b \pmod{m}.$$

First, we consider the case of a prime power p^k; we divide into two cases based on whether p divides d. If p does not divide d, then we can take advantage of the following.

Lemma 6.3 (Hensel's Lemma)**:** Suppose f is a polynomial with integer coefficients, $f(x) \equiv m \pmod{p^h}$ and $f'(x) \not\equiv 0 \pmod{p}$. Then there exists $x' = x + pt$ such that $f(x') \equiv m \pmod{p^{h+1}}$.

This allows us to get the following bound for Waring's constant for $\mathbb{Z}/p^h\mathbb{Z}$ in terms of Waring's constant for $\mathbb{Z}/p\mathbb{Z} = \mathbb{F}_p$.

Theorem 6.4: Let p be a prime, h a positive integer. Then

$$g(d,p) \le G(d,p^h) \le g(d,p) + 1.$$

Proof. Any residue modulo p^h not divisible by p can be written as a sum of $n = g(d,p)$ dth powers. Indeed take any r not divisible by p; by definition of $g(d,p)$ there exist $y_1, \ldots, y_n$ such that

$$y_1^d + \cdots + y_n^d \equiv r \pmod{p}.$$

Without loss of generality, we can assume p does not divide y_1. Since the polynomial x^d has derivative dx^{d-1}, which is not zero modulo p when $x \ne 0$, by repeatedly applying Hensel's Lemma we can find y_1' such that

$$y_1'^d \equiv r - (y_2^d + \cdots + y_n^d) \pmod{p^h}.$$

If r is divisible by p, then $r-1$ is not divisible by p, so by the above we can find y_i so that

$$y_1^d + \cdots + y_n^d \equiv r - 1 \pmod{p^h}.$$

Adding 1 to both sides expresses r as a sum of $n+1$ dth powers. Thus $G(d,p^h) \le g(d,p)+1$. The other inequality is obvious. □

If p divides d, then we have to rely on the following theorem.

Theorem 6.5: Let p be prime and h a positive integer. Suppose $d = p^\alpha e, e \nmid p$, and let $d' = p^{\min(\alpha,h)} \gcd(e, p-1)$. Then $G(d,p^h) \le 2d'$ for p odd and $G(d,p^h) \le 4d'$ for $p = 2$.

Proof. After noting that the set of dth powers and the set of d'th powers in $\mathbb{Z}/p^h\mathbb{Z}$ are the same (by an argument similar to Lemma 4.1), the result follows from [2, Lemma 5.8-10]. □

Theorem 6.6: If a and b are relatively prime then

$$G(d,ab) = \max(G(d,a), G(d,b))$$

Proof. Let $n = \max(G(d,a), G(d,b))$. Any representation of a number as a sum of dth powers modulo ab is also valid modulo a and modulo b, so $G(d,ab) \ge n$. Since $n \ge G(d,a), G(d,b)$, given a residue r modulo a, b, we can find $x_i, 1 \le i \le n$ and $y_i, 1 \le i \le n$ such that

$$x_1^d + \cdots + x_n^d \equiv r \pmod{a}$$
$$y_1^d + \cdots + y_n^d \equiv r \pmod{b}$$

By the Chinese Remainder Theorem we can choose z_i so that $z_i \equiv x_1 \pmod{a}$ and $z_i \equiv x_2 \pmod{b}$. Then

$$z_1^d + \cdots + z_n^d \equiv r \pmod{ab},$$

as needed. □

Together, these results provide a bound for Waring's constant for any modulus, given bounds for $g(d,p)$.

Since Theorem 6.5 is rather weak, I tried to get a bound similar to Theorem 5.1 by defining multiplicative and additive characters on $\mathbb{Z}/q\mathbb{Z}, q = p^h$ for odd p as follows:

$$\begin{aligned}\chi_a(k) &= e^{\frac{2\pi i a k}{q}}\\ \psi(\xi^r) &= e^{\frac{2\pi i r}{(p-1)p^{h-1}}}\end{aligned}$$

where ξ is a primitive root modulo p^h. Then we can define Gauss sums analogously. However, the proof does not carry over, because rather than just having to exclude one term (namely, 0) in a sum over $\mathbb{Z}/q\mathbb{Z}$ when dealing with multiplicative characters, we have to exclude every multiple of p. This gives too many extra terms, and the errors were hard to bound, so I could not find an analogue of the statement that $|G(\psi,\chi)| = \sqrt{q}$ for nontrivial characters. In conclusion, the method of character sums really does take advantage of the coherent additive and multiplicative structure in a finite field.

References

[1] R. Lidl and H. Niederreiter. *Finite Fields.* Cambridge University Press, 2nd edition, 1997.

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

[3] C. Small. Diagonal equations over large finite fields. *Canadian Journal of Mathematics*, XXXVI:249–262, 1984.

[4] T. Tao and V. Vu. *Additive Combinatorics.* Cambridge University Press, 2010.

[5] A. Winterhof. On waring's problem in finite fields. *Acta Arithmetica*, LXXXVII:171–177, 1998.

[6] A. Winterhof and C. van de Woestijne. Exact solutions to waring's problem for finite fields. October 2008.