Journal of Number Theory 186 (2018) 1–15

Contents lists available at ScienceDirect

Journal of Number Theory

www.elsevier.com/locate/jnt

A supercharacter approach to Heilbronn sums ☆

Stephan Ramon Garcia [a,*], Bob Lutz [b]

[a] *Department of Mathematics, Pomona College, 610 N. College Ave., Claremont, CA 91711, United States*
[b] *Department of Mathematics, University of Michigan, 2074 East Hall, 530 Church Street, Ann Arbor, MI 48109-1043, United States*

ARTICLE INFO

Article history:
Received 17 April 2017
Received in revised form 10 October 2017
Accepted 11 October 2017
Available online 16 November 2017
Communicated by S.J. Miller

Keywords:
Supercharacter
Superclass
Heilbronn sum

ABSTRACT

Various algebraic properties of Heilbronn's exponential sum can be deduced through the use of supercharacter theory, a novel extension of classical character theory due to Diaconis–Isaacs and André. This perspective yields a variety of formulas and provides a method for computing the number of solutions to Fermat-type congruences.

1. Introduction

The theory of *supercharacters*, of which classical character theory is a special case, was introduced by P. Diaconis and I.M. Isaacs in 2008 [9], generalizing the *basic characters* studied by C. André [1–3]. The original aim of supercharacter theory was to provide new tools for studying groups, such as the unipotent matrix groups $U_n(q)$, that had proven intractable from the perspective of classical character theory. How-

☆ Partially supported by NSF Grant DMS-1265973.
* Corresponding author.
E-mail addresses: Stephan.Garcia@pomona.edu (S.R. Garcia), boblutz@umich.edu (B. Lutz).
URL: http://pages.pomona.edu/~sg064747 (S.R. Garcia).

https://doi.org/10.1016/j.jnt.2017.10.010
0022-314X/

ever, recent work indicates that supercharacters on abelian groups are intimately tied to various exponential sums arising in the theory of numbers [6–8,10–12]. Our aim here is to explore another such connection, demonstrating that many standard properties of Heilbronn's exponential sum can be systematically deduced through supercharacter theory.

We adopt the standard notation $e(x) = \exp(2\pi i x)$, so that the function $e(x)$ is periodic with period 1. The letter p will always denote an odd prime number and g a primitive root modulo p^2. In this note, we show that *Heilbronn sums*[1]

$$H_p(a) = \sum_{\ell=1}^{p-1} e\left(\frac{a\ell^p}{p^2}\right) \tag{1.1}$$

arise as the values of *supercharacters* on $\mathbb{Z}/p^2\mathbb{Z}$ induced by the action of a certain subgroup of the unit group $(\mathbb{Z}/p^2\mathbb{Z})^\times$. This observation, coupled with the general techniques from [7,11], permit us to derive a variety of identities involving Heilbronn sums. The novelty of our approach lies in the use of supercharacter theory, which reduces many computations to matrix arithmetic.

A brief review of basic facts about supercharacters on abelian groups is undertaken in Section 2, after which we construct the relevant supercharacter theory for Heilbronn sums in Section 3. An exact formula involving Heilbronn sums for computing the number of solutions to Fermat-type congruences $ax^p + by^p \equiv cz^p \pmod{p^2}$ is given in Section 4. We conclude in Section 5 with an exact formula for quartic sums involving Heilbronn sums.

2. Supercharacters on abelian groups

Before proceeding, we recall a few basic facts about supercharacters on abelian groups. Since complete details can be found in [7,11], we content ourselves with a quick overview of the relevant facts required in our particular case.

Let A be a subgroup of $GL_d(\mathbb{Z}/n\mathbb{Z})$ that is closed under the transpose operation and let $X_1, X_2, \ldots, X_N$ denote the orbits in $G = (\mathbb{Z}/n\mathbb{Z})^d$ under the action of A. The functions

$$\sigma_i(\mathbf{y}) = \sum_{\mathbf{x}\in X_i} e\left(\frac{\mathbf{x}\cdot\mathbf{y}}{n}\right), \tag{2.1}$$

[1] The notation is not completely standardized. For instance, Heath-Brown denotes the sum running from 1 to p by $S(a,p)$ in [14], whereas Heath-Brown and Konyagin use $H_p(a)$ to denote the sum running from 1 to p in [15]. We adopt here the notation used in Kowalski's lecture notes on exponential sums [17], which invites less confusion with Kloosterman or Salíe sums and is also more suitable from the viewpoint of supercharacter theory.

Table 2.1
Gaussian periods, Ramanujan sums, Kloosterman sums, and Heilbronn sums appear as supercharacters arising from the action of a group A of automorphisms on an abelian group G. Here p denotes an odd prime number and g a primitive root modulo p.

Name	Expression	G	A
Gauss	$\eta_j = \sum_{\ell=0}^{d-1} e\left(\frac{g^{k\ell+j}}{p}\right)$	$\mathbb{Z}/p\mathbb{Z}$	Nonzero kth powers mod p
Ramanujan	$c_n(x) = \sum_{\substack{j=1 \\ (j,n)=1}}^{n} e\left(\frac{jx}{n}\right)$	$\mathbb{Z}/n\mathbb{Z}$	$(\mathbb{Z}/n\mathbb{Z})^\times$
Kloosterman	$K_p(a,b) = \sum_{\ell=0}^{p-1} e\left(\frac{a\ell + b\overline{\ell}}{p}\right)$	$(\mathbb{Z}/p\mathbb{Z})^2$	$\left\{\begin{bmatrix} u & 0 \\ 0 & u^{-1} \end{bmatrix} : u \in (\mathbb{Z}/p\mathbb{Z})^\times\right\}$
Heilbronn	$H_p(a) = \sum_{\ell=0}^{p-1} e\left(\frac{a\ell^p}{p^2}\right)$	$\mathbb{Z}/p^2\mathbb{Z}$	Nonzero pth powers mod p^2

where $\mathbf{x} \cdot \mathbf{y}$ denotes the formal dot product of two elements of $(\mathbb{Z}/n\mathbb{Z})^d$, are called *supercharacters* on $(\mathbb{Z}/n\mathbb{Z})^d$ and the sets X_i are referred to as *superclasses*. It turns out that supercharacters are constant on superclasses, and hence we may employ the notation $\sigma_i(X_j)$ without confusion. The $N \times N$ matrix

$$U = \frac{1}{\sqrt{n^d}} \left[\frac{\sigma_i(X_j)\sqrt{|X_j|}}{\sqrt{|X_i|}} \right]_{i,j=1}^{N} \tag{2.2}$$

is symmetric (i.e., $U = U^T$) and unitary. In fact, the matrix U encodes an analogue of discrete Fourier transform (DFT) on the space of all *superclass functions* (i.e., functions $f : (\mathbb{Z}/n\mathbb{Z})^d \to \mathbb{C}$ that are constant on each superclass) and satisfies many of the standard properties of the DFT [7]. More general supercharacter theories on certain abelian groups are studied in [4,16,19].

It turns out that a variety of exponential sums that are relevant to the theory of numbers can be realized as supercharacters on abelian groups in the manner described above. This approach was first undertaken to study Ramanujan sums [11] and, a short while later, Gaussian periods [10,12]. The general theory is developed in [7], where a number of such examples (see Table 2.1) are discussed. A novel and visually compelling class of exponential sums is considered from the supercharacter perspective in [6].

The main result we require is the following, which identifies the set of all matrices that are diagonalized by the unitary matrix (2.2) as the span of a certain family of matrices containing combinatorial information about the superclasses. A complete proof and further details can be found in [7] (see also [11]).

Lemma 2.3. *Let $A = A^T$ be a subgroup of $GL_d(\mathbb{Z}/n\mathbb{Z})$, let $\mathcal{X} = \{X_1, X_2, \ldots, X_N\}$ denote the set of superclasses induced by the action of A on $(\mathbb{Z}/n\mathbb{Z})^d$, and let $\sigma_1, \sigma_2, \ldots, \sigma_N$ denote the corresponding supercharacters. For each fixed z in X_k, let $c_{i,j,k}$ denote the number of solutions $(x_i, y_j) \in X_i \times X_j$ to the equation $x + y = z$.*

(1) $c_{i,j,k}$ *is independent of the representative* z *in* X_k *which is chosen,*
(2) *The identity*

$$\sigma_i(X_\ell)\sigma_j(X_\ell) = \sum_{k=1}^{N} c_{i,j,k}\sigma_k(X_\ell) \tag{2.4}$$

holds for $1 \le i, j, k, \ell \le N$.
(3) *The matrices* $T_1, T_2, \ldots, T_N$, *whose entries are given by*

$$[T_i]_{j,k} = \frac{c_{i,j,k}\sqrt{|X_k|}}{\sqrt{|X_j|}}, \tag{2.5}$$

each satisfy

$$T_i U = U D_i, \tag{2.6}$$

where

$$D_i = \operatorname{diag}\big(\sigma_i(X_1), \sigma_i(X_2), \ldots, \sigma_i(X_N)\big). \tag{2.7}$$

In particular, the T_i *are simultaneously unitarily diagonalizable.*
(4) *Each* T_i *is a normal matrix (i.e.,* $T_i^* T_i = T_i T_i^*$*) and the set* $\{T_1, T_2, \ldots, T_N\}$ *forms a basis for the algebra of all* $N \times N$ *matrices* T *such that* $U^* T U$ *is diagonal.*

3. A supercharacter theory for Heilbronn sums

We are now in a position to represent Heilbronn sums as the values of certain supercharacters on $(\mathbb{Z}/n\mathbb{Z})^d$, where $d = 1$ and $n = p^2$ for an odd prime p. Following the general outline described in Section 2, we first require a group of automorphisms A to act upon $G = \mathbb{Z}/p^2\mathbb{Z}$. To this end, we need the following lemma.

Lemma 3.1. *If* p *is an odd prime, then for all integers* x *and* y *we have* $x^p \equiv y^p \pmod{p^2}$ *if and only if* $x \equiv y \pmod{p}$.

Proof. If $x \equiv y \pmod{p}$, then $x = y + rp$ for some integer r. Therefore

$$x^p = (y + rp)^p = \sum_{k=0}^{p} \binom{p}{k} y^{p-k}(rp)^k \equiv y^p \pmod{p^2},$$

since $p \mid \binom{p}{k}$ for $k = 1, 2, \ldots, p-1$.

Suppose now that $x^p \equiv y^p \pmod{p^2}$. Let g be a primitive root modulo p^2, and write $x \equiv g^j$ and $y \equiv g^k \pmod{p^2}$. We see that $g^{jp} \equiv g^{kp} \pmod{p^2}$, whence $g^{(j-k)p} \equiv 1 \pmod{p^2}$. It follows that $(j-k)p$ is a multiple of $\phi(p^2) = p(p-1)$, so $(p-1) \mid (j-k)$. Writing $j = k + m(p-1)$, we see that

$$x \equiv g^j \equiv g^{k+m(p-1)} \equiv g^k (g^{p-1})^m \equiv g^k \equiv y, \pmod{p}$$

by Fermat's little theorem. □

It follows that

$$A = \{1^p, 2^p, \ldots, (p-1)^p\} \tag{3.2}$$

is a subgroup of $(\mathbb{Z}/p^2\mathbb{Z})^\times$ of order $p-1$. Letting A act upon $\mathbb{Z}/p^2\mathbb{Z}$ by multiplication, we obtain the orbits

$$\begin{aligned} X_1 &= gA, \\ X_2 &= g^2 A, \\ &\vdots \\ X_{p-1} &= g^{p-1} A, \\ X_p &= A, \\ X_{p+1} &= \{p, 2p, \ldots, (p-1)p\}, \\ X_{p+2} &= \{0\}, \end{aligned}$$

where g denotes a primitive root modulo p^2 that will remain fixed throughout this paper. We have adopted this somewhat unusual labeling scheme in order to simplify the structure of certain matrices and streamline a number of formulas which appear later. For $1 \leq i, j \leq p$, we find that

$$\sigma_i(X_j) = \sum_{\ell=1}^{p-1} e\left(\frac{g^j(g^i \ell^p)}{p^2}\right) = \sum_{\ell=1}^{p-1} e\left(\frac{g^{i+j}\ell^p}{p^2}\right) = H_p(g^{i+j}).$$

Additionally, since A is closed under negation and $e(-z) = \overline{e(z)}$ for all $z \in \mathbb{C}$, all Heilbronn sums are real. We pause to make the following observation.

Lemma 3.3. *The value of $H_p(g^k)$ depends only upon $k \pmod{p}$.*

Proof. Since $(g, p) = 1$, the map $\ell \mapsto g^j \ell$ is a permutation of $\mathbb{Z}/p\mathbb{Z}$ for each j. In light of Lemma 3.1 we conclude that

$$H_p(g^{k+jp}) = \sum_{\ell=1}^{p-1} e\left(\frac{g^{k+jp}\ell^p}{p^2}\right) = \sum_{\ell=1}^{p-1} e\left(\frac{g^k(g^j\ell)^p}{p^2}\right) = \sum_{r=1}^{p-1} e\left(\frac{g^k r^p}{p^2}\right) = H_p(g^k),$$

as desired. □

Table 3.1
The supercharacter table corresponding to the supercharacter theory on $\mathbb{Z}/p^2\mathbb{Z}$ arising from the action of the subgroup $A = \{1^p, 2^p, \ldots, (p-1)^p\}$.

$\lvert X_i\rvert$	X_1 $p-1$	X_2 $p-1$	$\cdots$ $\cdots$	X_p $p-1$	X_{p+1} $p-1$	X_{p+2} 1
σ_1	$H_p(g^2)$	$H_p(g^3)$	$\cdots$	$H_p(g)$	-1	$p-1$
σ_2	$H_p(g^3)$	$H_p(g^4)$	$\cdots$	$H_p(g^2)$	-1	$p-1$
$\vdots$	$\vdots$	$\vdots$	$\ddots$	$\vdots$	-1	$p-1$
σ_p	$H_p(g)$	$H_p(g^2)$	$\cdots$	$H_p(1)$	-1	$p-1$
σ_{p+1}	-1	-1	$\cdots$	-1	$p-1$	$p-1$
σ_{p+2}	1	1	$\cdots$	1	1	1

Upon performing some additional elementary computations to evaluate the remaining values of $\sigma_i(X_j)$, we obtain the *supercharacter table* corresponding to the supercharacter theory on $\mathbb{Z}/p^2\mathbb{Z}$ arising from the action of A (see Table 3.1). Also of relevance is the unitary matrix U defined by (2.2), which is given by

$$U = \frac{1}{p}\left[\begin{array}{ccccc|cc} H_p(g^2) & H_p(g^3) & H_p(g^4) & \cdots & H_p(g) & -1 & \sqrt{p-1} \\ H_p(g^3) & H_p(g^4) & H_p(g^5) & \cdots & H_p(g^2) & -1 & \sqrt{p-1} \\ H_p(g^4) & H_p(g^5) & H_p(g^6) & \cdots & H_p(g^3) & -1 & \sqrt{p-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots & \vdots \\ H_p(g) & H_p(g^2) & H_p(g^3) & \cdots & H_p(1) & -1 & \sqrt{p-1} \\ \hline -1 & -1 & -1 & \cdots & -1 & p-1 & \sqrt{p-1} \\ \sqrt{p-1} & \sqrt{p-1} & \sqrt{p-1} & \cdots & \sqrt{p-1} & \sqrt{p-1} & 1 \end{array}\right]. \tag{3.4}$$

We obtain the following identities from the fact that (3.4) is unitary:

$$\sum_{\ell=1}^{p} H_p(g^\ell) = 0, \tag{3.5}$$

$$\sum_{\ell=1}^{p} H_p^2(g^\ell) = p(p-1), \tag{3.6}$$

$$\sum_{\ell=1}^{p} H_p(g^\ell)H_p(g^{i+\ell}) = -p. \tag{3.7}$$

Identity (3.5) is obtained by taking the inner product of the first column of U with the $(p+1)$st. Identity (3.6) is obtained by noting that the first column of U has unit norm. Identity (3.7) is obtained by taking the inner product of any two columns of U among the first p columns. Squaring (3.5), expanding, and using (3.6) provides us with

$$\sum_{1\le r<s\le p} H_p(g^r)H_p(g^s) = -\frac{p(p-1)}{2}. \tag{3.8}$$

In light of the fact that U is a real symmetric unitary matrix, we see that $U^2 = I$ whence the only possible eigenvalues of U are ± 1. In fact, we can say much more.

Proposition 3.9. *The matrix U has eigenvalues 1 and -1 with multiplicities $(p+3)/2$ and $(p+1)/2$, respectively. In particular,*

$$\det U = \begin{cases} -1 & \text{if } p \equiv 1 \pmod 4, \\ 1 & \text{if } p \equiv 3 \pmod 4. \end{cases}$$

Proof. Since the only possible eigenvalues are ± 1, it suffices to show that $\operatorname{tr} U = 1$. In light of Lemma 3.3 and the fact that p is odd, it follows that

$$\operatorname{tr} U = \frac{1}{p}\Big(\sum_{\ell=0}^{p-1} H_p(g^{2\ell}) + (p-1) + 1\Big) = 1 + \frac{1}{p}\sum_{\ell=0}^{p-1} H_p(g^\ell) = 1,$$

by (3.5). Thus 1 and -1 have the multiplicities claimed. □

Proposition 3.10. *The upper-left $p \times p$ matrix*

$$H = \frac{1}{p}\begin{bmatrix} H_p(1) & H_p(g) & H_p(g^2) & \cdots & H_p(g^{p-1}) \\ H_p(g) & H_p(g^2) & H_p(g^3) & \cdots & H_p(1) \\ H_p(g^2) & H_p(g^3) & H_p(g^4) & \cdots & H_p(g) \\ \vdots & \vdots & \vdots & \iddots & \vdots \\ H_p(g^{p-1}) & H_p(1) & H_p(g) & \cdots & H_p(g^{p-2}) \end{bmatrix} \tag{3.11}$$

has the eigenvalues $0, 1, -1$ with multiplicities 1, $\frac{p-1}{2}$, $\frac{p-1}{2}$, respectively.

Proof. It follows immediately from (3.6) and (3.7) that

$$H^2 = \frac{1}{p}\begin{bmatrix} p-1 & -1 & -1 & \cdots & -1 \\ -1 & p-1 & -1 & \cdots & -1 \\ -1 & -1 & p-1 & \cdots & -1 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ -1 & -1 & -1 & \cdots & p-1 \end{bmatrix} = I - \frac{1}{p}\mathbf{u}\mathbf{u}^T, \tag{3.12}$$

where $\mathbf{u}$ denotes the $p \times 1$ vector consisting of all ones. Thus

$$H^3 = H(I - \frac{1}{p}\mathbf{u}\mathbf{u}^T) = H + \frac{1}{p}(H\mathbf{u})\mathbf{u}^T = H$$

since $H\mathbf{u} = \mathbf{0}$ by (3.5). Since $H^3 = H$, we conclude that the eigenvalues of H are among 0, 1, and -1. In light of (3.12), it follows that $\operatorname{tr} H^2 = p-1$ whence H has precisely $p-1$

nonzero eigenvalues. Since $\operatorname{tr} H = 0$ by (3.5), we next see that H has the eigenvalues $0, 1, -1$ with multiplicities 1, $\frac{p-1}{2}$, $\frac{p-1}{2}$, respectively. □

We now identify the matrices T_i from Lemma 2.3. Following the recipe developed there, we let $c_{i,j,k}$ denote the number of solutions (x, y) in $X_i \times X_j$ to

$$x + y \equiv z \pmod{p^2}, \tag{3.13}$$

where z is a fixed element of X_k, recalling that the value of $c_{i,j,k}$ is independent of the representative z of X_k. Lemma 2.3 ensures that U simultaneously diagonalizes the matrices $T_1, T_2, \ldots, T_{p+2}$ whose entries are given by (2.5). To be more specific, we have $T_i U = U D_i$, where

$$D_i = \operatorname{diag}\big(\sigma_i(X_1), \sigma_i(X_2), \ldots, \sigma_i(X_{p+2})\big). \tag{3.14}$$

Since each eigenvalue $\sigma_i(X_j)$ is real and U is unitary, it follows that each T_i is real and symmetric. In order to describe the matrices $T_1, T_2, \ldots, T_p$, we first require a few elementary facts about the $c_{i,j,k}$.

Lemma 3.15. *If $1 \le i, j, k \le p$, then $c_{i,j,k} = c_{\pi(i,j,k)}$ for any permutation $\pi(i, j, k)$.*

Proof. The identity $c_{i,j,k} = c_{j,i,k}$ is immediate. For any $z \in X_k$ the solutions $(x, y) \in X_i \times X_j$ of $x + y \equiv z \pmod{p^2}$ are also the solutions of $wx - wz \equiv -g^j \pmod{p^2}$, obtained by rearranging terms and multiplying through by $w = g^j y^{-1}$, where the inverse y^{-1} is taken modulo p^2. As the pair (x, y) ranges over $X_i \times X_j$, the pair $(wx, -wz)$ ranges over $X_i \times X_k$ since w is a pth power modulo p^2 and X_k is closed under negation. Hence $c_{i,j,k} = c_{i,k,j}$. The result follows. □

Lemma 3.16. *If $1 \le i \le p$ and $j \ne i$, then*

$$\sum_{k=1}^{p+2} c_{i,j,k} = p - 1. \tag{3.17}$$

Proof. We first note that if $1 \le i \le p$ and $j \ne i$, then $c_{i,j,p+2} = 0$, since $a^p g^i + b^p g^j \equiv 0 \pmod{p^2}$ has no solutions when $i \ne j$. Indeed, the preceding is equivalent to $a^p g^{i-j} \equiv (-b)^p \pmod{p^2}$, which is inconsistent because $g^{i-j} A \cap A = \varnothing$. Since $c_{i,j,p+2} = 0$ and $(\mathbb{Z}/p^2\mathbb{Z})\backslash\{0\} = X_1 \cup X_2 \cup \cdots \cup X_{p+1}$, it follows that any sum of the form $x + y$, where x and y belong to X_i and X_j, respectively, also belongs to $(\mathbb{Z}/p^2\mathbb{Z})\backslash\{0\}$. For $1 \le k \le p-1$, the superclass X_k has precisely $p-1$ distinct representatives whence $x + y$ belongs to X_k for precisely $(p-1)c_{i,j,k}$ pairs (x, y) in $X_i \times X_j$. Thus $(p-1)^2 = |X_i \times X_j| = \sum_{k=1}^{p+1} (p-1) c_{i,j,k}$, which implies (3.17). □

We now have all of the information required to describe the general structure of $T_1, T_2, \ldots, T_p$.

Lemma 3.18. *If $1 \leq i \leq p$, then*

$$T_i = \left[\begin{array}{cccccccc|cc} & & & & & & & & 1 & 0 \\ & & & & & & & & \vdots & \vdots \\ & & & & & & & & 1 & 0 \\ & & & & C_i & & & & 0 & \sqrt{p-1} \\ & & & & & & & & 1 & 0 \\ & & & & & & & & \vdots & \vdots \\ & & & & & & & & 1 & 0 \\ \hline 1 & \cdots & 1 & 0 & 1 & \cdots & 1 & & 0 & 0 \\ 0 & \cdots & 0 & \sqrt{p-1} & 0 & \cdots & 0 & & 0 & 0 \end{array}\right], \tag{3.19}$$

where $C_i = [c_{i,j,k}]_{j,k=1}^{p}$ and the $\sqrt{p-1}$ occurs in the ith row and ith column.

Proof. Suppose that $1 \leq i \leq p$. Since T_i is real and symmetric, it suffices to establish that the final two columns of T_i have the desired form. In what follows, a and b denote units modulo p.

We first show that the upper-right $p \times 2$ submatrix is of the form claimed. Let us consider the coefficients $c_{i,j,p+1}$ for $j \neq i$. Since

$$a^p g^i + b^p g^j \equiv p \,(\mathrm{mod}\, p^2) \quad \iff \quad a g^i + b g^j \equiv 0 \,(\mathrm{mod}\, p),$$

for each fixed a we may let $b \equiv -a g^{i-j} \,(\mathrm{mod}\, p)$ to obtain a solution to the preceding congruences. In particular, this implies that $c_{i,j,p+1} \geq 1$ for $j \neq i$. However, Lemmas 3.15 and 3.16 tell us that $\sum_{j=1}^{p+2} c_{i,j,p+1} = p - 1$, from which it follows that

$$c_{i,j,p+1} = \begin{cases} 1 & \text{if } j \neq i, \\ 0 & \text{if } j = i, \end{cases} \tag{3.20}$$

as claimed. Turning our attention to the final column of T_i, we note that the proof of Lemma 3.16 tells us that $c_{i,j,p+2} = 0$ for $j \neq i$. Moreover, $c_{i,i,p+2} = p - 1$ for $1 \leq i \leq p$ since

$$a^p g^i + b^p g^i = g^i (a^p + b^p) \equiv 0 \,(\mathrm{mod}\, p^2)$$

has exactly $p - 1$ solutions $\{(a, -a) : 1 \leq a \leq p - 1\}$. In other words,

$$c_{i,j,p+2} = \begin{cases} 0 & \text{if } j \neq i, \\ p-1 & \text{if } j = i. \end{cases} \tag{3.21}$$

That the lower-right 2×2 submatrix of T_i is identically zero follows easily from the fact that $a^p g^i$ is a unit modulo p^2. $\square$

Our final lemma will be useful in Section 5.

Lemma 3.22. *For* $1 \leq i \leq p$,

$$\sum_{k=1}^{p} c_{i,i,k} = p - 2. \tag{3.23}$$

Proof. First observe that there are exactly $(p-1)^2$ pairs (a,b) with $1 \leq a, b \leq p-1$. Since $c_{i,i,k}$ is independent of the representative from X_k which is chosen, it follows that as (x,y) ranges over $X_i \times X_i$, the sum $x+y$ assumes values in X_k exactly $|X_k|c_{i,i,k}$ times. In light of (3.20) and (3.21), we obtain

$$(p-1)^2 = \sum_{k=1}^{p+2} |X_k| c_{i,i,k} = \sum_{k=1}^{p} (p-1)c_{i,i,k} + 0 + (p-1),$$

which implies (3.23). □

4. The third moment and Fermat's Last Theorem

Although it is not obvious from their definition, Heilbronn's exponential sums are related to a certain family of congruences connected to Fermat's Last Theorem. Since the details and history of Fermat's Last Theorem are well-known, we make no attempt to discuss the topic in depth, recalling only that this famous conjecture (proved by Andrew Wiles [22]), asserts that the equation $x^n + y^n = z^n$ has no integral solutions $x, y, z \geq 1$ if $n \geq 3$. Moreover, the general case can be easily reduced to the consideration of odd prime exponents.

Theorem 4.1. *If* $p \nmid abc$, *then the number of solutions* (x,y,z) *in* $(\mathbb{Z}/p^2\mathbb{Z})^3$ *to the generalized Fermat congruence*

$$ax^p + by^p \equiv cz^p \pmod{p^2} \tag{4.2}$$

which satisfy $p \nmid xyz$ *is precisely*

$$p^3(p-1)F(p;a,b,c), \tag{4.3}$$

where $F(p;a,b,c)$ *denotes the nonnegative integer*

$$F(p;a,b,c) = 1 - \frac{2}{p} + \frac{1}{p^2} \sum_{\ell=1}^{p} H_p(ag^\ell) H_p(bg^\ell) H_p(cg^\ell) \tag{4.4}$$

and g *denotes a primitive root modulo* p^2. *In particular, the equation*

$$ax^p + by^p = cz^p$$

has no solutions in integers with $p \nmid xyz$ *whenever* $F(p; a, b, c) = 0$.

Proof. If $p \nmid abc$ then a, b, c are congruent modulo p^2 to some powers g^i, g^j, g^k of g. We may assume without loss of generality that $1 \leq i, j, k \leq p$ since $g^{i+\ell p}x^p \equiv g^i(g^\ell x)^p \pmod{p^2}$ and so forth.

Recall that $c_{i,j,k}$ denotes the number of solutions to the congruence

$$g^i x^p + g^j y^p \equiv g^k \pmod{p^2}$$

with $1 \leq x, y \leq p-1$. Since there are $p-1$ different representatives of the superclass $X_k = g^k A$, there are $(p-1)c_{i,j,k}$ solutions to (4.2) with $1 \leq x, y, z \leq p-1$. By considering $(x + rp, y + sp, z + tp)$ for $0 \leq r, s, t \leq p-1$ we obtain $p^3(p-1)c_{i,j,k}$ distinct solutions to (4.2).

We will be done if we can show that $c_{i,j,k}$ is equal to the right-hand side of (4.4). Compute the (j,k) entry of the matrix identity $T_i = UD_iU$ to obtain

$$\begin{aligned} c_{i,j,k} &= \frac{\sqrt{|X_j|}}{p^2\sqrt{|X_k|}} \sum_{\ell=1}^{p+2} \sigma_i(X_\ell)\sigma_j(X_\ell)\sigma_\ell(X_k) \\ &= \frac{1}{p^2} \sum_{\ell=1}^{p+2} \sigma_i(X_\ell)\sigma_j(X_\ell)\sigma_\ell(X_k) \\ &= \frac{1}{p^2|X_k|} \sum_{\ell=1}^{p+2} |X_\ell|\sigma_i(X_\ell)\sigma_j(X_\ell)\sigma_k(X_\ell) \qquad (4.5) \\ &= 1 - \frac{2}{p} + \frac{1}{p^2} \sum_{\ell=1}^{p} H_p(ag^\ell)H_p(bg^\ell)H_p(cg^\ell), \qquad (4.6) \end{aligned}$$

as desired, where (4.5) follows from the fact that $U = U^T$ and (4.6) follows from Table 3.1. □

As the preceding theorem illustrates, cubic sums of Heilbronn sums control, in a precise manner, whether the generalized Fermat congruence (4.2) possesses any nontrivial solutions. Indeed, we consider a solution satisfying $p|xyz$ trivial since if, say $p|x$, the congruence reduces to $by^p \equiv cz^p \pmod{p^2}$, which has no solutions if $b = g^i$ and $c = g^j$ for $i \not\equiv j \pmod{p}$ and has only the $p(p-1)$ obvious solutions otherwise.

We remark that (4.4) can be used to efficiently evaluate $F(p; a, b, c)$ for many triples (a, b, c) in succession. In fact, one can compute $F(p; a, b, c)$ for all triples (a, b, c) simultaneously by taking advantage of the identity $T_i = UD_iU$ and fast matrix multiplication.

We present in Table 4.1 numerical values of the function $F(p) = F(p; 1, 1, 1)$, which corresponds to the classical Fermat congruence $x^p + y^p \equiv z^p \pmod{p^2}$. In particular,

Table 4.1
Values of $F(p) = F(p;1,1,1)$ as p ranges over the first 174 odd primes. Primes p for which $F(p) = 0$ satisfy the property that the corresponding Fermat equation $x^p + y^p = z^p$ has no solutions in integers with $p \nmid xyz$.

p	$F(p)$	p	$F(p)$	p	$F(p)$	p	$F(p)$	p	$F(p)$	p	$F(p)$
3	0	127	2	281	0	461	0	647	0	853	2
5	0	131	0	283	2	463	2	653	0	857	6
7	2	137	0	293	0	467	0	659	0	859	2
11	0	139	2	307	2	479	0	661	2	863	0
13	2	149	0	311	0	487	2	673	2	877	2
17	0	151	2	313	2	491	0	677	0	881	0
19	2	157	2	317	0	499	2	683	0	883	2
23	0	163	2	331	2	503	0	691	8	887	6
29	0	167	0	337	8	509	0	701	12	907	8
31	2	173	0	347	0	521	0	709	2	911	6
37	2	179	6	349	2	523	2	719	0	919	2
41	0	181	2	353	0	541	2	727	2	929	6
43	2	191	0	359	0	547	8	733	2	937	2
47	0	193	8	367	2	557	0	739	2	941	0
53	0	197	0	373	2	563	0	743	0	947	0
59	12	199	2	379	2	569	0	751	2	953	0
61	2	211	2	383	0	571	2	757	8	967	2
67	2	223	2	389	0	577	2	761	0	971	6
71	0	227	6	397	2	587	0	769	2	977	6
73	2	229	2	401	0	593	0	773	0	983	0
79	8	233	0	409	2	599	0	787	8	991	2
83	6	239	0	419	6	601	8	797	0	997	2
89	0	241	2	421	8	607	2	809	0	1009	2
97	2	251	0	431	0	613	2	811	2	1013	0
101	0	257	0	433	2	617	0	821	0	1019	0
103	2	263	0	439	2	619	8	823	2	1021	2
107	0	269	0	443	6	631	2	827	0	1031	0
109	2	271	2	449	0	641	0	829	2	1033	2
113	0	277	2	457	8	643	2	839	0	1039	8

$F(p) = 0$ implies that the Fermat equation $x^p + y^p = z^p$ has no solutions in integers satisfying $p \nmid xyz$.

At this point it is worth mentioning Kummer's proof of Fermat's Last Theorem for regular primes. Recall that a prime p is called *regular* if p does not divide the class number of the cyclotomic field $\mathbb{Q}(\zeta)$ where $\zeta = e(\frac{1}{p})$. It is well-known that p is regular if and only if p does not divide the numerator of the Bernoulli numbers $B_2, B_4, \ldots, B_{p-3}$ [21, p. 198]. Although Kummer himself believed that there are infinitely many regular primes, this conjecture remains open. On the other hand, Jensen proved that there are infinitely many *irregular primes* (i.e., primes which are not regular), the first few of which are

37, 59, 67, **101**, 103, **131**, **149**, 157, **233**, **257**, **263**, 271, 283, **293**, 307, **311**, **347**, **353**, 379, **389**, **401**, 409, 421, 433, **461**, 463, 467, **491**, 523, 541, 547, **557**, 577, **587**, **593**, 607, 613, **617**, 619, 631, **647**, **653**, 659, 673, **677**, **683**, 691, 727, 751, 757, **761**, **773**, **797**, **809**, 811, **821**, **827**, **839**, 877, **881**, 887, 929, **953**, 971.

The first major step in Kummer's approach is establishing that if p is an odd regular prime, then $x^p + y^p = z^p$ has no integral solutions with $p \nmid xyz$ [21] (in the terminology of [5], this is referred to as the *first case* of Fermat's Last Theorem). A glance at Table 4.1

reveals we have actually established that the Fermat equation $x^p + y^p = z^p$ has no integral solutions $x, y, z \geq 1$ with $p \nmid xyz$ if p is one of the irregular primes highlighted in boldface above.

5. The fourth moment

Using the fact that the matrices T_i are simultaneously unitarily diagonalizable, we obtain a variety of quartic formulas involving Heilbronn sums.

Theorem 5.1. *Letting g denote a primitive root modulo p^2, for $1 \leq i, j, k, \ell \leq p$ we have*

$$p^2 \sum_{r=1}^{p} c_{i,k,r} c_{j,\ell,r} = \sum_{r=1}^{p} H_p(g^{i+r}) H_p(g^{j+r}) H_p(g^{k+r}) H_p(g^{\ell+r}) + \begin{cases} -2p^2 + 3p & \text{if } i = k \text{ and } j = \ell, \\ p^3 - 4p^2 + 3p & \text{if } i \neq k \text{ and } j \neq \ell, \\ 0 & \text{otherwise.} \end{cases}$$

In particular,

$$\sum_{\ell=1}^{p} H_p^4(g^\ell) = p^2 \sum_{\ell=1}^{p} c_{i,i,\ell}^2 + 2p^2 - 3p. \tag{5.2}$$

Proof. Since $U = U^*$ it follows from Lemma 2.3 that $T_i T_j = U D_i D_j U$ for $1 \leq i, j \leq p+2$. Letting $1 \leq i, j, k, \ell \leq p$ and recalling that $|X_i| = p - 1$ in this range, it follows from the symmetry of T_j, (3.20), and (3.21) that

$$\begin{aligned} [T_i T_j]_{k,\ell} &= \sum_{r=1}^{p+2} \frac{c_{i,k,r}\sqrt{|X_r|}}{\sqrt{|X_k|}} \cdot \frac{c_{j,r,\ell}\sqrt{|X_\ell|}}{\sqrt{|X_r|}} \\ &= \sum_{r=1}^{p+2} \frac{c_{i,k,r}\sqrt{|X_r|}}{\sqrt{|X_k|}} \cdot \frac{c_{j,\ell,r}\sqrt{|X_r|}}{\sqrt{|X_\ell|}} \\ &= \frac{1}{p-1} \sum_{r=1}^{p+2} |X_r| c_{i,k,r} c_{j,\ell,r} \\ &= \sum_{r=1}^{p} c_{i,k,r} c_{j,\ell,r} + \begin{cases} p-1 & \text{if } i = k \text{ and } j = \ell, \\ 1 & \text{if } i \neq k \text{ and } j \neq \ell, \\ 0 & \text{otherwise.} \end{cases} \end{aligned}$$

On the other hand, using the fact that $U = U^T$ we have

$$
\begin{aligned}
[UD_iD_jU]_{k,\ell} &= \frac{1}{p^2}\sum_{r=1}^{p+2} \frac{\sigma_k(X_r)\sqrt{|X_r|}}{\sqrt{|X_k|}} \cdot \sigma_i(X_r)\sigma_j(X_r) \cdot \frac{\sigma_r(X_\ell)\sqrt{|X_\ell|}}{\sqrt{|X_r|}} \\
&= \frac{1}{p^2}\sum_{r=1}^{p+2} \frac{|X_r|\sigma_i(X_r)\sigma_j(X_r)\sigma_k(X_r)\sigma_\ell(X_r)}{p-1} \\
&= \frac{1}{p^2}\Big(\sum_{r=1}^{p} \sigma_i(X_r)\sigma_j(X_r)\sigma_k(X_r)\sigma_\ell(X_r) + 1 + (p-1)^3\Big) \\
&= \frac{1}{p^2}\Big(\sum_{r=1}^{p} H_p(g^{i+r})H_p(g^{j+r})H_p(g^{k+r})H_p(g^{\ell+r}) + 1 + (p-1)^3\Big).
\end{aligned}
$$

Equating our expressions for the matrix entries $[T_iT_j]_{k,\ell}$ and $[UD_iD_jU]_{k,\ell}$ yields the desired result. □

Corollary 5.3. *If $1 \le i \le p$, then*

$$\max_{1\le k\le p} c_{i,i,k} \ll p^\beta \quad \Longrightarrow \quad H_p(u) \ll p^{\frac{3+\beta}{4}} \tag{5.4}$$

whenever $p \nmid u$.

Proof. As a consequence of (5.2), for $p \nmid u$ we obtain

$$H_p(u) \ll p^{\frac{1}{2}}\Big(\sum_{k=1}^{p} c_{i,i,k}^2\Big)^{\frac{1}{4}}, \tag{5.5}$$

thereby recovering Heath-Brown's observation [14, Lem. 1]. Lemma 3.22 and the assumption that $c_{i,i,k} \ll p^\beta$ ensure that

$$\sum_{k=1}^{p} c_{i,i,k}^2 \ll \sum_{k=1}^{p} p^\beta c_{i,i,k} = p^\beta(p-2) \le p^{1+\beta}. \quad \square$$

Plugging this into (5.5) we obtain (5.4).

A result of Mit'kin implies that we may take $\beta = \frac{2}{3}$ in (5.4) [18], which yields Heath-Brown's estimate $H_p(u) \ll p^{11/12}$ for $p \nmid u$ [13]. The upper bound was later improved by Heath-Brown and Konyagin to $p^{7/8}$ [15] and by Shkredov to $p^{59/68}\log^{5/34} p$ [20].

References

[1] Carlos A.M. André, Basic characters of the unitriangular group, J. Algebra 175 (1) (1995) 287–319, MR MR1338979 (96h:20081a).
[2] Carlos A.M. André, The basic character table of the unitriangular group, J. Algebra 241 (1) (2001) 437–471, MR MR1839342 (2002e:20082).

[3] Carlos A.M. André, Basic characters of the unitriangular group (for arbitrary primes), Proc. Amer. Math. Soc. 130 (7) (2002) 1943–1954 (electronic), MR MR1896026 (2003g:20075).
[4] Samuel G. Benidt, William R.S. Hall, Anders O.F. Hendrickson, Upper and lower semimodularity of the supercharacter theory lattices of cyclic groups, Comm. Algebra 42 (3) (2014) 1123–1135, MR 3169622.
[5] A.I. Borevich, I.R. Shafarevich, Number Theory, Translated from the Russian by Newcomb Greenleaf, Pure and Applied Mathematics, vol. 20, Academic Press, New York, 1966, MR 0195803 (33 #4001).
[6] J.L. Brumbaugh, Madeleine Bulkow, Luis Alberto Garcia German, Stephan Ramon Garcia, Matt Michal, Andrew P. Turner, The graphic nature of the symmetric group, Exp. Math. 22 (4) (2013) 421–442, MR 3171103.
[7] J.L. Brumbaugh, Madeleine Bulkow, Patrick S. Fleming, Luis Alberto Garcia German, Stephan Ramon Garcia, Gizem Karaali, Matt Michal, Andrew P. Turner, Hong Suh, Supercharacters, exponential sums, and the uncertainty principle, J. Number Theory 144 (2014) 151–175, MR 3239156.
[8] Paula Burkhardt, Alice Zhuo-Yu Chan, Gabriel Currier, Stephan Ramon Garcia, Florian Luca, Hong Suh, Visual properties of generalized Kloosterman sums, J. Number Theory 160 (2016) 237–253, MR 3425206.
[9] P. Diaconis, I.M. Isaacs, Supercharacters and superclasses for algebra groups, Trans. Amer. Math. Soc. 360 (5) (2008) 2359–2392, MR MR2373317 (2009c:20012).
[10] William Duke, Stephan Ramon Garcia, Bob Lutz, The graphic nature of Gaussian periods, Proc. Amer. Math. Soc. 143 (5) (2015) 1849–1863, MR 3314096.
[11] Christopher F. Fowler, Stephan Ramon Garcia, Gizem Karaali, Ramanujan sums as supercharacters, Ramanujan J. 35 (2) (2014) 205–241, MR 3266478.
[12] Stephan Ramon Garcia, Trevor Hyde, Bob Lutz, Gauss's hidden menagerie: from cyclotomy to supercharacters, Notices Amer. Math. Soc. 62 (8) (2015) 878–888, MR 3379072.
[13] D.R. Heath-Brown, An estimate for Heilbronn's exponential sum, in: Analytic Number Theory, Vol. 2, Allerton Park, IL, 1995, in: Progr. Math., vol. 139, Birkhäuser Boston, Boston, MA, 1996, pp. 451–463, MR 1409372 (97k:11120).
[14] D.R. Heath-Brown, Heilbronn's exponential sum and transcendence theory, in: A Panorama of Number Theory or the View from Baker's Garden, Zürich, 1999, Cambridge Univ. Press, Cambridge, 2002, pp. 353–356, MR 1975462 (2004d:11076).
[15] D.R. Heath-Brown, S. Konyagin, New bounds for Gauss sums derived from kth powers, and for Heilbronn's exponential sum, Q. J. Math. 51 (2) (2000) 221–235, MR 1765792 (2001h:11106).
[16] Anders O.F. Hendrickson, Supercharacter theory constructions corresponding to Schur ring products, Comm. Algebra 40 (12) (2012) 4420–4438, MR 2989654.
[17] E. Kowalski, Exponential sums over finite fields, I: elementary methods, preprint.
[18] D.A. Mit'kin, An estimate for the number of roots of some comparisons by the Stepanov method, Mat. Zametki 51 (6) (1992) 52–58, 157, MR 1187477 (93h:11137).
[19] Anders Olaf, Flasch Hendrickson, Supercharacter Theories of Cyclic p-Groups, ProQuest LLC, Ann Arbor, MI, Thesis (Ph.D.), The University of Wisconsin–Madison, 2008, MR 2711764.
[20] I.D. Shkredov, On Heilbronn's exponential sum, Q. J. Math. 64 (4) (2013) 1221–1230, MR 3151613.
[21] Ian Stewart, David Tall, Algebraic Number Theory and Fermat's Last Theorem, third ed., A K Peters Ltd., Natick, MA, 2002, MR 1876804 (2002k:11001).
[22] Andrew Wiles, Modular elliptic curves and Fermat's last theorem, Ann. of Math. (2) 141 (3) (1995) 443–551, MR 1333035 (96d:11071).