COORDINATE SUM AND DIFFERENCE SETS OF d-DIMENSIONAL MODULAR HYPERBOLAS[1]

Amanda Bower
Department of Mathematics and Statistics, University of Michigan-Dearborn, Dearborn, Michigan
amandarg@umd.umich.edu

Ron Evans
Dept. of Mathematics, University of California San Diego, La Jolla, California
revans@ucsd.edu

Victor Luo
Department of Mathematics and Statistics, Williams College, Williamstown, MA
victor.d.luo@williams.edu

Steven J Miller
Department of Mathematics and Statistics, Williams College, Williamstown, MA
sjm1@williams.edu, Steven.Miller.MC.96@aya.yale.edu

Received: 12/20/13, Revised: 3/16/13, Accepted: 4/4/13, Published: 5/24/13

Abstract

Many problems in additive number theory, such as Fermat's last theorem and the twin prime conjecture, can be understood by examining sums or differences of a set with itself. A finite set $A \subset \mathbb{Z}$ is considered sum-dominant if $|A+A| > |A-A|$. If we consider all subsets of $\{0, 1, \ldots, n-1\}$, as $n \to \infty$, it is natural to expect that almost all subsets should be difference-dominant, as addition is commutative but subtraction is not; however, Martin and O'Bryant in 2007 proved that a positive percentage are sum-dominant as $n \to \infty$. This motivates the study of "coordinate sum dominance." Given $V \subset (\mathbb{Z}/n\mathbb{Z})^2$, we call $S := \{x+y : (x,y) \in V\}$ a coordinate sumset and $D := \{x-y : (x,y) \in V\}$ a coordinate difference set, and we say V is coordinate sum dominant if $|S| > |D|$. An arithmetically interesting choice of V is $\bar{H}_2(a;n)$, which is the reduction modulo n of the modular hyperbola $H_2(a;n) := \{(x,y) : xy \equiv a \bmod n, 1 \le x, y < n\}$. In 2009, Eichhorn, Khan, Stein, and Yankov determined the sizes of S and D for $V = \bar{H}_2(1;n)$ and investigated conditions for coordinate sum dominance. We extend their results to reduced d-dimensional modular hyperbolas $\bar{H}_d(a;n)$ with a coprime to n.

[1]Keywords: Modular hyperbolas, coordinate sumset, coordinate difference set. MSC 2010 Subject Classification: 11P99, 14H99 (primary), 11T23 (secondary).

We thank Mizan R. Khan for introducing us to this problem and, along with the referee, for helpful comments on an earlier draft. The first and third named authors were supported by Williams College and NSF grant DMS0850577; the fourth named author was partially supported by NSF grant DMS0970067.

1. Introduction

Let $A \subset \mathbb{N} \cup \{0\}$. Two natural sets to study are

$$\begin{aligned} A+A &= \{x+y : x,y \in A\} \\ A-A &= \{x-y : x,y \in A\}. \end{aligned} \tag{1.1}$$

The former is called the sumset and the latter the difference set. Many problems in additive number theory can be understood in terms of sum and difference sets. For instance, the Goldbach conjecture says that the even numbers greater than 2 are a subset of $P+P$, where P is the set of primes. The twin prime conjecture states that there are infinitely many ways to write 2 as a difference of primes (and thus if P_N is the set of primes exceeding N, $P_N - P_N$ always contains 2). If we let A_n be the set of positive n^{th} powers, then Fermat's Last Theorem says $(A_n + A_n) \cap A_n = \emptyset$ for all $n > 2$.

Let $|S|$ denote the cardinality of a set S. A set A is sum dominant if $|A+A| > |A-A|$. We might expect that almost all sets are difference dominant since addition is commutative while subtraction is not. However, in 2007 Martin and O'Bryant [7] proved that a positive percentage of sets are sum dominant; i.e., if we look at all subsets of $\{0, 1, \dots, n-1\}$ then as $n \to \infty$ a positive percentage are sum dominant. One explanation is that choosing A uniformly from $\{0, 1, \dots, n-1\}$ is equivalent to taking each element from 0 to $n-1$ to be in A with probability $1/2$. By the Central Limit Theorem this implies that there are approximately $n/2$ elements in a typical A, yielding on the order of $n^2/4$ pairs whose sum must be one of $2n-1$ possible values. On average we thus have each possible value realized on the order of $n/8$ ways. It turns out most possible sums and differences are realized (the expected number of missing sums and differences are 10 and 6, respectively). Thus most sets are close to being balanced, and we just need a little assistance to push a set to being sum-dominant. This can be done by carefully controlling the fringes of A (the elements near 0 and $n-1$). Such constructions are the basis of numerous results in the field; see for example [6, 7, 8, 9, 15, 16].

This motivates the study of "coordinate sum dominance" on fringeless sets such as $(\mathbb{Z}/n\mathbb{Z})^2$. Given $V \subset (\mathbb{Z}/n\mathbb{Z})^2$, we call $S := \{x+y : (x,y) \in V\}$ a coordinate sumset and $D := \{x-y : (x,y) \in V\}$ a coordinate difference set, and we say V is coordinate sum dominant if $|S| > |D|$. An arithmetically interesting choice of V is $\bar{H}_2(a;n)$, which is the reduction modulo n of the modular hyperbola

$$H_2(a;n) := \{(x,y) : xy \equiv a \bmod n,\ 1 \le x,y < n\}, \tag{1.2}$$

where $(a,n) = 1$. Eichhorn, Khan, Stein, and Yankov [2] determined the cardinalities of S and D for $V = \bar{H}_2(1;n)$ and investigated conditions for coordinate sum dominance. See [10] for additional results on related problems in other modular settings.

The modular hyperbolas in (1.2) have very interesting structure, as is evidenced in Figure 1. See Figures 1 through 4 of [2] for additional examples.

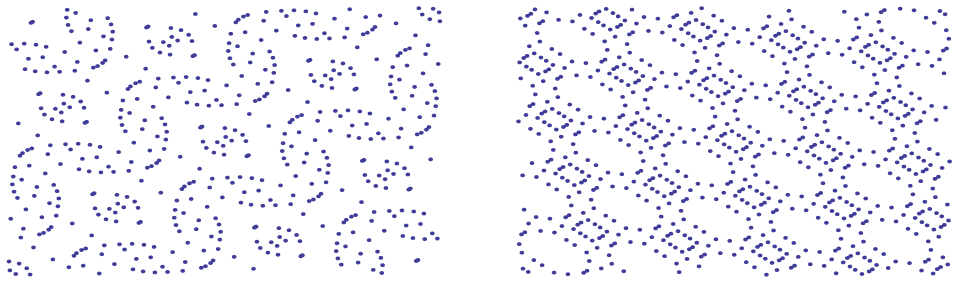

Figure 1: (a) Left: $H_2(51; 2^{10})$. (b) Right: $H_2(1325; 48^2)$.

In the sequel, coordinate sumsets will be the only type of sumset discussed. Hence we may drop the premodifier "coordinate" without fear of confusion. For a relatively prime to n, we define the sumset $S_2(a; n)$, the difference set $D_2(a; n)$, and their reduced counterparts as

$$\begin{aligned} S_2(a;n) &= \{x_1 + x_2 : (x_1, x_2) \in H_2(a;n)\} \\ D_2(a;n) &= \{x_1 - x_2 : (x_1, x_2) \in H_2(a;n)\} \\ \bar{S}_2(a;n) &= \{x_1 + x_2 \bmod n : (x_1, x_2) \in H_2(a;n)\} \\ \bar{D}_2(a;n) &= \{x_1 - x_2 \bmod n : (x_1, x_2) \in H_2(a;n)\}. \end{aligned} \tag{1.3}$$

From a geometric viewpoint, $\#S_2(a; n)$ counts the number of lines of slope -1 that intersect $H_2(a; n)$, and $\#D_2(a; n)$ counts the number of lines of slope 1 that intersect $H_2(a; n)$. When the ratio

$$c_2(a;n) := \#\bar{S}_2(a;n)/\#\bar{D}_2(a;n) \tag{1.4}$$

exceeds 1, we have sum-dominance of $\bar{H}_2(a; n)$.

A d-dimensional modular hyperbola is of the form

$$H_d(a;n) := \{(x_1, \ldots, x_d) : x_1 \cdots x_d \equiv a \bmod n, 1 \le x_1, \ldots, x_d < n\}, \tag{1.5}$$

where $(a, n) = 1$. We define the generalized signed sumset as

$$\bar{S}_d(m; a; n) = \{x_1 \ + \cdots + \ x_m - \cdots - x_d \bmod n : (x_1, \ldots, x_d) \in H_d(a; n)\}, \tag{1.6}$$

where m is the number of plus signs in $\pm x_1 \pm \cdots \pm x_d$. In particular, $\bar{S}_2(1; a; n) = \bar{D}_2(a; n)$ and $\bar{S}_2(2; a; n) = \bar{S}_2(a; n)$.

Modular hyperbolas have been extensively studied; see for example the recent survey by Shparlinski [11]. In particular, when a is not divisible by the prime p, Shparlinski and Winterhof [12] determined that the number of distances $|x-y|$ as (x,y) ranges over all points on the modular hyperbola $H_2(a;p)$ is

$$\frac{1}{4}\left(p+1+\left(\frac{a}{p}\right)\left(1+(-1)^{(p-1)/2}\right)\right). \tag{1.7}$$

In [13], they also found asymptotic formulas for the number of relatively prime points in $H_d(a;n)$.

The goal of this paper is to extend results of [2] to the general two-dimensional modular hyperbolas in (1.2), and to investigate the higher dimensional modular hyperbolas defined in (1.5) (this is a generalization of Question 24 of [11] to arbitrary dimensions and combinations). We prove explicit formulas for the cardinalities of the sumsets $\bar{S}_2(a;n)$ and difference sets $\bar{D}_2(a;n)$ (Theorems 3.3 and 3.6). This allows us to analyze the ratios $c_2(a;n)$ (Theorems 3.8 – 3.12), thus providing conditions on a and n for sum dominance and difference dominance of reduced modular hyperbolas $\bar{H}_2(a;n)$. For example, a special case of Theorem 3.9 shows that if $a=11$ and $n=3^t7^s$ with $t\geq 2$, then $c_2(a;n)>1$, i.e., we have sum dominance. A special case of Theorem 3.12 shows that when a is a fixed power of 4, we have sum dominance for more than 85% of those n relatively prime to a. For $d>2$ and positive integers n whose prime factors all exceed 7, we prove in Theorem 4.1 that $\#\bar{S}_d(m;a;n)=n$. This means that each such generalized sumset consists of all possible values mod n, i.e., all possible sums and differences occur.

2. Counting Preliminaries

In this section we present some counting results that are central to proving our main theorems. Many of these are natural generalizations of results from [2], so we refer the reader to the appendix for detailed proofs.

Throughout this paper, p always denotes a prime. The following proposition reduces the analysis of the cardinalities of $\bar{S}_d(m;a;n)$ to those of $\bar{S}_d(m;a;p^t)$, where p^t is a factor in the canonical factorization of n.

Proposition 2.1. *Let $n=\prod_{i=1}^{k}p_i^{e_i}$ be the factorization of n into distinct prime powers. Then*

$$\#\bar{S}_d(m;a;n) \;=\; \prod_{i=1}^{k}\#\bar{S}_d(m;a;p_i^{e_i}). \tag{2.1}$$

The proof is given in Appendix A.1.

Lemma 2.2 cuts our work in half, as once we understand the sumset we immediately have results for the corresponding difference set.

Lemma 2.2. *We have* $\bar{S}_2(a;n) = \bar{D}_2(-a;n)$.

Proof. We show $\bar{S}_2(a;n) \subseteq \bar{D}_2(-a;n)$; the reverse containment is handled similarly. Let $\tau \in \bar{S}_2(a;n)$. Then there exists $(x_0, y_0) \in H_2(a;n)$ such that $x_0 y_0 \equiv a \bmod n$ and $x_0 + y_0 \equiv \tau \bmod n$. Since $(x_0, n-y_0) \in H_2(-a;n)$ and $\tau \equiv x_0 - (n-y_0) \bmod n$, we see that $\tau \in \bar{D}_2(-a;n)$. □

Lemma 2.3. *We have* $(2k \bmod p^t) \in \bar{D}_2(a;p^t) \Leftrightarrow (k^2+a)$ *is a square modulo* p^t. *The map* $f(k) = 2k \bmod p^t$ *defines a bijection*

$$f : \{k : k^2 + a \text{ is a square mod } p^t, 0 \le k < p^t\} \to \bar{D}_2(a;p^t) \tag{2.2}$$

when $p > 2$. *If* $p = 2$, *then* f *defines a bijection*

$$f : \{k : k^2 + a \text{ is a square mod } 2^t, 0 \le k < 2^{t-1}\} \to \bar{D}_2(a;2^t). \tag{2.3}$$

See Appendix A.2 for the proof. By Lemma 2.2, a similar result for S in place of D follows by replacing a by $-a$.

3. Cardinalities of $\bar{S}_2(a;p^t)$ and $\bar{D}_2(a;p^t)$

In this section we compute the cardinalities of $\bar{S}_2(a;p^t)$ and $\bar{D}_2(a;p^t)$. We then give conditions on a and n for sum dominance and difference dominance of $\bar{H}_2(a;n)$.

3.1. Case 1: $p = 2$

We isolate a useful result that we need for the proof of the next lemma. For a proof, see Proposition A.2 in the Appendix.

Proposition 3.1 (Gauss [4]). *For* $t \ge 1$, *any integer of the form* $4^k(8n+1)$ *is a square modulo* 2^t.

The next result is used in investigating some of the cases of Theorem 3.3.

Lemma 3.2. *Write* $m = 4b + r$ *with* $0 \le r \le 3$. *For* $t \ge 5$, $k^2 + 3 + 8m$ *is a square* $\bmod 2^t$ *if and only if* $k \equiv \pm(4r+1) \bmod 16$.

Proof. We only prove the case $r = 0$, as the other proofs are similar. First assume that $k^2 + 3 + 8m$ is a square mod 2^t. Reducing mod 32, we have that $k^2 + 3 + 8m \equiv k^2 + 3 \bmod 32$, which implies that $k \equiv \pm 1 \bmod 16$. Conversely, assume that $k = 16l \pm 1$ for some $l \in Z$. Then $k^2 + 3 + 8m = (16l \pm 1)^2 + 3 + 8(4b) = 256l^2 \pm 32l + 4 + 32b = 4(8(8l^2 \pm l + b) + 1)$. Hence, by Proposition 3.1, $k^2 + 3 + 8m$ is a square mod 2^t. □

Theorem 3.3. *For $t \geq 5$,*

$$\begin{aligned} \#\bar{D}_2(a;2^t) &= \begin{cases} \frac{2^{t-4}}{3} + \frac{(-1)^{t-1}}{3} + 3 & a \equiv 7 \bmod 8 \\ 2^{t-3} & a \equiv 1,5 \bmod 8 \\ 2^{t-4} & a \equiv 3 \bmod 8 \end{cases} \\ \#\bar{S}_2(a;2^t) &= \begin{cases} \frac{2^{t-4}}{3} + \frac{(-1)^{t-1}}{3} + 3 & a \equiv 1 \bmod 8 \\ 2^{t-3} & a \equiv 3,7 \bmod 8 \\ 2^{t-4} & a \equiv 5 \bmod 8. \end{cases} \end{aligned} \tag{3.1}$$

Moreover, $\#\bar{S}_2(a;16) = 2$ for all a, and when $t \leq 3$, we have $\#\bar{S}_2(a;2^t) = 1$ with the exception that $\#\bar{S}_2(a;8) = 2$ when $a \equiv 1 \bmod 4$.

Proof. The claim for $t \leq 4$ can be checked by direct calculation, so assume $t \geq 5$. By Lemma 2.2, it is enough to prove the claims about $\#\bar{D}_2(a;2^t)$ when $a \equiv 1,3,5 \bmod 8$, and about $\#\bar{S}_2(a;2^t)$ when $a \equiv 1 \bmod 8$.

We refer to the Appendix A.3 for the proofs of the results for $\bar{D}_2(a;2^t)$ when $a \equiv 1,5 \bmod 8$ and for $\bar{S}_2(a;2^t)$ when $a \equiv 1 \bmod 8$. It remains to prove the result for the difference set when $a \equiv 3 \bmod 8$. Write $a = 3 + 8m$. We consider only the case where $m \equiv 0 \bmod 4$, since the cases $m \equiv 1,2,3 \bmod 4$ are proved similarly and lead to the same result. By Lemma 3.2, we see that if $m \equiv 0 \bmod 4$, then

$$\begin{aligned} &\#\{k : k^2 + 3 + 8m \text{ is a square } \bmod 2^t,\ 0 \leq k < 2^{t-1}\} \\ &\quad = \#\{1 + 16l : 0 \leq l < 2^{t-5}\} + \#\{15 + 16l : 0 \leq l < 2^{t-5}\} = 2^{t-4}. \end{aligned} \tag{3.2}$$

By Lemma 2.3, we know

$$\#\bar{D}(a;2^t) = \#\{k : k^2 + 3 + 8m \text{ is a square mod } 2^t,\ 0 \leq k < 2^{t-1}\}. \tag{3.3}$$

Hence $\#\bar{D}_2(a;2^t) = 2^{t-4}$. □

3.2. Case 2: $p > 2$

For this subsection, we adopt the following notation from [2]:

$$\begin{aligned} S_2'(a;p^t) &= \{k \bmod p^t : k^2 - a \text{ is a square mod } p^t,\ p \nmid (k^2 - a)\} \\ S_2''(a;p^t) &= \{k \bmod p^t : k^2 - a \text{ is a square mod } p^t,\ p|(k^2 - a)\}. \end{aligned} \tag{3.4}$$

By Lemma 2.3,

$$\#\bar{S}_2(a;p^t) = \#S_2'(a;p^t) + \#S_2''(a;p^t). \tag{3.5}$$

Lemma 3.4. *Let p be an odd prime. Then*

$$\#\bar{S}_2'(a;p^t) = \begin{cases} \frac{(p-1)p^{t-1}}{2} & \left(\frac{a}{p}\right) = -1 \\ \frac{(p-3)p^{t-1}}{2} & \left(\frac{a}{p}\right) = 1. \end{cases} \tag{3.6}$$

See Appendix A.4 for the proof.

Lemma 3.5. *Let p be an odd prime. If $\left(\frac{a}{p}\right) = -1$, then $\#S_2''(a;p^t) = 0$ and thus $\#S_2(a;p^t) = \frac{\phi(p^t)}{2}$. If $\left(\frac{a}{p}\right) = 1$,*

$$\#S_2''(a;p^t) \;=\; \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-1}(p-1)}{2(p+1)}. \tag{3.7}$$

See Appendix A.5 for the proof.

Theorem 3.6. *For $t \geq 1$ and $p > 2$,*

$$\begin{aligned}
\#\bar{S}_2(a,p^t) \quad &= \quad \begin{cases} \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-1}(p-1)}{2(p+1)} & \left(\frac{a}{p}\right) = 1 \\ \frac{\phi(p^t)}{2} & \left(\frac{a}{p}\right) = -1 \end{cases} \\
\#\bar{D}_2(a,p^t) \quad &= \quad \begin{cases} \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-1}(p-1)}{2(p+1)} & p \equiv 1 \bmod 4, \left(\frac{a}{p}\right) = 1 \\ \frac{\phi(p^t)}{2} & p \equiv 1 \bmod 4, \left(\frac{a}{p}\right) = -1 \\ \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-1}(p-1)}{2(p+1)} & p \equiv 3 \bmod 4, \left(\frac{a}{p}\right) = -1 \\ \frac{\phi(p^t)}{2} & p \equiv 3 \bmod 4, \left(\frac{a}{p}\right) = 1. \end{cases}
\end{aligned} \tag{3.8}$$

Proof. The result follows from Lemmas 3.4, 3.5, and 2.2. □

Corollary 3.7. *For $p \equiv 1 \bmod 4$, $c_2(a;p^k) = 1$.*

3.3. Ratios for $d = 2$

Now that we have explicit formulas for the cardinalities of the sum and difference sets, the next natural object to study is the ratio $c_2(a;n)$ of the size of the sumset to the size of the difference set. By Corollary 3.7, we only need to consider the prime factors of n which are congruent to 3 mod 4, since the primes which are congruent to 1 mod 4 do not change $c_2(a;n)$. When $p \equiv 3 \bmod 4$, it is sufficient to evaluate $c_2(a;p^t)$ in the case when $\left(\frac{a}{p}\right) = 1$, since $c_2(-a;p^t)$ is the reciprocal of $c_2(a;p^t)$.

Theorem 3.8. *For $p \equiv 3 \bmod 4$ and $\left(\frac{a}{p}\right) = 1$,*

$$c_2(a;p^t) \;=\; 1 - 2\sum_{i=0}^{[t/2]-1} \frac{1}{p^{2i+1}} \;+ \frac{2}{\phi(p^t)}. \tag{3.9}$$

Proof. By Theorem 3.6,

$$\begin{aligned}
c_2(a;p^t) \quad &= \quad \left(\frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-1}(p-1)}{2(p+1)}\right) \frac{1}{\phi(p^t)/2} \\
&= \quad \frac{p^2-2p-1}{p^2-1} + \frac{(-1)^{t-1}(p-1)+3p+3}{(p+1)\phi(p^t)}.
\end{aligned} \tag{3.10}$$

Therefore

$$\begin{aligned} c_2(a;p^t) - 1 - \frac{2}{\phi(p^t)} &= \frac{-2p}{p^2-1} + \frac{(-1)^{t-1}(p-1)+p+1}{(p+1)\phi(p^t)} \\ &= \frac{-2p}{p^2-1} + 2\sum_{[t/2]}^{\infty} \frac{1}{p^{2i+1}} = -2\sum_{i=0}^{[t/2]-1} \frac{1}{p^{2i+1}}. \quad (3.11) \end{aligned}$$

□

Theorem 3.9. *Let $p < q$ be primes, both congruent to* 3 mod 4*, and let $s, t \geq 2$. If a is a square* mod p*, then $c_2(a; p^t q^s) < 1$, so we have difference dominance. If a is not a square* mod p*, then $c_2(a; p^t q^s) > 1$, so we have sum dominance.*

Proof. It suffices to prove the first assertion, for then the second will follow by taking the reciprocal. By Theorem 3.8, $c_2(a; p^t) < 1$. If a is a square mod q, then also $c_2(a; q^s) < 1$, so that $c_2(a; p^t q^s) = c_2(a; p^t) c_2(a; q^s) < 1$, as desired. Finally, assume that a is not a square mod q. Then it remains to show that $c_2(-a; q^s) > c_2(a; p^t)$. By Theorem 3.8, $c_2(a; p^t)$ is monotone decreasing in t. Therefore it suffices to show that $\lim_{s\to\infty} c_2(-a; q^s) > c_2(a; p^2)$. This inequality is equivalent to $1 - 2q/(q^2-1) > 1 - (2p-4)/(p^2-p)$, so we must show that $(p-2)/(p^2-p) > q/(q^2-1)$. Since the right member is a decreasing function of q, it suffices to prove this inequality when $q = p+4$, and this is easily accomplished. □

It is not hard to show that the conclusion of Theorem 3.9 still holds in the case $s = 1$, $t \geq 2$. However, the inequalities are reversed in the case $t = 1$, $s \geq 1$.

As the next three theorems are straightforward generalizations of results from [2], we omit the proofs.

Theorem 3.10. *Let $N_k = \prod_{i=1}^{k} p_i$, where p_i is the i^{th} prime that is congruent to* 3 *modulo* 4*. Fix a perfect square a relatively prime to all of the p_i. Then*

$$c_2(a; N_k) \asymp \log\log N_k, \quad (3.12)$$

and for any $t \geq 2$,

$$c_2(a; N_k^t) \asymp (\log\log N_k)^{-1}. \quad (3.13)$$

Theorem 3.11. *Fix an integer a. Let n run through the positive integers relatively prime to a. Then*

$$(1) \qquad \frac{1}{\log\log n} \ll c_2(a; n) \ll \log\log n, \quad (3.14)$$

$$(2) \qquad \limsup_{n\to\infty} c_2(a; n) = \infty \quad \text{and} \quad \liminf_{n\to\infty} c_2(a; n) = 0, \quad (3.15)$$

$$(3) \qquad \limsup_{n\to\infty} \frac{\#S(a;n)}{\#D(a;n)} = \infty \quad \text{and} \quad \liminf_{n\to\infty} \frac{\#S(a;n)}{\#D(a;n)} = 0. \quad (3.16)$$

Theorem 3.12. *For a fixed nonzero integer a, let E_a denote the set of positive integers n relatively prime to a such that $\left(\frac{a}{p}\right) = 1$ for every prime $p \equiv 3 \bmod 4$ dividing n. Let $C_a(L) = \{n \in E_a : c_2(a;n) > L\}$. Define $E_a(x) = \{n \in E_a : n \le x\}$ and $C_a(L,x) = \{n \in C_a(L) : n \le x\}$. Then the lower density of $C_a(L)$ in E_a, defined by $\liminf \#C_a(L,x)/\#E_a(x)$, satisfies the inequality*

$$\liminf_{x\to\infty} \frac{\#C_a(1,x)}{\#E_a(x)} \ge K_a \prod \left(1 - \frac{1}{p^2}\right), \tag{3.17}$$

where the product is over all primes $p \equiv 3 \bmod 4$ for which $\left(\frac{a}{p}\right) = 1$, and where

$$K_a = \begin{cases} 1 & a \equiv 0 \bmod 2 \\ 63/64 & a \equiv 1 \bmod 8 \\ 31/32 & a \equiv 5 \bmod 8 \\ 15/16 & a \equiv 3 \bmod 4. \end{cases} \tag{3.18}$$

Furthermore, for any constant $L > 0$, the lower density of $C_a(L)$ in E_a is positive.

For example, if a is an odd power of 2, then the lower density in (3.17) exceeds 97%. Note that if the condition $\left(\frac{a}{p}\right) = 1$ is replaced by $\left(\frac{a}{p}\right) = -1$ throughout the statement of Theorem 3.12, then by Lemma 2.2, (3.17) holds with the inequality $c_2(a;n) > 1$ replaced by $c_2(a;n) < 1$.

4. Cardinality of $\bar{S}_d(m;a;n)$ for $d > 2$

We now turn our attention to modular hyperbolas with higher dimension ($d > 2$). Suppose that $p > 7$ for every prime p dividing n. Then Theorem 4.1 shows that the higher dimensional generalized sumsets $\bar{S}_d(m;a;n)$ all have cardinality n. In particular, this cardinality is the same for every value of m, i.e., there is no dependence on the number of plus and minus signs.

Theorem 4.1. *If the prime factors of n all exceed 7, then $\#\bar{S}_d(m;a;n) = n$.*

Proof. Let $q = p^t$ for a prime $p > 7$. By Proposition 2.1, it suffices to prove that $\#\bar{S}_d(m;a;q) = q$. We will show that for every a coprime to q and every $b \bmod q$, the system of congruences

$$\begin{aligned} x_1 + \cdots + x_d &\equiv b \bmod q \\ x_1 \cdots x_d &\equiv a \bmod q \end{aligned} \tag{4.1}$$

has a solution. This suffices, because x_i could be replaced by $q - x_i$ for any collection of subscripts i. If (4.1) can always be solved for $d = 3$, then it can always be solved for any $d > 3$, by setting $x_i = 1$ for $i > 3$. Thus assume that $d = 3$.

Solving (4.1) is equivalent to solving the congruence $xy(b-x-y) \equiv a \bmod q$ for $x, y \in (\mathbb{Z}/q\mathbb{Z})^*$. Replacing y by y^{-1} and then multiplying by y, we see that this is equivalent to solving

$$x^2 + x(y^{-1} - b) + ay \equiv 0 \bmod q. \tag{4.2}$$

The quadratic polynomial in x in (4.2) has discriminant

$$(-4ay^3 + b^2y^2 - 2by + 1)/y^2. \tag{4.3}$$

Let $R(y) \in (\mathbb{Z}/p\mathbb{Z})[y]$ denote the cubic polynomial in y obtained by reducing the numerator in (4.3) mod$p$. To solve (4.2), it remains to show that there exists $y \in (\mathbb{Z}/p\mathbb{Z})^*$ for which $R(y)$ is a non-zero square mod p; this is because a non-zero square mod p is also a square mod q (see Proposition A.2 in the Appendix).

Suppose for the purpose of contradiction that no term in the sum

$$\sum_{y=1}^{p-1} \left(\frac{R(y)}{p}\right) \tag{4.4}$$

is equal to 1. Then since $R(y)$ has at most 3 zeros in $(\mathbb{Z}/p\mathbb{Z})^*$, we have

$$S \;:=\; \sum_{y=0}^{p-1} \left(\frac{R(y)}{p}\right) = w - p, \tag{4.5}$$

for some $w \in \{1, 2, 3, 4\}$.

Let D denote the discriminant of $R(y)$. Then $D \equiv 16a(b^3 - 27a) \bmod p$, and so D vanishes if and only if $a \equiv (b/3)^3 \bmod p$. When D vanishes, it follows that $b \in (\mathbb{Z}/p\mathbb{Z})^*$ and $y = 3/(4b)$ is a simple zero of $R(y)$. We conclude that $R(y)$ cannot equal a constant times the square of a polynomial in $(\mathbb{Z}/p\mathbb{Z})[y]$. Therefore (see equation (6.0.2) in [1]) we can apply Weil's bound to conclude that $|S| < 2\sqrt{p}$. Together with (4.5), this yields

$$p - 2\sqrt{p} \;<\; w \;\leq\; 4, \tag{4.6}$$

which contradicts the fact that $p > 7$. □

We remark that the conditions $p > 7$ cannot be weakened in Theorem 4.1. For example, (4.2) has no solution when $p = q = 2$, $b = 0$ and $a = 1$; when $p = q = 3$ and $b = a = 1$; when $p = q = 5$, $b = 1$ and $a = 2$; and when $p = q = 7$, $b = 0$ and $a = 3$.

5. Conclusion and Future Research

We generalized work of [2] on the modular hyperbola $H_2(1, n)$ by examining more general modular hyperbolas $H_d(a; n)$. The two-dimensional case ($d = 2$) provided

interesting conditions on a and n for sum dominance and difference dominance. On the other hand, for higher dimensions ($d > 2$), all possible sums and differences are realized when the prime factors of n all exceed 7.

The following are some topics for future and ongoing research:

1. We can study the cardinality of sumsets and difference sets of the intersection of modular hyperbolas with other modular objects such as lower dimensional modular hyperbolas and modular ellipses. See [3] for work on the cardinality of the intersection of modular circles and $H_2(1; n)$.

2. Extend Theorem 3.9 by estimating $c_2(a; n)$ in cases where n has more than two prime factors of the form $4k + 3$.

3. Extend Theorem 4.1 by finding the cardinality of the generalized higher dimensional sumsets in cases where $(n, 210) > 1$.

4. In higher dimensions ($d > 2$), nearly every sum and difference is realized for $\bar{H}_d(a; n)$. The situation becomes more interesting if we replace $\bar{H}_d(a; n)$ by a random subset chosen according to some probability distribution depending on d. If S and D denote the corresponding sumset and difference set, we can then compare the random variables $\#S$ and $\#D$.

A. Additional Proofs

The following proofs are a natural extension of the proofs given by [2], and are included for completeness.

A.1. Proof of Proposition 2.1

Proof of Proposition 2.1. Consider

$$g : \bar{S}_d(m; a; n) \longrightarrow \prod_{i=1}^{k} \bar{S}_d(m; a \bmod p_i^{e_i}; p_i^{e_i}) \tag{A.1}$$

defined by

$$g(x) \;=\; (x \bmod p_1^{e_1}, \ldots, x \bmod p_k^{e_k}). \tag{A.2}$$

We claim g is a bijection.

To show g is injective, suppose $g(x) = g(y)$. Then we have $x \equiv y \bmod p_i^{e_i}$ for $i = 1, \ldots, k$. Thus, by the Chinese Remainder Theorem, $x \equiv y \bmod n$, so g is injective.

To show g is surjective, let $(\alpha_1, \ldots, \alpha_k) \in \prod_{i=1}^{k} \bar{S}_d(m; a \bmod p_i^{e_i}; p_i^{e_i})$. Then, for each $i \in \{1, \ldots, k\}$, there exists $(x_1(i), \ldots, x_d(i)) \in H_d(a; p_i^{e_i})$ such that

$$x_1(i) + \cdots + x_m(i) - \cdots - x_d(i) \equiv \alpha_i \bmod p_i^{e_i}.$$

By the Chinese Remainder Theorem, for each fixed r with $1 \leq r \leq d$, the system of congruences

$$x \equiv x_r(i) \bmod p_i^{e_i}, \quad (1 \leq i \leq k) \tag{A.3}$$

has a unique solution $x_r \bmod n$. Since $x_1(i) \cdots x_d(i) \equiv a \bmod p_i^{e_i}$ for all $i \in \{1, \ldots, k\}$, we have $x_1 \cdots x_d \equiv a \bmod n$. Thus $g(x_1 + \cdots + x_m - \cdots - x_d \bmod n) = (\alpha_1, \ldots, \alpha_k)$, so g is a bijection, which completes the proof. □

A.2. Proof of Lemma 2.3

Before proving Lemma 2.3, we state a useful lemma that is a simple observation and immediate generalization of a result from [2].

Lemma A.1. *Let $(x_0, y_0) \in H_2(a; p^t)$. Then $x_0 - y_0 \equiv 2k \bmod p^t$ for some $k \in \mathbb{Z}$.*

Proof. If $p = 2$, then x_0 and y_0 are both odd since they are coprime to p^t, so their difference is even. If $p \neq 2$, then 2^{-1} exists mod p^t, so $x_0 - y_0 \equiv 2k \bmod p^t$ has a solution k. □

Proof of Lemma 2.3. Let $(x_0, y_0) \in \bar{H}_2(a; p^t)$ so that $x_0 - y_0 \in \bar{D}_2(a; p)$. When $x_0 - y_0 \equiv 2k \bmod p^t$, we have $k^2 + a \equiv (x_0 - k)^2 \bmod p^t$, so that $k^2 + a$ is a square mod p^t.

Conversely, suppose $k^2 + a$ is a square mod p^t. Then there exists $c \in \mathbb{Z}$ such that $c^2 - k^2 \equiv a \bmod p^t$. It follows that

$$(x_0, y_0) := ((c + k) \bmod p^t, (c - k) \bmod p^t) \in \bar{H}_2(a; p^t)$$

and $x_0 - y_0 \equiv 2k \bmod p^t$.

Next we show that f is a bijection. If $p > 2$, then the inverse of the function f is $f^{-1}(x) = 2^{-1}x \bmod p^t$. Now suppose $p = 2$. Clearly f is injective, since $2k \equiv 2j \bmod 2^t$ implies $k \equiv j \bmod 2^{t-1}$. To show f is surjective, let $\tau \in \bar{D}_2(a; 2^t)$, so that there exists $(x_0, y_0) \in \bar{H}_2(a; 2^t)$ such that $x_0 - y_0 \equiv \tau \bmod 2^t$. Then by Lemma A.1, $\tau \equiv 2k \bmod 2^t$ for some $k \in \mathbb{Z}$ with $0 \leq k < 2^{t-1}$, so $f(k) = \tau$. □

A.3. Proof of Theorem 3.3

To prove the required cases of Theorem 3.3, we will need the following two propositions. The first proposition is from [5] (see page 46). It gives us a quick way to count squares modulo prime powers.

Proposition A.2. *Let a be an integer not divisible by the prime p. Then we have*

1. *If $p \neq 2$ and the congruence $x^2 \equiv a \bmod p$ is solvable, then for every $t \geq 1$ the congruence $x^2 \equiv a \bmod p^t$ is solvable with precisely two distinct solutions.*
2. *If $p = 2$ and the congruence $x^2 \equiv a \bmod 2^3$ is solvable, then for every $t \geq 3$ the congruence $x^2 \equiv a \bmod 2^t$ is solvable with precisely four distinct solutions.*

Proposition A.3 (Stangl [14]). *Let p be an odd prime. Then*

$$\#\{k^2 \bmod p^t\} = \tfrac{p^{t+1}}{2(p+1)} + (-1)^{t-1}\tfrac{p-1}{4(p+1)} + \tfrac{3}{4}.$$

For the prime 2, we have

$$\#\{k^2 \bmod 2^t\} = \tfrac{2^{t-1}}{3} + \tfrac{(-1)^{t-1}}{6} + \tfrac{3}{2}.$$

Proof of Theorem 3.3 cases. We now prove the remaining cases of the theorem.
Case 1: Difference set for $a \equiv 1 \bmod 8$. By Proposition 2.3 with $a = 8m+1$,

$$\#\bar{D}(a; 2^t) \;=\; \#\{k : k^2 + 1 + 8m \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\}. \tag{A.4}$$

We claim that

$$k^2 + 1 + 8m \text{ is a square mod } 2^t \;\Leftrightarrow\; k = 4l \text{ for some } l \in \mathbb{Z}. \tag{A.5}$$

First assume that k^2+1+8m is a square mod 2^t. Then k^2+1 is a square mod 8, which yields $k \equiv 0, 4 \bmod 8$. Hence $k = 4l$ for some $l \in \mathbb{Z}$.

Conversely, assume that $k = 4l$ for some $l \in \mathbb{Z}$. We want to show that $(4l)^2+1+8m$ is a square mod 2^t. Reducing modulo 8 gives us $(4l)^2+1+8m \equiv 1 \bmod 8$, which is a square modulo 8. Hence, by the second part of Proposition A.2, $(4l)^2+1+8m$ is a square mod 2^t. Thus

$$\{k : k^2 + 1 + 8m \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\} \;=\; \{4l : 0 \leq l < 2^{t-3}\}. \tag{A.6}$$

Case 2: Difference set for $a \equiv 5 \bmod 8$. We show that

$$k^2 + 5 + 8m \text{ is a square mod } 2^t \;\Leftrightarrow\; k = 2 + 4l \text{ for some } l \in \mathbb{Z}. \tag{A.7}$$

First assume that k^2+5+8m is a square mod 2^t. Then k^2+5+8m is a square mod 8, which implies $k \equiv 2, 6 \bmod 8$ or $k = 2 + 4l$ for some $l \in \mathbb{Z}$.

Conversely, assume that $k = 2 + 4l$ for some $l \in \mathbb{Z}$. Reducing modulo 8 gives us $k^2 + 5 + 8m \equiv 1 \bmod 8$, which is a square modulo 8. Hence, by the second part of Proposition A.2, $k^2 + 5 + 8m$ is a square mod 2^t. We conclude that

$$\{k : k^2+5+8m \text{ is a square mod } 2^t, 0 \leq k < 2^{t-1}\} \;=\; \{2+4l : 0 \leq l < 2^{t-3}\}. \tag{A.8}$$

Case 3: Sum set for $a \equiv 1 \bmod 8$. In view of Proposition A.3, it suffices to show that

$$\#\{k : k^2 - a \text{ is a square mod } 2^t, 0 \le k < 2^{t-1}\} \;=\; 2\#\{k^2 \bmod 2^{t-4}\}. \qquad \text{(A.9)}$$

If $k^2 - a$ is a square mod 2^t then k must be odd, since $-a$ is not a square mod 4. The equality (A.9) is equivalent to

$$\#\{k : k^2 - a \text{ is a square mod } 2^t, 0 < k < 2^{t-2}, 2 \nmid k\} \;=\; \#\{k^2 \bmod 2^{t-4}\}, \quad \text{(A.10)}$$

since $k^2 - a \bmod 2^t$ has the same value when k is replaced by $2^{t-1} - k$. The left member of (A.10) equals the number of (distinct) squares modulo 2^t of the form $k^2 - a \bmod 2^t$. Any square divisible by 8 is also divisible by 16, so the left member of (A.10) also equals the number of squares modulo 2^{t-4} of the form $(k^2 - a)/16 \bmod 2^{t-4}$. It remains to show that every square modulo 2^{t-4} has the form $(k^2 - a)/16 \bmod 2^{t-4}$, i.e., that $16u^2 + a$ is a square modulo 2^t for every integer u. This follows from the second part of Proposition A.2. □

A.4. Proof of Lemma 3.4

Proof of Lemma 3.4. If $l \in S_2'(a; p^t)$, then $\left(\frac{l^2-a}{p}\right) = 1$. Thus

$$\begin{aligned}
\#S_2'(a;p^t) &= \frac{1}{2} \sum_{\substack{l=0 \\ (l^2-a,p)=1}}^{p^t-1} \left(\left(\frac{l^2-a}{p}\right)+1\right) \\
&= \frac{1}{2} \sum_{k=0}^{p^{t-1}-1} \sum_{\substack{l=0 \\ l^2 \neq a \bmod p}}^{p-1} \left(\left(\frac{(l+kp)^2-a}{p}\right)+1\right) \\
&= \left(\sum_{\substack{l=0 \\ l^2 \neq a \bmod p}}^{p-1} \left(\left(\frac{l^2-a}{p}\right)+1\right)\right) \frac{p^{t-1}}{2} \\
&= \left(-1 + \sum_{\substack{l=0 \\ l^2 \neq a \bmod p}}^{p-1} 1\right) \frac{p^{t-1}}{2}, \qquad \text{(A.11)}
\end{aligned}$$

as (see for example page 63 of [5])

$$\sum_{i=0}^{p-1} \left(\frac{i^2-a}{p}\right) = -1. \qquad \text{(A.12)}$$

Substituting

$$\sum_{\substack{l=0 \\ l^2 \neq a \bmod p}}^{p-1} 1 = \begin{cases} p-2 & \left(\frac{a}{p}\right) = 1 \\ p & \left(\frac{a}{p}\right) = -1 \end{cases} \qquad \text{(A.13)}$$

into (A.11) gives us the desired result. □

A.5. Proof of Lemma 3.5

Proof. If $\left(\frac{a}{p}\right) = -1$, then the congruence $x^2 - a \equiv 0 \bmod p$ has no solutions, so $\#S_2''(a;p^t) = 0$. Now assume that $\left(\frac{a}{p}\right) = 1$. It is easily seen that $\#S_2''(a;p^t) = 2$ when $t = 1$ or $t = 2$, so let $t \geq 3$.

By Proposition A.3, it suffices to prove that

$$\#S_2''(a;p^t) = 2\#\{m^2 \bmod p^{t-2}\}. \tag{A.14}$$

Note that (A.14) is equivalent to

$$\#\{k : k^2 - a \text{ is a square mod } p^t, 0 < k < p^t/2, p \mid (k^2 - a)\} \;=\; \#\{m^2 \bmod p^{t-2}\}. \tag{A.15}$$

The left member of (A.15) also equals the number of squares modulo p^{t-2} of the form $(k^2 - a)/p^2 \bmod p^{t-2}$. It remains to show that every square modulo p^{t-2} has the form $(k^2 - a)/p^2 \bmod p^{t-2}$, i.e., that $p^2u^2 + a$ is a square modulo p^t for every integer u. This follows from the first part of Proposition A.2. □

References

[1] B. Berndt, R. Evans and K. Williams, *Gauss and Jacobi Sums*, Canadian Mathematical Society Series of Monographs and Advanced Texts, John Wiley & Sons, New York, 1998.

[2] D. Eichhorn, M. R. Khan, A. H. Stein and C. L. Yankov, *Sums and Differences of the Coordinates of Points on Modular Hyperbolas*, Integers **9** (2009), #A3.

[3] S. Hanrahan and M. R. Khan, *The cardinality of the value sets modulo n of $x^2 + x^{-2}$ and $x^2 + y^2$*, Involve **3** (2010), no. 2, 171–182.

[4] C.F. Gauss, *Disquisitiones Arithmeticae*, Art. 103.

[5] K. Ireland and M. Rosen, *A classical Introduction to Modern Number Theory*, second edition, Graduate Texts in Mathematics, Springer-Verlag, New York, 2010.

[6] G. Iyer, O. Lazarev, S. J. Miller and L. Zhang, *Generalized More Sums Than Differences Sets*, J. Number Theory **132** (2012), no. 5, 1054–1073.

[7] G. Martin and K. O'Bryant, *Many sets have more sums than differences*, in Additive Combinatorics, CRM Proc. Lecture Notes, vol. 43, AMS, Providence, RI, 2007, pp. 287-305.

[8] S. J. Miller, B. Orosz and D. Scheinerman, *Explicit constructions of infinite families of MSTD sets*, J. Number Theory **130** (2010) 1221–1233.

[9] S. J. Miller, S. Pegado and S. L. Robinson, *Explicit constructions of infinite families of generalized MSTD sets*, Integers **12** (2012), #A30.

[10] S. J. Miller and K. Vissuet, *Most sets are balanced in finite groups*, preprint.

[11] I. E. Shparlinski, *Modular hyperbolas*, Jap. J. Math **7** (2012), 235–294.

[12] I. E. Shparlinski and A. Winterhof, *On the number of distances between the coordinates of points on modular hyperbolas*, J. Number Theory **128** (2008), no. 5, 1224–1230.

[13] I. E. Shparlinski and A. Winterhof, *Visible points on multidimensional modular hyperbolas*, J. Number Theory **128** (2008), no. 9, 2695–2703.

[14] W. Stangl, *Counting squares in* $\mathbb{Z}_n$, Math. Mag. **69** (1996), 285–289.

[15] Y. Zhao, *Constructing MSTD Sets Using Bidirectional Ballot Sequences*, J. Number Theory **130** (2010), no. 5, 1212–1220.

[16] Y. Zhao, *Sets Characterized by Missing Sums and Differences*, J. Number Theory **131** (2011), 2107–2134.