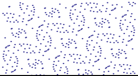
Generalized Sum and Difference Sets and *d*-dimensional Modular Hyperbolas

Amanda Bower[1] and Victor D. Luo[2]
Joint with: Steven J. Miller[2] and Ron Evans[3]

[1]U. of Michigan-Dearborn [2]Williams College [3]U. of California-San Diego

AMS Session on Undergraduate Research in Combinatorics and Number Theory
Joint Math Meetings
San Diego, California, January 12, 2013

http://web.williams.edu/Mathematics/sjmiller/public_html/jmm2013.html



Introduction

Let $A \subseteq \mathbb{N} \cup \{0\}$.

Definition

Sumset: $A + A = \{x + y : x, y \in A\}$

Introduction

Let $A \subseteq \mathbb{N} \cup \{0\}$.

Definition

Sumset: $A + A = \{x + y : x, y \in A\}$

Example: if $A = \{1, 2, 5\}$, then

$$A + A = \{2, 3, 4, 6, 7, 10\}.$$

Introduction

Let $A \subseteq \mathbb{N} \cup \{0\}$.

Definition

Sumset: $A + A = \{x + y : x, y \in A\}$

Example: if $A = \{1, 2, 5\}$, then

$$A + A = \{2, 3, 4, 6, 7, 10\}.$$

Why study sumsets?

Introduction

Let $A \subseteq \mathbb{N} \cup \{0\}$.

Definition

Sumset: $A + A = \{x + y : x, y \in A\}$

Example: if $A = \{1, 2, 5\}$, then

$$A + A = \{2, 3, 4, 6, 7, 10\}.$$

Why study sumsets?

- Goldbach's conjecture: $\{4, 6, 8, \cdots\} \subseteq P + P$.

Introduction

Let $A \subseteq \mathbb{N} \cup \{0\}$.

Definition

Sumset: $A + A = \{x + y : x, y \in A\}$

Example: if $A = \{1, 2, 5\}$, then

$$A + A = \{2, 3, 4, 6, 7, 10\}.$$

Why study sumsets?

- Goldbach's conjecture: $\{4, 6, 8, \cdots\} \subseteq P + P$.
- Fermat's last theorem: let A_n be the nth powers and then ask if $(A_n + A_n) \cap A_n = \emptyset$ for all $n > 2$.

Introduction

Let $A \subseteq \mathbb{N} \cup \{0\}$.

Definition

Sumset: $A + A = \{x + y : x, y \in A\}$

Example: if $A = \{1, 2, 5\}$, then

$$A + A = \{2, 3, 4, 6, 7, 10\}.$$

Why study sumsets?

- Goldbach's conjecture: $\{4, 6, 8, \cdots\} \subseteq P + P$.
- Fermat's last theorem: let A_n be the nth powers and then ask if $(A_n + A_n) \cap A_n = \emptyset$ for all $n > 2$.
- Twin prime conjecture: $P - P$ contains 2 infinitely often.

Motivation

- Martin and O'Bryant '07: positive percentage are sum-dominant.
  - Note $x + y = y + x$ but $x - y \neq y - x$.

Motivation

- Martin and O'Bryant '07: positive percentage are sum-dominant.
  - Note $x + y = y + x$ but $x - y \neq y - x$.

- Several ways to see new behavior usually dwarfed by large size of typical random set.

Motivation

- Martin and O'Bryant '07: positive percentage are sum-dominant.
  - Note $x + y = y + x$ but $x - y \neq y - x$.
- Several ways to see new behavior usually dwarfed by large size of typical random set.
- Can choose elements equally with probability tending to 0, or can choose sets with great structure.

Goals

- Eichhorn, Khan, Stein, and Yankov [EKSY] studied modular hyperbolas:

$$xy \equiv 1 \bmod n.$$

Goals

- Eichhorn, Khan, Stein, and Yankov [EKSY] studied modular hyperbolas:

$$xy \equiv 1 \bmod n.$$

- Generalize to:
  - $xy \equiv a \bmod n$.
  - higher dimensions: $x_1 \cdots x_k \equiv a \bmod n$.
  - various sum sets and difference sets $(\pm A \pm A \pm A \pm \cdots \pm A)$.

Goals

- Eichhorn, Khan, Stein, and Yankov [EKSY] studied modular hyperbolas:

$$xy \equiv 1 \bmod n.$$

- Generalize to:
  - $xy \equiv a \bmod n$.
  - higher dimensions: $x_1 \cdots x_k \equiv a \bmod n$.
  - various sum sets and difference sets ($\pm A \pm A \pm A \pm \cdots \pm A$).
- Discuss tools and techniques.

Pictures

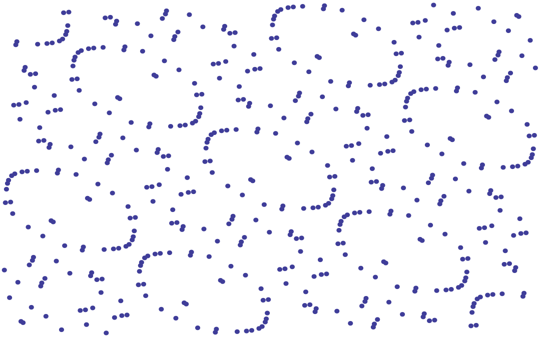


Figure: $xy \equiv 197 \bmod 2^{10}$

Pictures

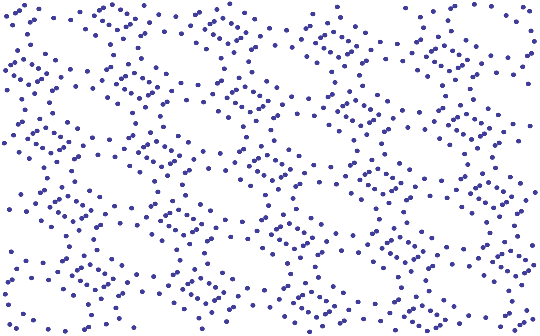


Figure: $xy \equiv 1325 \bmod 48^2$

Sums and Differences of the Coordinates of Points on Modular Hyperbolas

Dennis Eichhorn, Mizan R. Khan, Alan H. Stein, and Christian L. Yankov

Modular Hyperbolas

Definition (Modular Hyperbola)

Let a be coprime to n. A d-dimensional modular hyperbola is

$$H_d(a;n) = \{(x_1, x_2, \cdots, x_d) : x_1 \cdots x_d \equiv a \bmod n, 1 \leq x_i < n)\}.$$

[ESKY] studied $H_2(1;n)$.

Notation

We utilize the following notation:

$$\bar{D}_2(a;n) = \{x - y \bmod n : (x,y) \in H_2(a;n)\}$$

$$\bar{S}_2(a;n) = \{x + y \bmod n : (x,y) \in H_2(a;n)\}$$

For $d > 2$ and $m \geq 1$, where m is the number of plus signs in $\pm x_1 \pm x_2 \pm \cdots \pm x_d$, let

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

[EKSY] results

Theorem (EKSY 2009)

- *Found and proved explicit formulas for the cardinality of* $\bar{S}_2(1; n)$ *and* $\bar{D}_2(1; n)$.

[EKSY] results

Theorem (EKSY 2009)

- *Found and proved explicit formulas for the cardinality of* $\bar{S}_2(1; n)$ *and* $\bar{D}_2(1; n)$.
- *Analyzed ratios of the cardinalities of* $\bar{S}_2(1; n)$ *and* $\bar{D}_2(1; n)$, *found that at least* 84% *of the time,* $\bar{S}_2(1; n) > \bar{D}_2(1; n)$.

$xy \equiv a \pmod{n}$
New Results

Method

Proposition 1 Generalization

Let $n = \prod_{i=1}^{m} p_i^{e_i}$ be the canonical factorization of n. Then,

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

Sketch of proof:

Consider

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

where

$$g(x) = (x \bmod p_1^{e_1}, \cdots, x \bmod p_k^{e_k}).$$

By Chinese remainder theorem, g is a bijection.

Explicit Formulas

In the case when p is an odd prime, for $t \geq 1$,

$$\#\bar{S}_2(a;p^t) = \begin{cases} \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-3}(p-1)}{2(p+1)} & \left(\frac{a}{p}\right) = 1 \\ \frac{\phi(p^t)}{2} & \left(\frac{a}{p}\right) = -1 \end{cases}$$

$$\#\bar{D}_2(a;p^t) =$$

$$\begin{cases} \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-3}(p-1)}{2(p+1)} & p \equiv 1 \bmod 4, \left(\frac{a}{p}\right) = 1 \\ \frac{\phi(p^t)}{2} & p \equiv 1 \bmod 4 \left(\frac{a}{p}\right) = -1 \\ \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-3}(p-1)}{2(p+1)} & p \equiv 3 \bmod 4 \left(\frac{a}{p}\right) = -1 \\ \frac{\phi(p^t)}{2} & p \equiv 3 \bmod 4 \left(\frac{a}{p}\right) = 1. \end{cases}$$

Explicit Formulas

In the case when p is an odd prime, for $t \geq 1$,

$$\#\bar{S}_2(a;p^t) = \begin{cases} \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-3}(p-1)}{2(p+1)} & \left(\frac{a}{p}\right) = 1 \\ \frac{\phi(p^t)}{2} & \left(\frac{a}{p}\right) = -1 \end{cases}$$

$$\#\bar{D}_2(a;p^t) =$$

$$\begin{cases} \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-3}(p-1)}{2(p+1)} & p \equiv 1 \bmod 4, \left(\frac{a}{p}\right) = 1 \\ \frac{\phi(p^t)}{2} & p \equiv 1 \bmod 4 \left(\frac{a}{p}\right) = -1 \\ \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-3}(p-1)}{2(p+1)} & p \equiv 3 \bmod 4 \left(\frac{a}{p}\right) = -1 \\ \frac{\phi(p^t)}{2} & p \equiv 3 \bmod 4 \left(\frac{a}{p}\right) = 1. \end{cases}$$

- Idea: Count squares of the form $k^2 \pm a$.

Explicit Formulas

In the case when p is an odd prime, for $t \geq 1$,

$$\#\bar{S}_2(a;p^t) = \begin{cases} \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-3}(p-1)}{2(p+1)} & \left(\frac{a}{p}\right) = 1 \\ \frac{\phi(p^t)}{2} & \left(\frac{a}{p}\right) = -1 \end{cases}$$

$$\#\bar{D}_2(a;p^t) =$$

$$\begin{cases} \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-3}(p-1)}{2(p+1)} & p \equiv 1 \bmod 4, \left(\frac{a}{p}\right) = 1 \\ \frac{\phi(p^t)}{2} & p \equiv 1 \bmod 4 \left(\frac{a}{p}\right) = -1 \\ \frac{(p-3)p^{t-1}}{2} + \frac{p^{t-1}}{p+1} + \frac{3}{2} + \frac{(-1)^{t-3}(p-1)}{2(p+1)} & p \equiv 3 \bmod 4 \left(\frac{a}{p}\right) = -1 \\ \frac{\phi(p^t)}{2} & p \equiv 3 \bmod 4 \left(\frac{a}{p}\right) = 1. \end{cases}$$

- Idea: Count squares of the form $k^2 \pm a$.
- Can also get explicit formulas for $p = 2$ case.

Ratios

Theorem

1. *If* $p \equiv 1 \bmod 4$, *then* $\frac{\bar{S}_2(a;p^t)}{\bar{D}_2(a;p^t)} = 1$.

Ratios

Theorem

1. *If* $p \equiv 1 \bmod 4$*, then* $\frac{\bar{S}_2(a;p^t)}{\bar{D}_2(a;p^t)} = 1$.

2. *Let* $a > 0$ *be fixed.*
   - *Let* E_a *be the set of positive integers n such that* $(a, n) = 1$ *and* $\left(\frac{a}{p}\right) = 1$ *for every prime* $p \equiv 3 \bmod 4$ *dividing n.*
   - *Let* $C_a(L) = \{n \in E_a : c_2(a; n) > L\}$.
   - *Let* $E_a(x) = \{n \in E_a : n \leq x\}$.
   - *Let* $C_a(L, x) = \{n \in C_a(L) : n \leq x\}$.

   Then the lower density of $C_a(L)$ *in* E_a*, defined by* $\liminf \#C_a(L, x)/\#E_a(x)$*, satisfies the inequality*

$$\lim_{x \to \infty} \inf \frac{\#C_a(1, x)}{\#E_a(x)} \geq K_a \prod \left(1 - \frac{1}{p^2}\right),$$

   where K_a *is computable (and close to one) and the product is over all primes* $p \equiv 3 \bmod 4$ *for which* $\left(\frac{a}{p}\right) = 1$*. Furthermore, for any constant* $L > 0$*, the lower density of* $C_a(L)$ *in* E_a *is positive.*

Ratios

- Proof of 1 follows from cardinality formulas.

Ratios

- Proof of 1 follows from cardinality formulas.
- Proof of 2 and 3 follow from [EKSY]. Only need to look at $p \equiv 3 \bmod 4$.

Ratios

- Proof of 1 follows from cardinality formulas.
- Proof of 2 and 3 follow from [EKSY]. Only need to look at $p \equiv 3 \bmod 4$.
- A special case of shows that when a is a fixed power of 4, we have sum dominance for more than 84% of those n relatively prime to a. Follows from [EKSY].

d-dimensional Modular Hyperbolas

Cardinality

Theorem

If $2, 3, 5$ and $7 \nmid n$ and $d > 2$, the cardinality of $\bar{S}_d(m; a; n)$ is n.

Proof sketch:

- It is enough to show for $\bar{S}_d(m; a; p^t)$, where $d = 3$ and $p > 7$.

Cardinality

Theorem

If $2, 3, 5$ and $7 \nmid n$ and $d > 2$, the cardinality of $\bar{S}_d(m; a; n)$ is n.

Proof sketch:

- It is enough to show for $\bar{S}_d(m; a; p^t)$, where $d = 3$ and $p > 7$.
- Show there is a solution (x_0, y_0, z_0) for $xyz \equiv a \bmod p^t$ and $x + y + z \equiv b \bmod p^t$ for $p > 7$.

Cardinality

Theorem

If $2, 3, 5$ and $7 \nmid n$ and $d > 2$, the cardinality of $\bar{S}_d(m; a; n)$ is n.

Proof sketch:

- It is enough to show for $\bar{S}_d(m; a; p^t)$, where $d = 3$ and $p > 7$.
- Show there is a solution (x_0, y_0, z_0) for $xyz \equiv a \bmod p^t$ and $x + y + z \equiv b \bmod p^t$ for $p > 7$.
- Equivalent to showing there is a solution to $xy(b - x - y) \equiv a \bmod p^t$.

Cardinality

Theorem

If $2, 3, 5$ and $7 \nmid n$ and $d > 2$, the cardinality of $\bar{S}_d(m; a; n)$ is n.

Proof sketch:

- It is enough to show for $\bar{S}_d(m; a; p^t)$, where $d = 3$ and $p > 7$.
- Show there is a solution (x_0, y_0, z_0) for $xyz \equiv a \bmod p^t$ and $x + y + z \equiv b \bmod p^t$ for $p > 7$.
- Equivalent to showing there is a solution to $xy(b - x - y) \equiv a \bmod p^t$.
- Weil bound ensures solution.

Summary

- Higher dimensions sums/differences capture all possibilities.
- Behavior is the same for $\bar{S}_d(m; a; n)$ where $d > 2$.
- For $d = 2$, behavior is varied, so ratios lead to interesting behavior.

Future and Ongoing Research

Future Research

- Cardinality of the intersection of other modular objects (ellipses, lower dimensional modular hyperbolas) with modular hyperbolas.

Future Research

- Cardinality of the intersection of other modular objects (ellipses, lower dimensional modular hyperbolas) with modular hyperbolas.
- Pick elements randomly with probability depending on the dimension of the modular hyperbola.

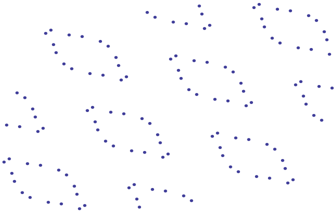
Future Research

- Cardinality of the intersection of other modular objects (ellipses, lower dimensional modular hyperbolas) with modular hyperbolas.
- Pick elements randomly with probability depending on the dimension of the modular hyperbola.
- Ratios for $H_2(a; n)$ where a is not a square mod n.

Acknowledgements

Thanks to ...

- NSF Grant DMS0850577
- NSF Grant DMS0970067
- The audience for your time



Reference

- Bower, Evans, Luo, Miller: Coordinate Sum and Difference Sets of d-dimensional Modular Hyperbolas.
  `http://arxiv.org/pdf/1212.2930v1.pdf`

- Amanda Bower: amandarg@umd.umich.edu
- Ron Evans: revans@ucsd.edu
- Victor Luo: victor.d.luo@williams.edu
- Steven J. Miller: steven.j.miller@williams.edu