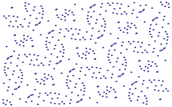
Generalized Sum and Difference Sets and d-dimensional Modular Hyperbolas

Amanda Bower[1] and Victor D. Luo[2]
Advisor: Steven J. Miller[2]

[1]University of Michigan-Dearborn [2]Williams College

http://www.williams.edu/Mathematics/sjmiller/

Young Mathematicians Conference
Columbus, Ohio, July 27-29, 2012



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

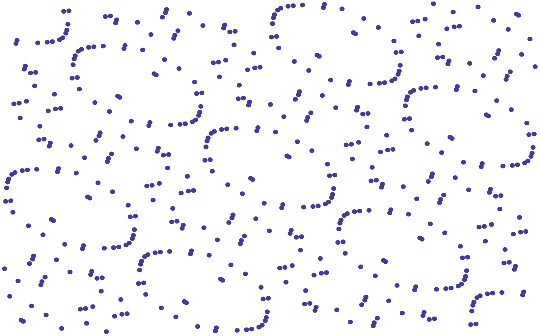


Figure : $xy \equiv 197 \bmod 2^{10}$

Pictures

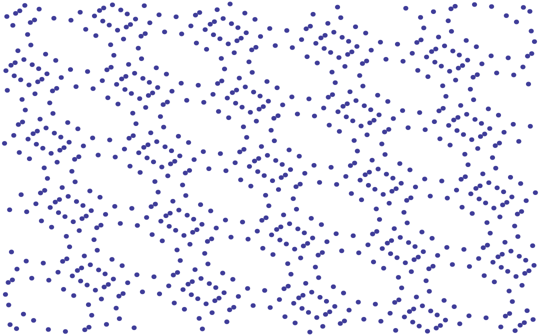


Figure : $xy \equiv 1325 \bmod 48^2$

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:

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

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

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 $\bar{D}_2(1; n)$,*

[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

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

where

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

By Chinese remainder theorem, g is a bijection.

Theorem 2 Generalization

Let $(x, y) \in H_2(a; p^t)$. Then

1. $x \pm y \equiv 2k \mod p^t$ for some $k \in Z$.

Theorem 2 Generalization

Let $(x, y) \in H_2(a; p^t)$. Then

1. $x \pm y \equiv 2k \mod p^t$ for some $k \in Z$.
2. $(2k \mod p^t) \in \bar{D}_2(a; p^t) \iff (k^2 + a)$ is a square modulo p^t.

Theorem 2 Generalization

Let $(x, y) \in H_2(a; p^t)$. Then

1. $x \pm y \equiv 2k \mod p^t$ for some $k \in Z$.
2. $(2k \mod p^t) \in \bar{D}_2(a; p^t) \iff (k^2 + a)$ is a square modulo p^t.
3. For odd primes p, there is a bijection between $\{k : k^2 + a \text{ is a square} \mod n, 0 < k < p^t\}$ and $\bar{D}_2(a; n)$.

Theorem 2 Generalization

Let $(x, y) \in H_2(a; p^t)$. Then

1. $x \pm y \equiv 2k \mod p^t$ for some $k \in Z$.
2. $(2k \mod p^t) \in \bar{D}_2(a; p^t) \iff (k^2 + a)$ is a square modulo p^t.
3. For odd primes p, there is a bijection between $\{k : k^2 + a$ is a square $\mod n, 0 < k < p^t\}$ and $\bar{D}_2(a; n)$.
4. For $p = 2$, there is a bijection between $\{k : k^2 + a$ is a square $\mod n, 0 < k < 2^{t-1}\}$ and $\bar{D}_2(a; n)$.

Theorem 2 Generalization

Let $(x, y) \in H_2(a; p^t)$. Then

1. $x \pm y \equiv 2k \mod p^t$ for some $k \in Z$.
2. $(2k \mod p^t) \in \bar{D}_2(a; p^t) \iff (k^2 + a)$ is a square modulo p^t.
3. For odd primes p, there is a bijection between $\{k : k^2 + a$ is a square mod $n, 0 < k < p^t\}$ and $\bar{D}_2(a; n)$.
4. For $p = 2$, there is a bijection between $\{k : k^2 + a$ is a square mod $n, 0 < k < 2^{t-1}\}$ and $\bar{D}_2(a; n)$.
5. Similar results for $\bar{S}_2(a; n)$.

Method

Theorem 3 (Stangl)

Let p be an odd prime. Then,

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

In the case $p = 2$,

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

Method

Proposition 4

For $p \nmid c$, we have the following:

1. $p \neq 2$: If $x^2 \equiv c \mod p$ is solvable, then for every $t \geq 2$, $x^2 \equiv c \mod p^t$ has exactly 2 distinct solutions.
2. $p = 2$: If $x^2 \equiv c \mod 2^3$ is solvable, then for every $t \geq 3$, $x^2 \equiv c \mod 2^t$ has exactly 4 distinct solutions.

Method

Proposition 5

$$\bar{S}_2(a;n) = \bar{D}_2(-a;n).$$

Sketch of proof:

- If $x + y \in \bar{S}_2(a;n)$, then $(x, -y) \in H_2(-a;n)$.
- Thus $x - (-y) \in \bar{D}_2(-a;n)$.

Explicit Formulas

In the case when $p = 2$,

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

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

Sketch of case $a \equiv 1 \bmod 8$ for $\bar{D}_2(a;n)$:

- Claim: $k^2 + 1 + 8m$ is a square mod $2^t \Leftrightarrow k = 4\ell$ for some $\ell \in \mathbb{Z}$.

Sketch of case $a \equiv 1 \bmod 8$ for $\bar{D}_2(a;n)$:

- Claim: k^2+1+8m is a square mod $2^t \Leftrightarrow k = 4\ell$ for some $\ell \in \mathbb{Z}$.

- "$\Rightarrow$" Reduce mod 8, so $k^2+1+8m \equiv k^2+1 \bmod 8$.

Sketch of case $a \equiv 1 \bmod 8$ for $\bar{D}_2(a; n)$:

- Claim: $k^2 + 1 + 8m$ is a square mod $2^t \Leftrightarrow k = 4\ell$ for some $\ell \in \mathbb{Z}$.
- " $\Rightarrow$ " Reduce mod 8, so $k^2 + 1 + 8m \equiv k^2 + 1 \bmod 8$.
- " $\Leftarrow$ " Reduce mod 8, so $(4\ell)^2 + 1 + 8m \equiv 1 \bmod 8$. Use Proposition 4.

Sketch of case $a \equiv 1 \bmod 8$ for $\bar{D}_2(a;n)$:

- Claim: k^2+1+8m is a square mod $2^t \Leftrightarrow k = 4\ell$ for some $\ell \in \mathbb{Z}$.
- " $\Rightarrow$ " Reduce mod 8, so $k^2+1+8m \equiv k^2+1 \bmod 8$.
- " $\Leftarrow$ " Reduce mod 8, so $(4\ell)^2+1+8m \equiv 1 \bmod 8$. Use Proposition 4.
- Then, by Theorem 2, $\#\{k : k^2+1+8m \text{ is a square mod } 2^t, 0 \le k < 2^{t-1}\}$ $= \#\{4\ell : 0 \le \ell < 2^{t-3}\}$.

Explicit Formulas contd.

In the case when p is an odd prime, for $t \geq 3$,

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

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

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

Ratios

Theorem

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

Ratios

Theorem

1. *If* $p \equiv 1 \bmod 4$, *then* $\frac{\bar{S}_2(a;n)}{\bar{D}_2(a;n)} = 1$.
2. *If a is a square* mod n, *then at least 84% of the time* $\frac{\bar{S}_2(a;n)}{\bar{D}_2(a;n)} > 1$.

Ratios

Theorem

1. *If* $p \equiv 1 \bmod 4$, *then* $\frac{\bar{S}_2(a;n)}{\bar{D}_2(a;n)} = 1$.
2. *If a is a square* mod n, *then at least 84% of the time* $\frac{\bar{S}_2(a;n)}{\bar{D}_2(a;n)} > 1$.
3. *If $-a$ is a square* mod n, *then at least 84% of the time* $\frac{\bar{S}_2(a;n)}{\bar{D}_2(a;n)} < 1$.

Ratios

Theorem

1. *If* $p \equiv 1 \bmod 4$, *then* $\frac{\bar{S}_2(a;n)}{\bar{D}_2(a;n)} = 1$.
2. *If a is a square* mod n, *then at least 84% of the time* $\frac{\bar{S}_2(a;n)}{\bar{D}_2(a;n)} > 1$.
3. *If* $-a$ *is a square* mod n, *then at least 84% of the time* $\frac{\bar{S}_2(a;n)}{\bar{D}_2(a;n)} < 1$.

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

d-dimensional Modular Hyperbolas

Lemma

Let $F(x_1, \cdots, x_k) \equiv 0 \bmod p^t$ where $p > 2$. Then, the number of solutions is

$$S = \frac{1}{p^t} \sum_{u, x_1, \cdots, x_k} e^{2\pi i u F(x_1, \cdots, x_k)/p^t}$$

where $0 \leq u, x_1, \cdots, x_k < p^t$.

Sketch of proof:
Note that

$$\frac{1}{p^t} \sum_{u=0}^{p^t - 1} e^{2\pi i u x/p^t} = \begin{cases} 1 & x \equiv 0 \bmod p^t \\ 0 & x \not\equiv 0 \bmod p^t. \end{cases}$$

Lemma

Let $F(x_1, \cdots, x_k) \equiv 0 \bmod p^t$ where $p > 2$. Then, the number of solutions is

$$S = \frac{1}{p^t} \sum_{u, x_1, \cdots, x_k} e^{2\pi i u F(x_1, \cdots, x_k)/p^t}$$

where $0 \le u, x_1, \cdots, x_k < p^t$.

Sketch of proof:
Note that

$$\frac{1}{p^t} \sum_{u=0}^{p^t - 1} e^{2\pi i u x/p^t} = \begin{cases} 1 & x \equiv 0 \bmod p^t \\ 0 & x \not\equiv 0 \bmod p^t. \end{cases}$$

Each solution contributes 1 to S, while a non-solution doesn't contribute to S.

Cardinality

Theorem

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

Proof sketch:

- It is enough to show for $\bar{S}_3(2; a; n)$ and $\bar{S}_3(1; a; n)$.

Cardinality

Theorem

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

Proof sketch:

- It is enough to show for $\bar{S}_3(2; a; n)$ and $\bar{S}_3(1; a; n)$.
- Show there is a solution (x_0, y_0, z_0) for $xyz \equiv a \bmod p^t$ and $x + y + \varepsilon z \equiv b \bmod p^t$ where $\epsilon = \pm 1$.

Cardinality

Theorem

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

Proof sketch:

- It is enough to show for $\bar{S}_3(2; a; n)$ and $\bar{S}_3(1; a; n)$.
- Show there is a solution (x_0, y_0, z_0) for $xyz \equiv a \bmod p^t$ and $x + y + \varepsilon z \equiv b \bmod p^t$ where $\epsilon = \pm 1$.
- Idea: show there are many solutions.

Cardinality Proof

- Want to show $xy\varepsilon(b - x - y) - a \equiv 0 \bmod p^t$ has many solutions.

Cardinality Proof

- Want to show $xy\varepsilon(b - x - y) - a \equiv 0 \bmod p^t$ has many solutions.
- Number of solutions is
$$\frac{1}{p^t} \sum_{u(p^t)} \sum_{x,y(p^t)} e^{2\pi iu(xy\varepsilon(b-x-y)-a)/p^t}.$$

Cardinality Proof

- Want to show $xy\varepsilon(b - x - y) - a \equiv 0 \bmod p^t$ has many solutions.

- Number of solutions is
$$\frac{1}{p^t} \sum_{u(p^t)} \sum_{x,y(p^t)} e^{2\pi iu(xy\varepsilon(b-x-y)-a)/p^t}.$$

- Equals $\frac{p^{2t}}{p^t} + \frac{1}{p^t} \sum_{u=1}^{p^t-1} \sum_{x,y(p^t)} e^{2\pi iu(xy\varepsilon(b-x-y)-a)/p^t}$.

Cardinality Proof

- Want to show $xy\varepsilon(b - x - y) - a \equiv 0 \bmod p^t$ has many solutions.
- Number of solutions is
  $$\frac{1}{p^t}\sum_{u(p^t)}\sum_{x,y(p^t)} e^{2\pi i u(xy\varepsilon(b-x-y)-a)/p^t}.$$
- Equals $\frac{p^{2t}}{p^t} + \frac{1}{p^t}\sum_{u=1}^{p^t-1}\sum_{x,y(p^t)} e^{2\pi i u(xy\varepsilon(b-x-y)-a)/p^t}.$
- Change of variables:
  $$p^t + \frac{1}{p^t}\sum_{u=1}^{p^t-1}\sum_{y(p^t)} e^{(-2\pi i u b+2\pi i(a+y)^2 4^{-1}\varepsilon u y)/p^t}\sum_{x=0}^{p^t-1} e^{2\pi i x^2 u y\varepsilon/p^t}.$$

Cardinality Proof

- Note, by generalized Gauss sums
$\sum_{x=0}^{p^t-1} e^{2\pi i x^2 u y \varepsilon / p^t} = c\sqrt{p^t}$ where c has magnitude 1.

Cardinality Proof

- Note, by generalized Gauss sums $\sum_{x=0}^{p^t-1} e^{2\pi i x^2 u y \varepsilon / p^t} = c\sqrt{p^t}$ where c has magnitude 1.
- Change of variables and Gauss sums again:

$$p^t + d\frac{\sqrt{p^t}\sqrt{p^t}}{p^t}\sum_{y=0}^{p^t-1}\left(\frac{(a+y)^2 4^{-1}\varepsilon y^2 - \varepsilon b y}{p^t}\right)$$

where the magnitude of d is 1.

Cardinality Proof

- Note, by generalized Gauss sums $\sum_{x=0}^{p^t-1} e^{2\pi i x^2 u y \varepsilon / p^t} = c\sqrt{p^t}$ where c has magnitude 1.
- Change of variables and Gauss sums again:
$$p^t + d\frac{\sqrt{p^t}\sqrt{p^t}}{p^t}\sum_{y=0}^{p^t-1}\left(\frac{(a+y)^2 4^{-1}\varepsilon y^2 - \varepsilon b y}{p^t}\right)$$
where the magnitude of d is 1.
- Main term is p^t. Rest of sum is bounded in magnitude by $p^t - 1$.

Summary

- Higher dimensions sums/differences capture all possibilities.

Summary

- Higher dimensions sums/differences capture all possibilities.
- Behavior is the same for $\bar{S}_d(m; a; n)$ where $d > 2$.

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 and Ongoing Research

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

Future and Ongoing 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 and Ongoing 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.

Thanks to ...

- Ohio State and YMC
- NSF Grant DMS0850577
- NSF Grant DMS0970067
- Our advisor Steven J. Miller
- The audience for your time