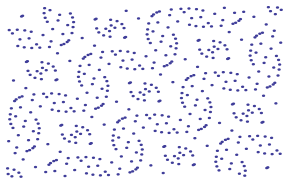
Coordinate Sum and Difference Sets of d-dimensional Modular Hyperbolas

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

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

New York Number Theory Seminar
Combinatorial and Additive Number Theory
CUNY Graduate Center, May 21, 2013



Intro

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

Definition

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

Intro

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

Definition

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

Why study sumsets?

Intro

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

Definition

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

Why study sumsets?

- Goldbach's conjecture: $\{4, 6, 8, \cdots\} \subseteq P + P$.
- Fermat's Last Theorem: Let A_n be the nth powers. Then $(A_n + A_n) \cap A_n = \emptyset$ for all $n > 2$.
- Twin prime conjecture: Let $P_n = \{p : p \in P, p > n\}$. Then $P_n - P_n$ contains 2 for all n.

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 $x - y \neq y - x$.
- Choose sets with great structure (depends on fringe).

Motivation

- Martin and O'Bryant '07: positive percentage are sum-dominant.
  - Note $x + y = y + x$ but $x - y \neq y - x$.
- Choose sets with great structure (depends on fringe).
- Leads to study of sumsets of "fringless" sets.

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:
  - $xy \equiv a \bmod n$.

Goals

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

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

- Generalize to:
  - $xy \equiv a \bmod n$.
  - higher dimensions: $x_1 \cdots x_k \equiv a \bmod n$.

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 ($\pm A \pm A \pm A \pm \cdots \pm A$).

Pictures

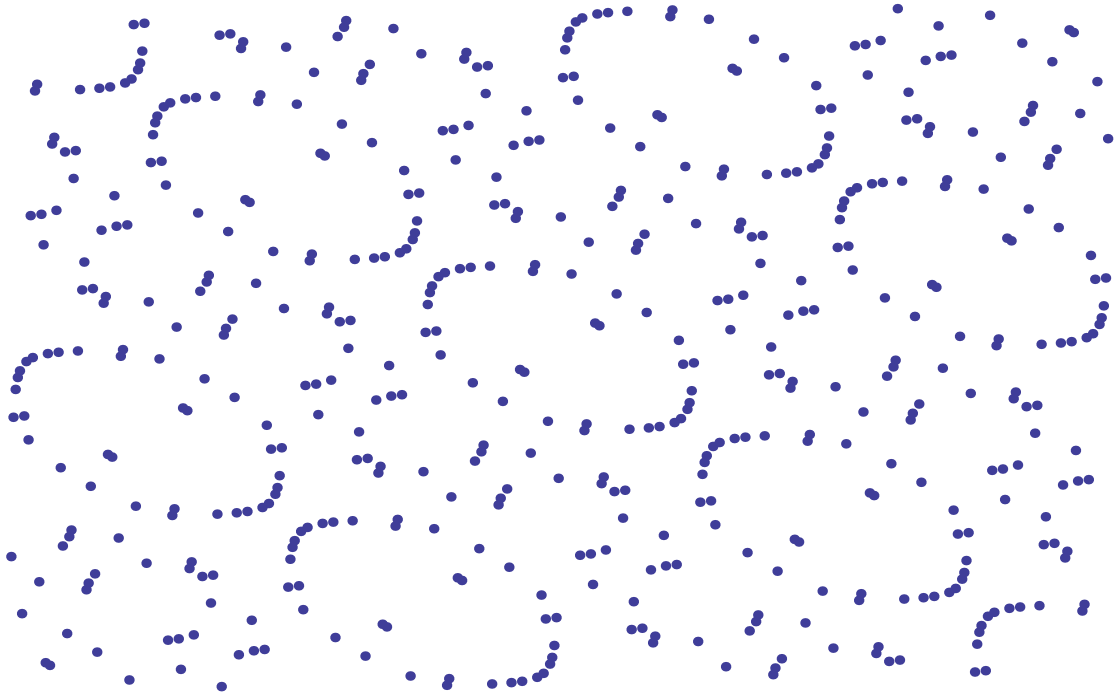


Figure : $xy \equiv 197 \bmod 2^{10}$

Pictures

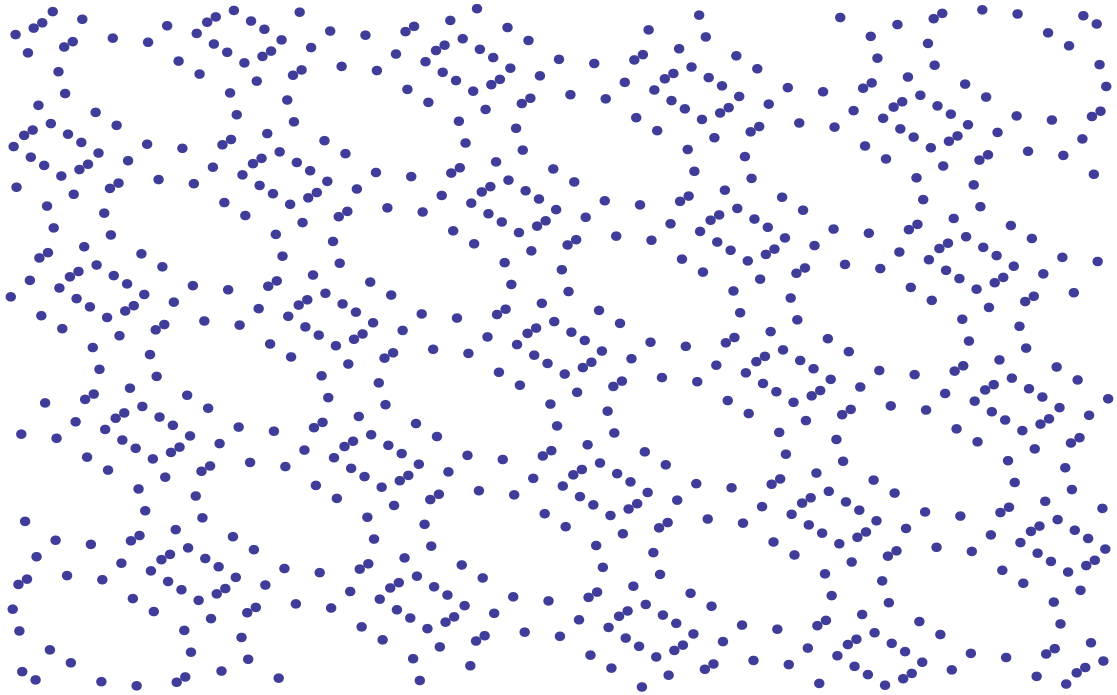


Figure : $xy \equiv 1325 \bmod 48^2$

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

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

[EKSY] 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 $0 \leq m \leq d$, 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,* $|\bar{S}_2(1;n)| > |\bar{D}_2(1;n)|$.

$H_2(a;n)$
New Results

Method

Proposition 1 Generalization

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

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

Natural extension of [EKSY]. 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.

Method

Lemma 2 Generalization

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

1. $x - y \equiv 2k \bmod p^t$ for some $k \in \mathbb{Z}$.

Method

Lemma 2 Generalization

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

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

Method

Lemma 2 Generalization

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

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

Method

Lemma 2 Generalization

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

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

Method

Lemma 2 Generalization

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

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

Natural generalization from a=1 case done by [EKSY].

Method

Lemma 3

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

Sketch of proof:

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

Method

Lemma 3

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

Sketch of proof:

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

Only need to understand prime powers and either sumset or difference set.

Explicit Formulas

In the case when $p = 2$,

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

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

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 $k^2 \pm a$.

Ratios for $H_2(a;n)$

Ratios

Theorem

Let $c_2(a;n) = \frac{|\bar{S}_2(a;n)|}{|\bar{D}_2(a;n)|}$.

1. *If* $p \equiv 1 \bmod 4$, *then* $c_2(a;p^t) = 1$.

Ratios

Theorem

Let $c_2(a;n) = \frac{|\bar{S}_2(a;n)|}{|\bar{D}_2(a;n)|}$.

1. *If* $p \equiv 1 \bmod 4$, *then* $c_2(a;p^t) = 1$.
2. *If* $p \equiv 3 \bmod 4$ *and* a *is a square* $\bmod p$,
   $c_2(a;p^t) = 1 - 2\sum_{i=0}^{[t/2]-1} \frac{1}{p^{2i+1}} + \frac{2}{\phi(p^t)}$.

Ratios

Theorem

Let $c_2(a;n) = \frac{|\bar{S}_2(a;n)|}{|\bar{D}_2(a;n)|}$.

1. *If* $p \equiv 1 \bmod 4$, *then* $c_2(a;p^t) = 1$.
2. *If* $p \equiv 3 \bmod 4$ *and* a *is a square* $\bmod p$, $c_2(a;p^t) = 1 - 2\sum_{i=0}^{[t/2]-1} \frac{1}{p^{2i+1}} + \frac{2}{\phi(p^t)}$.
3. *Let* $p < q$ *and* $p, q \equiv 3 \bmod 4$. *Let* $s, t \geq 2$. *If* $\left(\frac{a}{p}\right) = 1$, *then* $c_2(a;p^t q^s) < 1$. *Otherwise, then* $c_2(a;p^t q^s) > 1$.

Ratios

- Proof of 1 and 2 follow from cardinality formulas.

Ratios

- Proof of 1 and 2 follow from cardinality formulas.
- Proof of 3 follows from 2. Main ideas: Note $c_2(a;p^t) < 1$ and if $\left(\frac{a}{q}\right) = 1$, done. Otherwise, show that $c_2(-a;q^s) > c_2(a;p^t)$.

Ratios

Theorem

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

- A special case of shows that when a is a fixed power of 4, we have sum dominance for more than 84% of those $n \in E_a$. Follows from [EKSY].

Ratios

- A special case of shows that when a is a fixed power of 4, we have sum dominance for more than 84% of those $n \in E_a$. Follows from [EKSY].
- If the condition $\left(\frac{a}{p}\right) = 1$ is replaced by $\left(\frac{a}{p}\right) = -1$, results hold with the inequality $c_2(a;n) > 1$ replaced by $c_2(a;n) < 1$.

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 $p > 7$.
- Weil bound ensures solution.

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 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 in two dimensions for any n.

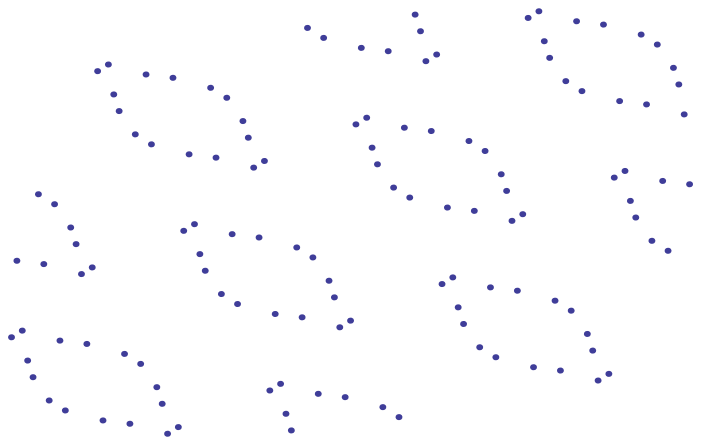
Future Research

- 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 in two dimensions for any n.
- Understand $\bar{S}_d(m; a; n)$ when $2, 3, 5$, or 7 divides n.

Acknowledgements

Thanks to ...

- NSF Grant DMS0850577 and DMS0970067
- Williams College and the SMALL REU
- Mizan R. Khan for introducing us to this problem
- The audience for your time



Reference

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

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