Gauss' Hidden Menagerie: the Graphic Nature of Gaussian Periods

Stephan Ramon Garcia

CMC^3 Recreational Math Conference

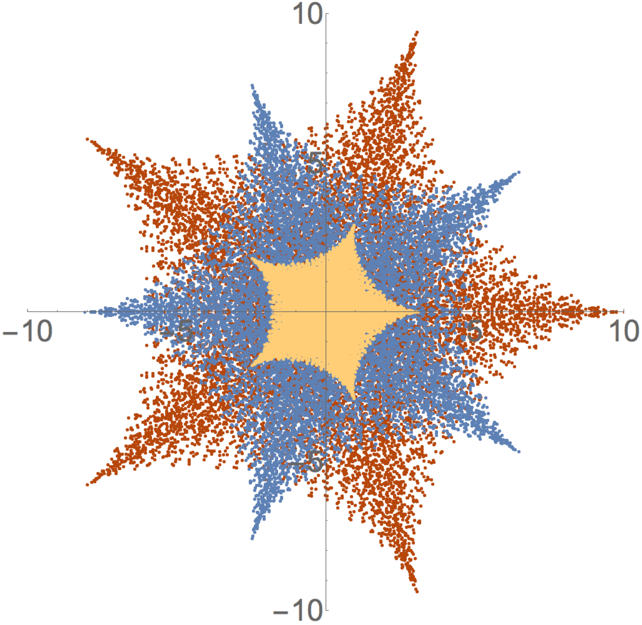
April 23, 2016

Abstract

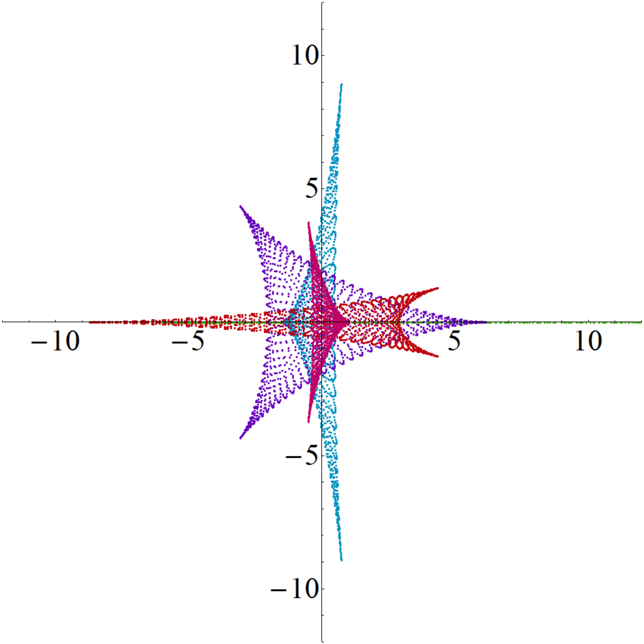
At the age of eighteen, Gauss established the constructibility of the 17-gon, a result that had eluded mathematicians for two millennia. At the heart of his argument was a keen study of certain sums of complex exponentials, known now as Gaussian periods. It turns out that these classical objects, when viewed appropriately, exhibit dazzling array of visual patterns of great complexity and remarkable subtlety. (Joint work with Bill Duke, Trevor Hyde, and Bob Lutz, and others).

Partially supported by NSF Grants DMS-1265973 & DMS-1001614 and by the Fletcher Jones Foundation.

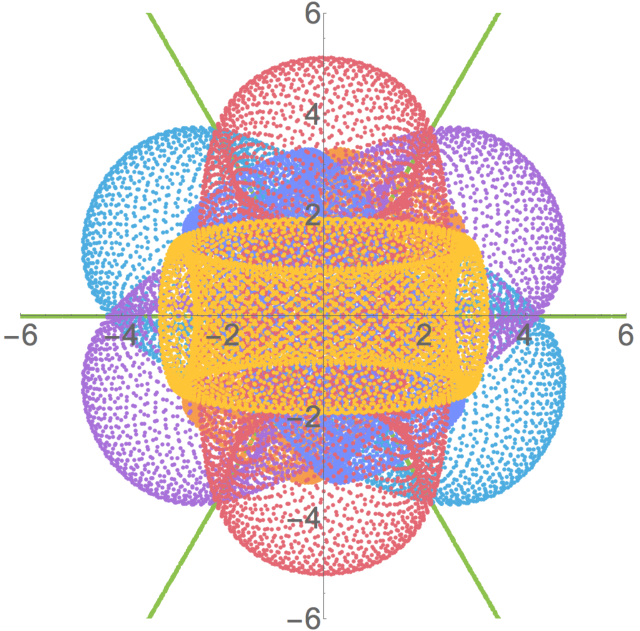
Sneak Preview



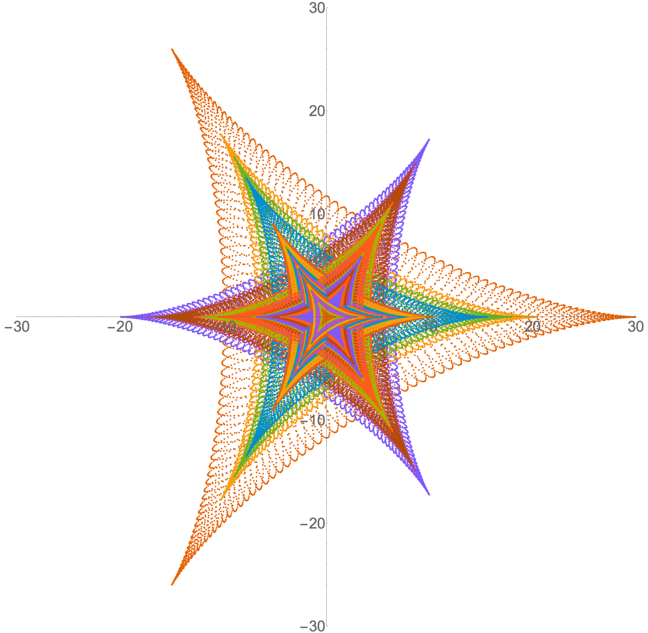
What sort of mathematical mechanism makes pictures like this?



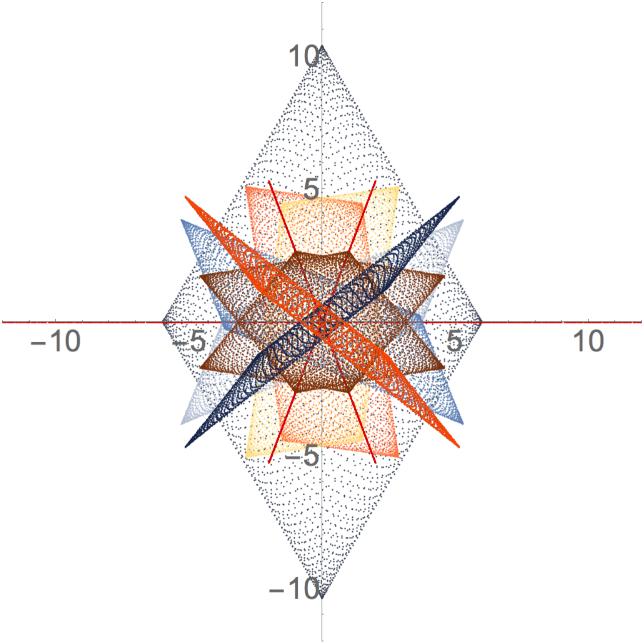
What sort of mathematical mechanism makes pictures like this?



What sort of mathematical mechanism makes pictures like this?



What sort of mathematical mechanism makes pictures like this?



What sort of mathematical mechanism makes pictures like this?

Modular Arithmetic

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} = \text{the remainder of } x \text{ upon division by } n.}$$

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} \; = \; \text{the remainder of } x \text{ upon division by } n.}$$

- $x \pmod{n}$ is always between 0 and $n - 1$.

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} \;=\; \text{the remainder of } x \text{ upon division by } n.}$$

- $x \pmod{n}$ is always between 0 and $n - 1$.
- For instance

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} \;=\; \text{the remainder of } x \text{ upon division by } n.}$$

- $x \pmod{n}$ is always between 0 and $n-1$.
- For instance
  - $1 \pmod{5} = 1$,

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} \; = \; \text{the remainder of } x \text{ upon division by } n.}$$

- $x \pmod{n}$ is always between 0 and $n-1$.
- For instance
  - $1 \pmod{5} = 1$,
  - $7 \pmod{5} = 2$,

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} \;=\; \text{the remainder of } x \text{ upon division by } n.}$$

- $x \pmod{n}$ is always between 0 and $n - 1$.
- For instance
  - $1 \pmod{5} = 1$,
  - $7 \pmod{5} = 2$,
  - $18 \pmod{5} = 3$,

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} \;=\; \text{the remainder of } x \text{ upon division by } n.}$$

- $x \pmod{n}$ is always between 0 and $n-1$.
- For instance
  - $1 \pmod{5} = 1$,
  - $7 \pmod{5} = 2$,
  - $18 \pmod{5} = 3$,
  - $-1 \pmod{5} = 4$,

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} \;=\; \text{the remainder of } x \text{ upon division by } n.}$$

- $x \pmod{n}$ is always between 0 and $n-1$.
- For instance
  - $1 \pmod{5} = 1$,
  - $7 \pmod{5} = 2$,
  - $18 \pmod{5} = 3$,
  - $-1 \pmod{5} = 4$,
  - $3 \cdot 4 \pmod{5} = 2$,

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} \;=\; \text{the remainder of } x \text{ upon division by } n.}$$

- $x \pmod{n}$ is always between 0 and $n - 1$.
- For instance
  - $1 \pmod{5} = 1$,
  - $7 \pmod{5} = 2$,
  - $18 \pmod{5} = 3$,
  - $-1 \pmod{5} = 4$,
  - $3 \cdot 4 \pmod{5} = 2$,
  - $2^5 \pmod{5} = 2$,

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} \;=\; \text{the remainder of } x \text{ upon division by } n.}$$

- $x \pmod{n}$ is always between 0 and $n-1$.
- For instance
  - $1 \pmod{5} = 1$,
  - $7 \pmod{5} = 2$,
  - $18 \pmod{5} = 3$,
  - $-1 \pmod{5} = 4$,
  - $3 \cdot 4 \pmod{5} = 2$,
  - $2^5 \pmod{5} = 2$,
  - $3^5 \pmod{5} = 3$,

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} \;=\; \text{the remainder of } x \text{ upon division by } n.}$$

- $x \pmod{n}$ is always between 0 and $n-1$.
- For instance
  - $1 \pmod{5} = 1$,
  - $7 \pmod{5} = 2$,
  - $18 \pmod{5} = 3$,
  - $-1 \pmod{5} = 4$,
  - $3 \cdot 4 \pmod{5} = 2$,
  - $2^5 \pmod{5} = 2$,
  - $3^5 \pmod{5} = 3$,
  - $4^5 \pmod{5} = 4$.

Modular Arithmetic

- If n is a positive whole number and x is an integer, then

$$\boxed{x \pmod{n} \;=\; \text{the remainder of } x \text{ upon division by } n.}$$

- $x \pmod{n}$ is always between 0 and $n-1$.
- For instance
  - $1 \pmod{5} = 1$,
  - $7 \pmod{5} = 2$,
  - $18 \pmod{5} = 3$,
  - $-1 \pmod{5} = 4$,
  - $3 \cdot 4 \pmod{5} = 2$,
  - $2^5 \pmod{5} = 2$,
  - $3^5 \pmod{5} = 3$,
  - $4^5 \pmod{5} = 4$.
- You use modular arithmetic all the time!

- Computing with hours is arithmetic modulo 12,

- Computing with hours is arithmetic modulo 12,
- Computing with minutes is arithmetic modulo 60,

- Computing with hours is arithmetic modulo 12,
- Computing with minutes is arithmetic modulo 60,
- Computing with seconds is arithmetic modulo 60.

Arithmetic Modulo n

We can do arithmetic in the set $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$.

Arithmetic Modulo n

We can do arithmetic in the set $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$. For instance, addition and multiplication in $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ is described by the tables:

Arithmetic Modulo n

We can do arithmetic in the set $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$. For instance, addition and multiplication in $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ is described by the tables:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Arithmetic Modulo n

We can do arithmetic in the set $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$. For instance, addition and multiplication in $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ is described by the tables:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Arithmetic Modulo n

We can do arithmetic in the set $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$. For instance, addition and multiplication in $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ is described by the tables:

+	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

×	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Arithmetic Modulo n

We can do arithmetic in the set $\mathbb{Z}/n\mathbb{Z} = \{0, 1, 2, \ldots, n-1\}$. For instance, addition and multiplication in $\mathbb{Z}/5\mathbb{Z} = \{0, 1, 2, 3, 4\}$ is described by the tables:

$+$	0	1	2	3	4
0	0	1	2	3	4
1	1	2	3	4	0
2	2	3	4	0	1
3	3	4	0	1	2
4	4	0	1	2	3

$\times$	0	1	2	3	4
0	0	0	0	0	0
1	0	1	2	3	4
2	0	2	4	1	3
3	0	3	1	4	2
4	0	4	3	2	1

Order of an integer modulo n

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	16	32	64	128	256	512	1024
$2^n \pmod{10}$	2	4	8	6	2	4	8	6	2	4

Order of an integer modulo n

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	16	32	64	128	256	512	1024
$2^n \pmod{10}$	2	4	8	6	2	4	8	6	2	4
$2^n \pmod{5}$	2	4	3	1	2	4	3	1	2	4

Order of an integer modulo n

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	16	32	64	128	256	512	1024
$2^n \pmod{10}$	2	4	8	6	2	4	8	6	2	4
$2^n \pmod{5}$	2	4	3	1	2	4	3	1	2	4
$2^n \pmod{7}$	2	4	1	2	4	1	2	4	1	2

Order of an integer modulo n

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	16	32	64	128	256	512	1024
$2^n \pmod{10}$	2	4	8	6	2	4	8	6	2	4
$2^n \pmod{5}$	2	4	3	1	2	4	3	1	2	4
$2^n \pmod{7}$	2	4	1	2	4	1	2	4	1	2
$2^n \pmod{9}$	2	4	8	7	5	1	2	4	8	7

Order of an integer modulo n

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	16	32	64	128	256	512	1024
$2^n \pmod{10}$	2	4	8	6	2	4	8	6	2	4
$2^n \pmod{5}$	2	4	3	1	2	4	3	1	2	4
$2^n \pmod{7}$	2	4	1	2	4	1	2	4	1	2
$2^n \pmod{9}$	2	4	8	7	5	1	2	4	8	7
$2^n \pmod{11}$	2	4	8	5	10	9	7	3	6	1

Order of an integer modulo n

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	16	32	64	128	256	512	1024
$2^n \pmod{10}$	2	4	8	6	2	4	8	6	2	4
$2^n \pmod{5}$	2	4	3	1	2	4	3	1	2	4
$2^n \pmod{7}$	2	4	1	2	4	1	2	4	1	2
$2^n \pmod{9}$	2	4	8	7	5	1	2	4	8	7
$2^n \pmod{11}$	2	4	8	5	10	9	7	3	6	1

Definition

Let $\gcd(a, n) = 1$. The *multiplicative order* of a modulo n is the smallest positive exponent d for which $a^d \equiv 1 \pmod{n}$.

Order of an integer modulo n

n	1	2	3	4	5	6	7	8	9	10
2^n	2	4	8	16	32	64	128	256	512	1024
$2^n \pmod{10}$	2	4	8	6	2	4	8	6	2	4
$2^n \pmod{5}$	2	4	3	1	2	4	3	1	2	4
$2^n \pmod{7}$	2	4	1	2	4	1	2	4	1	2
$2^n \pmod{9}$	2	4	8	7	5	1	2	4	8	7
$2^n \pmod{11}$	2	4	8	5	10	9	7	3	6	1

Definition

Let $\gcd(a, n) = 1$. The *multiplicative order* of a modulo n is the smallest positive exponent d for which $a^d \equiv 1 \pmod{n}$.

How to make some cool math pictures!

Not so random walks

1. Let n be a large whole number.

Not so random walks

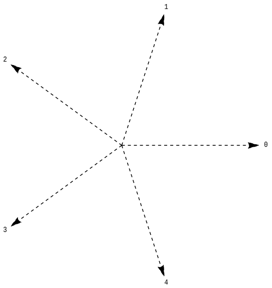
1. Let n be a large whole number.
2. Let a be a whole number with $\gcd(a, n) = 1$.

Not so random walks

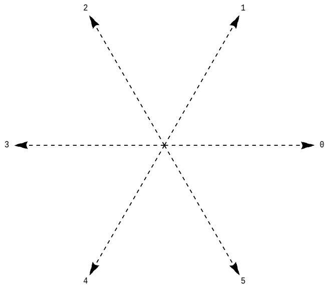
1. Let n be a large whole number.
2. Let a be a whole number with $\gcd(a, n) = 1$.
3. Let d be the multiplicative order of a modulo n.

Not so random walks

1. Let n be a large whole number.
2. Let a be a whole number with $\gcd(a, n) = 1$.
3. Let d be the multiplicative order of a modulo n.
4. For each integer x, take a d-step walk starting from $(0, 0)$ with unit steps in the directions $ax, a^2x, a^3x, \ldots, a^dx \pmod{n}$.



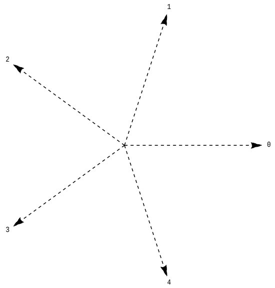
Allowable directions when $n = 5$



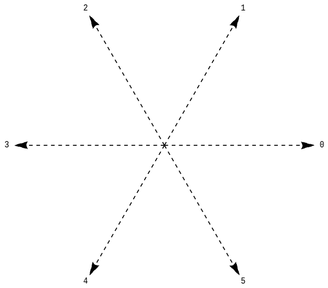
Allowable directions when $n = 6$

Not so random walks

1. Let n be a large whole number.
2. Let a be a whole number with $\gcd(a, n) = 1$.
3. Let d be the multiplicative order of a modulo n.
4. For each integer x, take a d-step walk starting from $(0, 0)$ with unit steps in the directions $ax, a^2x, a^3x, \ldots, a^dx \pmod{n}$.



Allowable directions when $n = 5$



Allowable directions when $n = 6$

5. Mark the endpoint of each walk with a colored dot.

Example

Let $n = 7$ and $a = 2$.

Example

Let $n = 7$ and $a = 2$. Working modulo 7 we have

$$a = 2, \qquad a^2 = 4, \qquad a^3 = 1, \qquad a^4 = 2, \qquad a^5 = 4, \ldots$$

Example

Let $n = 7$ and $a = 2$. Working modulo 7 we have

$$a = 2, \qquad a^2 = 4, \qquad a^3 = 1, \qquad a^4 = 2, \qquad a^5 = 4, \ldots$$

so our walk has 3 steps.

Example

Let $n = 7$ and $a = 2$. Working modulo 7 we have

$$a = 2, \qquad a^2 = 4, \qquad a^3 = 1, \qquad a^4 = 2, \qquad a^5 = 4, \ldots$$

so our walk has 3 steps. If $x = 4$, our steps will be in the directions

$$ax = 2 \cdot 4 = \mathbf{1}, \qquad a^2x = 4 \cdot 4 = \mathbf{2}, \qquad a^3x = 1 \cdot 4 = \mathbf{4}.$$

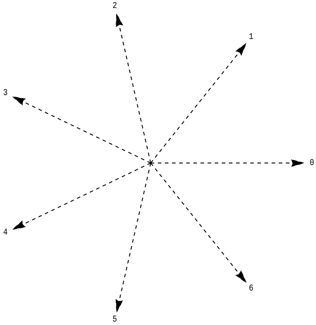
Example

Let $n = 7$ and $a = 2$. Working modulo 7 we have

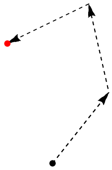
$$a = 2, \qquad a^2 = 4, \qquad a^3 = 1, \qquad a^4 = 2, \qquad a^5 = 4, \ldots$$

so our walk has 3 steps. If $x = 4$, our steps will be in the directions

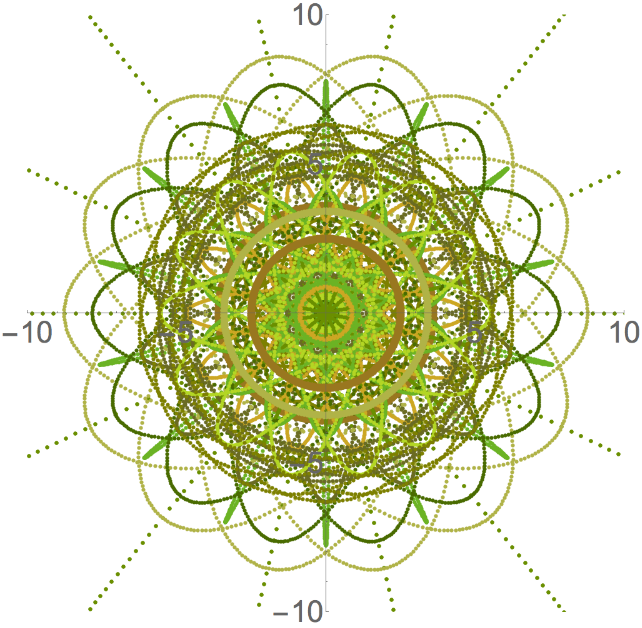
$$ax = 2 \cdot 4 = \mathbf{1}, \qquad a^2x = 4 \cdot 4 = \mathbf{2}, \qquad a^3x = 1 \cdot 4 = \mathbf{4}.$$



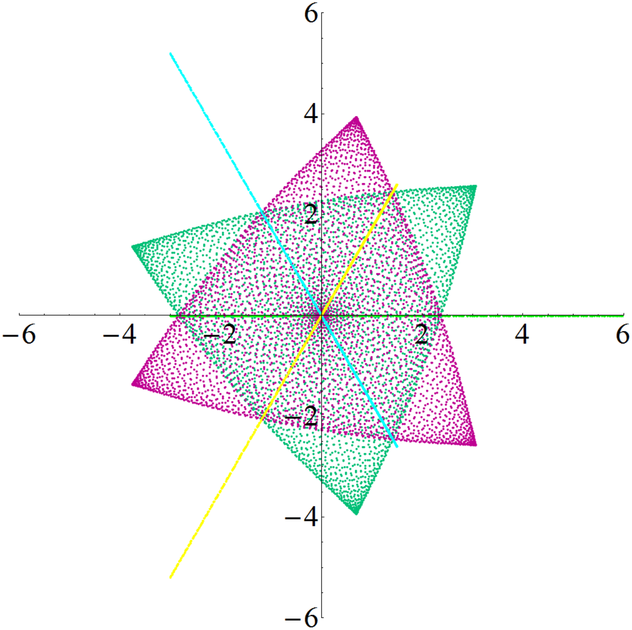
Allowable directions when $n = 7$



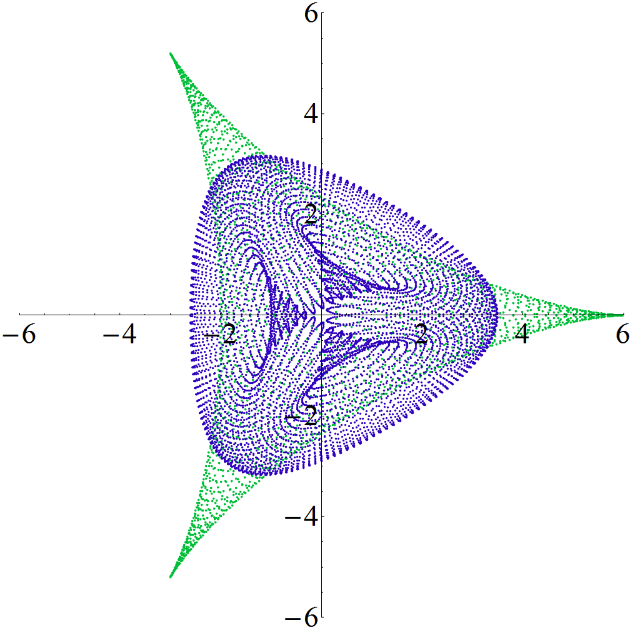
Walk with steps in directions 1, 2, 4.



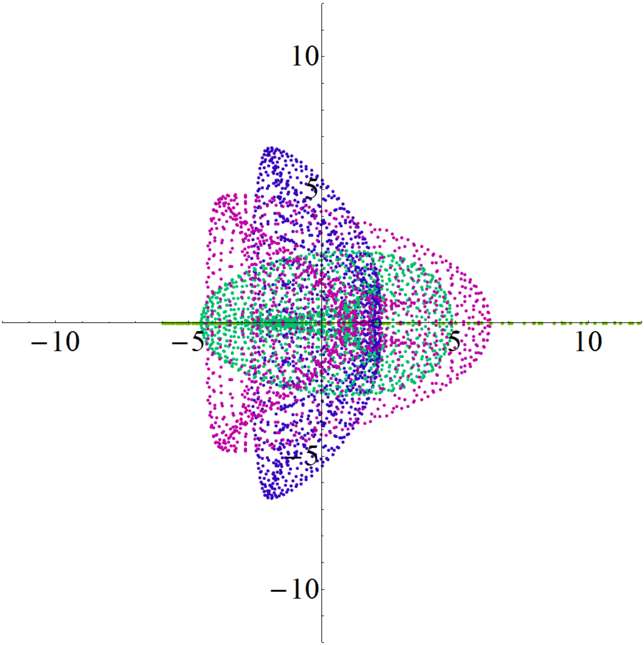
$n = 455175,\ a = 3599$



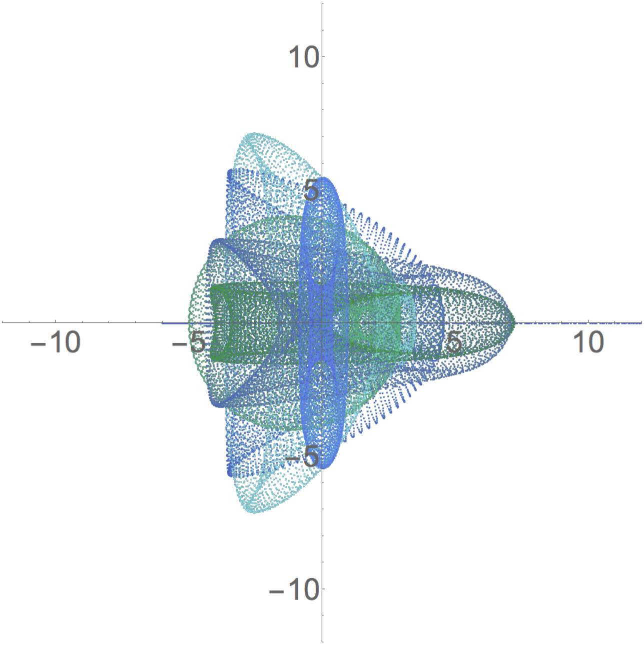
$n = 68913,\ a = 88$



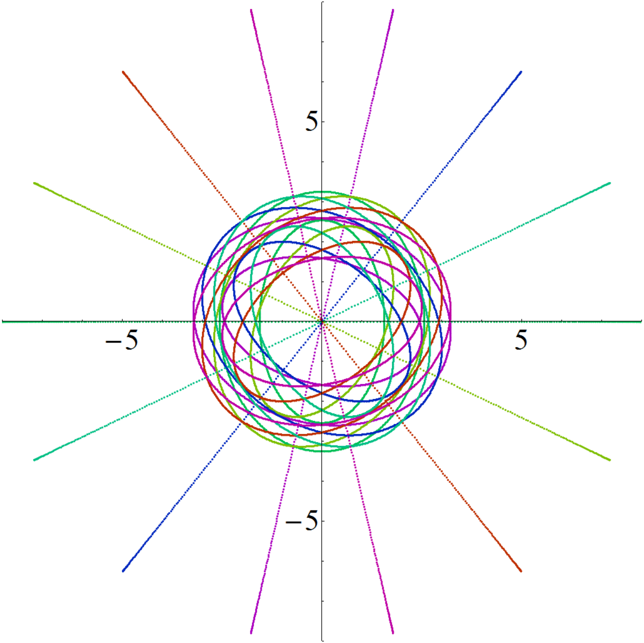
$n = 52059,\ a = 766$



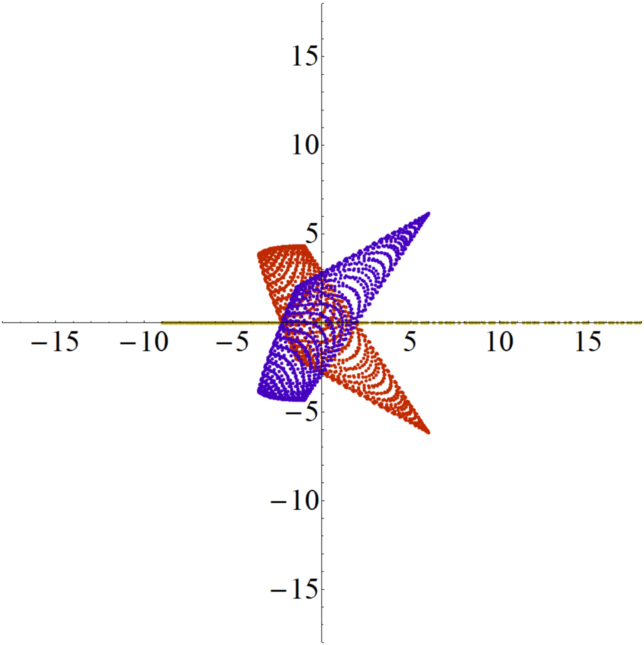
$n = 51319$, $a = 430$



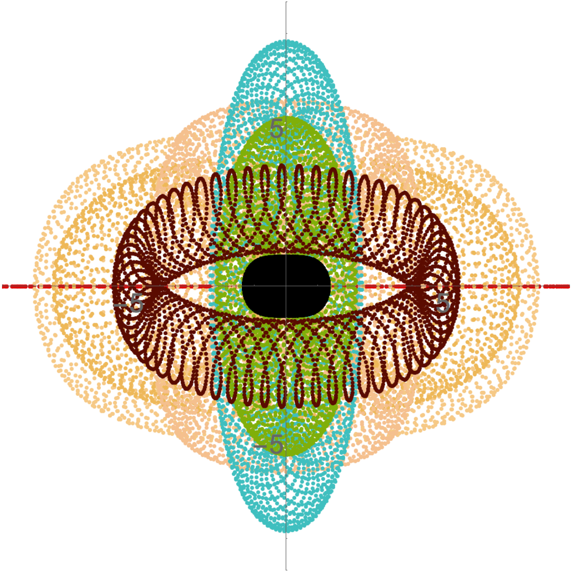
$n = 477493$, $a = 1463$



$n = 70091,\ a = 21792$



$n = 51319$, $a = 138$



$n = 357193$, $a = 8862$

"Eye of Sauron"

"Eye of Sauron"
(older visualization technique)

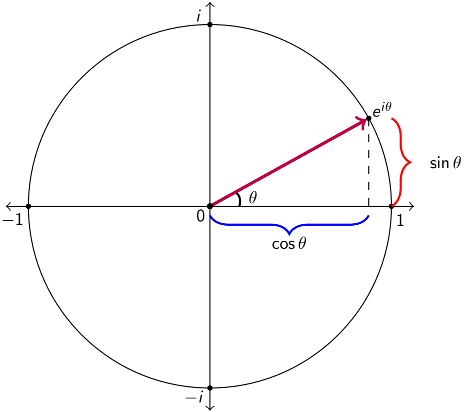
“Eye of Sauron”
(older visualization technique)

To simplify,
make things complex

Complex exponentials

Euler's Formula

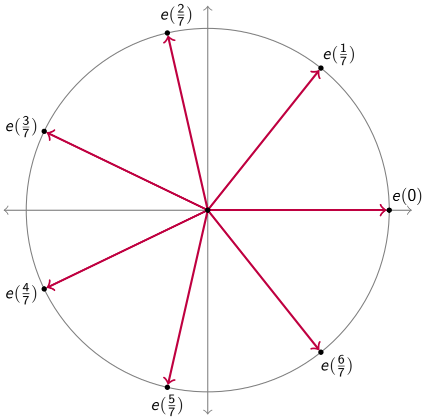
$$e^{i\theta} = \cos\theta + i\sin\theta, \qquad (i^2 = -1)$$



Complex exponentials

Definition

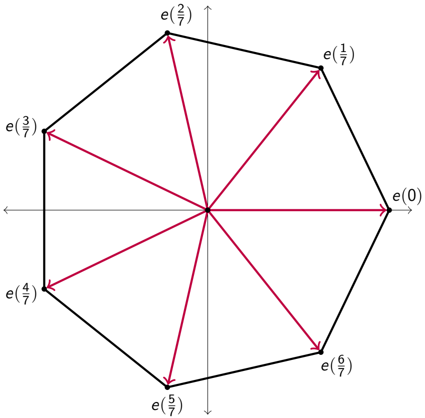
$$e(\theta) = e^{2\pi i\theta}$$



Complex exponentials

Definition

$$e(\theta) = e^{2\pi i\theta}$$



What is really going on?

To be more precise

We are plotting the function $f : \mathbb{Z} \to \mathbb{C}$ defined by

$$f(x) = \sum_{\ell=1}^{d} e\left(\frac{a^{\ell} x}{n}\right). \qquad (i = \sqrt{-1})$$

What is really going on?

To be more precise

We are plotting the function $f : \mathbb{Z} \to \mathbb{C}$ defined by

$$f(x) = \sum_{\ell=1}^{d} e\left(\frac{a^{\ell} x}{n}\right). \qquad (i = \sqrt{-1})$$

Amazingly

These exponential sums first arose in the work of Gauss (1777-1855).

What is really going on?

To be more precise

We are plotting the function $f : \mathbb{Z} \to \mathbb{C}$ defined by

$$f(x) = \sum_{\ell=1}^{d} e\left(\frac{a^\ell x}{n}\right). \qquad (i = \sqrt{-1})$$

Amazingly

These exponential sums first arose in the work of Gauss (1777-1855). Regarding the simplest case:

> *Demonstratio theorematis venustissimi supra 1801 Mai commemorati, quam per 4 annos et ultra omni contentione quaersiveramus, tandem perfecimus. – C.F. Gauss, August 30, 1805*

What is really going on?

To be more precise

We are plotting the function $f : \mathbb{Z} \to \mathbb{C}$ defined by

$$f(x) = \sum_{\ell=1}^{d} e\left(\frac{a^{\ell} x}{n}\right). \qquad (i = \sqrt{-1})$$

Amazingly

These exponential sums first arose in the work of Gauss (1777-1855). Regarding the simplest case:

> *At length we achieved a demonstration of the very elegant theorem mentioned before in May, 1801, which we had sought for more than four years with all efforts. – C.F. Gauss, August 30, 1805*

What is really going on?

To be more precise

We are plotting the function $f : \mathbb{Z} \to \mathbb{C}$ defined by

$$f(x) = \sum_{\ell=1}^{d} e\left(\frac{a^{\ell} x}{n}\right). \qquad (i = \sqrt{-1})$$

Amazingly

These exponential sums first arose in the work of Gauss (1777-1855). Regarding the simplest case:

> *At length we achieved a demonstration of the very elegant theorem mentioned before in May, 1801, which we had sought for more than four years with all efforts. – C.F. Gauss, August 30, 1805*

However, the graphical patterns we found went unnoticed for over two hundred years!

/how-to/

BOB LUTZ '13

HOW TO PUT NEW GRAPHS INTO OLD MATH

Drawing on the power of today's computers, Bob Lutz '13 in his senior year discovered new ways to present, in stunning graphics, mathematical expressions studied by math great C.F. Gauss two centuries ago. Presenting long-studied exponential sums in an entirely new visual form, Lutz was able to graph patterns nobody has seen before. Here is Lutz's path to a remarkable undergraduate achievement:

1 **TRANSFER in from Vassar set on** studying math. Finish your prerequisites. Declare your major. Get a warm welcome from the Math Department—and a nudge to consider doing research. Find opportunities "all over the place." Work with Professor Adolfo Rumbos for the summer.

2 **ATTEND a math lunch in the fall.** Meet Professor Stephan Garcia, who suggests your interest in functional analysis would mesh with his research. Get to work. Co-author a research paper that is accepted for publication in the *Proceedings of the American Mathematical Society.*

3 **JOIN another round of** research with Professor Garcia involving exponential sums first studied by Gauss. Run with the professor's suggestion that you come up with some code to graph them. Push the plots and discover they yield curvy triangles, vortices and other fascinating visual patterns on the computer screen.

4 **REALIZE you have found your** senior thesis—and maybe more. Work on the project for six months. Face rejection trying to get a paper published. Step back. Wait. Score your break after Professor Garcia includes your work as part of a talk he gives at UCLA attended by mathematician Bill Duke, who did related work years before. Get help from Duke in proving some of your conjectures.

5 **EARN Pomona's annual** award for outstanding senior in mathematics. Feel awe after Professor Garcia submits the paper on the graphing work to an editor on a Friday—and gets a "yes" the next morning. Spend the summer working with Garcia putting the finishing touches on this second paper for the *Proceedings of the AMS.* Set off for graduate studies in math at your first-choice school, the University of Michigan, Ann Arbor.

10 Pomona College Magazine

Photo by Mark Wood

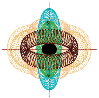
Pomona College Magazine, Fall 2013.

Gauss's Hidden Menagerie: From Cyclotomy to Supercharacters

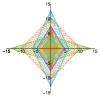
Stephan Ramon Garcia, Trevor Hyde, and Bob Lutz

At the age of eighteen, Gauss established the constructibility of the 17-gon, a result that had eluded mathematicians for two millennia. At the heart of his argument was a keen study of certain sums of complex exponentials, known now as *Gaussian periods*. These sums play starring roles in applications both classical and modern, including Kummer's development of arithmetic in the cyclotomic integers [28] and the optimized AKS primality test of H. W. Lenstra and C. Pomerance [1, 32]. In a poetic twist, this recent application of Gaussian periods realizes "Gauss's dream" of an efficient algorithm for distinguishing prime numbers from composites [24].

We seek here to study Gaussian periods from a graphical perspective. It turns out that these classical objects, when viewed appropriately, exhibit a dazzling and eclectic host of visual qualities. Some images contain discretized versions of familiar shapes, while others resemble natural phenomena. Many can be colorized to isolate certain features; for details, see "Cyclic Supercharacters."



(A) $n = 29 \cdot 109 \cdot 113$, $\omega = 8862$, $c = 113$



(B) $n = 37 \cdot 97 \cdot 113$, $\omega = 5507$, $c = 113$

Figure 1. Eye and jewel—images of *cyclic supercharacters* correspond to sets of Gaussian periods. For notation and terminology, see "Cyclic Supercharacters."

Historical Context

The problem of constructing a regular polygon with compass and straight-edge dates back to ancient times. Descartes and others knew that with only these tools on hand, the motivated geometer could draw, in principle, any segment whose length could be written as a finite composition of sums, products, and square roots of rational numbers [18]. Gauss's construction of the 17-gon relied on showing that

$$16\cos\left(\frac{2\pi}{17}\right) = -1 + \sqrt{17} + \sqrt{34 - 2\sqrt{17}} + 2\sqrt{17 + 3\sqrt{17} - \sqrt{34 - 2\sqrt{17}} - 2\sqrt{34 + 2\sqrt{17}}}$$

was such a length. After reducing the constructibility of the n-gon to drawing the length $\cos\left(\frac{2\pi}{n}\right)$, his result followed easily. So proud was Gauss of this discovery that he wrote about it throughout his

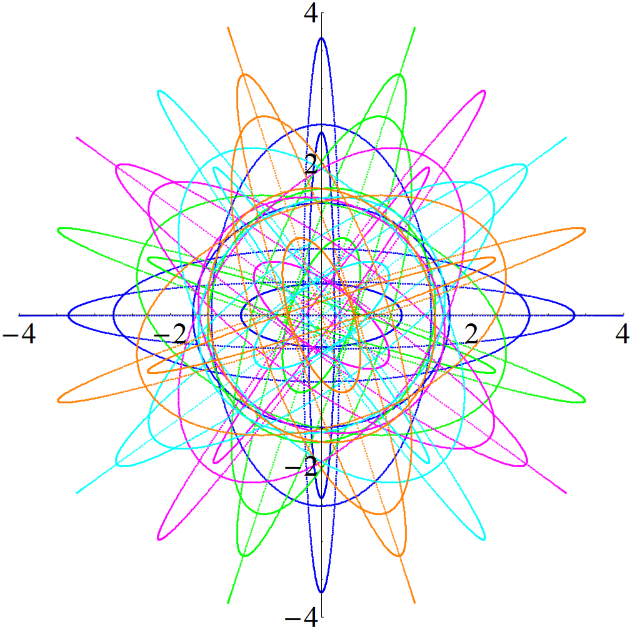
Stephan Ramon Garcia is associate professor of mathematics at Pomona College. His email address is Stephan.Garcia@pomona.edu.

Trevor Hyde is a graduate student at the University of Michigan. His email address is tghyde@umich.edu.

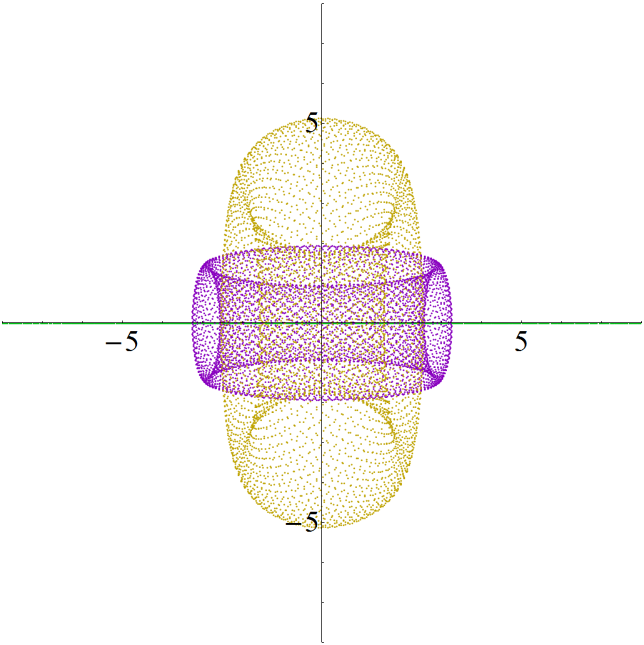
Bob Lutz is a graduate student at the University of Michigan. His email address is boblutz@umich.edu. *All article figures are courtesy of Bob Lutz.*

DOI: http://dx.doi.org/10.1090/noti1269

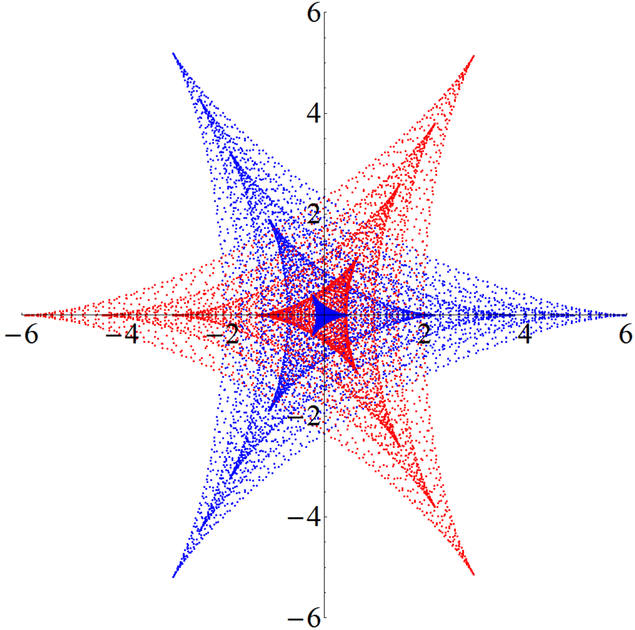
Notices of the AMS, Sept. 2015.



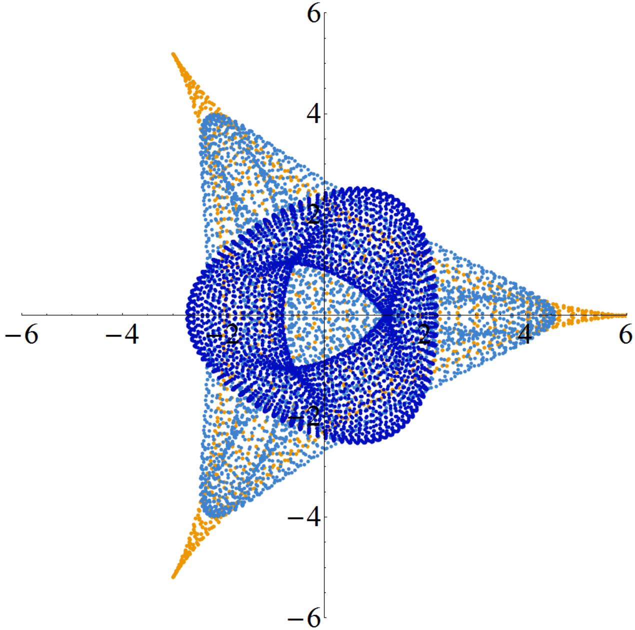
$n = 91205,\ a = 39626$



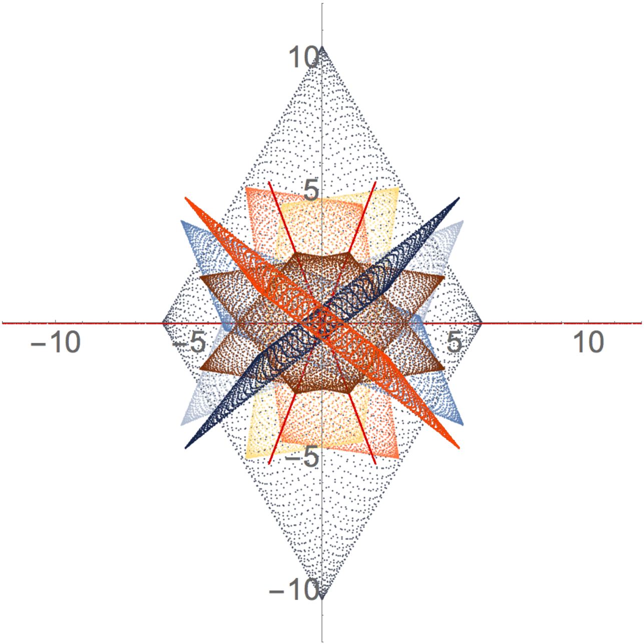
$n = 91205,\ a = 2337$



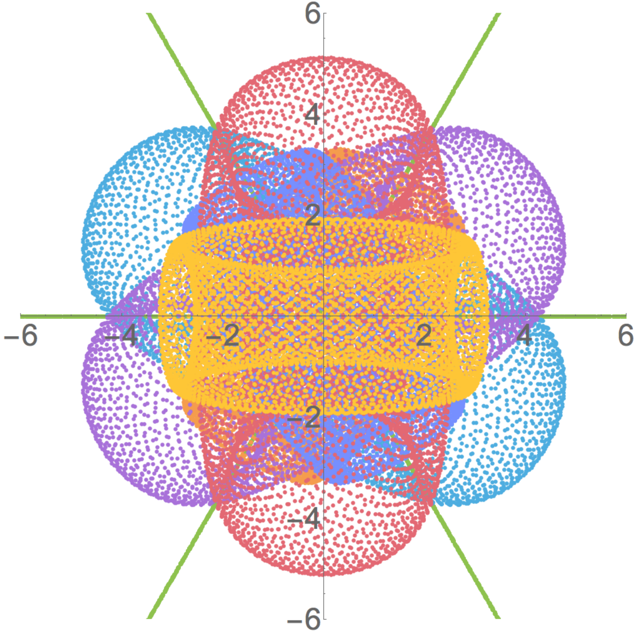
$n = 82677,\ a = 8147$



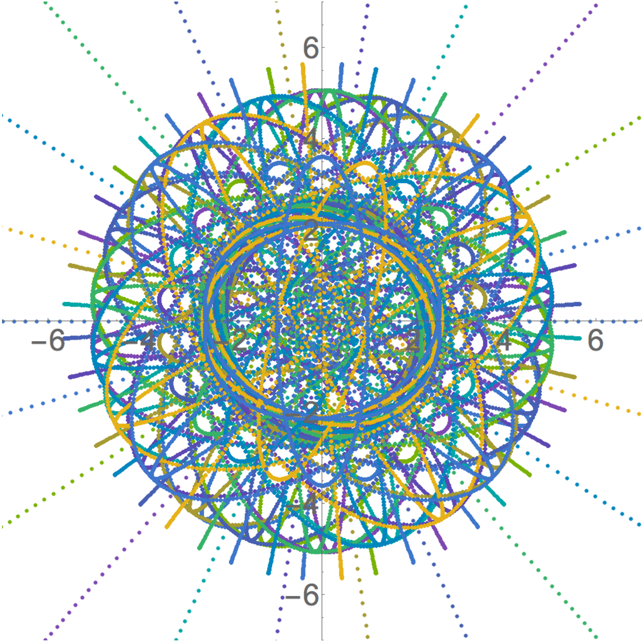
$n = 44161,\ a = 608$



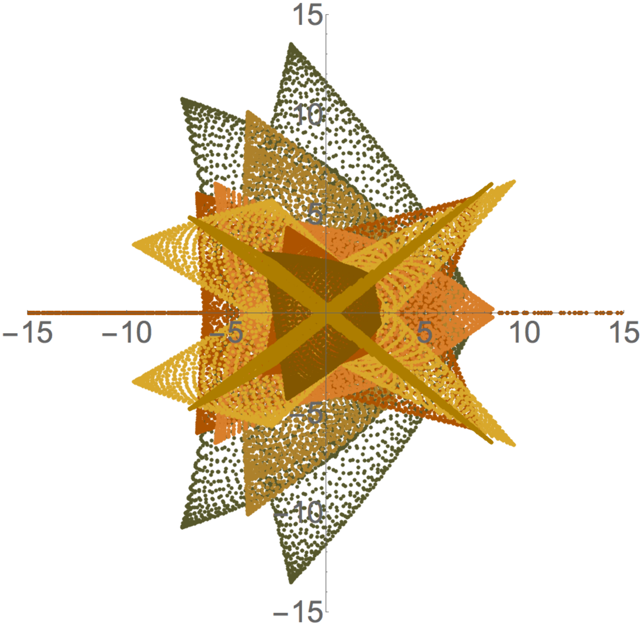
$n = 455175,\ a = 13043$



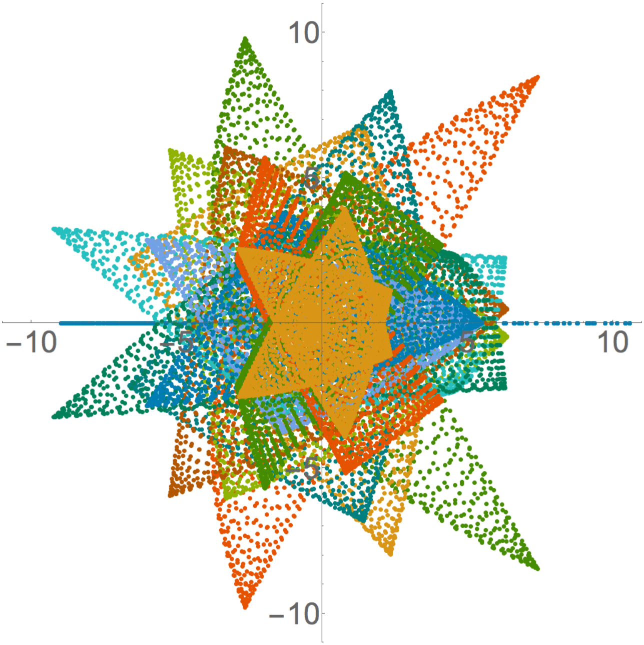
$n = 273615, \ a = 184747$



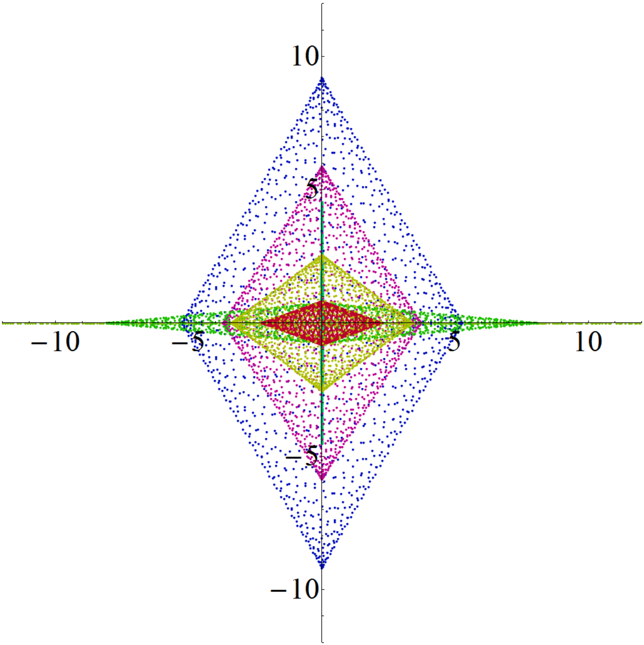
$n = 255255$, $a = 254$



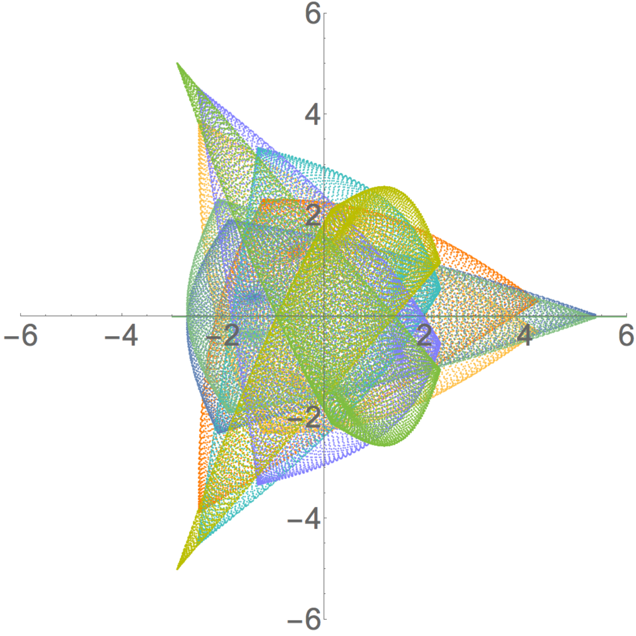
$n = 988113,\ a = 710216$



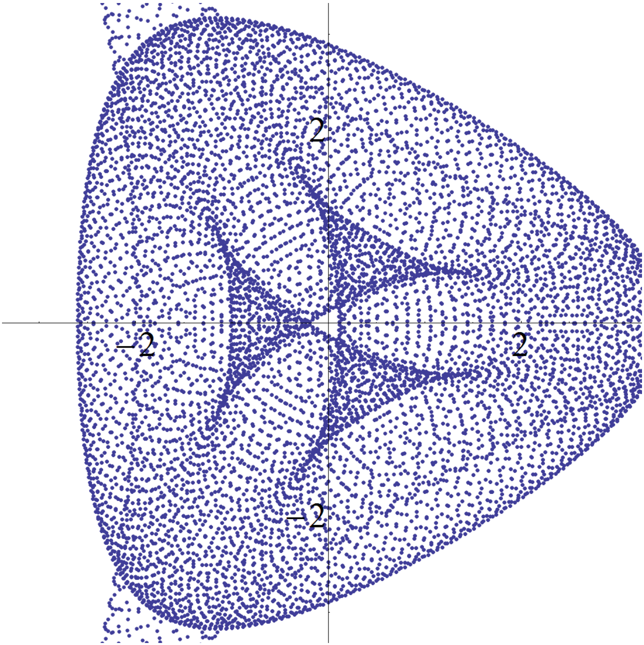
$n = 328549,\ a = 9247$



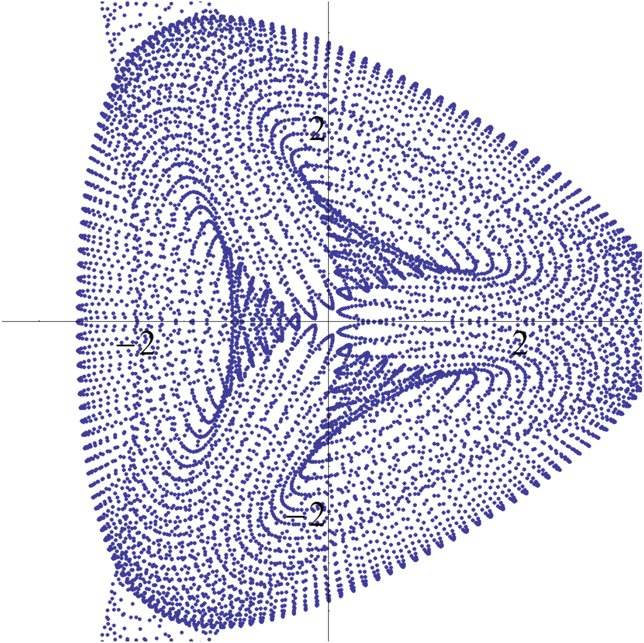
$n = 91205,\ a = 1322$



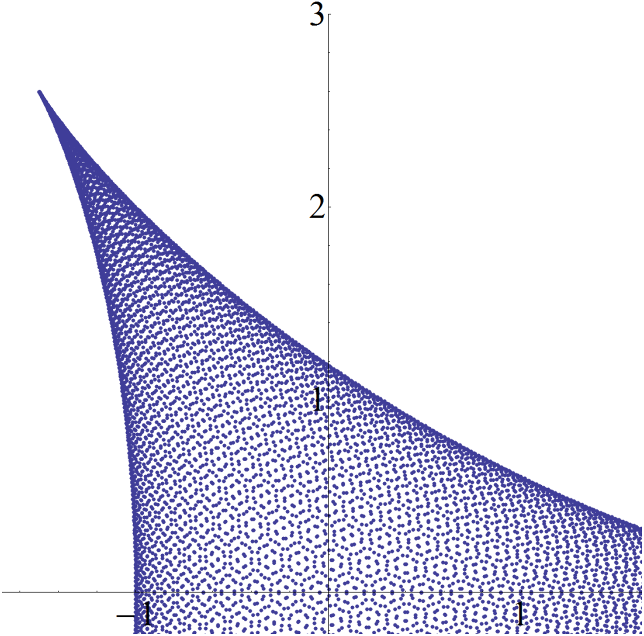
$n = 477493,\ a = 2547$



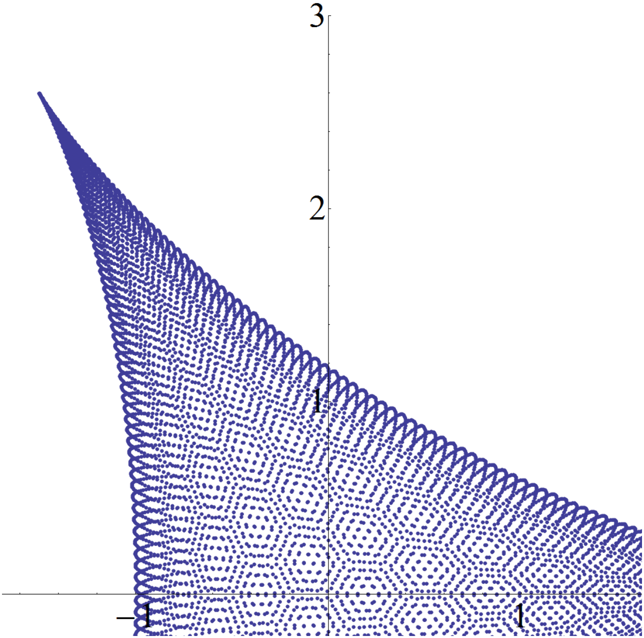
$n = 52059$, $a = 565$



$n = 52059$, $a = 766$



$n = 44161,\ a = 16376$



$n = 44161,\ a = 4637$

It's not all about pretty pictures

Theorem (W. Duke, SRG, B. Lutz '13)

Suppose that $p|n$ *and* $p \equiv 1 \,(mod\ 4)$ *is prime. Let*

$$Q_p = \{m \in \mathbb{Z}/p\mathbb{Z} : \left(\frac{m}{p}\right) = 1\}$$

denote the set of distinct nonzero quadratic residues modulo p. If

$$\Gamma = \{jn/k + 1 : j \in J_+\} \cup \{jn/k - 1 : j \in J_-\}$$

holds where

$$J_+ = \{aq + b : q \in Q_p\} \quad \text{and} \quad J_- = \{cq - b : q \in Q_p\}$$

for integers a, b, c *coprime to p with* $(\frac{a}{p}) = -(\frac{c}{p})$, *then* $\sigma_X(y)$ *belongs to the real interval* $[1-p, p-1]$ *whenever* $p|y$, *and otherwise belongs to the ellipse described by the equation* $(\mathrm{Re}\, z)^2 + (\mathrm{Im}\, z)^2/p = 1$.

Theorem (W. Duke, SRG, B. Lutz '13)

Suppose that $p|n$ *and* $p \equiv 1 \pmod 4$ *is prime. Let*

$$Q_p = \{m \in \mathbb{Z}/p\mathbb{Z} : \left(\frac{m}{p}\right) = 1\}$$

denote the set of distinct nonzero quadratic residues modulo p*. If*

$$\Gamma = \{jn/k + 1 : j \in J_+\} \cup \{jn/k - 1 : j \in J_-\}$$

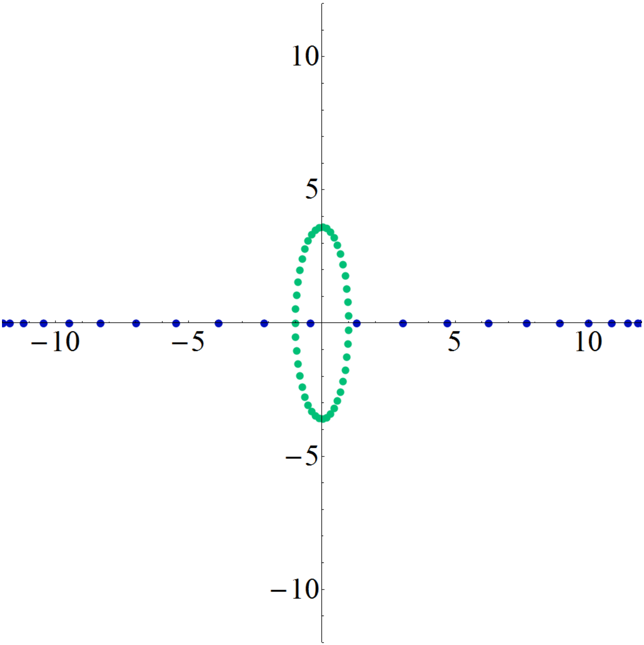
holds where

$$J_+ = \{aq + b : q \in Q_p\} \quad \text{and} \quad J_- = \{cq - b : q \in Q_p\}$$

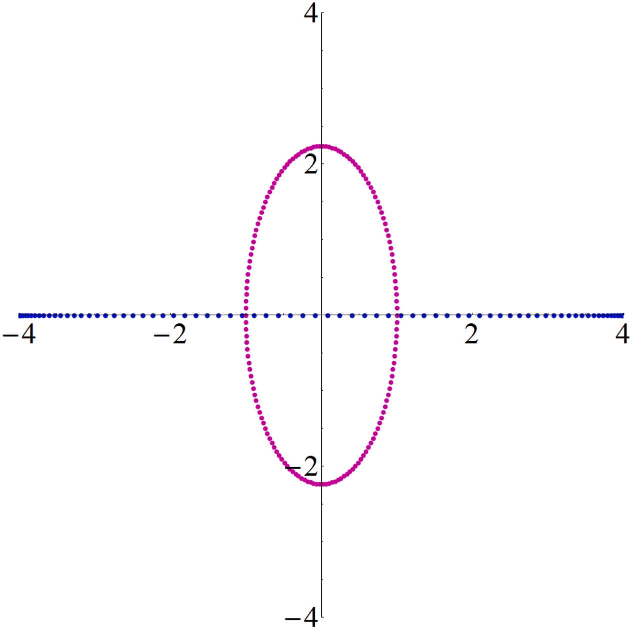
for integers a, b, c *coprime to* p *with* $(\frac{a}{p}) = -(\frac{c}{p})$*, then* $\sigma_X(y)$ *belongs to the real interval* $[1 - p, p - 1]$ *whenever* $p|y$*, and otherwise belongs to the ellipse described by the equation* $(\mathrm{Re}\, z)^2 + (\mathrm{Im}\, z)^2/p = 1$*.*

Translation

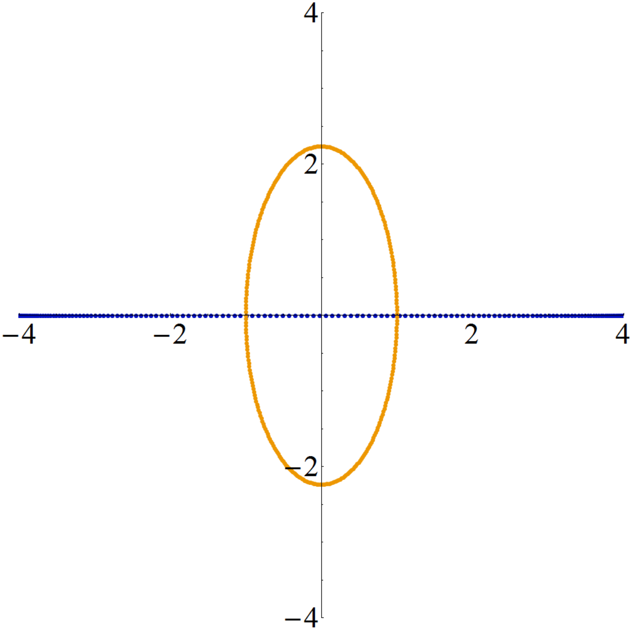
Certain combinations of parameters yield ellipses.



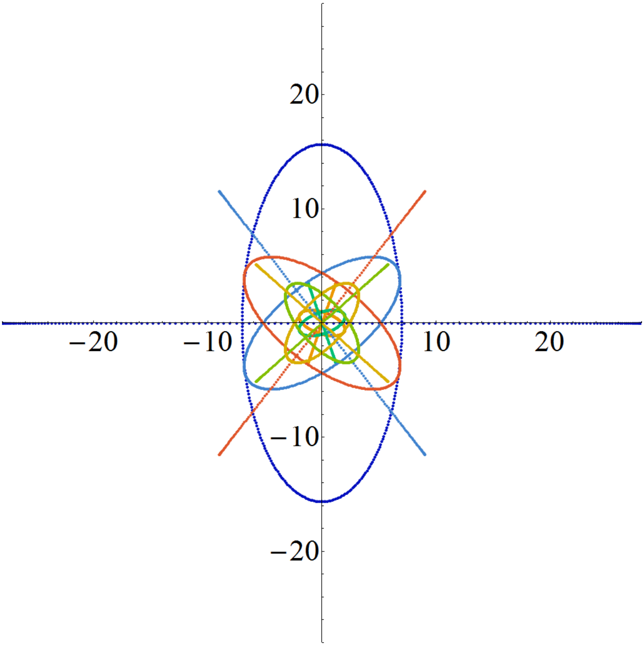
$n = 559,\ a = 171$



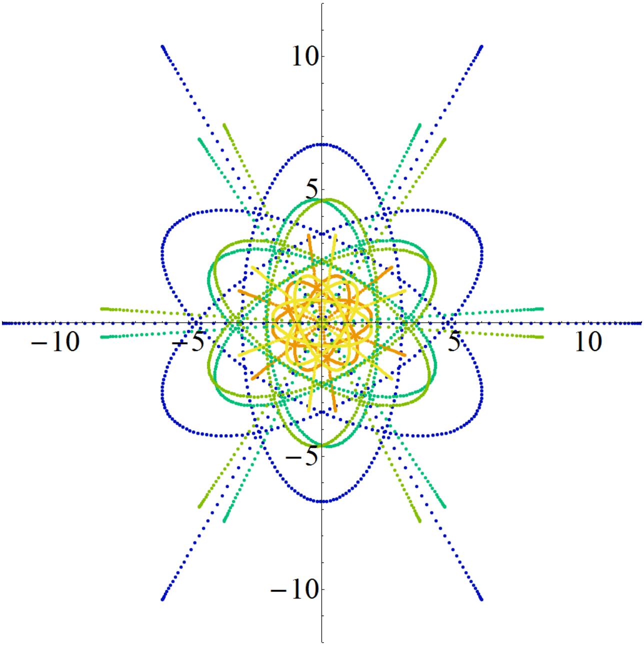
$n = 770,\ a = 153$



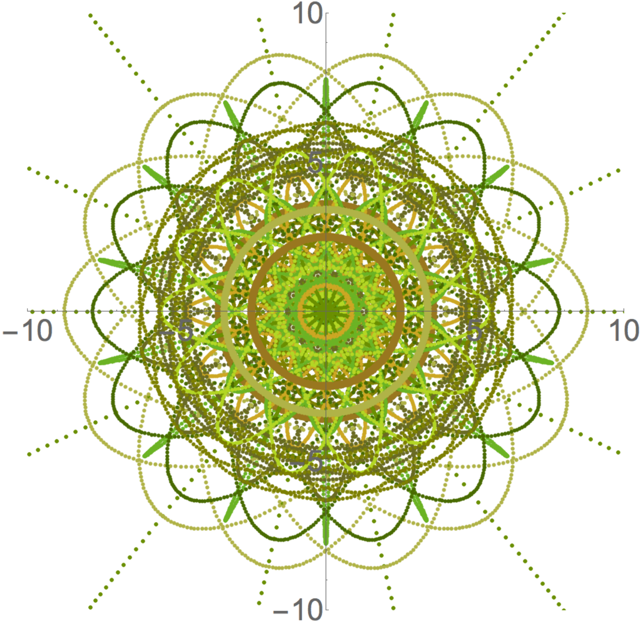
$n = 1535,\ a = 613$



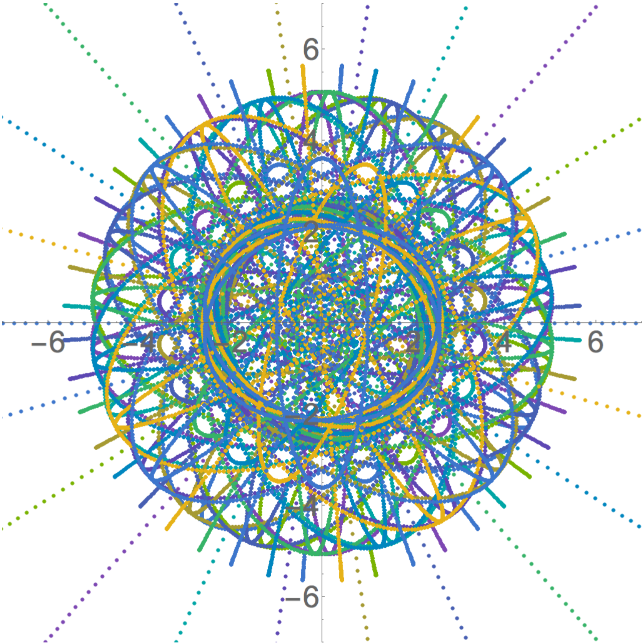
$n = 66005,\ a = 613$



$n = 30030,\ a = 1693$



$n = 455175,\ a = 3599$



$n = 255255,\ a = 254$

Theorem (W. Duke, SRG, B. Lutz '13)

Let r belong to $\mathbb{Z}/n\mathbb{Z}$, and suppose that $(r, n) = \frac{n}{d}$ for some positive divisor d of n, so that $\xi = \frac{rd}{n}$ is a unit modulo n. Also let

$$\psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$$

denote the natural homomorphism.

(i) *The images of $\sigma_{\Gamma r}$, $\sigma_{\Gamma (r,n)}$, and $\sigma_{\psi_d(\Gamma)1}$ are equal.*

(ii) *The image in (i), when scaled by $\frac{|\Gamma|}{|\psi_d(\Gamma)|}$, is a subset of the image of $\sigma_{\Gamma \xi}$.*

Theorem (W. Duke, SRG, B. Lutz '13)

Let r belong to $\mathbb{Z}/n\mathbb{Z}$, and suppose that $(r, n) = \frac{n}{d}$ for some positive divisor d of n, so that $\xi = \frac{rd}{n}$ is a unit modulo n. Also let

$$\psi : \mathbb{Z}/n\mathbb{Z} \to \mathbb{Z}/d\mathbb{Z}$$

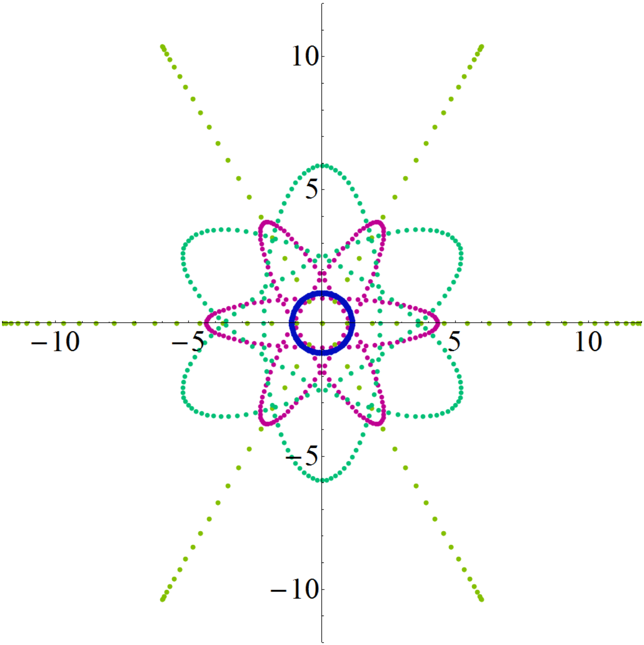
denote the natural homomorphism.

(i) *The images of $\sigma_{\Gamma r}$, $\sigma_{\Gamma(r,n)}$, and $\sigma_{\psi_d(\Gamma)1}$ are equal.*

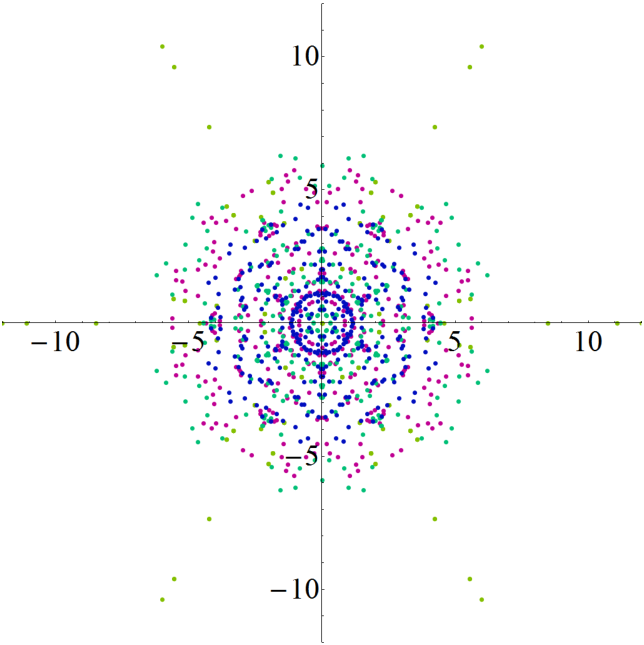
(ii) *The image in (i), when scaled by $\frac{|\Gamma|}{|\psi_d(\Gamma)|}$, is a subset of the image of $\sigma_{\Gamma\xi}$.*

Translation

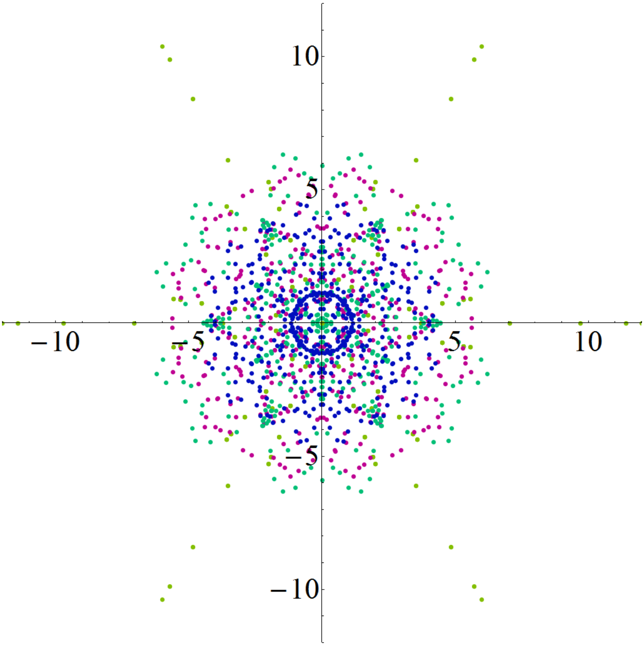
If a bunch of n's and a's are chosen appropriately, the corresponding images "grow" or "nest."



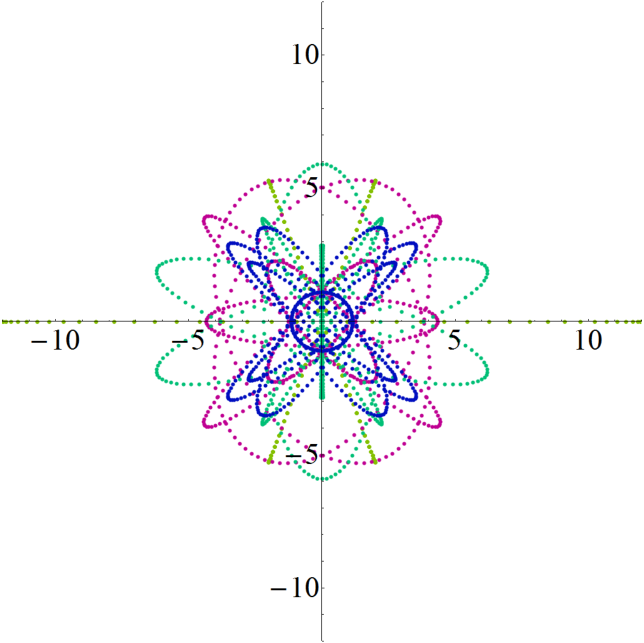
$n = 8880,\ a = 319$



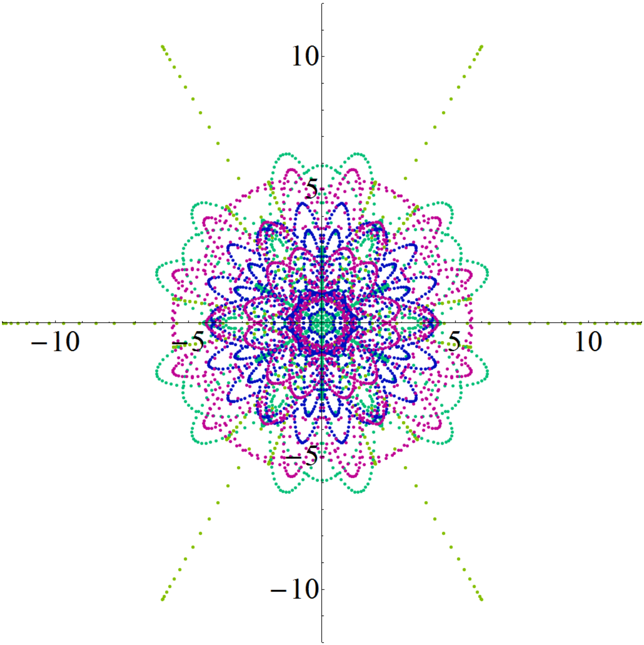
$n = 12432,\ a = 319$



$n = 15540,\ a = 319$



$n = 20720,\ a = 319$



$n = 62160,\ a = 319$

Theorem (W. Duke, SRG, B. Lutz '13)

Let σ_X be a cyclic supercharacter of $\mathbb{Z}/q\mathbb{Z}$, where q is a nonzero power of an odd prime p. If $X = A1$ and $|X| = d$ divides $p-1$, then the image of σ_X is contained in the image of the function $g : \mathbb{T}^{\phi(d)} \to \mathbb{C}$ defined by

$$g(z_1, z_2, \ldots, z_{\phi(d)}) = \sum_{k=0}^{d-1} \prod_{j=0}^{\phi(d)-1} z_{j+1}^{b_{k,j}}$$

where the integers $b_{k,j}$ are given by

$$t^k \equiv \sum_{j=0}^{\phi(d)-1} b_{k,j} t^j \pmod{\Phi_d(t)}.$$

For a fixed d, as q becomes large, the image of σ_X fills out the image of g, in the sense that, given $\epsilon > 0$, there exists some $q \equiv 1 \pmod{d}$ such that if $\sigma_X : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ is a cyclic supercharacter with $|X| = d$, then every open ball of radius $\epsilon > 0$ in the image of g has nonempty intersection with the image of σ_X.

Theorem (W. Duke, SRG, B. Lutz '13)

Let σ_X be a cyclic supercharacter of $\mathbb{Z}/q\mathbb{Z}$, where q is a nonzero power of an odd prime p. If $X = A1$ and $|X| = d$ divides $p-1$, then the image of σ_X is contained in the image of the function $g : \mathbb{T}^{\phi(d)} \to \mathbb{C}$ defined by

$$g(z_1, z_2, \ldots, z_{\phi(d)}) = \sum_{k=0}^{d-1} \prod_{j=0}^{\phi(d)-1} z_{j+1}^{b_{k,j}}$$

where the integers $b_{k,j}$ are given by

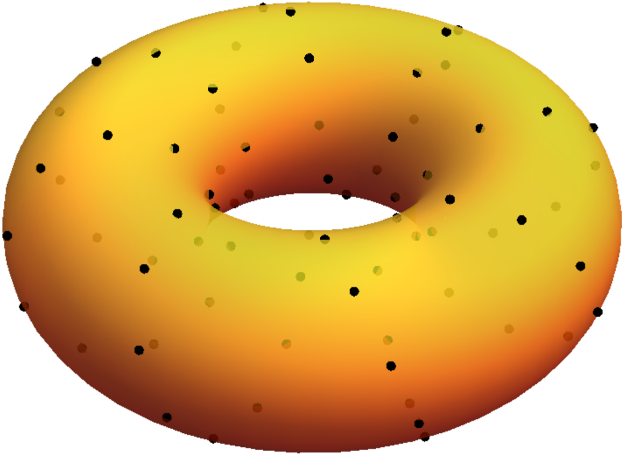
$$t^k \equiv \sum_{j=0}^{\phi(d)-1} b_{k,j} t^j \pmod{\Phi_d(t)}.$$

For a fixed d, as q becomes large, the image of σ_X fills out the image of g, in the sense that, given $\epsilon > 0$, there exists some $q \equiv 1 \pmod{d}$ such that if $\sigma_X : \mathbb{Z}/q\mathbb{Z} \to \mathbb{C}$ is a cyclic supercharacter with $|X| = d$, then every open ball of radius $\epsilon > 0$ in the image of g has nonempty intersection with the image of σ_X.

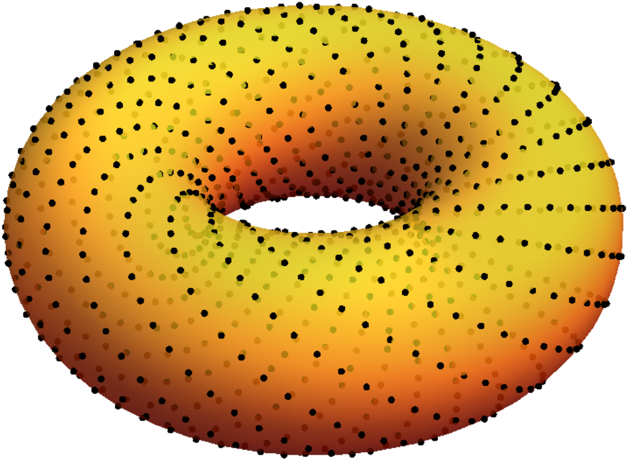
Translation

Plots can "fill out" the image of simple "mapping functions" $g : \mathbb{T}^m \to \mathbb{C}$ from high-dimensional tori into $\mathbb{C}$.

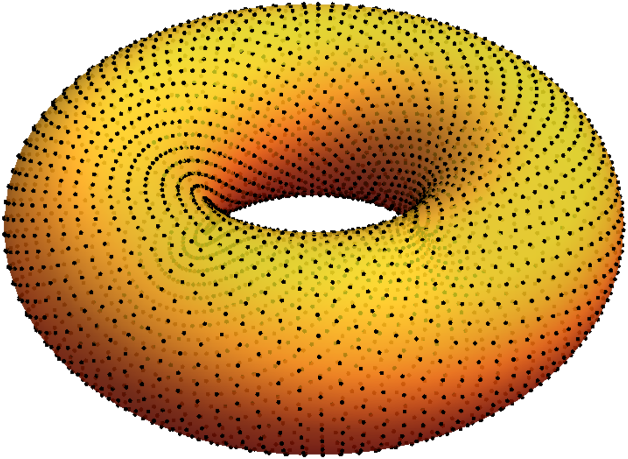
Deformation of a torus



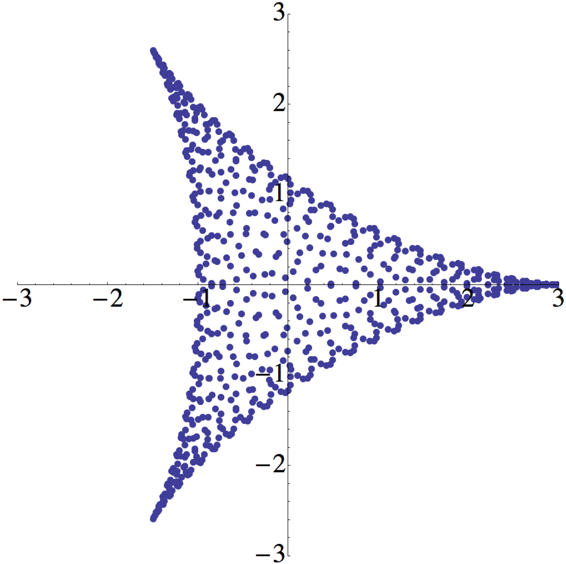
$n = 73$



$n = 961$

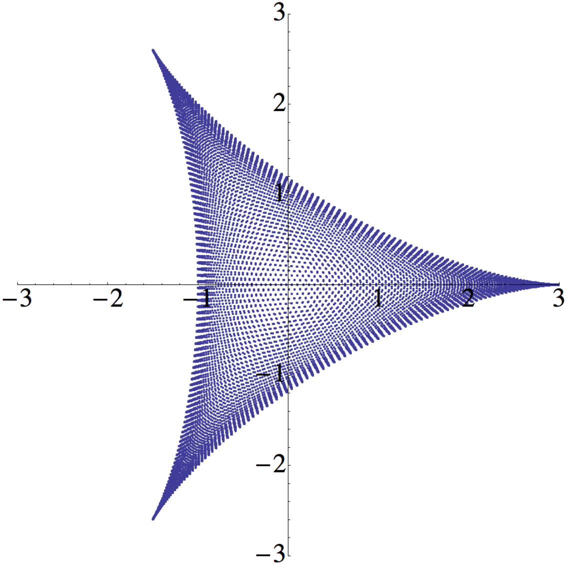


$n = 3571$



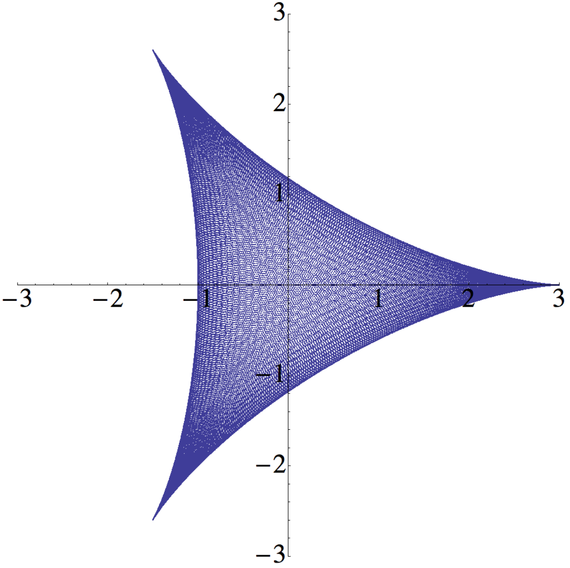
$n = 2017$, $a = 294$

$g(z_1, z_2) = z_1 + z_2 + z_1^{-1} z_2^{-1}$



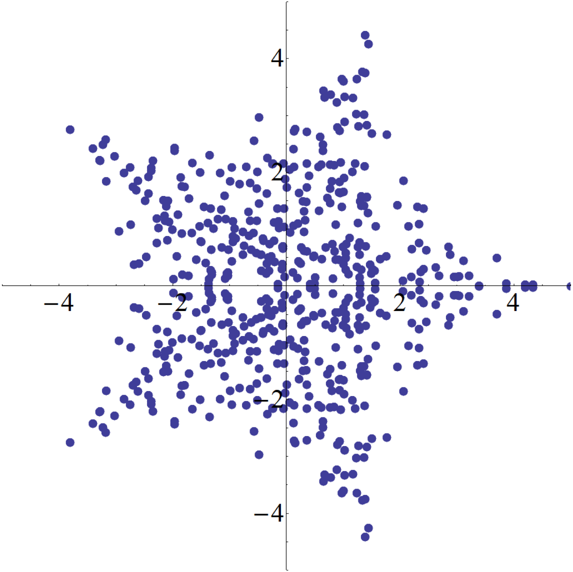
$n = 32587,\ a = 10922$

$g(z_1, z_2) = z_1 + z_2 + z_1^{-1} z_2^{-1}$



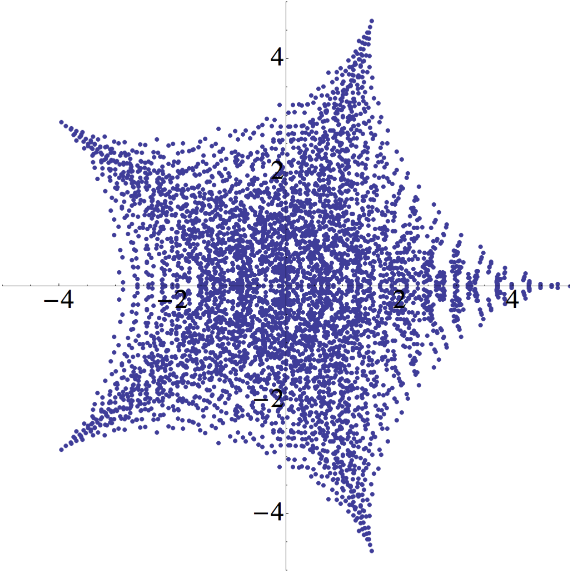
$n = 200017,\ a = 35098$

$g(z_1, z_2) = z_1 + z_2 + z_1^{-1} z_2^{-1}$



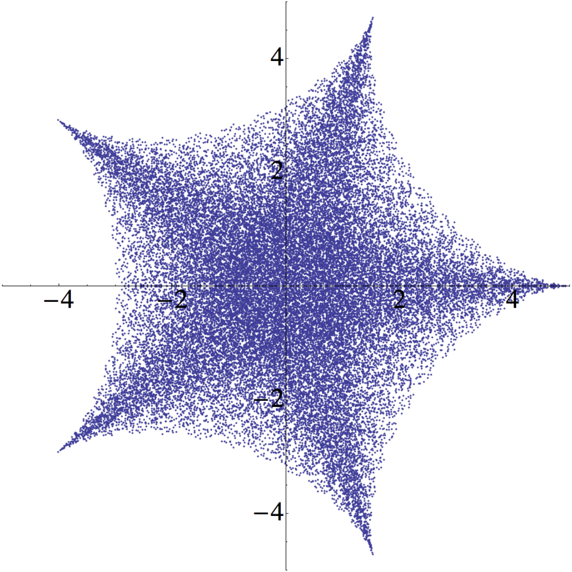
$n = 2791,\ a = 800$

$g(z_1, z_2, z_3, z_4) = z_1 + z_2 + z_3 + z_4 + z_1^{-1} z_2^{-1} z_3^{-1} z_4^{-1}$



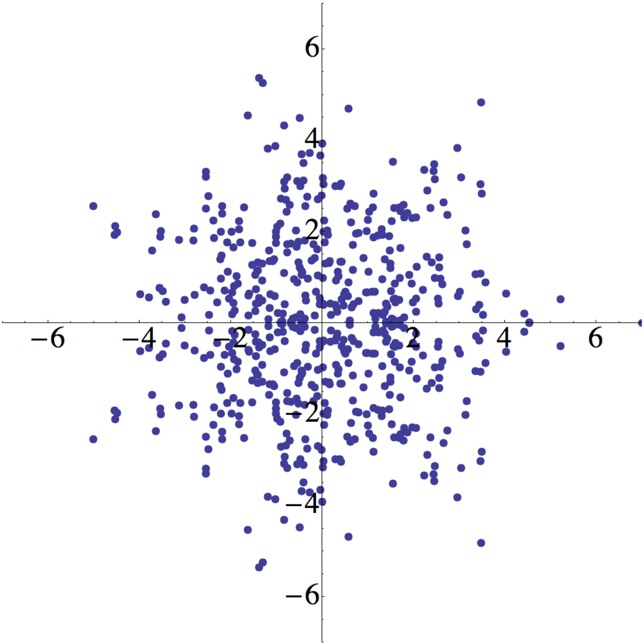
$n = 27011,\ a = 9360$

$g(z_1, z_2, z_3, z_4) = z_1 + z_2 + z_3 + z_4 + z_1^{-1} z_2^{-1} z_3^{-1} z_4^{-1}$

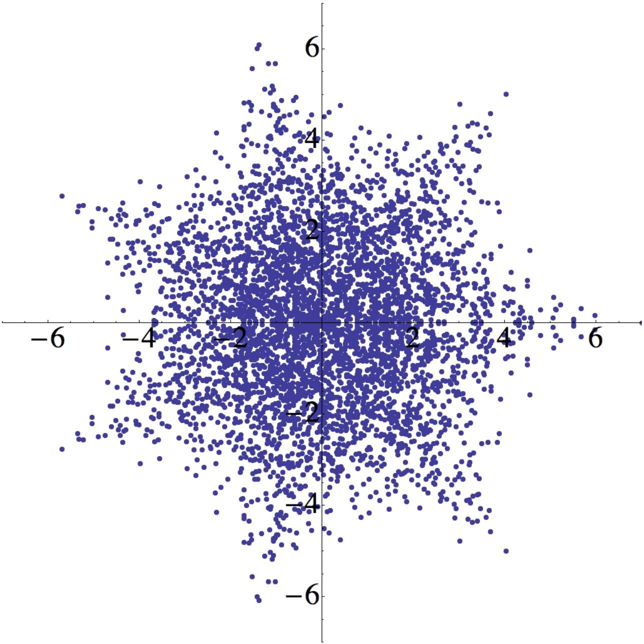


$n = 202231$, $a = 61576$

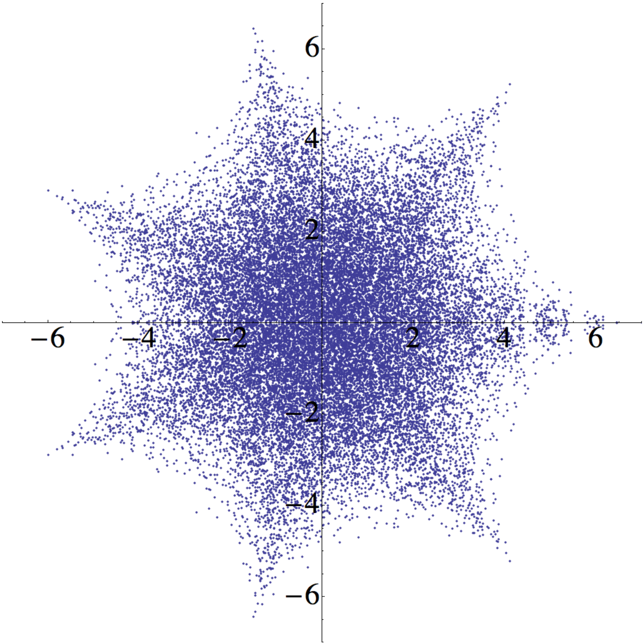
$$g(z_1, z_2, z_3, z_4) = z_1 + z_2 + z_3 + z_4 + z_1^{-1} z_2^{-1} z_3^{-1} z_4^{-1}$$



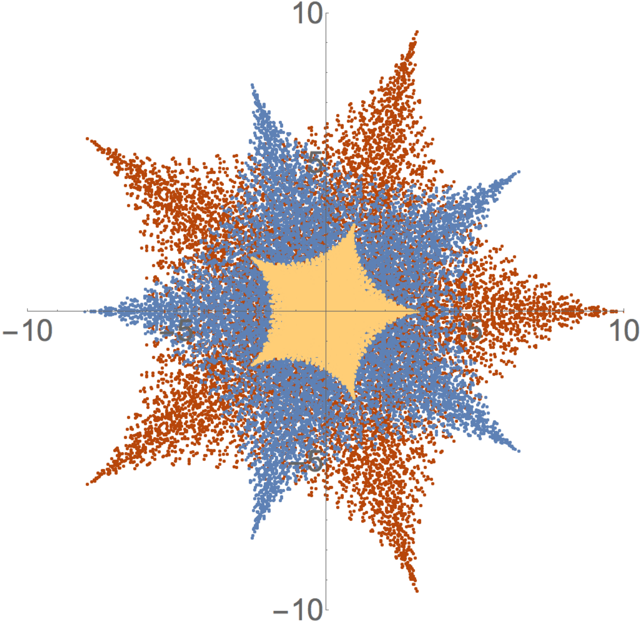
$n = 4019$, $a = 1551$



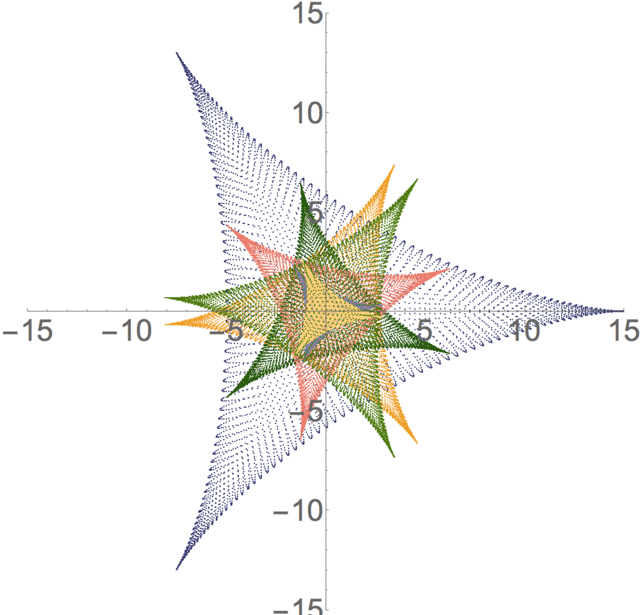
$n = 32173,\ a = 3223$



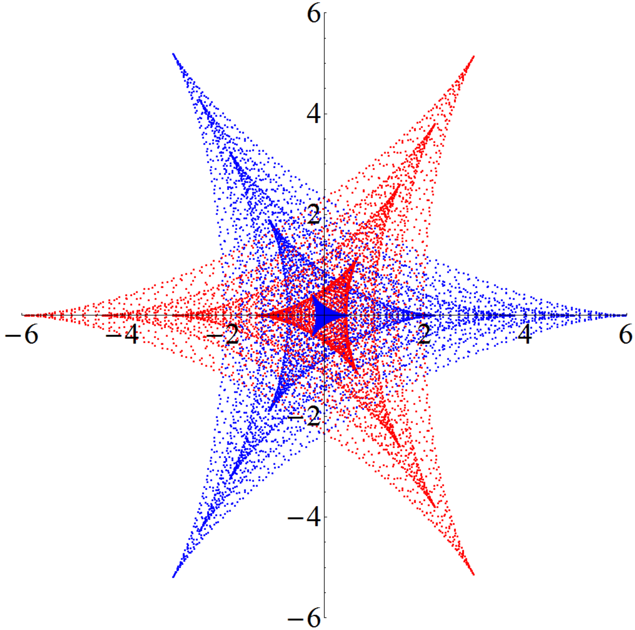
$n = 200033$, $a = 11073$



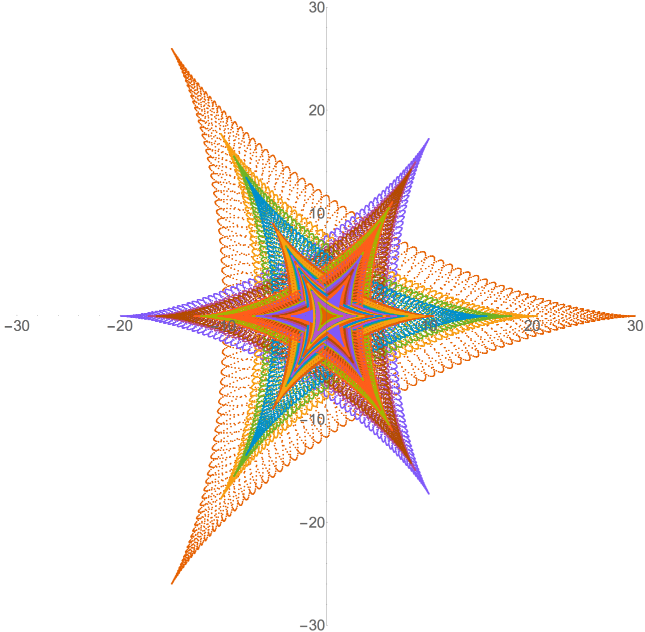
$n = 352655,\ a = 54184$



$n = 477493,\ a = 2546$



$n = 82677,\ a = 8147$



$n = 6467729,\ a = 6085605$

Exponential sums

S. Ramanujan

$$\sum_{\substack{j=1 \\ (j,n)=1}}^{n} e^{\frac{2\pi ijx}{n}}$$

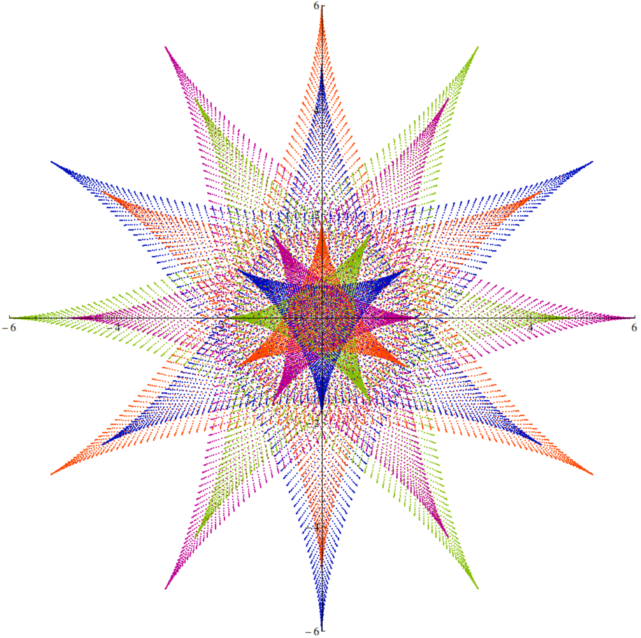
H. Kloosterman

$$\sum_{\substack{\ell=1 \\ (\ell,n)=1}}^{n} e^{\frac{2\pi i(a\ell+b\bar{\ell})}{n}}$$

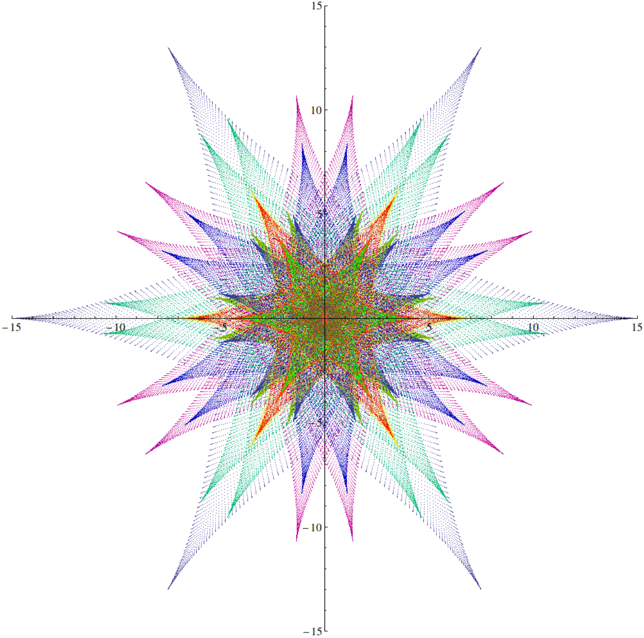
C.F. Gauss

$$\sum_{k=1}^{n} e^{\frac{2\pi ixk^2}{n}}$$

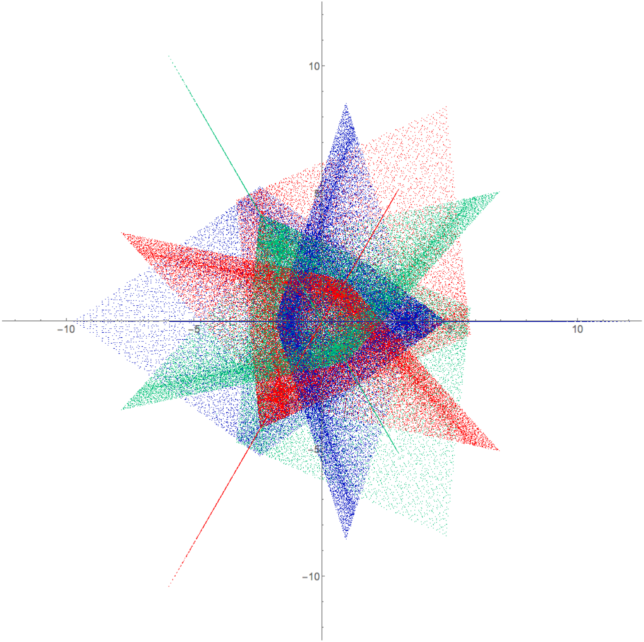
My students and I established a general framework under which a wide variety of exponential sums of interest in number theory can be studied. Some of these sums, such as *generalized Kloosterman sums*, yield interesting images as well.



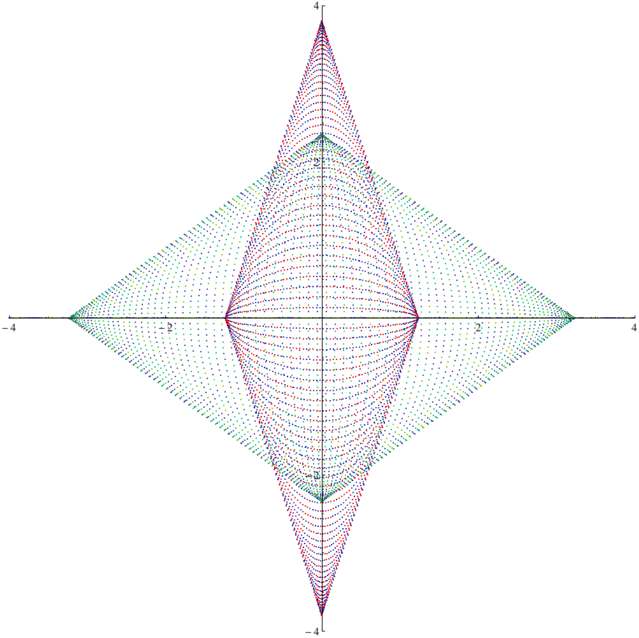
$n = 3020,\ a = 1089$



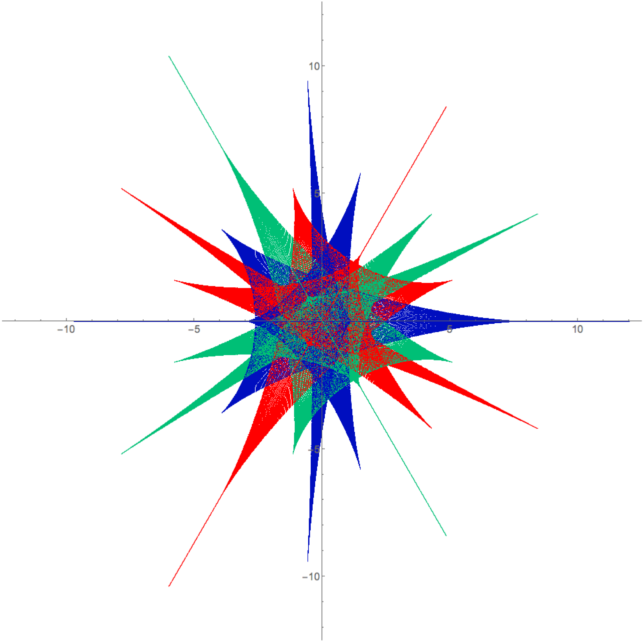
$n = 4378,\ a = 291$



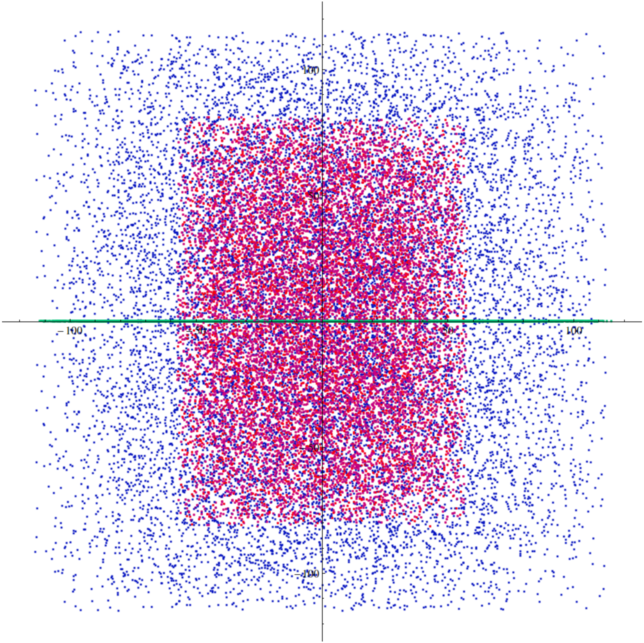
$n = 9015,\ a = 2284$



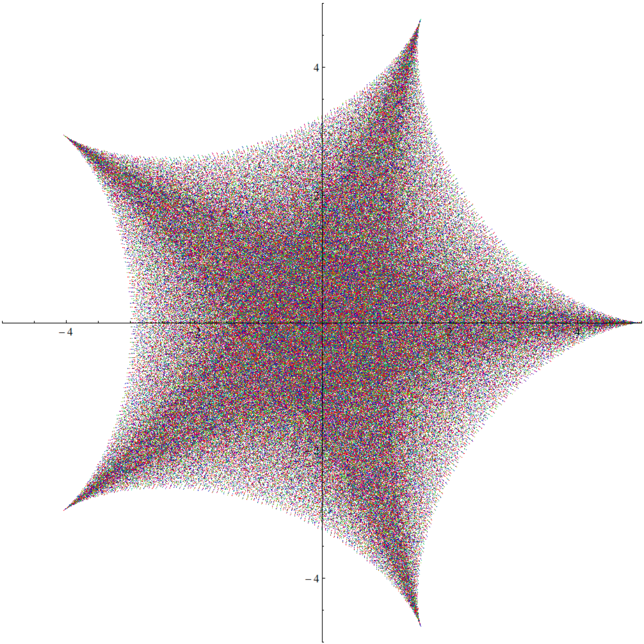
$n = 890$, $a = 479$



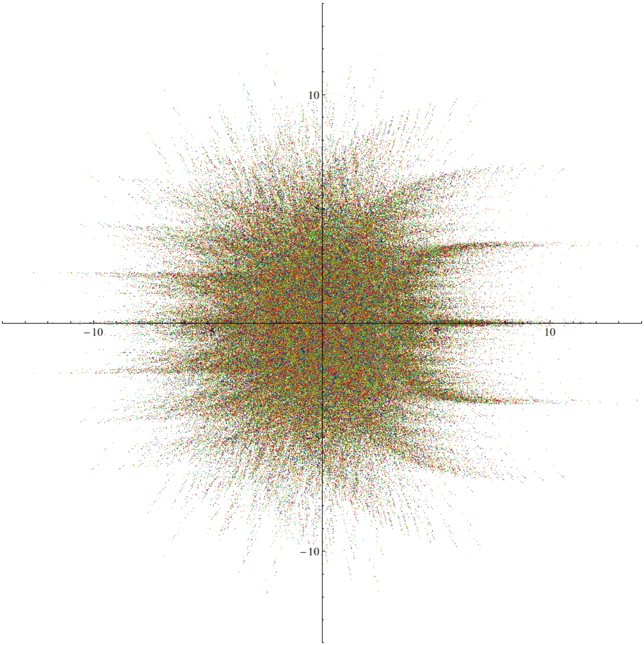
$n = 9015,\ a = 577$



$n = 13309, \ a = 7$



$n = 2221$, $a = 71$



$n = 3571,\ a = 47$

Alice Chan, Cooper Galvin & Gabriella Heller Win National Science Foundation Fellowships

By Cynthia Peters 1:30 pm April 28, 2014 Students, Research

Pomona College seniors Alice Chan, Galvin Cooper and Gabriella Heller have been awarded National Science Foundation (NSF) Graduate Research Fellowships along with seven Pomona alumni. The grants provide an annual stipend of $32,000 for three years and a $12,000 cost-of-education allowance to the institution. Recipients are selected “based on their demonstrated potential for significant achievements in science and engineering.”

Alice Chan

Alice Chan, a mathematics major from Westford, Mass., will pursue a Ph.D. in mathematics, at UC San Diego. Her NSF proposal, "Reconstruction without Phase and Finite Frame Decomposition," involves applying frame theory to the field of compressed sensing, which studies the problem of reconstructing signals when they are sparse in some domain. This is critical, she says, in areas such as reducing the length of MRI scanning sessions and increasing the power of computational photography.

At Pomona, she has conducted research with Prof. Stephan Garcia and fellow students Luis Garcia German and Amy Shoemaker (both PO'14), which has resulted in the publication "On the matrix equation XA+AX^T=0, II: Type 0-I interactions" in the journal *Linear Algebra and its Applications*. Her senior thesis focuses on an extension of Kloosterman sums, which comprise a standard tool in analytic number theory.

http://www.pomona.edu/news/2014/04/28-nsf-fellowships.aspx

What's the big deal about exponential sums?

Concerning Zhang's work on bounded gaps between primes:

> *"For the Type I and Type II sums, it was the classical Weil bound on Kloosterman sums that were the key source of power saving... For the Type III sums, one needs a significantly deeper consequence of the Weil conjectures, namely the estimate of Bombieri and Birch on a three-dimensional variant of a Kloosterman sum. Furthermore, the Ramanujan sums... make a crucial appearance... This improvement over the square root heuristic, which is ultimately due to the presence of a Ramanujan sum inside this three-dimensional exponential sum in certain degenerate cases, is crucial to Zhang's argument." - Terence Tao*

Source: `http://terrytao.wordpress.com/2013/06/14/estimation-of-the-type-iii-sums/`

Faux symmetry

For the record

The first interesting “supercharacter plots” were discovered by my 2012 REU group. In fact, they discovered an entirely new class of intriguing exponential sums.

Faux symmetry

For the record

The first interesting "supercharacter plots" were discovered by my 2012 REU group. In fact, they discovered an entirely new class of intriguing exponential sums.

For your safety

I won't even attempt to describe the math behind the REU plots. Let's just say that the parameters involved are

- a modulus n,
- a dimension d,
- a list $\mathbf{x} = (x_1, x_2, \ldots, x_d)$ of integers.

Faux symmetry

For the record

The first interesting "supercharacter plots" were discovered by my 2012 REU group. In fact, they discovered an entirely new class of intriguing exponential sums.

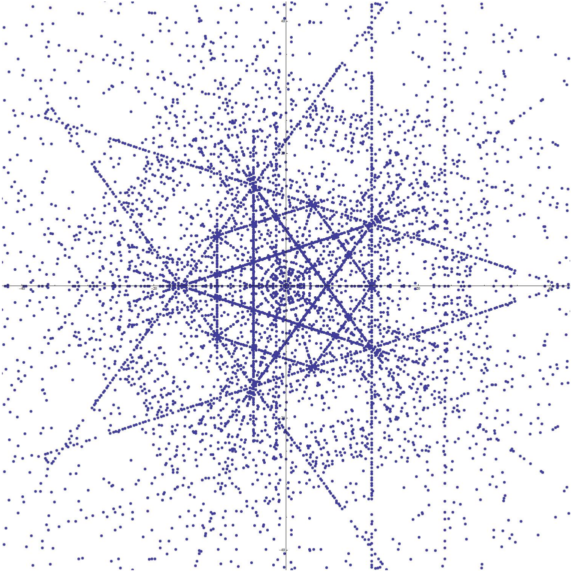
For your safety

I won't even attempt to describe the math behind the REU plots. Let's just say that the parameters involved are

- a modulus n,
- a dimension d,
- a list $\mathbf{x} = (x_1, x_2, \ldots, x_d)$ of integers.

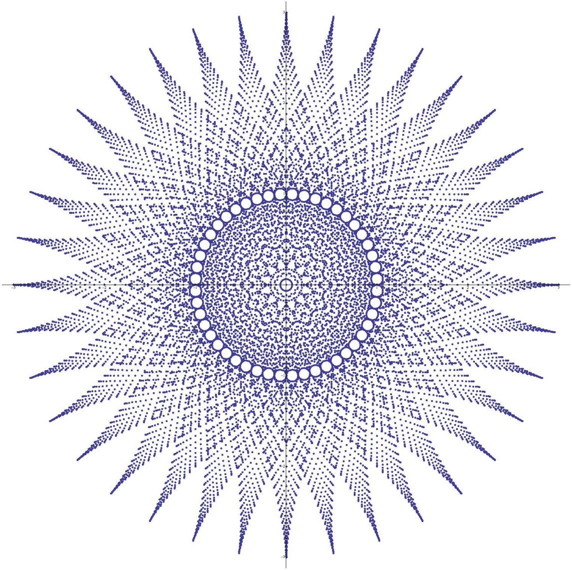
Beware of *faux symmetry*

A puzzling feature of some REU plots is "faux symmetry" - the sneaky appearance of fraudulent large scale symmetry!



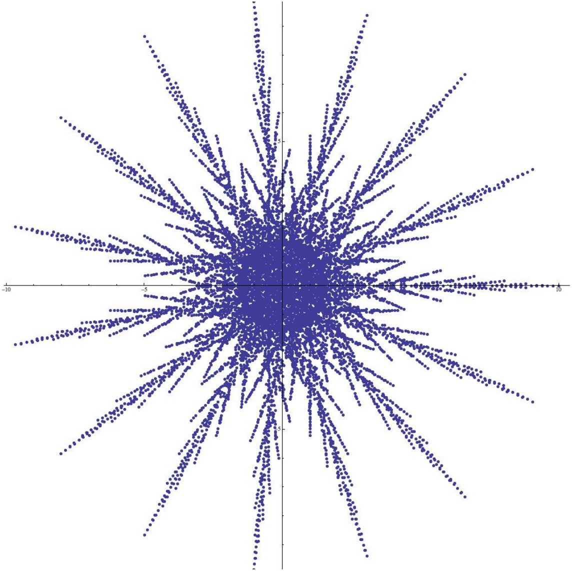
$n = 10,\ d = 8,\ \mathbf{x} = (0, 1, 3, 8, 8, 8, 8, 8)$

5-fold rotational symmetry



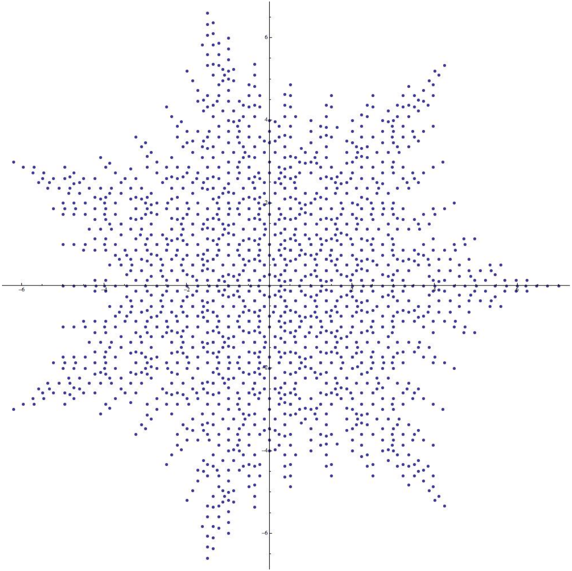
$n = 96,\ d = 3,\ \mathbf{x} = (1, 1, 6)$

36-fold faux symmetry, 12-fold rotational symmetry



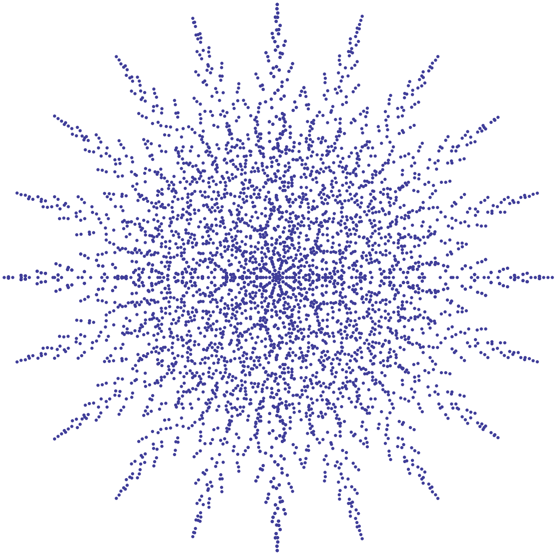
$n = 24$, $d = 5$, $\mathbf{x} = (1, 1, 2, 2, 2)$

15-fold faux symmetry, 3-fold rotational symmetry



$n = 12,\ d = 7,\ \mathbf{x} = (1, 1, 1, 1, 1, 1, 6)$

7-fold faux symmetry, no rotational symmetry



$n = 25,\ d = 4,\ \mathbf{x} = (1,1,1,2)$

20-fold faux symmetry, 5-fold rotational symmetry

Large scale order

Certain families of plots exhibit "coherence" and their asymptotic behavior can be finely described.

Large scale order

Certain families of plots exhibit "coherence" and their asymptotic behavior can be finely described.

Theorem

Fix n and d and let $X = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_r\}$ be a S_d-orbit in $(\mathbb{Z}/n\mathbb{Z})^d$. Suppose that the $d \times r$ matrix $A = [\mathbf{x}_1 \ \mathbf{x}_2 \ \ldots \ \mathbf{x}_r]$ can be row reduced modulo n to obtain a simpler matrix $B = [\mathbf{b}_1 \ \mathbf{b}_2 \ \ldots \ \mathbf{b}_r]$. If the final k rows of B are zero, then the image of $\sigma_X : (\mathbb{Z}/n\mathbb{Z})^d \to \mathbb{C}$ "roughly approximates" the image of the function $g : \mathbb{T}^{d-k} \to \mathbb{C}$ defined by

$$g(z_1, z_2, \ldots, z_{d-k}) = \sum_{\ell=1}^{r} \prod_{j=1}^{d-k} z_j^{b_{j\ell}}.$$

Large scale order

Certain families of plots exhibit "coherence" and their asymptotic behavior can be finely described.

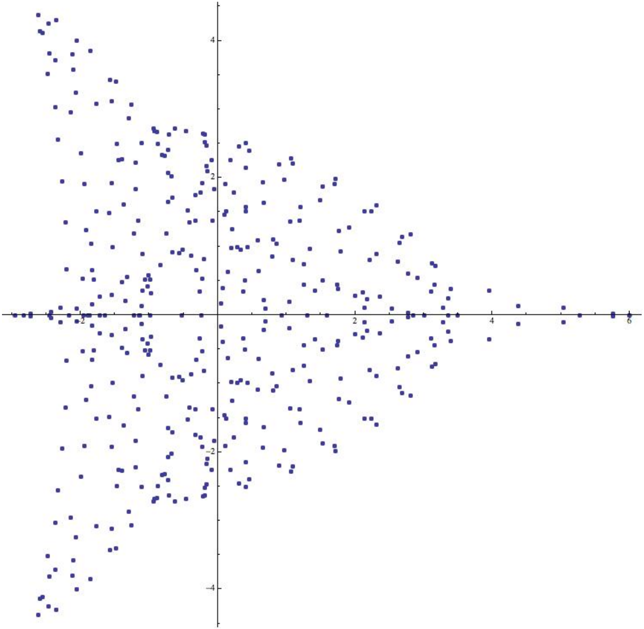
Theorem

Fix n and d and let $X = \{\mathbf{x}_1, \mathbf{x}_2, \ldots, \mathbf{x}_r\}$ be a S_d-orbit in $(\mathbb{Z}/n\mathbb{Z})^d$. Suppose that the $d \times r$ matrix $A = [\mathbf{x}_1\ \mathbf{x}_2\ \ldots\ \mathbf{x}_r]$ can be row reduced modulo n to obtain a simpler matrix $B = [\mathbf{b}_1\ \mathbf{b}_2\ \ldots\ \mathbf{b}_r]$. If the final k rows of B are zero, then the image of $\sigma_X : (\mathbb{Z}/n\mathbb{Z})^d \to \mathbb{C}$ "roughly approximates" the image of the function $g : \mathbb{T}^{d-k} \to \mathbb{C}$ defined by

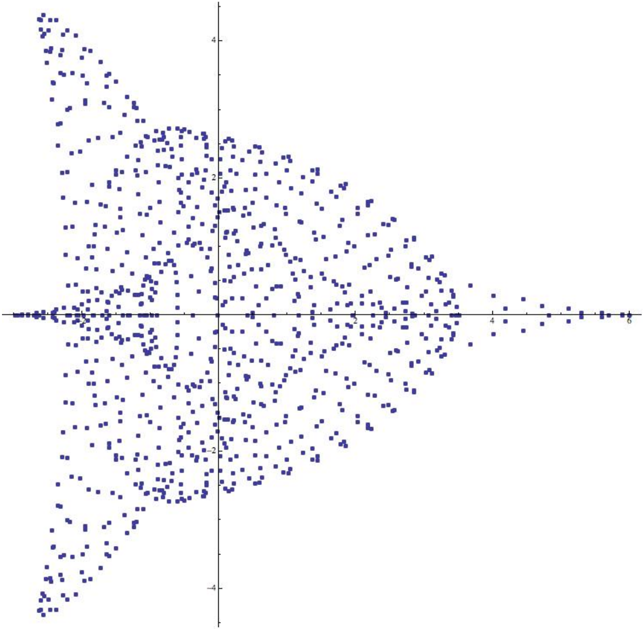
$$g(z_1, z_2, \ldots, z_{d-k}) = \sum_{\ell=1}^{r} \prod_{j=1}^{d-k} z_j^{b_{j\ell}}.$$

Translation

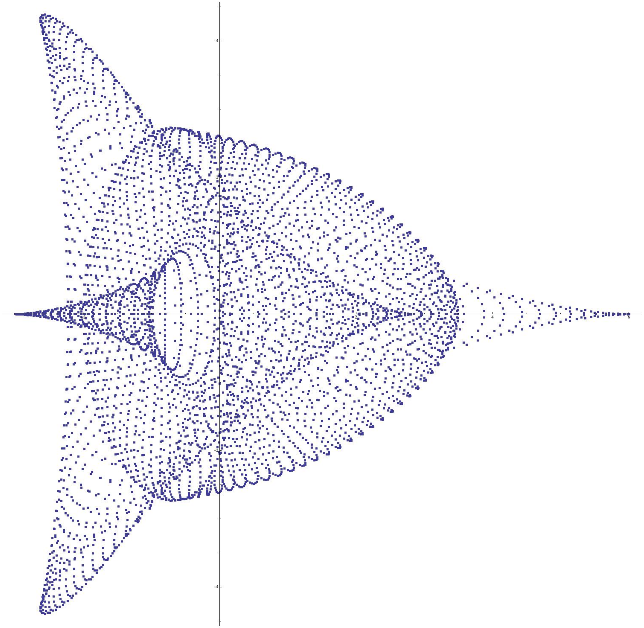
Hummingbirds and manta rays exist, mathematically speaking.



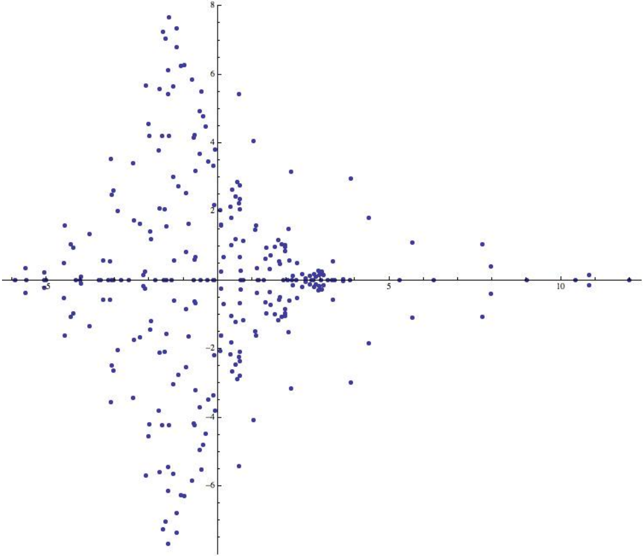
$n = 47,\ d = 3,\ \mathbf{x} = (1, 2, 44)$



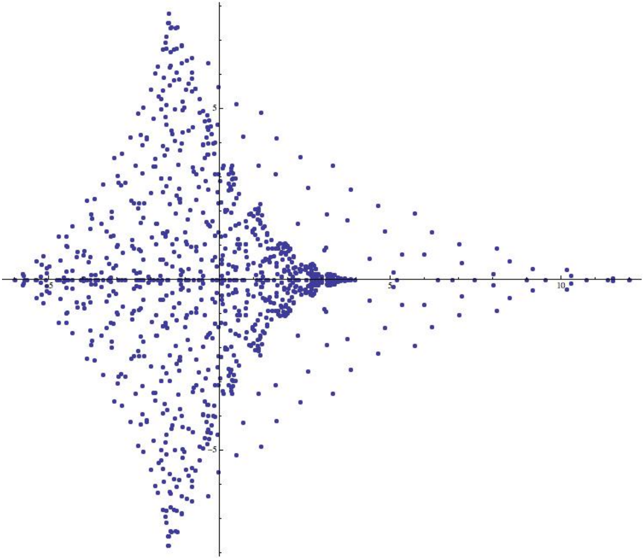
$n = 73,\ d = 3,\ \mathbf{x} = (1, 2, 70)$



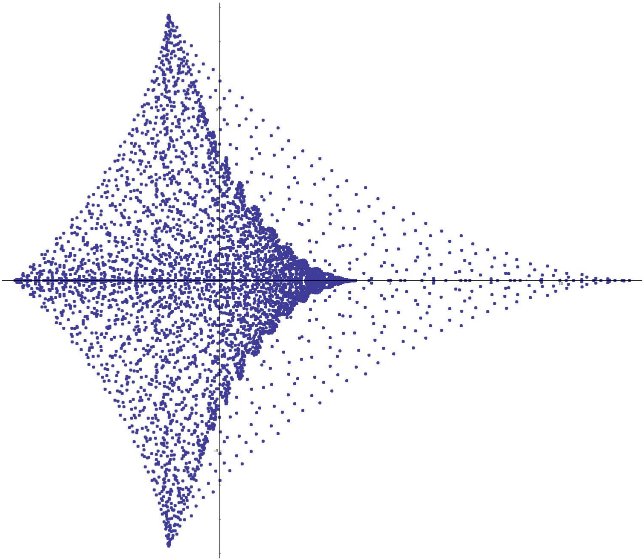
$n = 173,\ d = 3,\ \mathbf{x} = (1, 2, 170)$



$n = 17,\ d = 4,\ \mathbf{x} = (0, 1, 1, 15)$



$n = 27$, $d = 4$, $\mathbf{x} = (0, 1, 1, 25)$

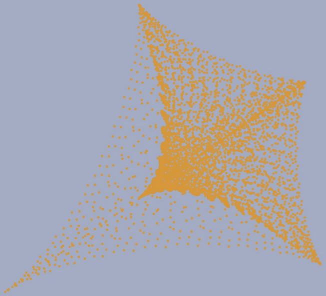


$n = 47,\ d = 4,\ \mathbf{x} = (0, 1, 1, 45)$

Vol. 47, No. 1, January 2016

MAA

THE COLLEGE MATHEMATICS JOURNAL



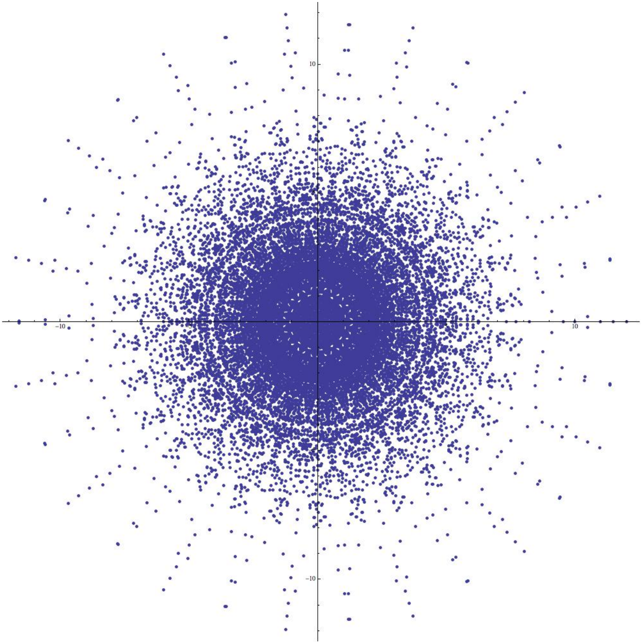
Manta Ray Modulo 47 by Stephan Garcia

In this issue:

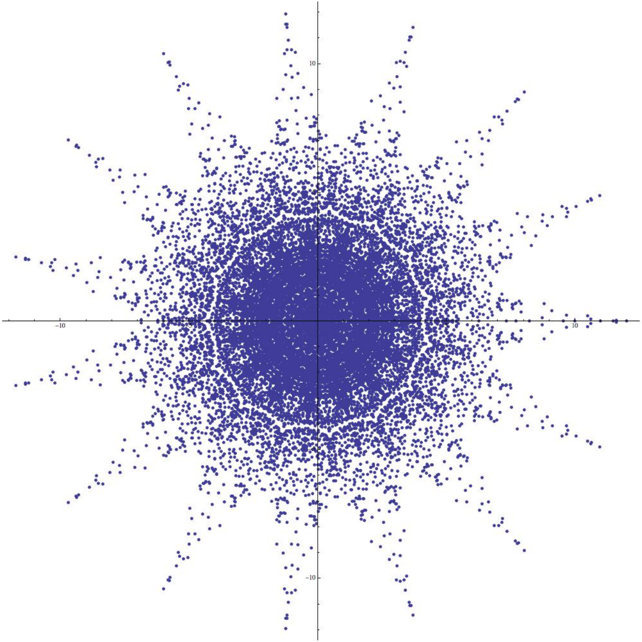
- Analyzing the National Football League's new overtime system
- William Neile's discovery of how to measure "a Crooked line"
- Review of smartphone apps for graph theory

An Official Publication of the Mathematical Association of America

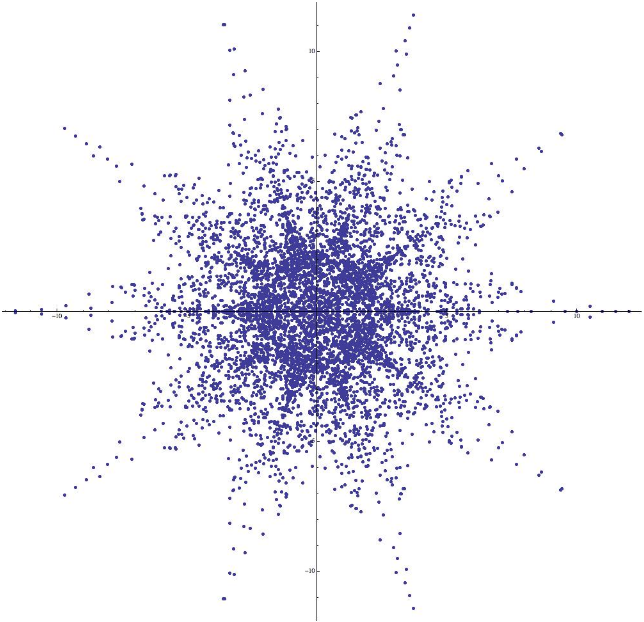
College Mathematics Journal, January 2016



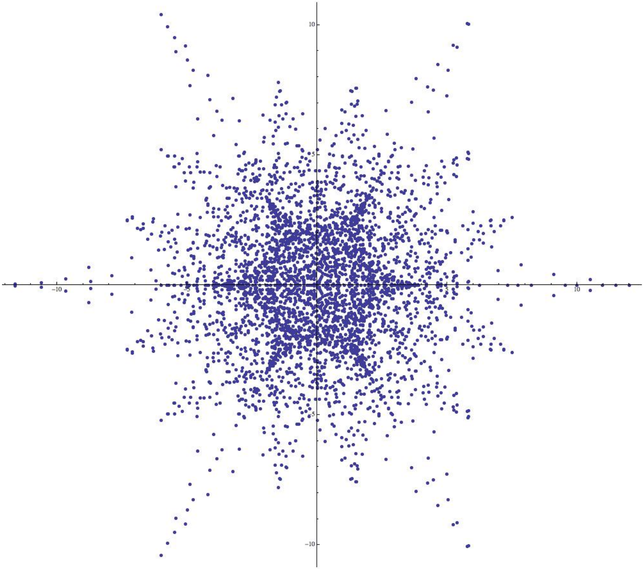
$n = 30,\ d = 4,\ \mathbf{x} = (1, 2, 2, 29)$



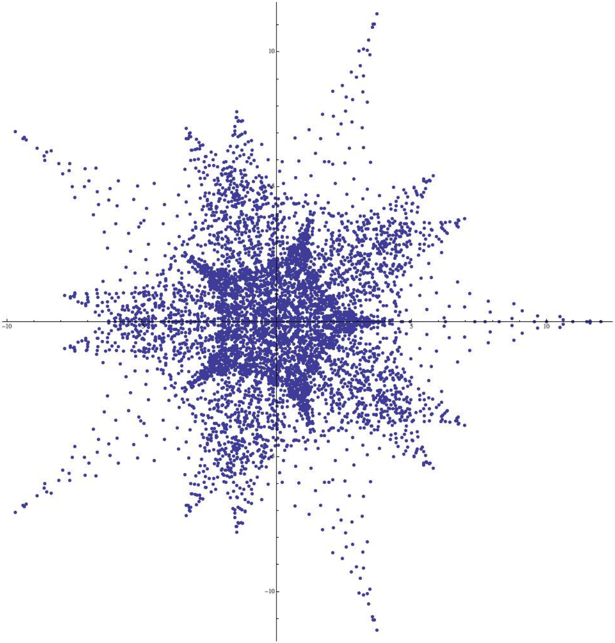
$n = 30,\ d = 4,\ \mathbf{x} = (2, 3, 3, 0)$



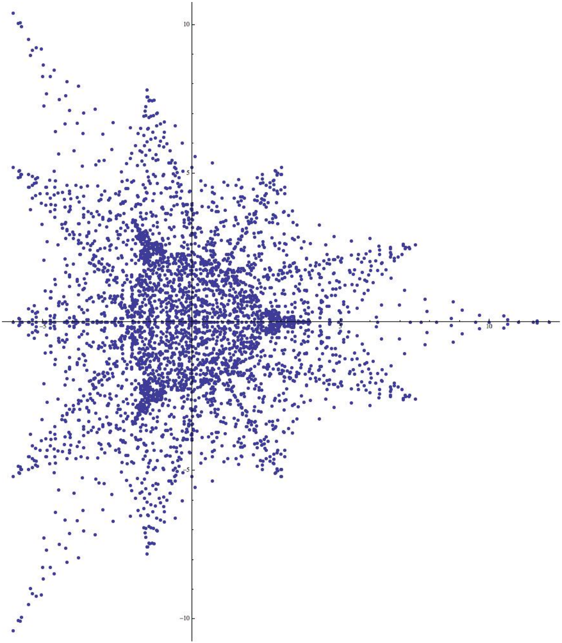
$n = 30,\ d = 4,\ \mathbf{x} = (3, 4, 4, 1)$



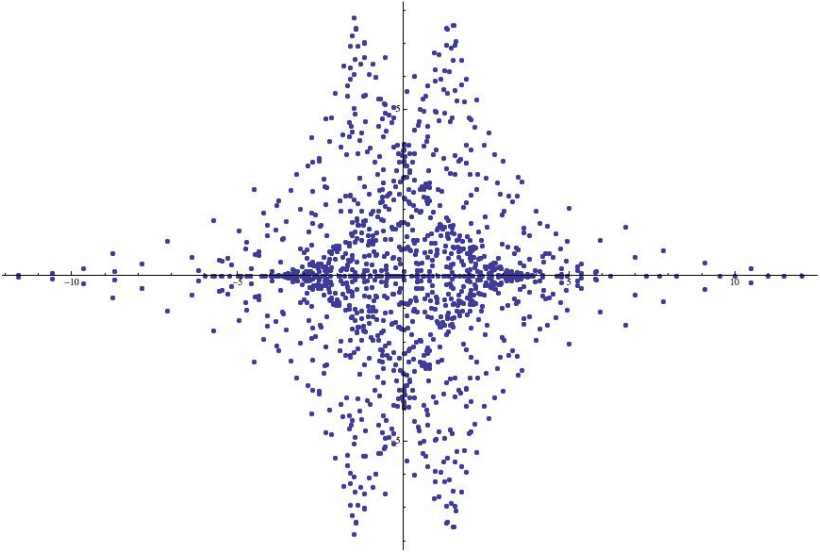
$n = 30,\ d = 4,\ \mathbf{x} = (5, 6, 6, 3)$



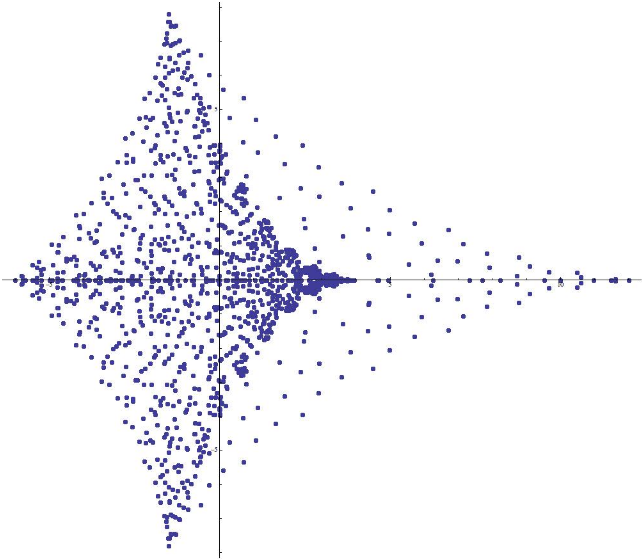
$n = 30,\ d = 4,\ \mathbf{x} = (6, 7, 7, 4)$



$n = 30,\ d = 4,\ \mathbf{x} = (10, 11, 11, 8)$



$n = 30,\ d = 4,\ \mathbf{x} = (15, 16, 16, 13)$



$n = 30,\ d = 4,\ \mathbf{x} = (0, 1, 1, 28)$

“I was thrown into deep water, but learned how to swim.”

Andrew Turner ’14

EVEN AS A SEVENTH GRADER, ANDREW TURNER ’14 knew that Harvey Mudd College was the right place for him. In high school, he excelled in mathematics and physics and augmented his knowledge by taking classes at the University of Missouri near his hometown of Ashland. His father, a scientist and musician, taught Turner music theory to augment piano lessons, band and choir activities.

When it came time to select his academic focus, Turner went straight for the rigor and became a physics and mathematics double major, managing a schedule overload (more than 18 units) every semester.

During his first-year summer, he focused on physics, interning at Los Alamos National Laboratories where he worked on modeling the fluid and thermodynamics of laser chemical vapor deposition. “I learned a ton of numerical analysis and partial differential equations with the help of a great team. I was thrown into deep water, but I learned how to swim,” he says.

My balance tip: Combine work and play. It’s good for time management and sanity.

This past summer, as the recipient of a Fletcher Jones Fellowship through the Claremont Center for the Mathematical Sciences, he focused on math, exploring, with Pomona College Professor Stephan Garcia, the new subject of supercharacter theory, a powerful algebraic mechanism which his team used to study certain exponential sums that arise in number theory. Turner is co-author of the paper “Supercharacters, exponential sums, and the uncertainty principle,” which has been submitted for publication, and he is working with Garcia and his team on another.

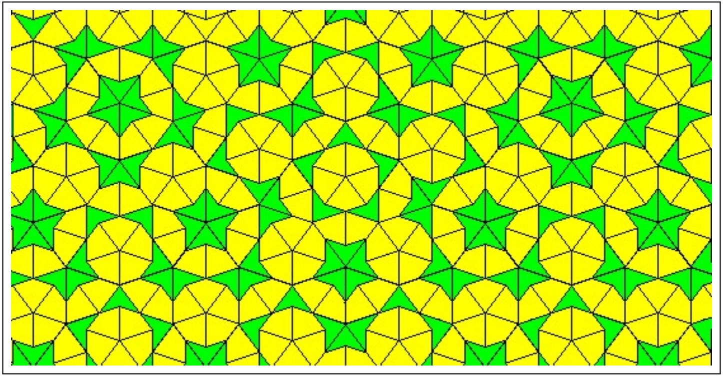
Next summer, Turner is debating a math or physics internship versus a teaching assistant position at the Harvard Summer Science Program. He attended the camp in 2009 and studied the position of a near-earth asteroid, writing code to determine the asteroid’s orbital elements.

Despite his hectic academic schedule, Turner still plays piano and sings (he’s a member of the Claremont Chamber Choir). Regarding science and music, he’s still deciding which he’ll pursue as a profession and which as a hobby. For now, Turner said, obtaining a Ph.D. in mathematics or physics sounds like a good plan, but only after spending some time traveling, perhaps in Norway, Finland or New Zealand.

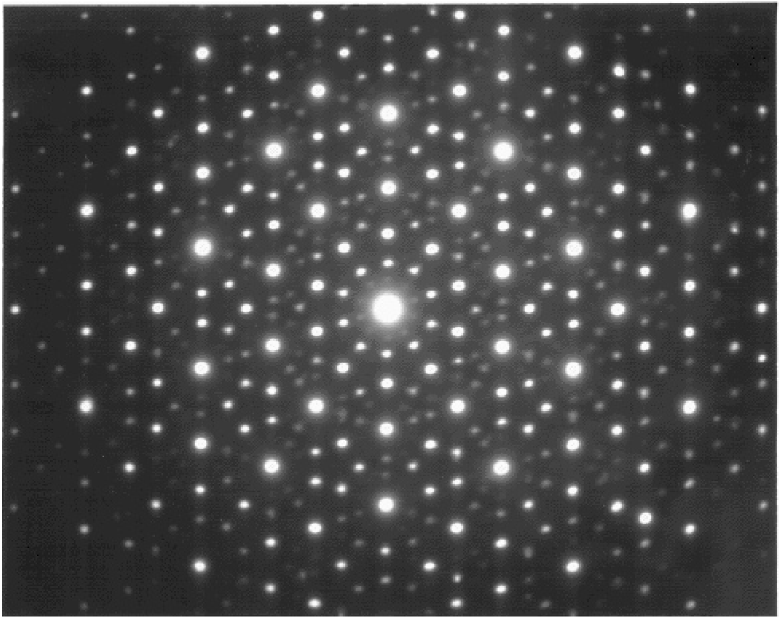
Harvey Mudd College Bulletin, Fall 2012.

Further research

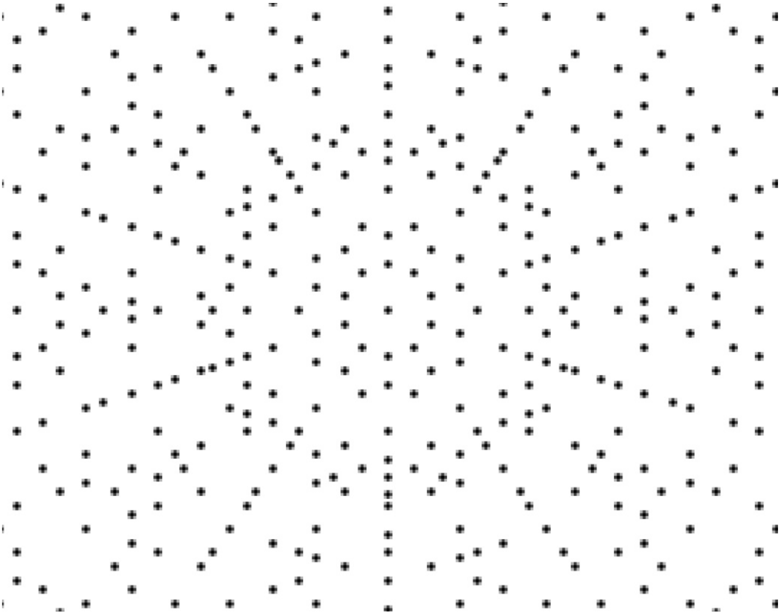
Certain supercharacter plots resemble diffraction patterns produced by *quasicrystals* – chemical structures which are three-dimensional, physical, real-world analogues of Penrose tilings (Dan Shechtman earned the 2011 Nobel Prize in Chemistry for their discovery).



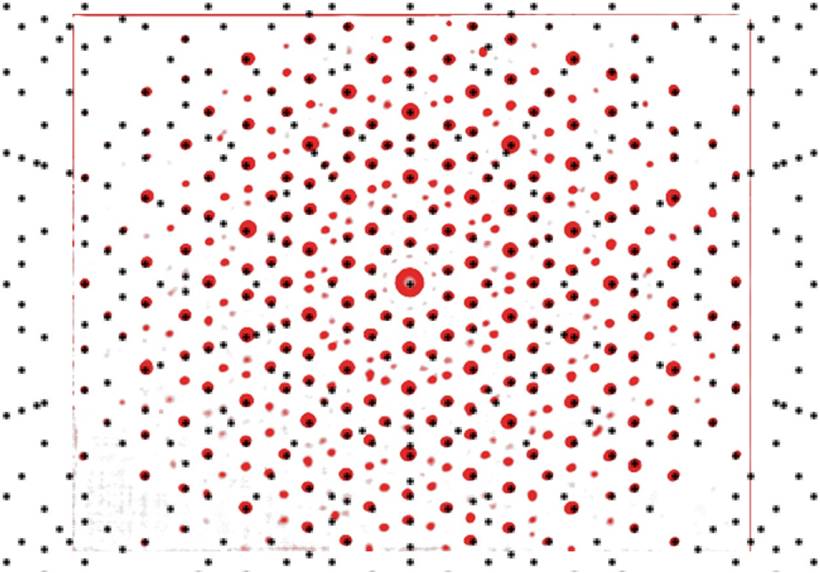
A *Penrose tiling* is a certain aperiodic tiling of the plane with "faux" five-fold symmetry.



Laue diffraction pattern for the chemical $Al_{65}Cu_{15}Co_{20}$



Plot of all supercharacters arising from the action of S_4 on $(\mathbb{Z}/10\mathbb{Z})^4$



Both images together

Super Characters

1. J.L. Brumbaugh (POM '13)
2. Madeleine Bulkow (SCR '14, UCLA)
3. Paula Burkhardt (POM '16, UC Berkeley)
4. Alice Z.-Y. Chan (POM '14, UC San Diego)
5. Gabriel Currier (POM '16)
6. Christopher Fowler (POM '12, U. Washington)
7. Luis A. Garcia German (POM '14, Washington U.)
8. Trevor Hyde (University of Michigan)
9. Bob Lutz (POM '13, University of Michigan)
10. Matt Michal (CGU '15)
11. Hong Suh (POM '16, UC Berkeley)
12. Andrew P. Turner (HMC '14, MIT)

Bibliography

1. Brumbaugh, J.L. ('13), Bulkow, M. (SCR '14), Fleming, P.S., Garcia German, L.A. ('14), Garcia, S.R., Karaali, G., Michal, M. (CGU '15), Turner, A.P. (HMC '14), *Superchracters, exponential sums, and the uncertainty principle*, J. Number Theory **144** (2014), 151-175.
2. Brumbaugh, J.L. ('13), Bulkow, M. (SCR '14), Garcia German, L.A. ('14), Garcia, S.R., Michal, M. (CGU '15), Turner, A.P. (HMC '14), *The graphic nature of the symmetric group*, Experimental Math. **22** (2013), no. 4, 421-442.
3. Burkhardt, P. ('16), Chan, A.Z.-Y. ('14), Currier, G. ('16), Garcia, S.R., Luca, F., Suh, H. ('16), *Visual properties of generalized Kloosterman sums*, J. Number Theory **160** (2016), 237-253.
4. Diaconis, P., Isaacs, I.M., *Supercharacters and superclasses for algebra groups*, Trans. Amer. Math. Soc. **360** (2008), no. 5, 2359-2392.
5. Duke, W.D., Garcia, S.R., Lutz, B. ('13), *The graphic nature of Gaussian periods*, Proc. Amer. Math. Soc. **143** (2015), no. 5, 1849-1863.
6. Fowler, C. ('12), Garcia, S.R., Karaali, G., *Ramanujan sums as supercharacters*, Ramanujan J. **35** (2014), no. 2, 205-241.
7. Garcia, S.R., Hyde, T., Lutz, B., *Gauss' hidden menagerie: from cyclotomy to supercharacters*, Notices Amer. Math. Soc. **62** (2015), no. 8, 878-888.
8. Lutz, B., *Graphical cyclic supercharacters for composite moduli*, Proc. Amer. Math. Soc. (in press).