

# Primes dividing the ECHO sequence

Alexi Block Gorman, Tyler Genao, Heesu Hwang,  
Noam Kantor, Sarah Parsons

Wake Forest University

July 30, 2015

## Theorem (Jones and Rouse)

*The Somos-4 sequence is defined by  $a_0 = a_1 = a_2 = a_3 = 1$  and further recursively defined by*

$$a_n a_{n-4} = a_{n-1} a_{n-3} + a_{n-2}^2.$$

*The density of primes dividing a term of this sequence is  $\frac{11}{21}$ .*

## Question

*What is the density of primes  $p$  such that  $p$  divides some  $2^n + 1$  term for  $n \geq 0$ ?*

## Question

*What is the density of primes  $p$  such that  $p$  divides some  $L_n$ , a term of the Lucas sequence?*

## Question

*What is the density of primes  $p$  such that  $p$  divides some  $2^n + 1$  term for  $n \geq 0$ ?*

## Answer

$\frac{17}{24}$  (Hasse).

## Question

*What is the density of primes  $p$  such that  $p$  divides some  $L_n$ , a term of the Lucas sequence?*

## Question

*What is the density of primes  $p$  such that  $p$  divides some  $2^n + 1$  term for  $n \geq 0$ ?*

## Answer

$\frac{17}{24}$  (Hasse).

## Question

*What is the density of primes  $p$  such that  $p$  divides some  $L_n$ , a term of the Lucas sequence?*

## Answer

$\frac{2}{3}$  (Lagarias).

Lagarias and Hasse derived number fields with behaviors dependent entirely on whether  $p$  is a “good” prime or not. They then calculated the density using the Chebotarev density theorem.

We do the same by analyzing Galois groups attached to elliptic curves.

- Sequence and Elliptic Curves
- Numerical Approximations
- Galois Toolbox
- Calculating the Fraction
- Conclusion

# The ECHO Sequence

- The ECHO sequence is defined by  
 $b_0 = 1, b_1 = 2, b_2 = 1, b_3 = -3$ , and for  $n > 3$ ,

# The ECHO Sequence

- The ECHO sequence is defined by

$b_0 = 1, b_1 = 2, b_2 = 1, b_3 = -3$ , and for  $n > 3$ ,

- $$b_n = \begin{cases} \frac{b_{n-1}b_{n-3} - b_{n-2}^2}{b_{n-4}} & \text{if } n \not\equiv 2 \pmod{3}, \\ \frac{b_{n-1}b_{n-3} - 3b_{n-2}^2}{b_{n-4}} & \text{if } n \equiv 2 \pmod{3}. \end{cases}$$

# The ECHO Sequence

- The ECHO sequence is defined by

$b_0 = 1, b_1 = 2, b_2 = 1, b_3 = -3$ , and for  $n > 3$ ,

- $$b_n = \begin{cases} \frac{b_{n-1}b_{n-3} - b_{n-2}^2}{b_{n-4}} & \text{if } n \not\equiv 2 \pmod{3}, \\ \frac{b_{n-1}b_{n-3} - 3b_{n-2}^2}{b_{n-4}} & \text{if } n \equiv 2 \pmod{3}. \end{cases}$$

- The next few terms are

$-7, -17, 2, 101, 247, 571, -1669,$   
 $-13766, -43101, -205897, 1640929, 8217293,$   
 $101727662, 173114917, -5439590147, -70987557871, \dots$

# The ECHO Sequence

- The ECHO sequence is defined by

$$b_0 = 1, b_1 = 2, b_2 = 1, b_3 = -3, \text{ and for } n > 3,$$

$$b_n = \begin{cases} \frac{b_{n-1}b_{n-3} - b_{n-2}^2}{b_{n-4}} & \text{if } n \not\equiv 2 \pmod{3}, \\ \frac{b_{n-1}b_{n-3} - 3b_{n-2}^2}{b_{n-4}} & \text{if } n \equiv 2 \pmod{3}. \end{cases}$$

- The next few terms are

$$\begin{aligned} & -7, \quad -17, \quad 2, \quad 101, \quad 247, \quad 571, \quad -1669, \\ & -13766, \quad -43101, \quad -205897, \quad 1640929, \quad 8217293, \\ & 101727662, \quad 173114917, \quad -5439590147, \quad -70987557871, \dots \end{aligned}$$

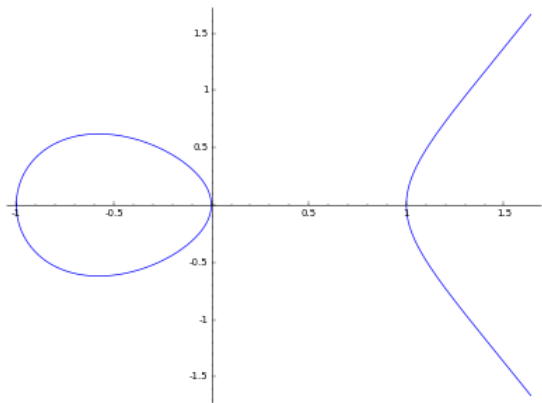
- Fact:  $b_n \in \mathbb{Z} \forall n \geq 0$ .

- We want to know more about the number of primes dividing the sequence. It turns out that we can relate this problem to elliptic curves.

# Elliptic Curves

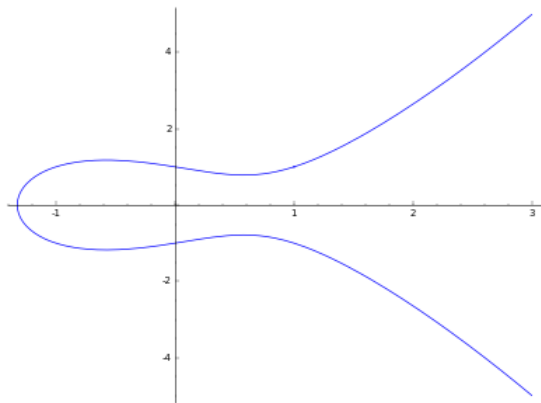
- We want to know more about the number of primes dividing the sequence. It turns out that we can relate this problem to elliptic curves.
- Generally speaking, a normal elliptic curve  $E$  is a polynomial of the form  $y^2 = x^3 + Ax + B$ , where  $A, B$  are in a field  $\mathbb{F}$ .

# Elliptic Curves (Examples)



$$y^2 = x^3 - x$$

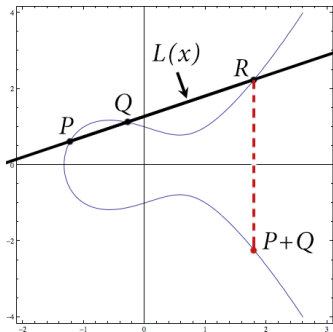
# Elliptic Curves (Examples)



$$y^2 = x^3 - x + 1$$

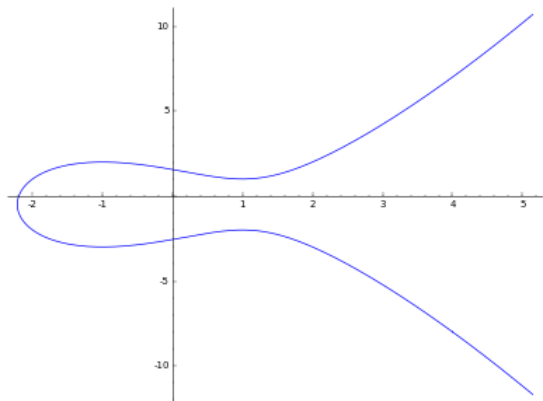
# Elliptic Curves (Group Law)

- It turns out that in most cases, one can turn the curve into a group: if  $P$  and  $Q$  are two points on the curve, one can define the operation for  $P$  add  $Q$ : take the line intersecting both  $P$  and  $Q$ : it will intersect the curve at another point, say  $R$ . Then reflect that point over the  $y$  axis, and call this point  $P + Q$ .



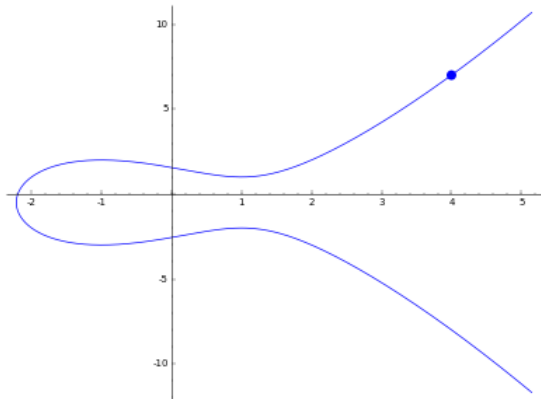
# The Elliptic Curve $y^2 + y = x^3 - 3x + 4$

- The elliptic curve we considered for this project was  $E : y^2 + y = x^3 - 3x + 4$ , and is pictured below:



# The Elliptic Curve $y^2 + y = x^3 - 3x + 4$

- The elliptic curve we considered for this project was  $E : y^2 + y = x^3 - 3x + 4$ , and is pictured below:



- A point on this curve is  $P = (4, 7)$ .

# The Elliptic Curve $y^2 + y = x^3 - 3x + 4$

- It turns out that

$$(2n + 3)P = \left( \frac{g(n)}{b_n^2}, \frac{f(n)}{b_n^3} \right)$$

where

$$g(n) = 2b_n^2 - b_{n-3}b_{n+3},$$

and

$$f(n) = \begin{cases} b_n^3 + b_{n-1}^2 b_{n+2} & \text{if } n \equiv 0 \pmod{3}, \\ b_n^3 + 9b_{n-1}^2 b_{n+2} & \text{if } n \equiv 1 \pmod{3}, \\ b_n^3 + 3b_{n-1}^2 b_{n+2} & \text{if } n \equiv 2 \pmod{3}, \end{cases}$$

and this point is in reduced form.

# The Elliptic Curve $y^2 + y = x^3 - 3x + 4$

- Since

$$(2n + 3)P = \left( \frac{g(n)}{b_n^2}, \frac{f(n)}{b_n^3} \right),$$

in projective coordinates we have

$$(2n + 3)P = (b_n g(n) : f(n) : b_n^3).$$

Since the point is in reduced form,  $\gcd(b_n, f(n)) = 1$ .

# The Elliptic Curve $y^2 + y = x^3 - 3x + 4$

- Since

$$(2n + 3)P = \left( \frac{g(n)}{b_n^2}, \frac{f(n)}{b_n^3} \right),$$

in projective coordinates we have

$$(2n + 3)P = (b_n g(n) : f(n) : b_n^3).$$

Since the point is in reduced form,  $\gcd(b_n, f(n)) = 1$ .

- One can reduce  $P$  modulo  $p$  by modding out the projective coordinates of  $P$  by  $p$ .

# The Elliptic Curve $y^2 + y = x^3 - 3x + 4$

- Since

$$(2n + 3)P = \left( \frac{g(n)}{b_n^2}, \frac{f(n)}{b_n^3} \right),$$

in projective coordinates we have

$$(2n + 3)P = (b_n g(n) : f(n) : b_n^3).$$

Since the point is in reduced form,  $\gcd(b_n, f(n)) = 1$ .

- One can reduce  $P$  modulo  $p$  by modding out the projective coordinates of  $P$  by  $p$ .
- This implies that  $p | b_n$  for some  $n \geq 0$  if and only if  $P$  reduced mod  $p$  has odd order.

# The Elliptic Curve $y^2 + y = x^3 - 3x + 4$

- Since

$$(2n + 3)P = \left( \frac{g(n)}{b_n^2}, \frac{f(n)}{b_n^3} \right),$$

in projective coordinates we have

$$(2n + 3)P = (b_n g(n) : f(n) : b_n^3).$$

Since the point is in reduced form,  $\gcd(b_n, f(n)) = 1$ .

- One can reduce  $P$  modulo  $p$  by modding out the projective coordinates of  $P$  by  $p$ .
- This implies that  $p|b_n$  for some  $n \geq 0$  if and only if  $P$  reduced mod  $p$  has odd order.
- So, the fraction of primes dividing the sequence is equivalent to the fraction of primes modulo which  $P$  has odd order.

# Numerical Computation of the Fraction

Consider the fractions of  $\pi'(x)/\pi(x)$

$x$	$\pi'(x)$	$\pi(x)$	$\frac{\pi'(x)}{\pi(x)}$
10	3	4	0.75
$10^2$	13	25	0.52
$10^3$	91	168	0.541666667
$10^4$	636	1229	0.517493897
$10^5$	5118	9592	0.533569641
$10^6$	41856	78498	0.533211037
$10^7$	354158	664579	0.532905794
$10^8$	3069170	5761455	0.532707450
$10^9$	27092923	50847534	0.532826685
$10^{10}$	242426819	455052511	0.532744712
$10^{11}$	2193850226	4118054813	0.532739443

•  $\frac{179}{336} \approx 0.532738095$

# Understanding $\text{Gal}(\mathbb{Q}(E[N])/\mathbb{Q})$ : Galois Representations

- Fact:  $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$ .
- We adjoin to  $\mathbb{Q}$  the coordinates of the  $N$ -torsion points of  $E$ , and use the action of the Galois group on the torsion :

## Definition

$$\rho_N : \text{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \longrightarrow \text{Aut}(E[N]) = \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

- Fact:  $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$ .
- We adjoin to  $\mathbb{Q}$  the coordinates of the  $N$ -torsion points of  $E$ , and use the action of the Galois group on the torsion :

## Definition

$$\rho_N : \text{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \longrightarrow \text{Aut}(E[N]) = \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

- This map is injective!

- Fact:  $E[N] \cong (\mathbb{Z}/N\mathbb{Z})^2$ .
- We adjoin to  $\mathbb{Q}$  the coordinates of the  $N$ -torsion points of  $E$ , and use the action of the Galois group on the torsion :

## Definition

$$\rho_N : \text{Gal}(\mathbb{Q}(E[N])/\mathbb{Q}) \longrightarrow \text{Aut}(E[N]) = \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

- This map is injective!
- Some uses: determine the curve up to isogeny (Faltings), FLT

# Arboreal Representations

- Takes into account arithmetic of non-torsion points.

# Arboreal Representations

- Takes into account arithmetic of non-torsion points.
- Given a curve  $E$  and a rational point  $P$  on  $E$ . Fix an  $N$ -division pt. of  $P$ ,  $\beta$ .

- Takes into account arithmetic of non-torsion points.
- Given a curve  $E$  and a rational point  $P$  on  $E$ . Fix an  $N$ -division pt. of  $P$ ,  $\beta$ .
- Beefed Up Galois Representation:

## Definition

$$\omega_N : \text{Gal}(\mathbb{Q}([N]^{-1}P)/\mathbb{Q}) \longrightarrow \text{AGL}_2(\mathbb{Z}/N\mathbb{Z})$$

$$\text{AGL}_2(\mathbb{Z}/N\mathbb{Z}) := (\mathbb{Z}/N\mathbb{Z})^2 \rtimes \text{GL}_2(\mathbb{Z}/N\mathbb{Z})$$

$$\sigma \longmapsto (\sigma(\beta) - \beta, \rho_N(\sigma))$$

- Note  $a \in G$  has odd order iff for all  $k \in \mathbb{Z}$  there is  $\beta_k \in G$  such that  $2^k \beta_k = a$
- Form the number field  $K_k := \mathbb{Q}([2^k]^{-1}P)$  by adjoining the coordinates of all such  $\beta_k$  to  $\mathbb{Q}$
- Want the primes  $p$  unramified such that  $\sigma_p \in Gal(K_k/\mathbb{Q})$  fixes some  $\beta_k : 2^k \beta_k = P$ . If  $\sigma_p$  fixes  $\beta_k$  then  $\beta_k \in E(\mathbb{F}_p)$  as desired.

Recall the homomorphism

$$\omega_k : Gal(K_k/\mathbb{Q}) \rightarrow AGL_2(\mathbb{Z}/2^k\mathbb{Z}) := (\mathbb{Z}/2^k\mathbb{Z})^2 \rtimes GL_2(\mathbb{Z}/2^k\mathbb{Z})$$

which is given by  $\omega_k(\sigma_p) = (\vec{v}, M)$ .

## Definition

The action of  $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$  on  $(\mathbb{Z}/2^k\mathbb{Z})^2$  is given by

$$(\vec{v}, M)(\vec{x}) = M\vec{x} + \vec{v}.$$

## Theorem

*Let  $\omega_k(\sigma_p) = (\vec{v}, M)$ . There exists a fixed point  $\beta_k$  of  $\sigma_p$  iff  $(M - I)\vec{x} = \vec{v}$  for some  $\vec{x}$ .*

This is because  $\sigma_p$  has a fixed point iff  $M\vec{x} + \vec{v} = \vec{x}$  for some  $\vec{x}$ , or equivalently  $(M - I)\vec{x} = \vec{v}$ , and any such fixed point for  $\sigma_p$  is a  $\beta_k$ .

Now we need only understand the image of  $\omega_k$  in order to compute the fraction.

# Kinetic Subgroups of $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$

## Definition (Kinetic)

Let a subgroup  $G \subset AGL_2(\mathbb{Z}/2^k\mathbb{Z})$  for  $k \geq 2$  be called kinetic if both the maps are surjective:

$$\text{pr} : G \rightarrow GL_2(\mathbb{Z}/2^k\mathbb{Z})$$

$$\phi : G \rightarrow AGL_2(\mathbb{Z}/2\mathbb{Z}).$$

# Kinetic Subgroups of $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$

## Definition (Kinetic)

Let a subgroup  $G \subset AGL_2(\mathbb{Z}/2^k\mathbb{Z})$  for  $k \geq 2$  be called kinetic if both the maps are surjective:

$$\text{pr} : G \rightarrow GL_2(\mathbb{Z}/2^k\mathbb{Z})$$

$$\phi : G \rightarrow AGL_2(\mathbb{Z}/2\mathbb{Z}).$$

## Proposition

*The image of  $\omega_k$  must be kinetic.*

# Kinetic Subgroups of $AGL_2(\mathbb{Z}/2^k\mathbb{Z})$

## Proposition

*For all  $k \geq 2$ , there is one proper subgroup (up to conjugacy)  $H_k \subset AGL_2(\mathbb{Z}/2^k\mathbb{Z})$  that is kinetic.*

## Proposition

*For our curve, the image  $\omega_k : \text{Gal}(K_k/\mathbb{Q}) \rightarrow AGL_2(\mathbb{Z}/2^k\mathbb{Z})$  is  $H_k$ .*

# The fraction at the limit

Recall that by the Chebotarev density theorem

$$\lim_{x \rightarrow \infty} \frac{|\{p \text{ prime, unramified in } K_k : p \leq x, [\frac{K_k/\mathbb{Q}}{p}] \subseteq S\}|}{\pi(x)} = \frac{|S|}{|\text{Gal}(K_k/\mathbb{Q})|}$$

where  $S$  is a union of conjugacy classes in  $\text{Gal}(K_k/\mathbb{Q})$ . We need to evaluate this fraction for all  $k \in \mathbb{Z}$ .

# The fraction at the limit

- We make two choices for  $S$ :
  - ① Elements of  $\text{Gal}(K_k/\mathbb{Q})$  such that for all  $(\vec{v}, M) \in H_k$ ,  $\vec{v}$  is in the column space of  $M - I$ .
  - ② same set except  $(\vec{v}, M)$  such that  $\det(M - I) \equiv 0 \pmod{2^k}$
- We observe that the set of elements  $(\vec{v}, M) \in H_k$  we desire for  $S$  sits between those two sets but at the limit as  $k \rightarrow \infty$  the sizes of both sets over  $|\text{Gal}(K_k/\mathbb{Q})|$  are equal.

# Theoretical Computation of the Fraction

Thus our final job was to compute the limit

$$\lim_{k \rightarrow \infty} \frac{|\{(\vec{v}, M) \in H_k \mid \vec{v} \in \text{im}(M - I)\}|}{|H_k|} = \lim_{k \rightarrow \infty} \frac{\pi'(x)}{\pi(x)}.$$

# Theoretical Computation of the Fraction

Thus our final job was to compute the limit

$$\lim_{k \rightarrow \infty} \frac{|\{(\vec{v}, M) \in H_k \mid \vec{v} \in \text{im}(M - I)\}|}{|H_k|} = \lim_{k \rightarrow \infty} \frac{\pi'(x)}{\pi(x)}.$$

Our process: partition the numerator based on its reduction mod 4, because we understand the image at  $k = 2$  very well.

$$\frac{179}{336}$$

Are there infinitely many curves  $E/\mathbb{Q}$  for which there is a point  $P \in E(\mathbb{Q})$  so that  $\text{im}(\omega_k) = H_k$ ?

- $E : y^2 + axy + by = x^3 + bx^2$
- $P = (0, 0)$
- Compute  $f_{a,b}$ , a two-parameter, degree 4 polynomial.

## Theorem

*The density of primes dividing the ECHO sequence is the following:*

$$\lim_{x \rightarrow \infty} \frac{\pi'(x)}{\pi(x)} = \frac{179}{336} \approx 0.532738095.$$

## Theorem

*Let  $E$  be an elliptic curve over  $\mathbb{Q}$  and let  $P$  be a rational point on  $E$ . Suppose further that the image of the classical Galois representation is surjective, and that  $P$  has no rational 2-division points. Then there are only two possibilities for the image of the 2-adic arboreal representation up to conjugacy. As a consequence, the density of primes  $p$  for which the reduction of  $P$  modulo  $p$  has odd order is either  $\frac{11}{21}$  or  $\frac{179}{336}$ .*

# Acknowledgements

We would like to thank the NSF for providing our grant, as well as Magma, SageMath, PARI/GP, and Jeremy Rouse for his guidance and support.

Special thanks to UGA and the organizers of the conference.