Elliptic Fermat Numbers

Skye Binegar Randy Dominick

Meagan Kenney Alex Walsh

July 27, 2017

Outline

1. Introduction
   - Elliptic Curves
   - Fermat Numbers
   - Elliptic Fermat Numbers
2. Properties
   - Order Universality
   - Coprimality
   - Recurrence
   - Primality
3. Special Curve
4. Conclusion

Elliptic Curves

An elliptic curve is a *smooth* curve defined by the equation

$$E : y^2 = x^3 + ax^2 + bx + c$$

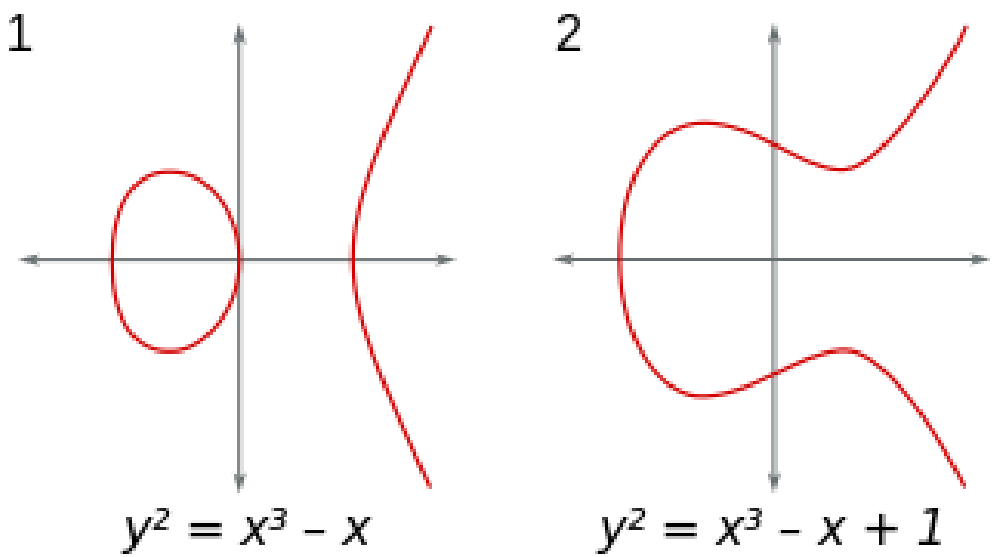
$$\text{for } a, b, c \in \mathbb{Z}.$$

Elliptic Curves

An elliptic curve is a *smooth* curve defined by the equation

$$E : y^2 = x^3 + ax^2 + bx + c$$
$$\text{for } a, b, c \in \mathbb{Z}.$$

Geometrically, elliptic curves take one of two forms:



Group Structure

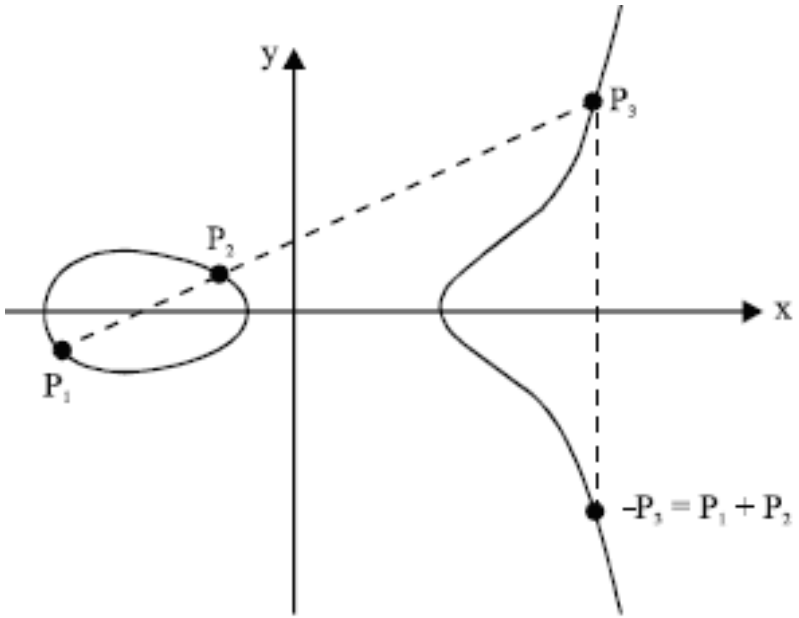
- We will focus on $E(\mathbb{Q})$. We can also define a homomorphism $E(\mathbb{Q}) \to E(\mathbb{F}_p)$ by reducing each point *mod* p.

Group Structure

- We will focus on $E(\mathbb{Q})$. We can also define a homomorphism $E(\mathbb{Q}) \to E(\mathbb{F}_p)$ by reducing each point *mod* p.
- We can make $E(\mathbb{Q})$ into an abelian group!

Group Structure

- We will focus on $E(\mathbb{Q})$. We can also define a homomorphism $E(\mathbb{Q}) \to E(\mathbb{F}_p)$ by reducing each point *mod* p.
- We can make $E(\mathbb{Q})$ into an abelian group!
- To do so, we add points as follows:

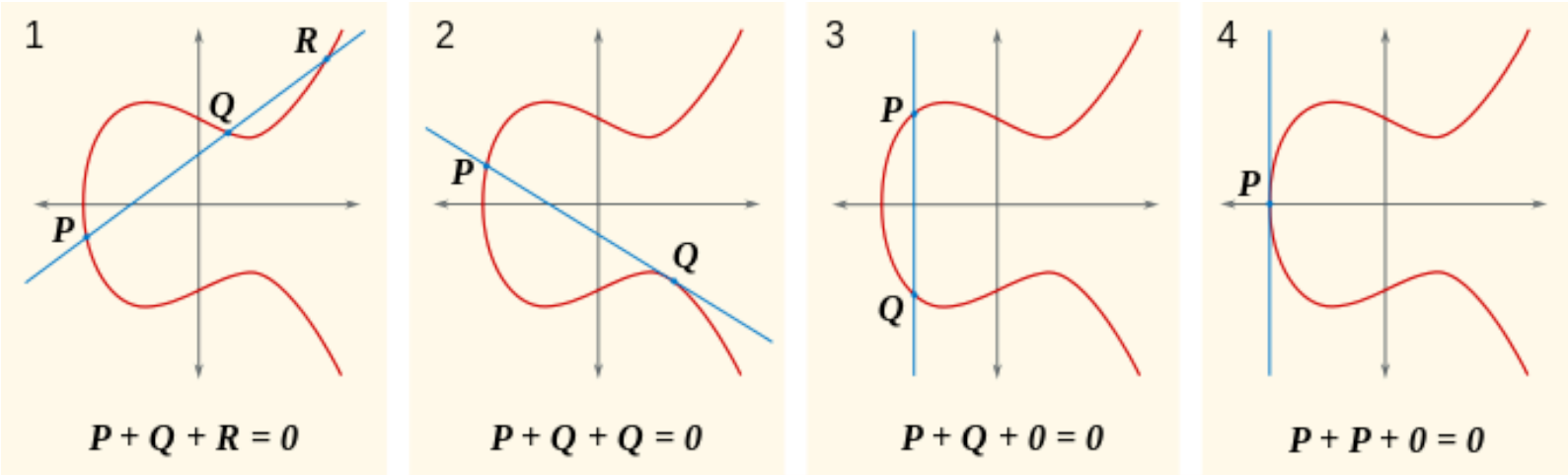


Group Structure (cont'd)

- We call the identity the *point at infinity*, which we write as $(0 : 1 : 0)$, or simply O.

Group Structure (cont'd)

- We call the identity the *point at infinity*, which we write as $(0 : 1 : 0)$, or simply O.
- This identity satisfies the desired conditions.



Duplication Formula

- What happens when we add $P = (x, y)$ to itself?

Duplication Formula

- What happens when we add $P = (x, y)$ to itself?
- Geometrically, we take the tangent line of P.

Duplication Formula

- What happens when we add $P = (x, y)$ to itself?
- Geometrically, we take the tangent line of P.
- Algebraically, we use the *duplication formula*

$$X(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)},$$

Duplication Formula

- What happens when we add $P = (x, y)$ to itself?
- Geometrically, we take the tangent line of P.
- Algebraically, we use the *duplication formula*

$$X(2P) = \frac{x^4 - 2bx^2 - 8cx + b^2 - 4ac}{4(x^3 + ax^2 + bx + c)},$$

where $X(2P)$ is the x-coordinate of $2P$ and a, b and c are the coefficients of $E : y^2 = x^3 + ax^2 + bx + c$.

Duplication Formula (cont'd)

- We can express any $P \in E(\mathbb{Q})$ as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$ for $m, n, e \in \mathbb{Z}$ with $gcd(m, e) = gcd(n, e) = 1$.

Duplication Formula (cont'd)

- We can express any $P \in E(\mathbb{Q})$ as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$ for $m, n, e \in \mathbb{Z}$ with $gcd(m, e) = gcd(n, e) = 1$.
- This allows us to express $X(2P)$ in terms of m, n and e:

$$X(2P) = \frac{m^4 - 2bm^2e^4 - 8cme^6 + b^2e^8 - 4ace^8}{4n^2e^2}.$$

Duplication Formula (cont'd)

- We can express any $P \in E(\mathbb{Q})$ as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$ for $m, n, e \in \mathbb{Z}$ with $gcd(m, e) = gcd(n, e) = 1$.
- This allows us to express $X(2P)$ in terms of m, n and e:

$$X(2P) = \frac{m^4 - 2bm^2e^4 - 8cme^6 + b^2e^8 - 4ace^8}{4n^2e^2}.$$

- For simplicity, we write $X(2P) = \frac{A}{B}$.

Singular Points

- Recall that an elliptic curve is *smooth*, which means each point has a well-defined tangent line.

Singular Points

- Recall that an elliptic curve is *smooth*, which means each point has a well-defined tangent line.
- $E(\mathbb{Q})$ must be smooth. However, reducing a certain $P \in E(\mathbb{Q})$ *mod* p might yield a point whose tangent line is *not* well-defined!

Singular Points

- Recall that an elliptic curve is *smooth*, which means each point has a well-defined tangent line.
- $E(\mathbb{Q})$ must be smooth. However, reducing a certain $P \in E(\mathbb{Q})$ *mod* p might yield a point whose tangent line is *not* well-defined!
- We call such points *singular points*.

Fermat Numbers

Fermat numbers are integers of the form

$$F_k = 2^{2^k} + 1$$

$$k \in \mathbb{Z}_{\geq 0}$$

Fermat Numbers

Fermat numbers are integers of the form

$$F_k = 2^{2^k} + 1$$
$$k \in \mathbb{Z}_{\geq 0}$$

whose notable properties include:

Fermat Numbers

Fermat numbers are integers of the form

$$F_k = 2^{2^k} + 1$$
$$k \in \mathbb{Z}_{\geq 0}$$

whose notable properties include:

- Order universality

Fermat Numbers

Fermat numbers are integers of the form

$$F_k = 2^{2^k} + 1$$
$$k \in \mathbb{Z}_{\geq 0}$$

whose notable properties include:

- Order universality
- Coprimality

Fermat Numbers

Fermat numbers are integers of the form

$$F_k = 2^{2^k} + 1$$
$$k \in \mathbb{Z}_{\geq 0}$$

whose notable properties include:

- Order universality
- Coprimality
- Recurrence

Fermat Numbers

Fermat numbers are integers of the form

$$F_k = 2^{2^k} + 1$$
$$k \in \mathbb{Z}_{\geq 0}$$

whose notable properties include:

- Order universality
- Coprimality
- Recurrence
- Primality

Fermat Numbers

Fermat numbers are integers of the form

$$F_k = 2^{2^k} + 1$$
$$k \in \mathbb{Z}_{\geq 0}$$

whose notable properties include:

- Order universality
- Coprimality
- Recurrence
- Primality (or lack thereof)

Definition of Elliptic Fermat Numbers

- Recall that all $P \in E(\mathbb{Q})$ can be expressed as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$.

Definition of Elliptic Fermat Numbers

- Recall that all $P \in E(\mathbb{Q})$ can be expressed as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$.
- Denote $2^k P = \left(\frac{m_k}{e_k^2}, \frac{n_k}{e_k^3}\right)$ for each k.

Definition of Elliptic Fermat Numbers

- Recall that all $P \in E(\mathbb{Q})$ can be expressed as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$.
- Denote $2^k P = \left(\frac{m_k}{e_k^2}, \frac{n_k}{e_k^3}\right)$ for each k.
- For a curve E and a point P of infinite order, we define the kth elliptic Fermat number as follows:

Definition of Elliptic Fermat Numbers

- Recall that all $P \in E(\mathbb{Q})$ can be expressed as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$.
- Denote $2^k P = \left(\frac{m_k}{e_k^2}, \frac{n_k}{e_k^3}\right)$ for each k.
- For a curve E and a point P of infinite order, we define the kth elliptic Fermat number as follows:

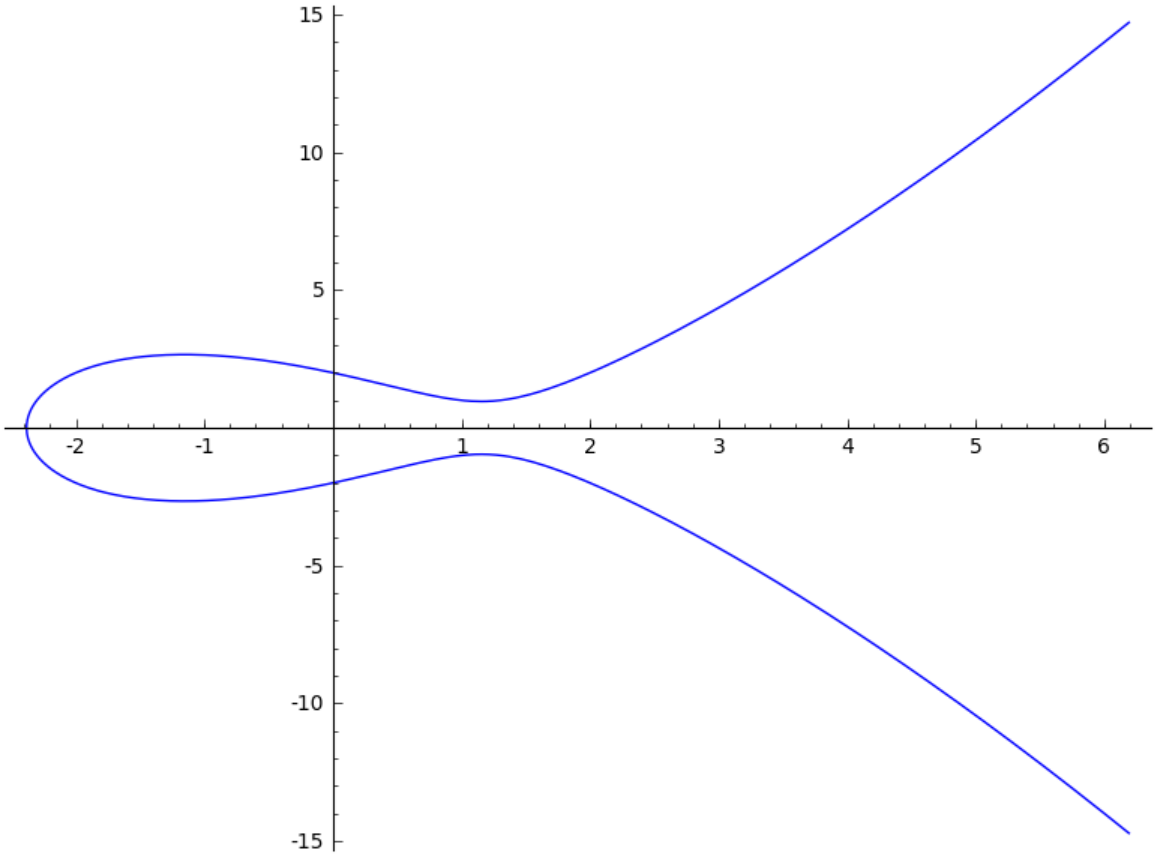
Definition

$$F_k(E, P) = \begin{cases} \dfrac{e_k}{e_{k-1}} & \text{for } k \geq 1 \\ e_0 & \text{for } k = 0 \end{cases}$$

An Example: $y^2 = x^3 - 4x + 4$

$E : y^2 = x^3 - 4x + 4$

$P = (2, -2)$



An Example: $y^2 = x^3 - 4x + 4$

An Example: $y^2 = x^3 - 4x + 4$

$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right)$

An Example: $y^2 = x^3 - 4x + 4$

$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right)$

$F_0(E, P) = 1$

An Example: $y^2 = x^3 - 4x + 4$

$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right)$

$2P = \left(\frac{0}{1^2}, \frac{-2}{1^3}\right)$

$F_0(E, P) = 1$

An Example: $y^2 = x^3 - 4x + 4$

$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right)$

$2P = \left(\frac{0}{1^2}, \frac{-2}{1^3}\right)$

$F_0(E, P) = 1$

$F_1(E, P) = \frac{1}{1} = 1$

An Example: $y^2 = x^3 - 4x + 4$

$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right)$

$2P = \left(\frac{0}{1^2}, \frac{-2}{1^3}\right)$

$4P = \left(\frac{1}{1^2}, \frac{1}{1^3}\right)$

$F_0(E, P) = 1$

$F_1(E, P) = \frac{1}{1} = 1$

An Example: $y^2 = x^3 - 4x + 4$

$$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right)$$

$$2P = \left(\frac{0}{1^2}, \frac{-2}{1^3}\right)$$

$$4P = \left(\frac{1}{1^2}, \frac{1}{1^3}\right)$$

$$F_0(E, P) = 1$$

$$F_1(E, P) = \frac{1}{1} = 1$$

$$F_2(E, P) = \frac{1}{1} = 1$$

An Example: $y^2 = x^3 - 4x + 4$

$$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right)$$

$$2P = \left(\frac{0}{1^2}, \frac{-2}{1^3}\right)$$

$$4P = \left(\frac{1}{1^2}, \frac{1}{1^3}\right)$$

$$8P = \left(\frac{-7}{2^2}, \frac{-19}{2^3}\right)$$

$$F_0(E, P) = 1$$

$$F_1(E, P) = \frac{1}{1} = 1$$

$$F_2(E, P) = \frac{1}{1} = 1$$

An Example: $y^2 = x^3 - 4x + 4$

$$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right) \qquad F_0(E,P) = 1$$

$$2P = \left(\frac{0}{1^2}, \frac{-2}{1^3}\right) \qquad F_1(E,P) = \frac{1}{1} = 1$$

$$4P = \left(\frac{1}{1^2}, \frac{1}{1^3}\right) \qquad F_2(E,P) = \frac{1}{1} = 1$$

$$8P = \left(\frac{-7}{2^2}, \frac{-19}{2^3}\right) \qquad F_3(E,P) = \frac{2}{1} = 2$$

An Example: $y^2 = x^3 - 4x + 4$

$$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right)$$

$$2P = \left(\frac{0}{1^2}, \frac{-2}{1^3}\right)$$

$$4P = \left(\frac{1}{1^2}, \frac{1}{1^3}\right)$$

$$8P = \left(\frac{-7}{2^2}, \frac{-19}{2^3}\right)$$

$$16P = \left(\frac{27105}{76^2}, \frac{4131247}{76^3}\right)$$

$$F_0(E, P) = 1$$

$$F_1(E, P) = \frac{1}{1} = 1$$

$$F_2(E, P) = \frac{1}{1} = 1$$

$$F_3(E, P) = \frac{2}{1} = 2$$

An Example: $y^2 = x^3 - 4x + 4$

$$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right)$$

$$2P = \left(\frac{0}{1^2}, \frac{-2}{1^3}\right)$$

$$4P = \left(\frac{1}{1^2}, \frac{1}{1^3}\right)$$

$$8P = \left(\frac{-7}{2^2}, \frac{-19}{2^3}\right)$$

$$16P = \left(\frac{27105}{76^2}, \frac{4131247}{76^3}\right)$$

$$F_0(E, P) = 1$$

$$F_1(E, P) = \frac{1}{1} = 1$$

$$F_2(E, P) = \frac{1}{1} = 1$$

$$F_3(E, P) = \frac{2}{1} = 2$$

$$F_4(E, P) = \frac{76}{2} = 38$$

An Example: $y^2 = x^3 - 4x + 4$

$$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right) \qquad F_0(E,P) = 1$$

$$2P = \left(\frac{0}{1^2}, \frac{-2}{1^3}\right) \qquad F_1(E,P) = \frac{1}{1} = 1$$

$$4P = \left(\frac{1}{1^2}, \frac{1}{1^3}\right) \qquad F_2(E,P) = \frac{1}{1} = 1$$

$$8P = \left(\frac{-7}{2^2}, \frac{-19}{2^3}\right) \qquad F_3(E,P) = \frac{2}{1} = 2$$

$$16P = \left(\frac{27105}{76^2}, \frac{4131247}{76^3}\right) \qquad F_4(E,P) = \frac{76}{2} = 38$$

$$32P = \left(\frac{58\ldots1}{627949544^2}, \frac{28\ldots1}{627949544^3}\right)$$

An Example: $y^2 = x^3 - 4x + 4$

$$P = \left(\frac{2}{1^2}, \frac{-2}{1^3}\right) \qquad F_0(E,P) = 1$$

$$2P = \left(\frac{0}{1^2}, \frac{-2}{1^3}\right) \qquad F_1(E,P) = \frac{1}{1} = 1$$

$$4P = \left(\frac{1}{1^2}, \frac{1}{1^3}\right) \qquad F_2(E,P) = \frac{1}{1} = 1$$

$$8P = \left(\frac{-7}{2^2}, \frac{-19}{2^3}\right) \qquad F_3(E,P) = \frac{2}{1} = 2$$

$$16P = \left(\frac{27105}{76^2}, \frac{4131247}{76^3}\right) \qquad F_4(E,P) = \frac{76}{2} = 38$$

$$32P = \left(\frac{58\ldots1}{627949544^2}, \frac{28\ldots1}{627949544^3}\right) \qquad F_5(E,P) = \frac{627949544}{76} = 8262494$$

Analogous Fermat Properties

We have shown that the following familiar properties hold for the elliptic Fermat numbers:

Analogous Fermat Properties

We have shown that the following familiar properties hold for the elliptic Fermat numbers:

- Order universality
- Coprimality (with a twist)
- Recurrence
- Primality

Analogous Fermat Properties

We have shown that the following familiar properties hold for the elliptic Fermat numbers:

- Order universality
- Coprimality (with a twist)
- Recurrence
- Primality (or lack thereof)

Fermat Order Universality

For the kth Fermat number $F_k = 2^{2^k} + 1$,

Fermat Order Universality

For the kth Fermat number $F_k = 2^{2^k} + 1$,

Theorem

$$N \mid F_0 \cdots F_k \text{ and } N \nmid F_0 \cdots F_{k-1}$$

$$\iff$$

$$2 \text{ has order } 2^{k+1} \text{ in } (\mathbb{Z}/N\mathbb{Z})^\times.$$

Elliptic Fermat Order Universality

For the kth elliptic Fermat number $F_k(E, P) = \frac{e_k}{e_{k-1}}$,

Elliptic Fermat Order Universality

For the kth elliptic Fermat number $F_k(E,P) = \frac{e_k}{e_{k-1}}$,

Theorem (BDKRW, 2017)

$$N \mid F_0(E,P)\cdots F_k(E,P) \text{ and } N \nmid F_0(E,P)\cdots F_{k-1}(E,P)$$

$$\Longleftrightarrow$$

$$P \text{ has order } 2^k \text{ in } E(\mathbb{Z}/N\mathbb{Z}).$$

Elliptic Fermat Order Universality

When $N = p$ for some prime p, we have a stronger result:

Elliptic Fermat Order Universality

When $N = p$ for some prime p, we have a stronger result:

Theorem (BDKRW, 2017)

$$p \mid F_k(E, P)$$

$$\Longleftrightarrow$$

$$P \text{ has order } 2^k \text{ in } E(\mathbb{Z}/p\mathbb{Z}).$$

Coprimality

For the classic Fermat numbers, we have the following theorem:

Theorem

$\gcd(F_k, F_\ell) = 1$ *for any* $k \neq \ell$.

Coprimality

For the classic Fermat numbers, we have the following theorem:

Theorem

$\gcd(F_k, F_\ell) = 1$ *for any* $k \neq \ell$.

For the elliptic Fermat numbers, we have the following theorem:

Theorem (BDKRW, 2017)

$\gcd(F_k(E,P), F_\ell(E,P)) \in \{1, 2\}$ *for any* $k \neq \ell$.

We derived this result using the duplication formula.

Recurrence: Classical Fermat Numbers

The classical Fermat numbers can be expressed by several different recurrence relations:

- $F_k = (F_{k-1} - 1)^2 + 1$ for $k \geq 1$
- $F_k = F_{k-1} + 2^{2^{k-1}} \cdot F_0 \cdots F_{k-2}$ for $k \geq 2$
- $F_k = F_{k-1}^2 - 2 \cdot (F_{n-2} - 1)^2$ for $k \geq 2$
- $F_k = F_0 \cdots F_{k-1} + 2$ for $k \geq 2$

Intro to τ_k

Recall that every point $2^k P$ can be written in the form $\left(\frac{m_k}{e_k^2}, \frac{n_k}{e_k^3}\right)$.

Intro to τ_k

Recall that every point $2^k P$ can be written in the form $\left(\frac{m_k}{e_k^2}, \frac{n_k}{e_k^3}\right)$.

Definition

τ_k is defined by the following equation: $F_k \tau_k = 2n_{k-1}$.

Intro to τ_k

Recall that every point $2^k P$ can be written in the form $\left(\frac{m_k}{e_k^2}, \frac{n_k}{e_k^3}\right)$.

Definition

τ_k is defined by the following equation: $F_k \tau_k = 2n_{k-1}$.

Fact: $\tau_k^2 = gcd(A, B)$.

Recurrence: Elliptic Fermat Numbers

Theorem (BDKRW, 2017)

The following is a recurrence relation for the elliptic Fermat numbers:

$$F_k(E,P) = \frac{2n_{k-1}}{\tau_k}$$

$$n_k(E,P) = \frac{-2am_{k-1}m_k e_{k-1}^4 e_k - bm_{k-1}e_{k-1}^4 e_k^3 - bm_k e_{k-1}^6 e_k - 2ce_{k-1}^6 e_k^3 + m_{k-1}^3 e_k^3 - 3m_{k-1}^2 m_k e_{k-1}^2 e_k}{2n_{k-1}e_{k-1}^3}$$

$$m_k(E,P) = \frac{m_{k-1}^4 - 2bm_{k-1}^2 e_{k-1}^4 - 8cm_{k-1}e_{k-1}^6 + b^2 e_{k-1}^8 - 4ace_{k-1}^8}{\tau_k^2}$$

$$e_k(E,P) = F_0 \cdot F_1 \cdot F_2 \cdots F_{k-1} \cdot F_k$$

The duplication formula and the algorithm for adding points on a curve played a large role in determining this relation.

Calculating τ_k

Theorem (BDKRW, 2017)

The sequence of τ_k is eventually periodic.

Calculating τ_k

Theorem (BDKRW, 2017)

The sequence of τ_k is eventually periodic.

Theorem (BDKRW, 2017)

There is an algorithm to calculate all τ_k.

τ-Relation to the discriminant

Definition

Let $\Delta = 64a^3c + 16a^2b^2 + 288abc - 64b^3 - 432c^2$ be the discriminant of E.

τ-Relation to the discriminant

Definition

Let $\Delta = 64a^3c + 16a^2b^2 + 288abc - 64b^3 - 432c^2$ be the discriminant of E.

Lemma

$\tau_k^2 | \frac{\Delta(E)}{4}$.

τ-Relation to the discriminant

Definition

Let $\Delta = 64a^3c + 16a^2b^2 + 288abc - 64b^3 - 432c^2$ be the discriminant of E.

Lemma

$\tau_k^2 | \frac{\Delta(E)}{4}$.

Theorem (BDKRW, 2017)

$\tau_k^2 | \Delta(E)$.

An Example: $y^2 = x^3 - 45x + 100$

$F_k \tau_k = 2n_{k-1}$
$\Delta = -1 \cdot 2^8 \cdot 3^2 \cdot 19$
$P = (3, 6)$

An Example: $y^2 = x^3 - 45x + 100$

$F_k \tau_k = 2n_{k-1}$
$\Delta = -1 \cdot 2^8 \cdot 3^2 \cdot 19$
$P = (3, 6)$

$F_1 = 1, n_0 = 6$

An Example: $y^2 = x^3 - 45x + 100$

$F_k \tau_k = 2n_{k-1}$
$\Delta = -1 \cdot 2^8 \cdot 3^2 \cdot 19$
$P = (3, 6)$

$F_1 = 1, n_0 = 6$ | $\tau_1 = \frac{2 \cdot 6}{1} = 12$

An Example: $y^2 = x^3 - 45x + 100$

$F_k \tau_k = 2n_{k-1}$
$\Delta = -1 \cdot 2^8 \cdot 3^2 \cdot 19$
$P = (3, 6)$

$F_1 = 1, n_0 = 6$

$F_2 = 1, n_1 = 2$

$\tau_1 = \frac{2 \cdot 6}{1} = 12$

An Example: $y^2 = x^3 - 45x + 100$

$F_k \tau_k = 2n_{k-1}$
$\Delta = -1 \cdot 2^8 \cdot 3^2 \cdot 19$
$P = (3, 6)$

$F_1 = 1, n_0 = 6$

$F_2 = 1, n_1 = 2$

$\tau_1 = \frac{2 \cdot 6}{1} = 12$

$\tau_2 = \frac{2 \cdot 2}{1} = 4$

An Example: $y^2 = x^3 - 45x + 100$

$F_k \tau_k = 2n_{k-1}$
$\Delta = -1 \cdot 2^8 \cdot 3^2 \cdot 19$
$P = (3, 6)$

$F_1 = 1, n_0 = 6$ | $\tau_1 = \frac{2 \cdot 6}{1} = 12$

$F_2 = 1, n_1 = 2$ | $\tau_2 = \frac{2 \cdot 2}{1} = 4$

$F_3 = 9, n_2 = -18$

An Example: $y^2 = x^3 - 45x + 100$

$F_k \tau_k = 2n_{k-1}$
$\Delta = -1 \cdot 2^8 \cdot 3^2 \cdot 19$
$P = (3, 6)$

$F_1 = 1, n_0 = 6$	$\tau_1 = \frac{2 \cdot 6}{1} = 12$
$F_2 = 1, n_1 = 2$	$\tau_2 = \frac{2 \cdot 2}{1} = 4$
$F_3 = 9, n_2 = -18$	$\tau_3 = \frac{2 \cdot (-18)}{9} = -4$

An Example: $y^2 = x^3 - 45x + 100$

$F_k \tau_k = 2n_{k-1}$
$\Delta = -1 \cdot 2^8 \cdot 3^2 \cdot 19$
$P = (3, 6)$

$F_1 = 1, n_0 = 6$	$\tau_1 = \frac{2 \cdot 6}{1} = 12$
$F_2 = 1, n_1 = 2$	$\tau_2 = \frac{2 \cdot 2}{1} = 4$
$F_3 = 9, n_2 = -18$	$\tau_3 = \frac{2 \cdot (-18)}{9} = -4$
$F_4 = 1327, n_3 = -2654$	

An Example: $y^2 = x^3 - 45x + 100$

$F_k \tau_k = 2n_{k-1}$
$\Delta = -1 \cdot 2^8 \cdot 3^2 \cdot 19$
$P = (3, 6)$

$F_1 = 1, n_0 = 6$	$\tau_1 = \frac{2 \cdot 6}{1} = 12$
$F_2 = 1, n_1 = 2$	$\tau_2 = \frac{2 \cdot 2}{1} = 4$
$F_3 = 9, n_2 = -18$	$\tau_3 = \frac{2 \cdot (-18)}{9} = -4$
$F_4 = 1327, n_3 = -2654$	$\tau_4 = \frac{2 \cdot (-2654)}{1327} = -4$

τ-Singular Points

Theorem (BDKRW, 2017)

Suppose that $p|\tau_k$ and p is an odd prime. Then $2^{k-1}P$ reduces to a singular point mod p with $Y(2^{k-1}P) \equiv 0 \pmod{p}$

τ-Singular Points

Theorem (BDKRW, 2017)

Suppose that $p|\tau_k$ and p is an odd prime. Then $2^{k-1}P$ reduces to a singular point mod p with $Y(2^{k-1}P) \equiv 0 \pmod{p}$

Theorem (BDKRW, 2017)

Let p be an odd prime. Suppose that $2^{k-1}P$ and 2^kP both reduce to singular points $\pmod{p}$. Then $p|\tau_k$.

τ-Singular Points

Theorem (BDKRW, 2017)

Suppose that $p|\tau_k$ and p is an odd prime. Then $2^{k-1}P$ reduces to a singular point mod p with $Y(2^{k-1}P) \equiv 0 \pmod{p}$

Theorem (BDKRW, 2017)

Let p be an odd prime. Suppose that $2^{k-1}P$ and 2^kP both reduce to singular points $\pmod{p}$. Then $p|\tau_k$.

- These can be proved using the ideas of divisibility, the definition of elliptic Fermat numbers, and equations for the singular points.

Primality in the Elliptic Fermat Numbers

Theorem (BDKRW, 2017)

If $2 | e_t$, then for all $k \geq t$, either $F_k = 2$ or F_k is composite.

Primality in the Elliptic Fermat Numbers

Theorem (BDKRW, 2017)

If $2 | e_t$, then for all $k \geq t$, either $F_k = 2$ or F_k is composite.

- The proof of this theorem considers which points reduce to $(0 : 1 : 0) \pmod 2$.

Primality in the Elliptic Fermat Numbers

Theorem (BDKRW, 2017)

If $2 | e_t$, then for all $k \geq t$, either $F_k = 2$ or F_k is composite.

- The proof of this theorem considers which points reduce to $(0 : 1 : 0) \pmod 2$.

Corollary

Suppose $F_t = 2$. Then $F_k \neq 2$ for all $k > \ell$ for some sufficiently large ℓ.

Primality in the Elliptic Fermat Numbers

Theorem (BDKRW, 2017)

For an elliptic curve $E : y^2 = x^3 + ax^2 + bx$, *assume the following:*

(i) $E(\mathbb{Q}) = \langle P, T \rangle$, *where* P *is a generator and a point of infinite order of* $E(\mathbb{Q})$ *and* $T = (0, 0)$ *is a rational point of order 2.*

(ii) T *is the only integral point.*

(iii) $\gcd(b, m_0) = 1$.

(iv) $|\tau_k| = 2$ *for all* k.

(v) $2 \nmid e_k$ *for all* k.

(vi) *The equation* $x^4 + ax^2y^2 + by^4 = 1$ *has no integer solutions where* $y \notin \{0, \pm 1\}$.

Then F_k *is composite for all* k.

Primality in the Elliptic Fermat Numbers

Theorem (BDKRW, 2017)

For an elliptic curve $E : y^2 = x^3 + ax^2 + bx$, assume the following:

(i) $E(\mathbb{Q}) = \langle P, T \rangle$, *where P is a generator and a point of infinite order of $E(\mathbb{Q})$ and $T = (0, 0)$ is a rational point of order 2.*

(ii) *T is the only integral point.*

(iii) $\gcd(b, m_0) = 1$.

(iv) $|\tau_k| = 2$ *for all k.*

(v) $2 \nmid e_k$ *for all k.*

(vi) *The equation $x^4 + ax^2y^2 + by^4 = 1$ has no integer solutions where $y \notin \{0, \pm 1\}$.*

Then F_k is composite for all k.

- $2 \cdot (2^{k-1}P + T) = 2^k P$

Primality in the Elliptic Fermat Numbers

Theorem (BDKRW, 2017)

For an elliptic curve $E : y^2 = x^3 + ax^2 + bx$, assume the following:

(i) $E(\mathbb{Q}) = \langle P, T \rangle$, *where P is a generator and a point of infinite order of $E(\mathbb{Q})$ and $T = (0, 0)$ is a rational point of order 2.*

(ii) *T is the only integral point.*

(iii) $\gcd(b, m_0) = 1$.

(iv) $|\tau_k| = 2$ *for all k.*

(v) $2 \nmid e_k$ *for all k.*

(vi) *The equation $x^4 + ax^2y^2 + by^4 = 1$ has no integer solutions where $y \notin \{0, \pm 1\}$.*

Then F_k is composite for all k.

- $2 \cdot (2^{k-1}P + T) = 2^k P$
- This gives us the ability to utilize both $2^{k-1}P + T$ and $2^{k-1}P$ to construct F_k.

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

Let $E : y^2 = x^3 - 2x$ be an elliptic curve and let $P = (2, 2)$ a rational point on E.
The curve and this point have interesting properties.

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

Let $E : y^2 = x^3 - 2x$ be an elliptic curve and let $P = (2, 2)$ a rational point on E.
The curve and this point have interesting properties.

i E is equipped with complex multiplication.

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

Let $E : y^2 = x^3 - 2x$ be an elliptic curve and let $P = (2, 2)$ a rational point on E.
The curve and this point have interesting properties.

i. E is equipped with complex multiplication.
ii. We have a good understanding of the order of $E(\mathbb{F}_p)$ for a prime p.

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

Let $E : y^2 = x^3 - 2x$ be an elliptic curve and let $P = (2, 2)$ a rational point on E.
The curve and this point have interesting properties.

i. E is equipped with complex multiplication.
ii. We have a good understanding of the order of $E(\mathbb{F}_p)$ for a prime p.
iii. The elliptic Fermat sequence of E at P contains several Fermat primes and Mersenne primes as factors.

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

For this particular curve and this sequence we find another classical Fermat analogue.

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

For this particular curve and this sequence we find another classical Fermat analogue.

Theorem

Let p be a prime dividing the classical Fermat number $F_k = 2^{2^k} + 1$, then

$$p \equiv 1 \pmod{2^{k+2}}$$

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

For this particular curve and this sequence we find another classical Fermat analogue.

Theorem

Let p be a prime dividing the classical Fermat number $F_k = 2^{2^k} + 1$, then

$$p \equiv 1 \pmod{2^{k+2}}$$

Theorem (BDKRW, 2017)

Let p be a prime dividing $F_k(E, P)$, then

$$p \equiv \pm 1 \pmod{2^k}$$

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

A partial converse can be made too.

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

A partial converse can be made too.

Theorem (BDKRW, 2017)

If p is a Fermat or a Mersenne prime and $p \neq 5, 17$, then $p \mid F_k(E, P)$ for some $k \in \mathbb{N}$.

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

A partial converse can be made too.

Theorem (BDKRW, 2017)

If p is a Fermat or a Mersenne prime and $p \neq 5, 17$, then $p \mid F_k(E, P)$ for some $k \in \mathbb{N}$.

Both of the previous theorems rely on three crucial points:

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

A partial converse can be made too.

Theorem (BDKRW, 2017)

If p is a Fermat or a Mersenne prime and $p \neq 5, 17$, then $p \mid F_k(E, P)$ for some $k \in \mathbb{N}$.

Both of the previous theorems rely on three crucial points:

i Order universality tells us $|P|$ is a power of 2 modulo p.

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

A partial converse can be made too.

Theorem (BDKRW, 2017)

If p is a Fermat or a Mersenne prime and $p \neq 5, 17$, then $p \mid F_k(E, P)$ for some $k \in \mathbb{N}$.

Both of the previous theorems rely on three crucial points:

i. Order universality tells us $|P|$ is a power of 2 modulo p.
ii. Lagrange's theorem tells us then that the order must divide the order of the group.

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

A partial converse can be made too.

Theorem (BDKRW, 2017)

If p is a Fermat or a Mersenne prime and $p \neq 5, 17$, then $p \mid F_k(E, P)$ for some $k \in \mathbb{N}$.

Both of the previous theorems rely on three crucial points:

i. Order universality tells us $|P|$ is a power of 2 modulo p.
ii. Lagrange's theorem tells us then that the order must divide the order of the group.
iii. The order of $E(\mathbb{F}_p)$ has a good formula dependent on p which leads to nice algebra.

Closing remarks

- This summer we defined the elliptic Fermat numbers and developed theory to position them as an analogue of the classic Fermat number sequence.

Closing remarks

- This summer we defined the elliptic Fermat numbers and developed theory to position them as an analogue of the classic Fermat number sequence.

- To this end, we have shown similar characterizations of order universality, coprimality, and recurrence in both sequences.

Closing remarks

- This summer we defined the elliptic Fermat numbers and developed theory to position them as an analogue of the classic Fermat number sequence.

- To this end, we have shown similar characterizations of order universality, coprimality, and recurrence in both sequences.

- We have also presented results that reveal further analogs in special elliptic curves.

Thank you ☺

We would like to thank Jeremy Rouse, Kate Thompson, the Wake Forest math and statistics department for their mentorship and hospitality as we conducted our research this summer. We would also like to thank the NSF for supporting this opportunity for undergraduate research. Finally, we thank UGA for hosting us this week.