Anomalous Primes and Elliptic Carmichael Numbers

L. Babinkostova, J. Bahr, Y. Kim, E. Neyman, G. Taylor

Boise State University

2016 REU CAD Symposium

Outline

Introduction

Problems in Cryptography

Problems in Cryptography

- Encryption

Problems in Cryptography

- Encryption
- Primality testing

Problems in Cryptography

- Encryption
- Primality testing

Elliptic curves can tackle both of these problems!

Elliptic Curves

Elliptic Curves

Definition

An **elliptic curve** $E(K)$ is the set

$$\{(x, y) \in K^2 \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$$

where $4a^3 + 27b^2 \neq 0$ and K is a field with characteristic neither 2 nor 3.

Elliptic Curves

Definition

An **elliptic curve** $E(K)$ is the set

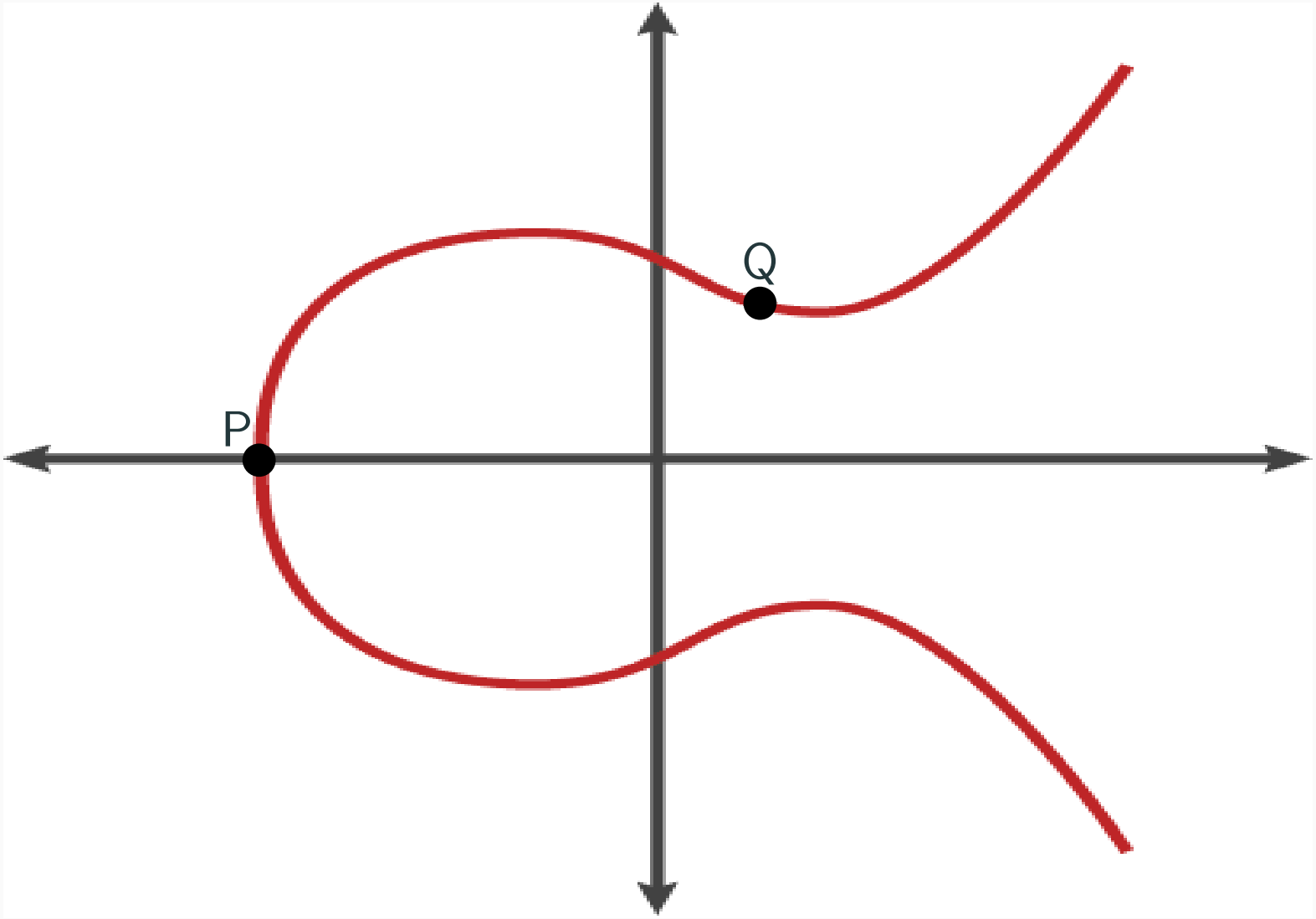
$$\{(x, y) \in K^2 \mid y^2 = x^3 + ax + b\} \cup \{\infty\}$$

where $4a^3 + 27b^2 \neq 0$ and K is a field with characteristic neither 2 nor 3.

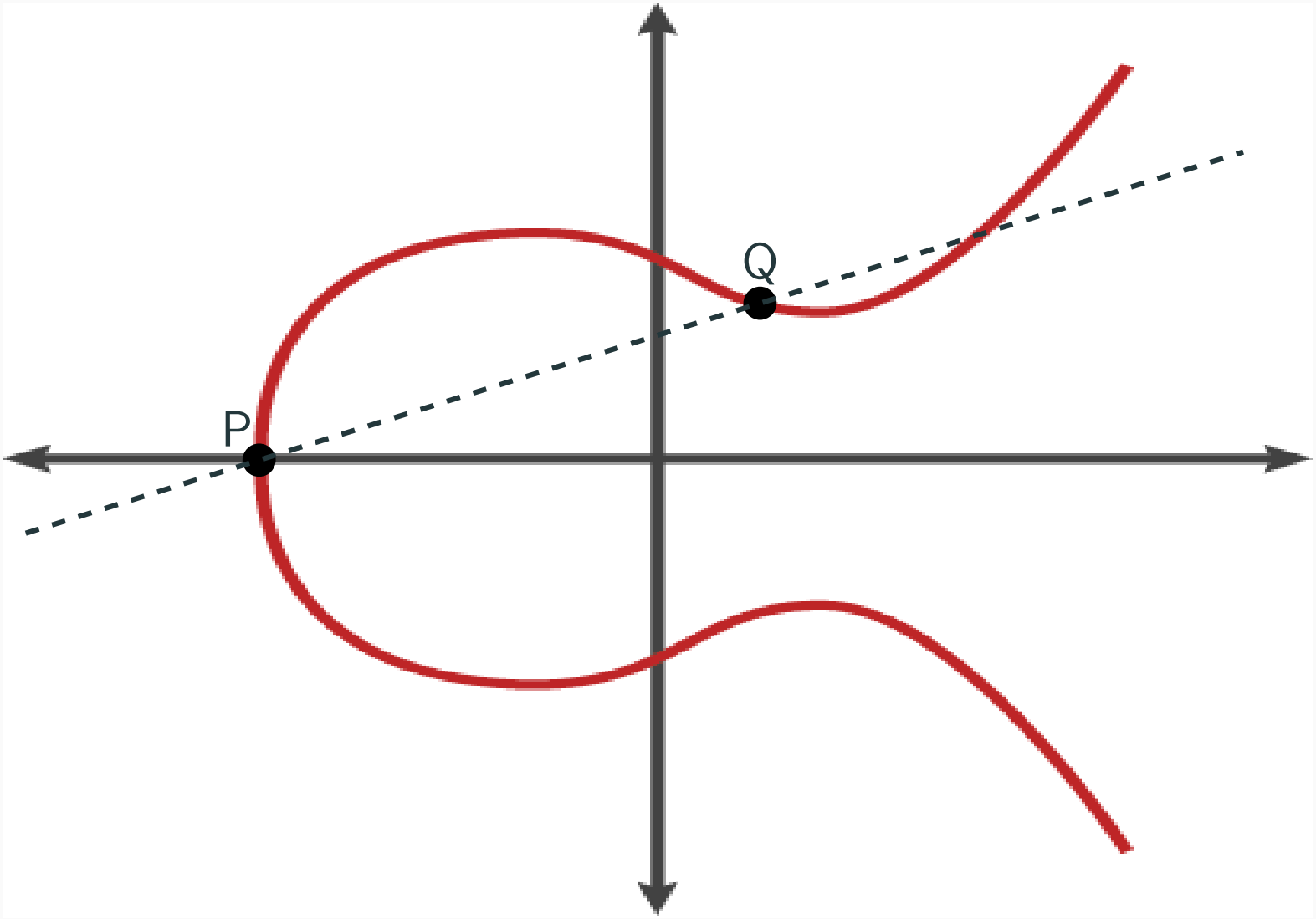
Usually K is $\mathbb{F}_p$ for a prime p or $\mathbb{F}_q$ for q a prime power.

Elliptic Curves are Groups

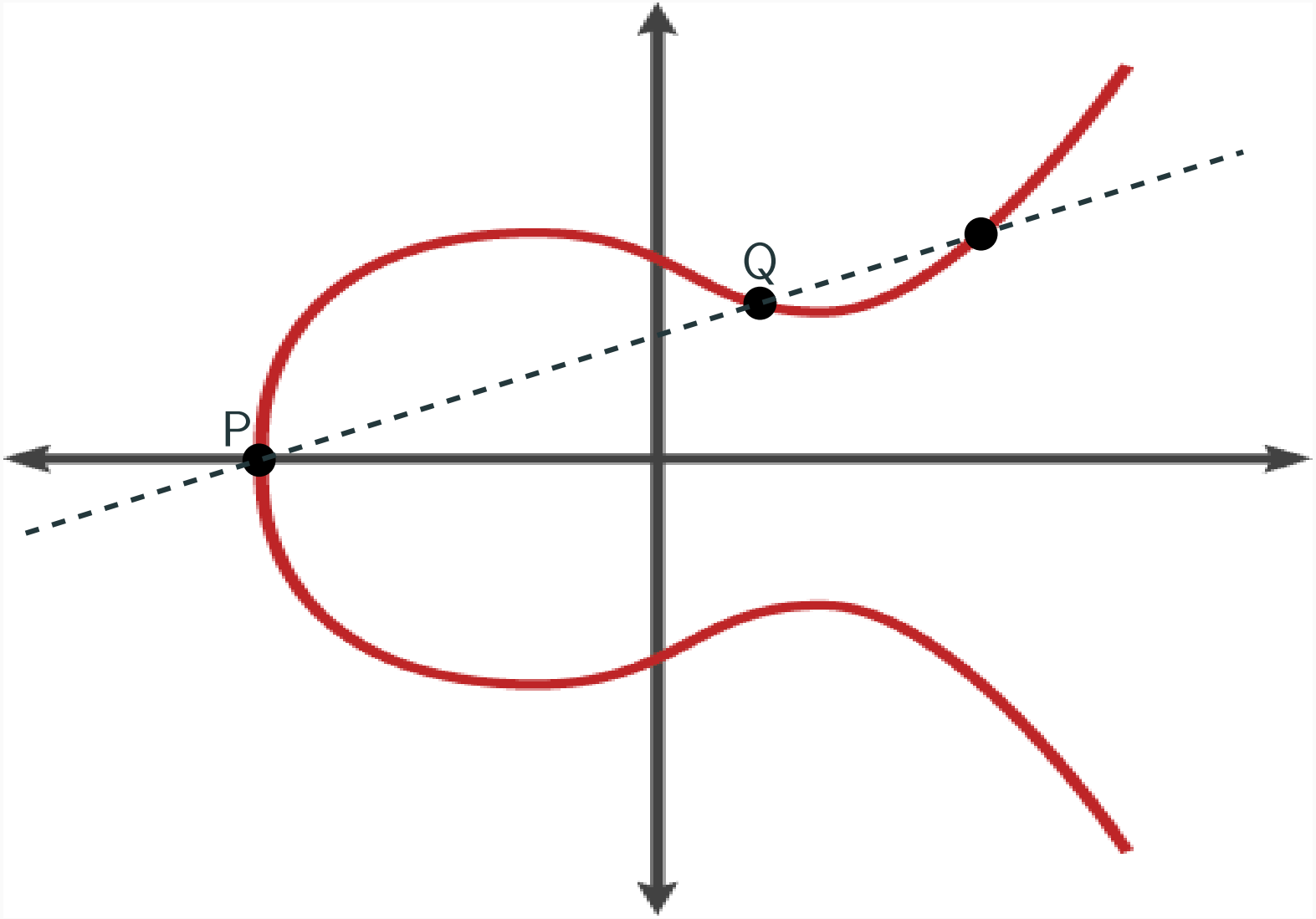
Elliptic Curves are Groups



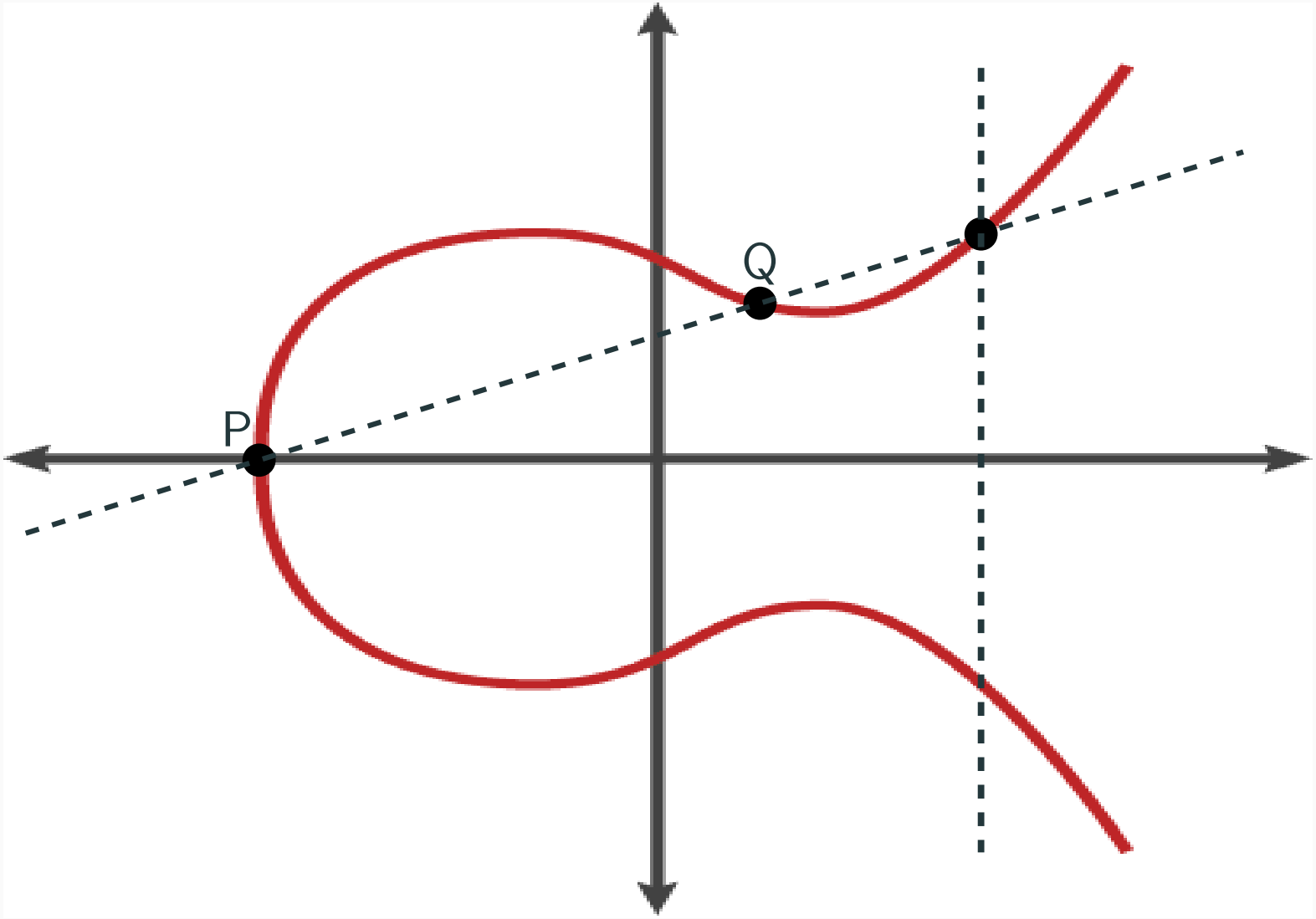
Elliptic Curves are Groups



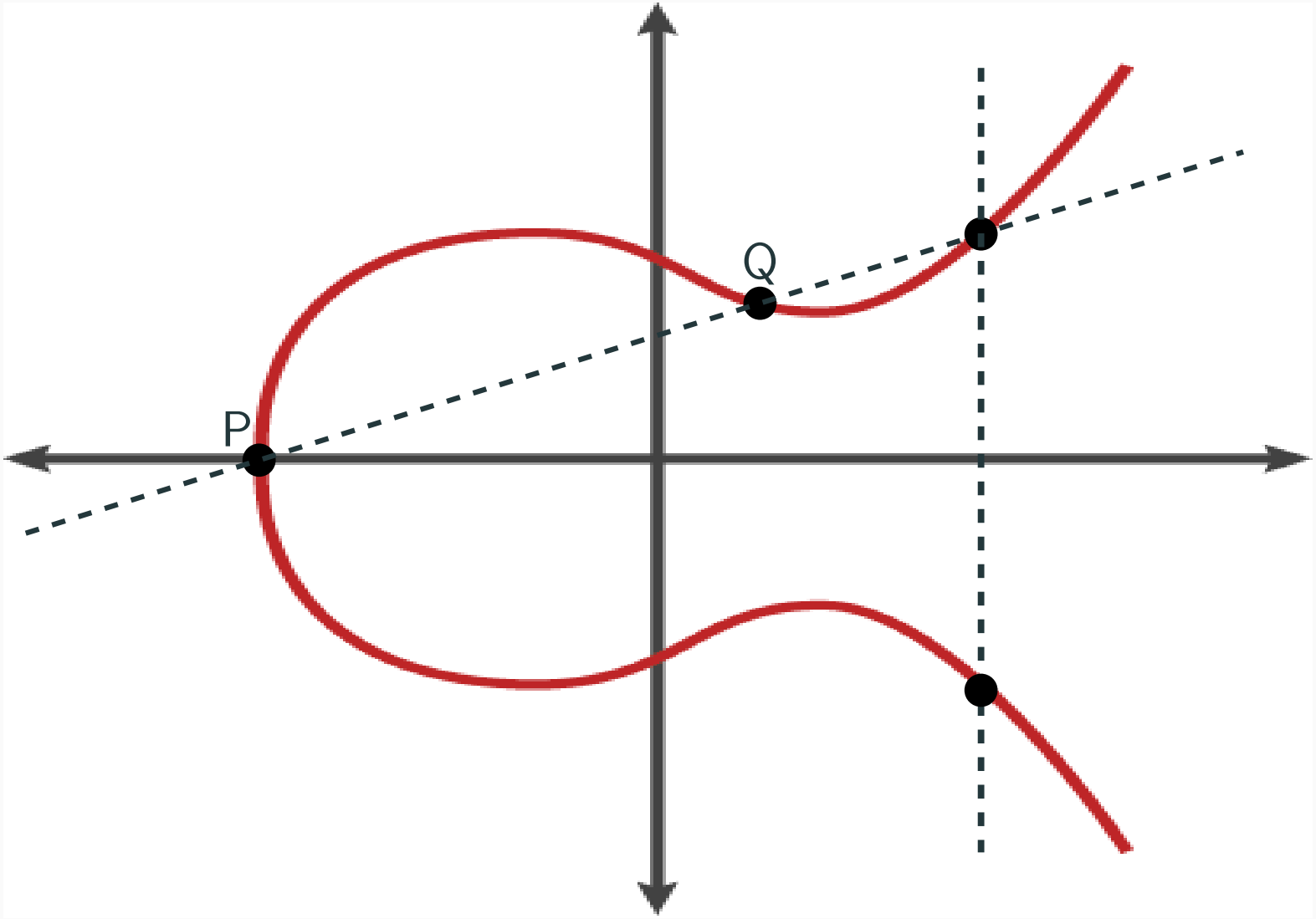
Elliptic Curves are Groups



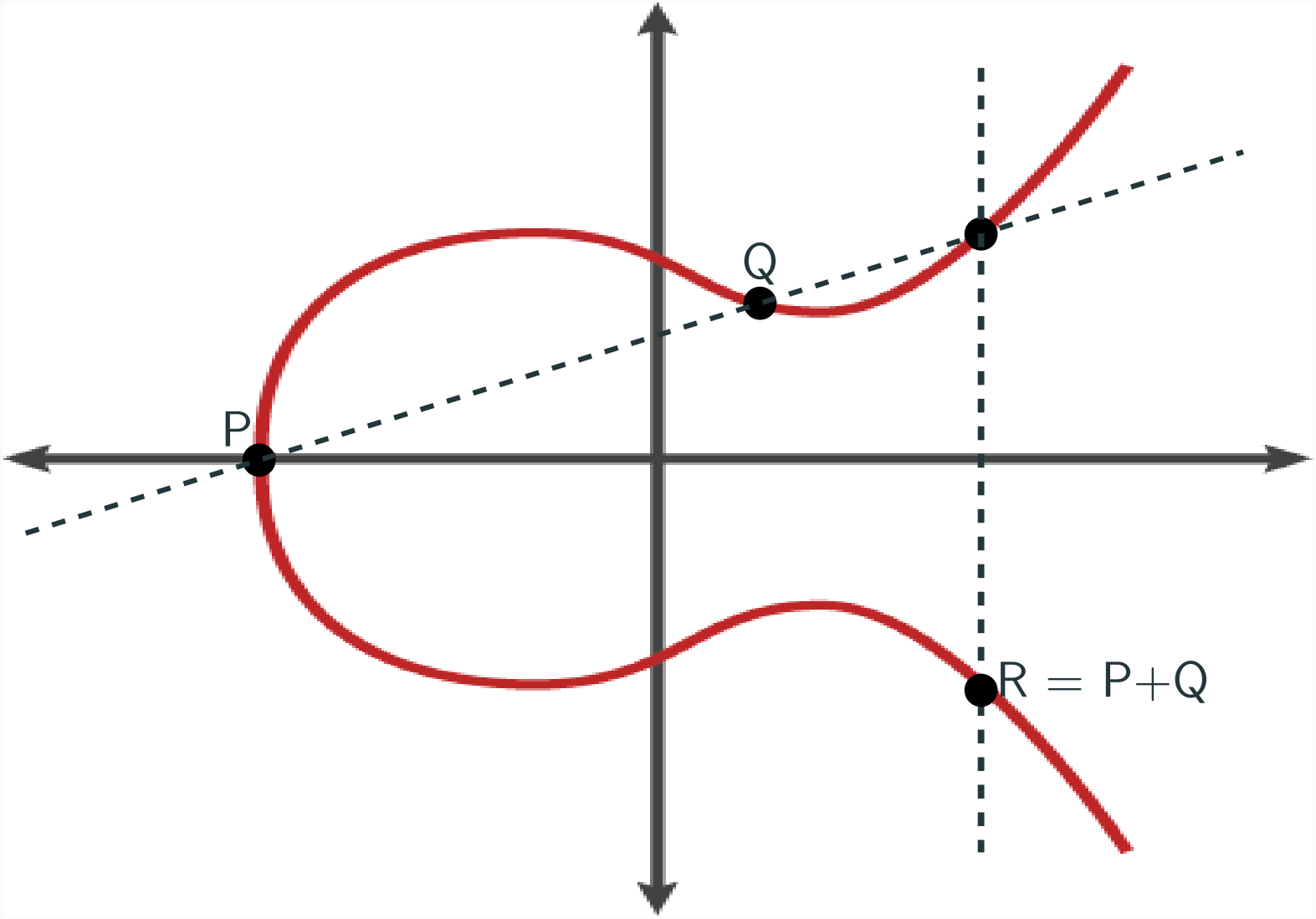
Elliptic Curves are Groups



Elliptic Curves are Groups



Elliptic Curves are Groups



The j-invariant

The j-invariant

How do we classify elliptic curves?

The j-invariant

How do we classify elliptic curves?

Definition

The **j-invariant** of an elliptic curve $E : y^2 = x^3 + ax + b$ is

$$j(E) = 1728\frac{4a^3}{4a^3 + 27b^2}$$

The Trace

The order of $E(\mathbb{F}_q)$ is "centered around" $q + 1$.

The Trace

The order of $E(\mathbb{F}_q)$ is "centered around" $q+1$.

Definition

The **trace** of an elliptic curve $E(\mathbb{F}_q)$ is

$$a_q = \#(q+1) - E(\mathbb{F}_q)$$

where $\#E(\mathbb{F}_q)$ is the order.

The Trace

The order of $E(\mathbb{F}_q)$ is "centered around" $q+1$.

Definition

The **trace** of an elliptic curve $E(\mathbb{F}_q)$ is

$$a_q = \#(q+1) - E(\mathbb{F}_q)$$

where $\#E(\mathbb{F}_q)$ is the order.

Theorem (Hasse)

Let q be a prime power and $E(\mathbb{F}_q)$ an elliptic curve with trace a_q. Then $|a_q| \leq 2\sqrt{q}$.

Elliptic Curve Orders

Curves with $j \neq 0, 1728$

Curves with $j \neq 0, 1728$

- $\mathbb{F}_q$ denotes the finite field with q elements, where $q = p^r$ for a prime p.

Curves with $j \neq 0, 1728$

- $\mathbb{F}_q$ denotes the finite field with q elements, where $q = p^r$ for a prime p.
- If $j \neq 0, 1728$ for E, then E is defined by an equation

$$y^2 = x^3 + Ax + B$$

where $A, B \neq 0$.

Curves with $j \neq 0, 1728$

- $\mathbb{F}_q$ denotes the finite field with q elements, where $q = p^r$ for a prime p.
- If $j \neq 0, 1728$ for E, then E is defined by an equation

$$y^2 = x^3 + Ax + B$$

where $A, B \neq 0$.

Theorem

If $j_0 \neq 0, 1728$, then there is an integer $a_q(j_0)$ such that for all curves $E(\mathbb{F}_q)$ with j-invariant equal to j_0

$$\#E(\mathbb{F}_q) \in \{q + 1 \pm a_q(j_0)\}$$

Moreover, each order is realized by some curve.

Curves with $j = 0$

Curves with $j = 0$

- If $E(\mathbb{F}_q)$ has $j = 0$, then E is defined by

$$y^2 = x^3 + B.$$

Curves with $j = 0$

- If $E(\mathbb{F}_q)$ has $j = 0$, then E is defined by

$$y^2 = x^3 + B.$$

Theorem

Let $E(\mathbb{F}_q)$ be an elliptic curve with $j = 0$. If $q \equiv 2 \pmod 3$, then

$$\#E(F_q) = q + 1.$$

Curves with $j = 0$

- If $E(\mathbb{F}_q)$ has $j = 0$, then E is defined by

$$y^2 = x^3 + B.$$

Theorem

Let $E(\mathbb{F}_q)$ be an elliptic curve with $j = 0$. If $q \equiv 2 \pmod 3$, then

$$\#E(F_q) = q + 1.$$

Theorem

Let $E(\mathbb{F}_q)$ be an elliptic curve with $j = 0$. If $q \equiv 1 \pmod 3$, then E takes on one of 6 possible orders. Moreover, there are curves with $j = 0$ that realize each order.

A Special Case

A Special Case

- If $p \equiv 2 \pmod 3$, then q^r switches cases depending on the parity of r.

A Special Case

- If $p \equiv 2 \pmod 3$, then q^r switches cases depending on the parity of r.
- When r is even, we can compute the orders explicitly.

A Special Case

- If $p \equiv 2 \pmod 3$, then q^r switches cases depending on the parity of r.
- When r is even, we can compute the orders explicitly.

Theorem

If $q = p^r$ where $p \equiv 2 \pmod 3$ and r even, then if $E(\mathbb{F}_q)$ has $j = 0$, then

$$\#E(\mathbb{F}_q) \in \{p + 1 \pm 2p^{r/2}, p + 1 \pm p^{r/2}\}$$

Curves with $j = 1728$

Curves with $j = 1728$

- If $E(\mathbb{F}_q)$ has $j = 1728$, then E is defined by

$$y^2 = x^3 + Ax.$$

Curves with $j = 1728$

- If $E(\mathbb{F}_q)$ has $j = 1728$, then E is defined by

$$y^2 = x^3 + Ax.$$

Theorem

Let $E(\mathbb{F}_q)$ be an elliptic curve with $j = 1728$. If $q \equiv 3 \pmod 4$, then

$$\#E(F_q) = q + 1.$$

Curves with $j = 1728$

- If $E(\mathbb{F}_q)$ has $j = 1728$, then E is defined by

$$y^2 = x^3 + Ax.$$

Theorem

Let $E(\mathbb{F}_q)$ be an elliptic curve with $j = 1728$. If $q \equiv 3 \pmod 4$, then

$$\#E(F_q) = q + 1.$$

Theorem

Let $E(\mathbb{F}_q)$ be an elliptic curve with $j = 1728$. If $q \equiv 1 \pmod 4$, then E takes on one of 4 possible orders. Moreover, there are curves with $j = 1728$ that realize each order.

A Special Case

A Special Case

- If $q = p^r$ where $p \equiv 3 \pmod 4$ and r is even, then we can compute the orders explicitly.

A Special Case

- If $q = p^r$ where $p \equiv 3 \pmod 4$ and r is even, then we can compute the orders explicitly.

Theorem

If $q = p^r$ where $p \equiv 3 \pmod 4$ and r even, then if $E(\mathbb{F}_q)$ has $j = 1728$, then

$$\#E(\mathbb{F}_q) \in \{p + 1, p + 1 \pm 2p^{r/2}\}$$

Summary

	$j = 0$		$j = 1728$		$j \notin \{0, 1728\}$
	$p \equiv 1 \pmod 3$	$p \equiv 2 \pmod 3$	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$	
$\mathbb{F}_p$	6 orders	1 order	4 orders	1 order	2 orders
F_{p^r} (r odd)	6 orders	1 order	4 orders	1 order	2 orders
F_{p^r} (r even)	6 orders	4 orders	4 orders	3 orders	2 orders

Bachet Anomalous Primes and Bachet Anomalous Numbers

Changing Focus

Changing Focus

- In the previous section, we characterized all possible orders of all possible elliptic curves, given a finite field.

Changing Focus

- In the previous section, we characterized all possible orders of all possible elliptic curves, given a finite field.
- Now, we focus on *one* kind of order of *one* kind of elliptic curve, given a finite field.

Changing Focus

- In the previous section, we characterized all possible orders of all possible elliptic curves, given a finite field.
- Now, we focus on *one* kind of order of *one* kind of elliptic curve, given a finite field.

	$j=0$		$j=1728$		$j \notin \{0, 1728\}$
	$p \equiv 1 \pmod 3$	$p \equiv 2 \pmod 3$	$p \equiv 1 \pmod 4$	$p \equiv 3 \pmod 4$	
$\mathbb{F}_p$	6 orders	1 order	4 orders	1 order	2 orders
F_{p^r} (r odd)	6 orders	1 order	4 orders	1 order	2 orders
F_{p^r} (r even)	6 orders	4 orders	4 orders	3 orders	2 orders

Bachet Anomalous Primes

Bachet Anomalous Primes

Definition— One Kind of Order

A prime p is called **anomalous** if there exists an elliptic curve E defined over the finite field $\mathbb{F}_p$ with order $\#E(\mathbb{F}_p) = p$.

Bachet Anomalous Primes

Definition— One Kind of Order

A prime p is called **anomalous** if there exists an elliptic curve E defined over the finite field $\mathbb{F}_p$ with order $\#E(\mathbb{F}_p) = p$.

Definition— One Kind of Order of One Kind of Curve

p is called a **Bachet anomalous prime** if there exists an elliptic curve E of the form $y^2 = x^3 + B$ such that $\#E(\mathbb{F}_p) = p$.

Bachet Anomalous Primes

Definition— One Kind of Order

A prime p is called **anomalous** if there exists an elliptic curve E defined over the finite field $\mathbb{F}_p$ with order $\#E(\mathbb{F}_p) = p$.

Definition— One Kind of Order of One Kind of Curve

p is called a **Bachet anomalous prime** if there exists an elliptic curve E of the form $y^2 = x^3 + B$ such that $\#E(\mathbb{F}_p) = p$.

Bachet Anomalous Primes

Definition— One Kind of Order

A prime p is called **anomalous** if there exists an elliptic curve E defined over the finite field $\mathbb{F}_p$ with order $\#E(\mathbb{F}_p) = p$.

Definition— One Kind of Order of One Kind of Curve

p is called a **Bachet anomalous prime** if there exists an elliptic curve E of the form $y^2 = x^3 + B$ such that $\#E(\mathbb{F}_p) = p$.

- Elliptic curves of the form $y^2 = x^3 + B$ are exactly the curves with j-invariant 0.

Bachet Anomalous Primes

Definition— One Kind of Order

A prime p is called **anomalous** if there exists an elliptic curve E defined over the finite field $\mathbb{F}_p$ with order $\#E(\mathbb{F}_p) = p$.

Definition— One Kind of Order of One Kind of Curve

p is called a **Bachet anomalous prime** if there exists an elliptic curve E of the form $y^2 = x^3 + B$ such that $\#E(\mathbb{F}_p) = p$.

- Elliptic curves of the form $y^2 = x^3 + B$ are exactly the curves with j-invariant 0.
    - These curves are known as **Bachet elliptic curves**.

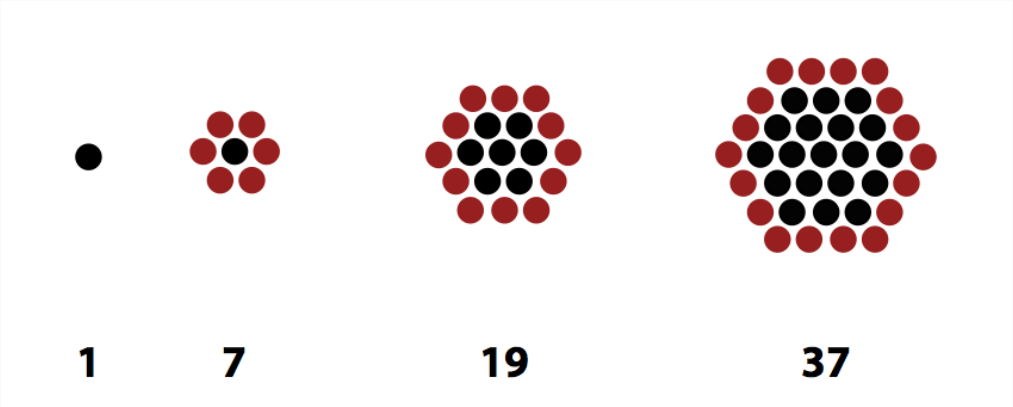
Bachet Anomalous Primes and Centered Hexagonal Numbers

Centered Hexagonal Numbers

A **centered hexagonal number** is any number that can be expressed as a difference of consecutive cubes:
$(n+1)^3 - n^3 = 3n^2 + 3n + 1$

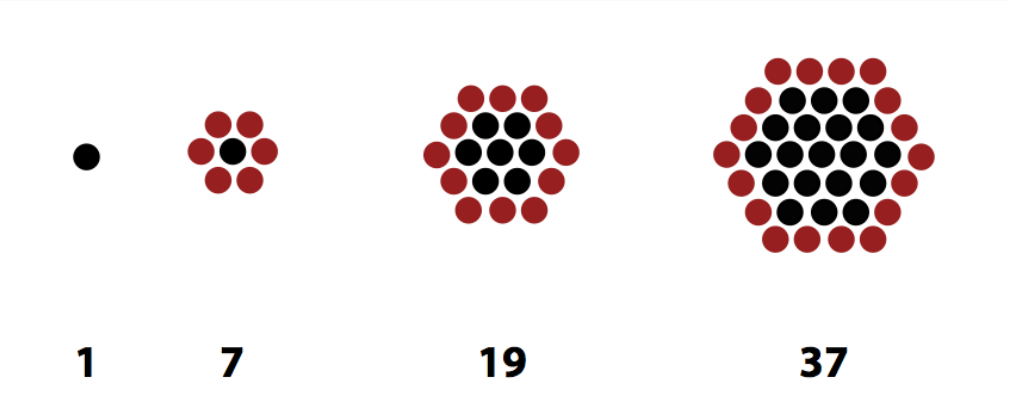
Centered Hexagonal Numbers

A **centered hexagonal number** is any number that can be expressed as a difference of consecutive cubes:
$(n+1)^3 - n^3 = 3n^2 + 3n + 1$



Centered Hexagonal Numbers

A **centered hexagonal number** is any number that can be expressed as a difference of consecutive cubes:
$(n+1)^3 - n^3 = 3n^2 + 3n + 1$



Theorem

A prime number p is a Bachet anomalous prime if and only if it is a centered hexagonal number.

Generalizing to Powers of Primes

Generalizing to Powers of Primes

- Just like before, we now work to generalize our results to general finite field $\mathbb{F}_{p^r}$.

Generalizing to Powers of Primes

- Just like before, we now work to generalize our results to general finite field $\mathbb{F}_{p^r}$.

Definition (Generalizing Bachet anomalous primes)

A prime power p^r is called a **Bachet anomalous number** if there exists an elliptic curve $E : y^2 = x^3 + B$ defined over the finite field $\mathbb{F}_{p^r}$ with order $\#E(\mathbb{F}_{p^r}) = p^r$.

Generalizing to Powers of Primes

- Just like before, we now work to generalize our results to general finite field $\mathbb{F}_{p^r}$.

Definition (Generalizing Bachet anomalous primes)

A prime power p^r is called a **Bachet anomalous number** if there exists an elliptic curve $E : y^2 = x^3 + B$ defined over the finite field $\mathbb{F}_{p^r}$ with order $\#E(\mathbb{F}_{p^r}) = p^r$.

Theorem

All Bachet anomalous numbers p^r are centered hexagonal numbers.

Generalizing to Powers of Primes

- Just like before, we now work to generalize our results to general finite field $\mathbb{F}_{p^r}$.

Definition (Generalizing Bachet anomalous primes)

A prime power p^r is called a **Bachet anomalous number** if there exists an elliptic curve $E : y^2 = x^3 + B$ defined over the finite field $\mathbb{F}_{p^r}$ with order $\#E(\mathbb{F}_{p^r}) = p^r$.

Theorem

All Bachet anomalous numbers p^r are centered hexagonal numbers.

Theorem

Let $p^r = (n+1)^3 - n^3$ be a prime power centered hexagonal number. When $r \in \{1, 2\}$, p^r is always a Bachet anomalous number.

The Tidjeman-Zagier Conjecture

The Tidjeman-Zagier Conjecture

Conjecture

Let A, B, C, x, y, and z be positive integers, with $x, y, z > 2$. If A, B, and C are relatively prime, then $A^x + B^y = C^z$ has no integer solutions (A, B, C).

The Tidjeman-Zagier Conjecture

Conjecture

Let A, B, C, x, y, and z be positive integers, with $x, y, z > 2$. If A, B, and C are relatively prime, then $A^x + B^y = C^z$ has no integer solutions (A, B, C).

- Every Bachet anomalous number p^r can be expressed as $(n+1)^3 - n^3$.

The Tidjeman-Zagier Conjecture

Conjecture

Let A, B, C, x, y, and z be positive integers, with $x, y, z > 2$. If A, B, and C are relatively prime, then $A^x + B^y = C^z$ has no integer solutions (A, B, C).

- Every Bachet anomalous number p^r can be expressed as $(n+1)^3 - n^3$. $p^r = (n+1)^3 - n^3$

The Tidjeman-Zagier Conjecture

Conjecture

Let A, B, C, x, y, and z be positive integers, with $x, y, z > 2$. If A, B, and C are relatively prime, then $A^x + B^y = C^z$ has no integer solutions (A, B, C).

- Every Bachet anomalous number p^r can be expressed as $(n+1)^3 - n^3$. $p^r = (n+1)^3 - n^3 \iff A^r = B^3 + C^3$

The Tidjeman-Zagier Conjecture

Conjecture

Let A, B, C, x, y, and z be positive integers, with $x, y, z > 2$. If A, B, and C are relatively prime, then $A^x + B^y = C^z$ has no integer solutions (A, B, C).

- Every Bachet anomalous number p^r can be expressed as $(n+1)^3 - n^3$. $p^r = (n+1)^3 - n^3 \iff A^r = B^3 + C^3$
- $gcd(n, n+1) = 1 \Rightarrow gcd(p, n, n+1) = 1$

The Tidjeman-Zagier Conjecture

Conjecture

Let A, B, C, x, y, and z be positive integers, with $x, y, z > 2$. If A, B, and C are relatively prime, then $A^x + B^y = C^z$ has no integer solutions (A, B, C).

- Every Bachet anomalous number p^r can be expressed as $(n+1)^3 - n^3$. $p^r = (n+1)^3 - n^3 \iff A^r = B^3 + C^3$
- $gcd(n, n+1) = 1 \Rightarrow gcd(p, n, n+1) = 1$
- T-Z conjecture $\Rightarrow$ when $r \geq 3$ there are no solutions to $p^r = (n+1)^3 - n^3$

The Tidjeman-Zagier Conjecture

Conjecture

Let A, B, C, x, y, and z be positive integers, with $x, y, z > 2$. If A, B, and C are relatively prime, then $A^x + B^y = C^z$ has no integer solutions (A, B, C).

- Every Bachet anomalous number p^r can be expressed as $(n+1)^3 - n^3$. $p^r = (n+1)^3 - n^3 \iff A^r = B^3 + C^3$
- $gcd(n, n+1) = 1 \Rightarrow gcd(p, n, n+1) = 1$
- T-Z conjecture $\Rightarrow$ when $r \geq 3$ there are no solutions to $p^r = (n+1)^3 - n^3$

Theorem

Let $p^r = (n+1)^3 - n^3$ be a prime power centered hexagonal number. When $r \in \{1, 2\}$, p^r is always a Bachet anomalous number.

The Tidjeman-Zagier Conjecture

Conjecture

Let A, B, C, x, y, and z be positive integers, with $x, y, z > 2$. If A, B, and C are relatively prime, then $A^x + B^y = C^z$ has no integer solutions (A, B, C).

- Every Bachet anomalous number p^r can be expressed as $(n+1)^3 - n^3$. $p^r = (n+1)^3 - n^3 \iff A^r = B^3 + C^3$
- $gcd(n, n+1) = 1 \Rightarrow gcd(p, n, n+1) = 1$
- T-Z conjecture $\Rightarrow$ when $r \geq 3$ there are no solutions to $p^r = (n+1)^3 - n^3$

Theorem

Let $p^r = (n+1)^3 - n^3$ be a prime power centered hexagonal number. When $r \in \{1, 2\}$, p^r is always a Bachet anomalous number. Assuming T-Z conjecture, there are no Bachet anomalous numbers p^r when $r \geq 3$.

Type I Elliptic Korselt Numbers

Elliptic Carmichael Numbers

Elliptic Carmichael Numbers

- Elliptic curves can also be defined over $\mathbb{Z}/n\mathbb{Z}$.

Elliptic Carmichael Numbers

- Elliptic curves can also be defined over $\mathbb{Z}/n\mathbb{Z}$.
  - Over $\mathbb{F}_p$, we can define $a_p = p + 1 - \#E(\mathbb{F}_p)$.

Elliptic Carmichael Numbers

- Elliptic curves can also be defined over $\mathbb{Z}/n\mathbb{Z}$.
  - Over $\mathbb{F}_p$, we can define $a_p = p + 1 - \#E(\mathbb{F}_p)$.
  - Over $\mathbb{Z}/n\mathbb{Z}$, a_n can be defined as the n^{th} coefficient of the L-series of E.

Elliptic Carmichael Numbers

- Elliptic curves can also be defined over $\mathbb{Z}/n\mathbb{Z}$.
  - Over $\mathbb{F}_p$, we can define $a_p = p + 1 - \#E(\mathbb{F}_p)$.
  - Over $\mathbb{Z}/n\mathbb{Z}$, a_n can be defined as the n^{th} coefficient of the L-series of E.

Definition

An **elliptic Carmichael number** for a curve E is a composite number n such that for every $\mathcal{P} \in E(\mathbb{Z}/n\mathbb{Z})$,

Elliptic Carmichael Numbers

- Elliptic curves can also be defined over $\mathbb{Z}/n\mathbb{Z}$.
  - Over $\mathbb{F}_p$, we can define $a_p = p + 1 - \#E(\mathbb{F}_p)$.
  - Over $\mathbb{Z}/n\mathbb{Z}$, a_n can be defined as the n^{th} coefficient of the L-series of E.

Definition

An **elliptic Carmichael number** for a curve E is a composite number n such that for every $\mathcal{P} \in E(\mathbb{Z}/n\mathbb{Z})$,

$$(n + 1 - a_n)\mathcal{P} = \infty.$$

Elliptic Carmichael Numbers

- Elliptic curves can also be defined over $\mathbb{Z}/n\mathbb{Z}$.
  - Over $\mathbb{F}_p$, we can define $a_p = p + 1 - \#E(\mathbb{F}_p)$.
  - Over $\mathbb{Z}/n\mathbb{Z}$, a_n can be defined as the n^{th} coefficient of the L-series of E.

Definition

An **elliptic Carmichael number** for a curve E is a composite number n such that for every $\mathcal{P} \in E(\mathbb{Z}/n\mathbb{Z})$,

$$(n + 1 - a_n)\mathcal{P} = \infty.$$

- Just like regular Carmichael numbers, these are numbers that pass a primality test despite being composite.

Type I Elliptic Korselt Numbers

Type I Elliptic Korselt Numbers

Definition

For an elliptic curve E, a positive integer n is called a **Type I elliptic Korselt Number (EK-I Number)** if it has at least two distinct prime factors and for each prime factor p,

$$p + 1 - a_p \mid n + 1 - a_n \text{ and}$$

$$\operatorname{ord}_p(a_n - 1) \geq \operatorname{ord}_p(n) - \begin{cases} 1 & \text{if } a_p \not\equiv 1 \pmod{p} \\ 0 & \text{otherwise.} \end{cases}$$

Type I Elliptic Korselt Numbers

Definition

For an elliptic curve E, a positive integer n is called a **Type I elliptic Korselt Number (EK-I Number)** if it has at least two distinct prime factors and for each prime factor p,

$$p+1-a_p \mid n+1-a_n \text{ and}$$

$$\operatorname{ord}_p(a_n-1) \geq \operatorname{ord}_p(n) - \begin{cases} 1 & \text{if } a_p \not\equiv 1 \pmod{p} \\ 0 & \text{otherwise.} \end{cases}$$

Theorem

If n is an EK-I number for an elliptic curve E, then n is an elliptic Carmichael number for E [S, Proposition 11].

Products of Anomalous Primes are EK-I Numbers

Products of Anomalous Primes are EK-I Numbers

Definition

A prime p is **anomalous** for an elliptic curve E if $\#E(\mathbb{F}_p) = p$.

Products of Anomalous Primes are EK-I Numbers

Definition

A prime p is **anomalous** for an elliptic curve E if $\#E(\mathbb{F}_p) = p$.

- Equivalently, $a_p = 1$.

Products of Anomalous Primes are EK-I Numbers

Definition

A prime p is **anomalous** for an elliptic curve E if $\#E(\mathbb{F}_p) = p$.

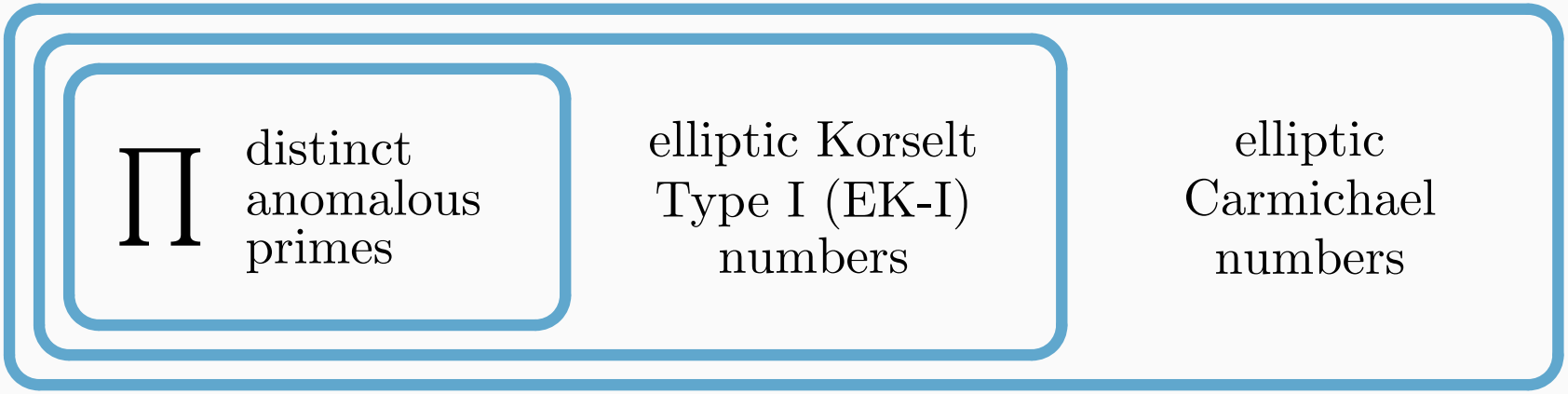
- Equivalently, $a_p = 1$.

Theorem

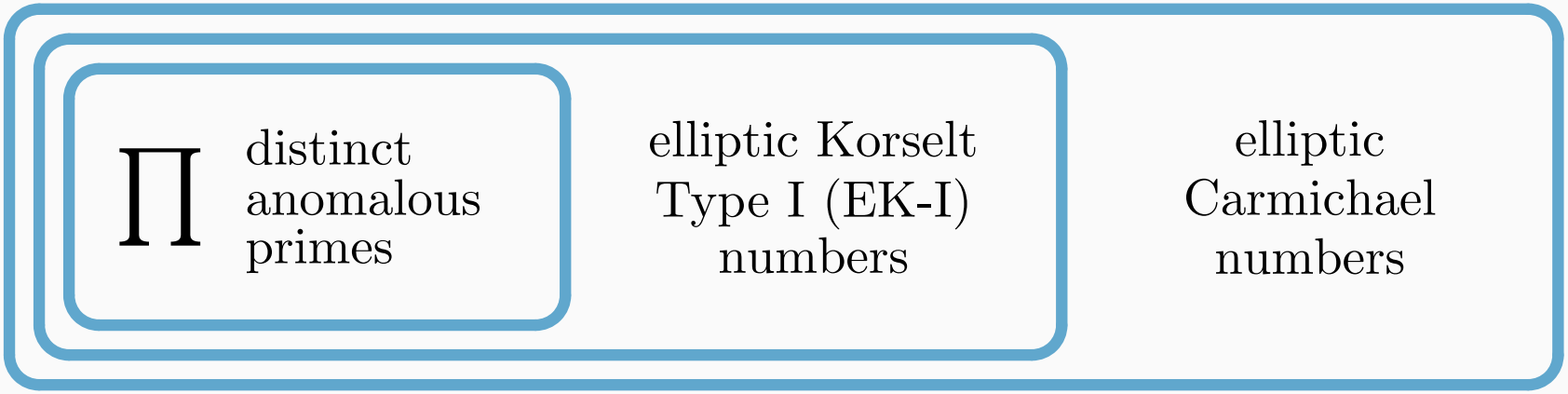
Every product of distinct anomalous primes for an elliptic curve E is a Type I elliptic Korselt number for E.

Relevant Inclusions

Relevant Inclusions

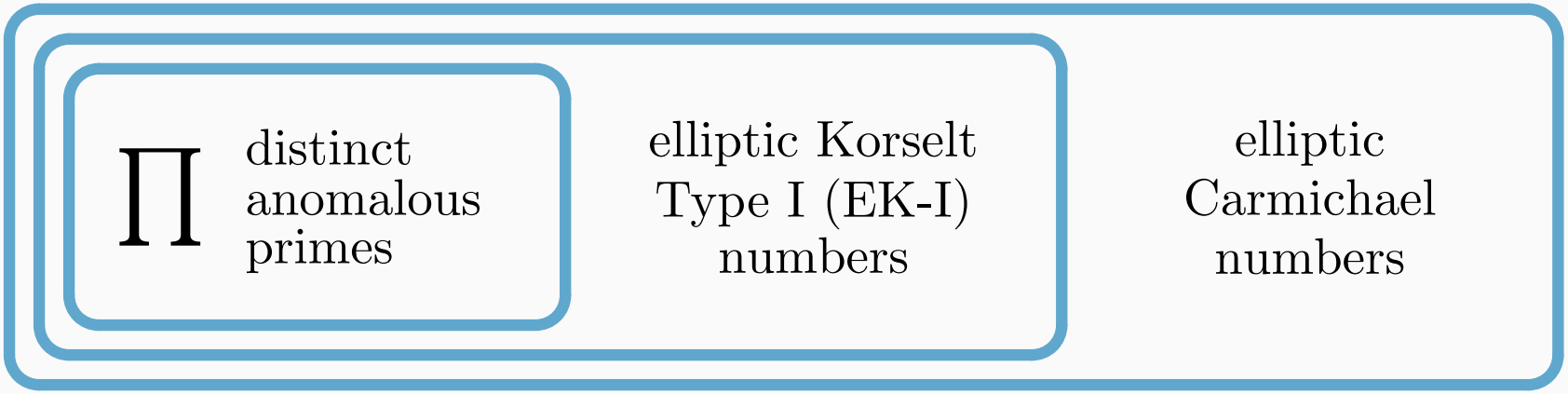


Relevant Inclusions



- This raises the question: how strict are the inclusions?

Relevant Inclusions



- This raises the question: how strict are the inclusions?
- We made progress on that question for the inner inclusion.

A Restriction on EK-I Numbers

A Restriction on EK-I Numbers

Theorem

Let E be an elliptic curve and $n = p_1 p_2 \dots p_m$ be a Type I elliptic Korselt number for E such that $5 \leq p_1 < p_2 < \cdots < p_m$, for $m \geq 2$.

A Restriction on EK-I Numbers

Theorem

Let E be an elliptic curve and $n = p_1 p_2 \dots p_m$ be a Type I elliptic Korselt number for E such that $5 \leq p_1 < p_2 < \cdots < p_m$, for $m \geq 2$. If

$$4^m < p_1 p_2 \dots p_{m-1} < \frac{\sqrt{p_m}}{4^m},$$

A Restriction on EK-I Numbers

Theorem

Let E be an elliptic curve and $n = p_1 p_2 \dots p_m$ be a Type I elliptic Korselt number for E such that $5 \leq p_1 < p_2 < \cdots < p_m$, for $m \geq 2$. If

$$4^m < p_1 p_2 \dots p_{m-1} < \frac{\sqrt{p_m}}{4^m},$$

then $a_{p_m} = 1$, and for $1 \leq i \leq m-1$, $a_{p_i} = -1$ for an even number of values of i and the remaining traces are equal to 1.

A Restriction on EK-I Numbers

Theorem

Let E be an elliptic curve and $n = p_1 p_2 \dots p_m$ be a Type I elliptic Korselt number for E such that $5 \leq p_1 < p_2 < \cdots < p_m$, for $m \geq 2$. If

$$4^m < p_1 p_2 \dots p_{m-1} < \frac{\sqrt{p_m}}{4^m},$$

then $a_{p_m} = 1$, and for $1 \leq i \leq m-1$, $a_{p_i} = -1$ for an even number of values of i and the remaining traces are equal to 1.

- This places a restriction on the traces of E over the F_{p_i} when the conditions are satisfied.

A Restriction on EK-I Numbers

Theorem

Let E be an elliptic curve and $n = p_1 p_2 \dots p_m$ be a Type I elliptic Korselt number for E such that $5 \leq p_1 < p_2 < \cdots < p_m$, for $m \geq 2$. If

$$4^m < p_1 p_2 \dots p_{m-1} < \frac{\sqrt{p_m}}{4^m},$$

then $a_{p_m} = 1$, and for $1 \leq i \leq m-1$, $a_{p_i} = -1$ for an even number of values of i and the remaining traces are equal to 1.

- This places a restriction on the traces of E over the F_{p_i} when the conditions are satisfied.
- For $m = 2$ this gives us a circumstance under which E must be anomalous over p_1 and p_2 (when $16 < p_1 < \sqrt{p_2}16$), correcting Silverman's result.

A Restriction on EK-I Numbers

Theorem

Let E be an elliptic curve and $n = p_1 p_2 \dots p_m$ be a Type I elliptic Korselt number for E such that $5 \leq p_1 < p_2 < \cdots < p_m$, for $m \geq 2$. If

$$4^m < p_1 p_2 \dots p_{m-1} < \frac{\sqrt{p_m}}{4^m},$$

then $a_{p_m} = 1$, and for $1 \leq i \leq m-1$, $a_{p_i} = -1$ for an even number of values of i and the remaining traces are equal to 1.

- This places a restriction on the traces of E over the F_{p_i} when the conditions are satisfied.
- For $m = 2$ this gives us a circumstance under which E must be anomalous over p_1 and p_2 (when $16 < p_1 < \sqrt{p_2}16$), correcting Silverman's result.
- The drawback: these conditions are "rarely" satisfied.

The Order Divisibility Conjecture

The Order Divisibility Conjecture

Order Divisibility Conjecture

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$.

The Order Divisibility Conjecture

Order Divisibility Conjecture

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve with good reduction over $\mathbb{F}_p$ and $\mathbb{F}_q$ such that $\#E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_q)$ divide $n + 1 - a_n$.

The Order Divisibility Conjecture

Order Divisibility Conjecture

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve with good reduction over $\mathbb{F}_p$ and $\mathbb{F}_q$ such that $\#E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_q)$ divide $n + 1 - a_n$. Then

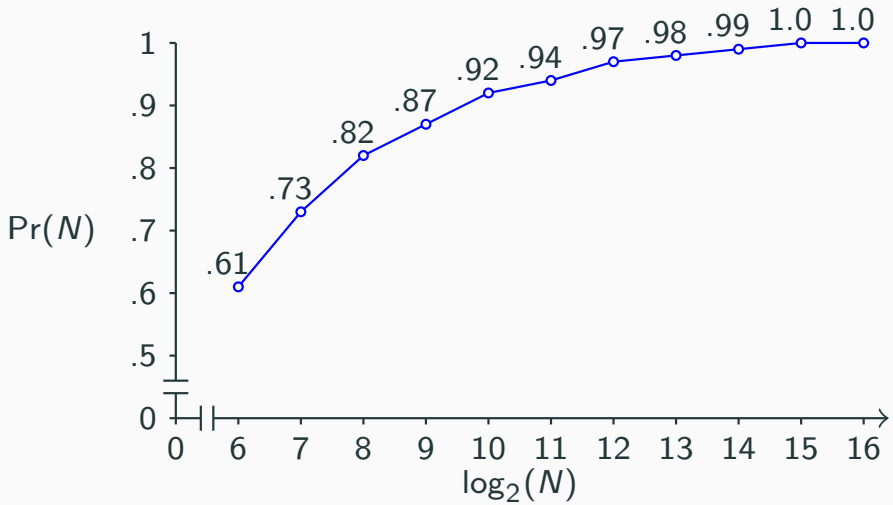
$$\lim_{N \to \infty} \Pr[\#E(\mathbb{Z}/n\mathbb{Z}) = n + 1 - a_n] = 1.$$

The Order Divisibility Conjecture

Order Divisibility Conjecture

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve with good reduction over $\mathbb{F}_p$ and $\mathbb{F}_q$ such that $\#E(\mathbb{F}_p)$ and $\#E(\mathbb{F}_q)$ divide $n + 1 - a_n$. Then

$$\lim_{N \to \infty} \Pr[\#E(\mathbb{Z}/n\mathbb{Z}) = n + 1 - a_n] = 1.$$



A Probabilistic Restriction on EK-I Numbers

A Probabilistic Restriction on EK-I Numbers

Theorem

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$.

A Probabilistic Restriction on EK-I Numbers

Theorem

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve for which n is a Type I elliptic Korselt number.

A Probabilistic Restriction on EK-I Numbers

Theorem

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve for which n is a Type I elliptic Korselt number. Assuming the Order Divisibility Conjecture,

A Probabilistic Restriction on EK-I Numbers

Theorem

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve for which n is a Type I elliptic Korselt number. Assuming the Order Divisibility Conjecture, we have

$$\lim_{N \to \infty} \Pr[p \text{ and } q \text{ are anomalous primes for } E] = 1.$$

A Probabilistic Restriction on EK-I Numbers

Theorem

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve for which n is a Type I elliptic Korselt number. Assuming the Order Divisibility Conjecture, we have

$$\lim_{N \to \infty} \Pr[p \text{ and } q \text{ are anomalous primes for } E] = 1.$$

- This means that "almost all" EK-I numbers $n = pq$ for E have p and q anomalous for E.

A Probabilistic Restriction on EK-I Numbers

Theorem

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve for which n is a Type I elliptic Korselt number. Assuming the Order Divisibility Conjecture, we have

$$\lim_{N \to \infty} \Pr[p \text{ and } q \text{ are anomalous primes for } E] = 1.$$

- This means that "almost all" EK-I numbers $n = pq$ for E have p and q anomalous for E.
- Drawback: theorem is only for two primes.

A Probabilistic Restriction on EK-I Numbers

Theorem

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve for which n is a Type I elliptic Korselt number. Assuming the Order Divisibility Conjecture, we have

$$\lim_{N \to \infty} \Pr[p \text{ and } q \text{ are anomalous primes for } E] = 1.$$

- This means that "almost all" EK-I numbers $n = pq$ for E have p and q anomalous for E.
- Drawback: theorem is only for two primes.
- Future work: potentially extend theorem to m primes.

A Probabilistic Restriction on EK-I Numbers

Theorem

For $N \geq 7$, let $5 \leq p, q \leq N$ be randomly chosen distinct primes, and let $n = pq$. Let $E(\mathbb{Z}/n\mathbb{Z})$ be a randomly chosen elliptic curve for which n is a Type I elliptic Korselt number. Assuming the Order Divisibility Conjecture, we have

$$\lim_{N \to \infty} \Pr[p \text{ and } q \text{ are anomalous primes for } E] = 1.$$

- This means that "almost all" EK-I numbers $n = pq$ for E have p and q anomalous for E.
- Drawback: theorem is only for two primes.
- Future work: potentially extend theorem to m primes.
- If such an extension is plausible, then anomalous primes are the cornerstone to understanding EK-I numbers.

References

- J.H. Silverman, Elliptic Carmichael Numbers and Elliptic Korselt Criteria, Acta Arithmetica Vol. 155:3, (2012) 233–246.
- J.H. Silverman and K.E. Stange
  Amicable pairs and aliquot cycles for elliptic curves
  Experimental Mathematics, 20:3 (2011), 329–357.
- L.C. Washington
  Number Theory: Elliptic Curves and Cryptography
  Vol. 50 of Discrete Mathematics and Its Applications, Chapman & Hall/CRC, 2nd ed., (2008).

Acknowledgments

Supported by the National Science Foundation grant DMS-1359425 and Boise State University.