ABC Triples and Elliptic Curves: Research on a Connection

Elise Alvarez-Salazar[1] and Barry Henaku[2]

Pomona College

August 1, 2022

[1]University of California, Santa Barbara
[2]Washington University in St. Louis

Table of Contents

Why ABC triples?

ABC triples lead to a discussion of the ABC conjecture.

Why ABC triples?

ABC triples lead to a discussion of the ABC conjecture.

Who cares about the ABC conjecture?

Why ABC triples?

ABC triples lead to a discussion of the ABC conjecture.

Who cares about the ABC conjecture?

If proven to be true, it could:

Why ABC triples?

ABC triples lead to a discussion of the ABC conjecture.

Who cares about the ABC conjecture?

If proven to be true, it could:

- Give an explicit proof of Falting's Theorem.

Why ABC triples?

ABC triples lead to a discussion of the ABC conjecture.

Who cares about the ABC conjecture?

If proven to be true, it could:

- Give an explicit proof of Falting's Theorem.
- Provide a proof of Fermat's Last Theorem with the explicit form of the ABC conjecture where $n \geq 6$.

Why ABC triples?

ABC triples lead to a discussion of the ABC conjecture.

Who cares about the ABC conjecture?

If proven to be true, it could:

- Give an explicit proof of Falting's Theorem.
- Provide a proof of Fermat's Last Theorem with the explicit form of the ABC conjecture where $n \geq 6$.
- Conclude Roth's theorem.

What is the link to elliptic curves?

Why ABC triples?

ABC triples lead to a discussion of the ABC conjecture.

Who cares about the ABC conjecture?

If proven to be true, it could:

- Give an explicit proof of Falting's Theorem.
- Provide a proof of Fermat's Last Theorem with the explicit form of the ABC conjecture where $n \geq 6$.
- Conclude Roth's theorem.

What is the link to elliptic curves?

There is an equivalent statement about the ABC conjecture in terms of elliptic curves:

Why ABC triples?

ABC triples lead to a discussion of the ABC conjecture.

Who cares about the ABC conjecture?

If proven to be true, it could:

- Give an explicit proof of Falting's Theorem.
- Provide a proof of Fermat's Last Theorem with the explicit form of the ABC conjecture where $n \geq 6$.
- Conclude Roth's theorem.

What is the link to elliptic curves?

There is an equivalent statement about the ABC conjecture in terms of elliptic curves: the **Modified Szpiro Conjecture**.

Table of Contents

Definitions

Definition

Euler's totient function, $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Definitions

Definition

Euler's totient function, $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Example

$\phi(3)$

Definitions

Definition

Euler's totient function, $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Example

$\phi(3) = |\{1, 2\}|$

Definitions

Definition

Euler's totient function, $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Example

$\phi(3) = |\{1, 2\}| = 2$

Definitions

Definition

Euler's totient function, $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Example

$\phi(3) = |\{1, 2\}| = 2$

Example

$\phi(10)$

Definitions

Definition

Euler's totient function, $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Example

$\phi(3) = |\{1, 2\}| = 2$

Example

$\phi(10) = \phi(5 \cdot 2)$

Definitions

Definition

Euler's totient function, $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Example

$\phi(3) = |\{1, 2\}| = 2$

Example

$\phi(10) = \phi(5 \cdot 2) = |\{1, 3, 7, 9\}|$

Definitions

Definition

Euler's totient function, $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Example

$\phi(3) = |\{1, 2\}| = 2$

Example

$\phi(10) = \phi(5 \cdot 2) = |\{1, 3, 7, 9\}| = 4$

Definitions

Definition

Euler's totient function, $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Example

$\phi(3) = |\{1, 2\}| = 2$

Example

$\phi(10) = \phi(5 \cdot 2) = |\{1, 3, 7, 9\}| = 4$

Example

$\phi(27)$

Definitions

Definition

Euler's totient function, $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Example

$\phi(3) = |\{1, 2\}| = 2$

Example

$\phi(10) = \phi(5 \cdot 2) = |\{1, 3, 7, 9\}| = 4$

Example

$\phi(27) = \phi(3^3)$

Definitions

Definition

Euler's totient function, $\phi(n)$, counts the positive integers up to a given integer n that are relatively prime to n.

Example

$\phi(3) = |\{1, 2\}| = 2$

Example

$\phi(10) = \phi(5 \cdot 2) = |\{1, 3, 7, 9\}| = 4$

Example

$\phi(27) = \phi(3^3) = 18$

What is an ABC Triple?

Definition

An **ABC triple** is a triple of positive integers, (a, b, c), such that $a + b = c$, $a \leq b < c$, and $\gcd(a, b) = 1$.

What is an ABC Triple?

Definition

An **ABC triple** is a triple of positive integers, (a, b, c), such that $a + b = c$, $a \leq b < c$, and $\gcd(a, b) = 1$.

Example

(1, 2, 3)

What is an ABC Triple?

Definition

An **ABC triple** is a triple of positive integers, (a, b, c), such that $a + b = c$, $a \leq b < c$, and $\gcd(a, b) = 1$.

Example

(1, 2, 3)

$(1, 8, 9)$

What is an ABC Triple?

Definition

An **ABC triple** is a triple of positive integers, (a, b, c), such that $a + b = c$, $a \leq b < c$, and $\gcd(a, b) = 1$.

Example

(1, 2, 3)

$(1, 8, 9) = (1, 2^3, 3^2)$

What is an ABC Triple?

Definition

An **ABC triple** is a triple of positive integers, (a, b, c), such that $a + b = c$, $a \leq b < c$, and $\gcd(a, b) = 1$.

Example

(1, 2, 3)

$(1, 8, 9) = (1, 2^3, 3^2)$

$(3, 125, 128)$

What is an ABC Triple?

Definition

An **ABC triple** is a triple of positive integers, (a, b, c), such that $a + b = c$, $a \leq b < c$, and $\gcd(a, b) = 1$.

Example

(1, 2, 3)

$(1, 8, 9) = (1, 2^3, 3^2)$

$(3, 125, 128) = (3, 5^3, 2^7)$

Definition

The **radical of a**, denoted $\text{rad}(a)$, is defined to be the product of the distinct primes of a's prime factorization.

Definition

The **radical of a**, denoted rad(a), is defined to be the product of the distinct primes of a's prime factorization.

Example

rad(27)

Definition

The **radical of a**, denoted rad(a), is defined to be the product of the distinct primes of a's prime factorization.

Example

$\text{rad}(27) = \text{rad}(3^3)$

Definition

The **radical of a**, denoted $\mathrm{rad}(a)$, is defined to be the product of the distinct primes of a's prime factorization.

Example

$\mathrm{rad}(27) = \mathrm{rad}(3^3) = 3$

Definition

The **radical of a**, denoted $\text{rad}(a)$, is defined to be the product of the distinct primes of a's prime factorization.

Example

$\text{rad}(27) = \text{rad}(3^3) = 3$

Example

$\text{rad}(735)$

Definition

The **radical of a**, denoted $\text{rad}(a)$, is defined to be the product of the distinct primes of a's prime factorization.

Example

$\text{rad}(27) = \text{rad}(3^3) = 3$

Example

$\text{rad}(735) = \text{rad}(3 \cdot 7^2 \cdot 5)$

Definition

The **radical of a**, denoted $\text{rad}(a)$, is defined to be the product of the distinct primes of a's prime factorization.

Example

$\text{rad}(27) = \text{rad}(3^3) = 3$

Example

$\text{rad}(735) = \text{rad}(3 \cdot 7^2 \cdot 5) = 3 \cdot 7 \cdot 5 = 105$

Good ABC Triples

Definition

An ABC triple, (a, b, c), is **good** if $\text{rad}(abc) < c$.

Good ABC Triples

Definition

An ABC triple, (a, b, c), is **good** if $\text{rad}(abc) < c$.

Example

$(1, 2, 3)$

Good ABC Triples

Definition

An ABC triple, (a, b, c), is **good** if $\text{rad}(abc) < c$.

Example

$(1, 2, 3)$

$\text{rad}(1 \cdot 2 \cdot 3)$

Good ABC Triples

Definition

An ABC triple, (a, b, c), is **good** if $\mathrm{rad}(abc) < c$.

Example

$(1, 2, 3)$

$\mathrm{rad}(1 \cdot 2 \cdot 3) = 6 > 3$

Examples

Example

$(1, 8, 9)$

Examples

Example

$(1, 8, 9) = (1, 2^3, 3^2)$

Examples

Example

$(1, 8, 9) = (1, 2^3, 3^2)$

$\text{rad}(1 \cdot 8 \cdot 9)$

Examples

Example

$(1, 8, 9) = (1, 2^3, 3^2)$

$\text{rad}(1 \cdot 8 \cdot 9) = \text{rad}(2^3 \cdot 3^2)$

Examples

Example

$(1, 8, 9) = (1, 2^3, 3^2)$

$\text{rad}(1 \cdot 8 \cdot 9) = \text{rad}(2^3 \cdot 3^2) = 6 < 9$

Examples

Example

$(1, 8, 9) = (1, 2^3, 3^2)$

$\text{rad}(1 \cdot 8 \cdot 9) = \text{rad}(2^3 \cdot 3^2) = 6 < 9$

Example

$(3, 125, 128)$

Examples

Example

$(1, 8, 9) = (1, 2^3, 3^2)$

$\text{rad}(1 \cdot 8 \cdot 9) = \text{rad}(2^3 \cdot 3^2) = 6 < 9$

Example

$(3, 125, 128) = (3, 5^3, 2^7)$

Examples

Example

$(1, 8, 9) = (1, 2^3, 3^2)$

$\text{rad}(1 \cdot 8 \cdot 9) = \text{rad}(2^3 \cdot 3^2) = 6 < 9$

Example

$(3, 125, 128) = (3, 5^3, 2^7)$

$\text{rad}(3 \cdot 125 \cdot 128)$

Examples

Example

$(1, 8, 9) = (1, 2^3, 3^2)$

$\text{rad}(1 \cdot 8 \cdot 9) = \text{rad}(2^3 \cdot 3^2) = 6 < 9$

Example

$(3, 125, 128) = (3, 5^3, 2^7)$

$\text{rad}(3 \cdot 125 \cdot 128) = \text{rad}(3 \cdot 5^3 \cdot 2^7)$

Examples

Example

$(1, 8, 9) = (1, 2^3, 3^2)$

$\mathrm{rad}(1 \cdot 8 \cdot 9) = \mathrm{rad}(2^3 \cdot 3^2) = 6 < 9$

Example

$(3, 125, 128) = (3, 5^3, 2^7)$

$\mathrm{rad}(3 \cdot 125 \cdot 128) = \mathrm{rad}(3 \cdot 5^3 \cdot 2^7) = 30 < 128$

The table below lists all good ABC triples $P = (a, b, c)$ with $a < b < c < 200$.

The table below lists all good ABC triples $P = (a, b, c)$ with $a < b < c < 200$.

a	b	c	rad(abc)
1	8	9	6
5	27	32	30
1	48	49	42
1	63	64	30
1	80	81	30
32	49	81	42
4	121	125	110
3	125	128	30

The table below lists all good *ABC* triples $P = (a, b, c)$ with $a < b < c < 200$.

a	b	c	rad(abc)
1	8	9	6
5	27	32	30
1	48	49	42
1	63	64	30
1	80	81	30
32	49	81	42
4	121	125	110
3	125	128	30

Remark

Intuitively for $c < 200$, there should be a larger number of good ABC triples,

The table below lists all good ABC triples $P = (a, b, c)$ with $a < b < c < 200$.

a	b	c	$\text{rad}(abc)$
1	8	9	6
5	27	32	30
1	48	49	42
1	63	64	30
1	80	81	30
32	49	81	42
4	121	125	110
3	125	128	30

Remark

Intuitively for $c < 200$, there should be a larger number of good ABC triples, yet only 8 appear!

ABC Conjecture

Example

Are there finitely many good ABC Triples?

ABC Conjecture

Example

Are there finitely many good ABC Triples?

ABC Conjecture

For $\epsilon > 0$, there exist only finitely many triples (a, b, c) of coprime positive integers, with $a + b = c$ such that

$$c > \text{rad}(abc)^{1+\epsilon}$$

Question

What does computational evidence suggest about the ABC conjecture?

ABC@Home Project: An Overview

- The **ABC@Home Project** was a computerized effort to classify all good ABC triples under $c < 10^{18}$.

ABC@Home Project: An Overview

- The **ABC@Home Project** was a computerized effort to classify all good ABC triples under $c < 10^{18}$.
- Created to assist in collecting computational evidence towards the ABC Conjecture.

ABC@Home Project: An Overview

- The **ABC@Home Project** was a computerized effort to classify all good ABC triples under $c < 10^{18}$.
- Created to assist in collecting computational evidence towards the ABC Conjecture.
- It ran until 2015 and collected around 14.5 million ABC triples.

ABC@Home Project: An Overview

- The **ABC@Home Project** was a computerized effort to classify all good ABC triples under $c < 10^{18}$.
- Created to assist in collecting computational evidence towards the ABC Conjecture.
- It ran until 2015 and collected around 14.5 million ABC triples.

Remark

From the ABC@Home Project, approximately 45,000 good ABC triples were of the form $(a, b, c) = (1, b, c)$

ABC@Home Project: An Overview

- The **ABC@Home Project** was a computerized effort to classify all good ABC triples under $c < 10^{18}$.
- Created to assist in collecting computational evidence towards the ABC Conjecture.
- It ran until 2015 and collected around 14.5 million ABC triples.

Remark

From the ABC@Home Project, approximately 45,000 good ABC triples were of the form $(a, b, c) = (1, b, c)$

Question

Can we find general forms, (a, b, c), that create infinite sequences of good ABC triples?

Current Results

Proposition (1985)

An ABC triple of the form $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$ is good.

Current Results

Proposition (1985)

An ABC triple of the form $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$ is good.

Example

$(1, 9^2 - 1, 9^2)$

Current Results

Proposition (1985)

An ABC triple of the form $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$ is good.

Example

$(1, 9^2 - 1, 9^2) = (1, 80, 81)$

Current Results

Proposition (1985)

An ABC triple of the form $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$ is good.

Example

$(1, 9^2 - 1, 9^2) = (1, 80, 81)$

$\text{rad}(80 \cdot 81)$

Current Results

Proposition (1985)

An ABC triple of the form $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$ is good.

Example

$(1, 9^2 - 1, 9^2) = (1, 80, 81)$

$\mathrm{rad}(80 \cdot 81) = \mathrm{rad}(2^4 \cdot 5 \cdot 3^4)$

Current Results

Proposition (1985)

An ABC triple of the form $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$ is good.

Example

$(1, 9^2 - 1, 9^2) = (1, 80, 81)$

$\text{rad}(80 \cdot 81) = \text{rad}(2^4 \cdot 5 \cdot 3^4) = 30$

Proof

Proof

Consider the ABC triple $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$.

Proof

Proof

Consider the ABC triple $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$. To prove this triple is good requires proof that $\text{rad}(abc) < c$.

Proof

Proof

Consider the ABC triple $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$. To prove this triple is good requires proof that $\text{rad}(abc) < c$.
Consider the expression:

$$\text{rad}(9^k(9^k - 1))$$

Proof

Proof

Consider the ABC triple $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$. To prove this triple is good requires proof that $\text{rad}(abc) < c$.
Consider the expression:

$$\text{rad}(9^k(9^k - 1)) = 3 \cdot \text{rad}(9^k - 1)$$

Proof

Proof

Consider the ABC triple $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$. To prove this triple is good requires proof that $\text{rad}(abc) < c$.
Consider the expression:

$$\text{rad}(9^k(9^k - 1)) = 3 \cdot \text{rad}(9^k - 1)$$

We see that $9^k - 1 \equiv 0 \mod 8$,

Proof

Proof

Consider the ABC triple $(1, 9^k - 1, 9^k)$ where $k \in \mathbb{N}$. To prove this triple is good requires proof that $\text{rad}(abc) < c$.
Consider the expression:

$$\text{rad}(9^k(9^k - 1)) = 3 \cdot \text{rad}(9^k - 1)$$

We see that $9^k - 1 \equiv 0 \mod 8$, then $9^k - 1 = 2^3 s$ where $s \in \mathbb{N}$.

Proof (continued)

Substituting $2^3 s$:

Proof (continued)

Substituting $2^3 s$:

$$3 \cdot \mathrm{rad}(2^3 s)$$

Proof (continued)

Substituting $2^3 s$:

$$3 \cdot \mathrm{rad}(2^3 s) \leq 6s$$

Proof (continued)

Substituting $2^3 s$:

$$3 \cdot \text{rad}(2^3 s) \leq 6s$$

Since $b = 2^3 s$, then $c = 2^3 s + 1$.

Proof (continued)

Substituting $2^3 s$:

$$3 \cdot \text{rad}(2^3 s) \leq 6s$$

Since $b = 2^3 s$, then $c = 2^3 s + 1$. Thus,

$$\text{rad}(9^k(9^k - 1)) = 3 \cdot \text{rad}(2^3 s) < 6s < 2^3 s + 1$$

□

Proposition (Granville, Tucker, 2002)

An ABC triple of the following form: $(1, 2^{p(p-1)} - 1, 2^{p(p-1)})$ is good where p is an odd prime and $k \in \mathbb{N}$.

Proposition (Granville, Tucker, 2002)

An ABC triple of the following form: $(1, 2^{p(p-1)} - 1, 2^{p(p-1)})$ is good where p is an odd prime and $k \in \mathbb{N}$.

Example

$(1, 2^{7\cdot 6} - 1, 2^{7\cdot 6})$

Proposition (Granville, Tucker, 2002)

An ABC triple of the following form: $(1, 2^{p(p-1)} - 1, 2^{p(p-1)})$ is good where p is an odd prime and $k \in \mathbb{N}$.

Example

$(1, 2^{7\cdot 6} - 1, 2^{7\cdot 6}) = (1,\ 3^2 \cdot 7^2 \cdot 43 \cdot 127 \cdot 337 \cdot 5419,\ 2^{7\cdot 6})$

Proposition (Granville, Tucker, 2002)

An ABC triple of the following form: $(1, 2^{p(p-1)} - 1, 2^{p(p-1)})$ is good where p is an odd prime and $k \in \mathbb{N}$.

Example

$(1, 2^{7\cdot 6} - 1, 2^{7\cdot 6}) = (1,\ 3^2 \cdot 7^2 \cdot 43 \cdot 127 \cdot 337 \cdot 5419,\ 2^{7\cdot 6})$

$\text{rad}(3^2 \cdot 7^2 \cdot 43 \cdot 127 \cdot 337 \cdot 5419 \cdot 2^{7\cdot 6})$

Proposition (Granville, Tucker, 2002)

An ABC triple of the following form: $(1, 2^{p(p-1)} - 1, 2^{p(p-1)})$ is good where p is an odd prime and $k \in \mathbb{N}$.

Example

$(1, 2^{7 \cdot 6} - 1, 2^{7 \cdot 6}) = (1,\ 3^2 \cdot 7^2 \cdot 43 \cdot 127 \cdot 337 \cdot 5419,\ 2^{7 \cdot 6})$

$\text{rad}(3^2 \cdot 7^2 \cdot 43 \cdot 127 \cdot 337 \cdot 5419 \cdot 2^{7 \cdot 6}) = 418861572486$

Proposition (Barrios, 2020)

An ABC triple of the following form: $(1, p^{(p-1)k} - 1, p^{(p-1)k})$ is good where p is an odd prime and $k \in \mathbb{N}$.

Proposition (Barrios, 2020)

An ABC triple of the following form: $(1, p^{(p-1)k} - 1, p^{(p-1)k})$ is good where p is an odd prime and $k \in \mathbb{N}$.

Example

$(1, 7^6 - 1, 7^6)$

Proposition (Barrios, 2020)

An ABC triple of the following form: $(1, p^{(p-1)k} - 1, p^{(p-1)k})$ is good where p is an odd prime and $k \in \mathbb{N}$.

Example

$(1, 7^6 - 1, 7^6) = (1,\ \ 2^4 \cdot 3^2 \cdot 19 \cdot 43,\ \ 7^6)$

Proposition (Barrios, 2020)

An ABC triple of the following form: $(1, p^{(p-1)k} - 1, p^{(p-1)k})$ is good where p is an odd prime and $k \in \mathbb{N}$.

Example

$(1, 7^6 - 1, 7^6) = (1,\ 2^4 \cdot 3^2 \cdot 19 \cdot 43,\ 7^6)$

$\text{rad}(2^4 \cdot 3^2 \cdot 19 \cdot 43 \cdot 7^6)$

Proposition (Barrios, 2020)

An ABC triple of the following form: $(1, p^{(p-1)k} - 1, p^{(p-1)k})$ is good where p is an odd prime and $k \in \mathbb{N}$.

Example

$$(1, 7^6 - 1, 7^6) = (1,\ 2^4 \cdot 3^2 \cdot 19 \cdot 43,\ 7^6)$$

$$\text{rad}(2^4 \cdot 3^2 \cdot 19 \cdot 43 \cdot 7^6) = 34314$$

Current Work During PRiME

Theorem (A-S, H)

Let n be an odd integer and $k \in \mathbb{N}$, then

$$\left(1, n^{(n-1)k} - 1, n^{(n-1)k}\right)$$

is a good ABC triple.

Current Work During PRiME

Theorem (A-S, H)

Let n be an odd integer and $k \in \mathbb{N}$, then

$$\left(1, n^{(n-1)k} - 1, n^{(n-1)k}\right)$$

is a good ABC triple.

- This result extends from Barrios

Current Work During PRiME

Theorem (A-S, H)

Let n be an odd integer and $k \in \mathbb{N}$, then

$$\left(1, n^{(n-1)k} - 1, n^{(n-1)k}\right)$$

is a good ABC triple.

- This result extends from Barrios
- The fact that ABC triples of this form can be good is not a special attribute of primes but of odd integers

Current Work During Prime

Theorem (A-S,H)

Let n be an even integer and k an odd integer, then

$$(1, n^{(n+1)k}, n^{(n+1)k} + 1)$$

is an ABC triple.

- This result is completely new and is distinct from the other ones since n is even and this case
- In addition, it is not of the form $(1, n^m - 1, n^m)$

Theorem (A-S, H)

Let n, m be relatively prime positive integers and $k \in \mathbb{N}$. Let ϕ denote Euler's totient function, then the triple

$$\left(1, n^{\phi(m)k} - 1, n^{\phi(m)k}\right)$$

is an ABC triple whenever $\frac{m}{\text{rad}(m)} > n$.

Theorem (A-S, H)

Let n, m be relatively prime positive integers and $k \in \mathbb{N}$. Let ϕ denote Euler's totient function, then the triple

$$\left(1, n^{\phi(m)k} - 1, n^{\phi(m)k}\right)$$

is an ABC triple whenever $\frac{m}{\mathrm{rad}(m)} > n$.

- This result extends from Granville and Tucker

Theorem (A-S, H)

Let n, m be relatively prime positive integers and $k \in \mathbb{N}$. Let ϕ denote Euler's totient function, then the triple

$$\left(1, n^{\phi(m)k} - 1, n^{\phi(m)k}\right)$$

is an ABC triple whenever $\frac{m}{\mathrm{rad}(m)} > n$.

- This result extends from Granville and Tucker

Example

When $n = 2$, take $m = k = p$ where p is an odd prime.

Theorem (A-S, H)

Let n, m be relatively prime positive integers and $k \in \mathbb{N}$. Let ϕ denote Euler's totient function, then the triple

$$\left(1, n^{\phi(m)k} - 1, n^{\phi(m)k}\right)$$

is an ABC triple whenever $\frac{m}{\mathrm{rad}(m)} > n$.

- This result extends from Granville and Tucker

Example

When $n = 2$, take $m = k = p$ where p is an odd prime. The $\gcd(n, m) = 1$.

Theorem (A-S, H)

Let n, m be relatively prime positive integers and $k \in \mathbb{N}$. Let ϕ denote Euler's totient function, then the triple

$$\left(1, n^{\phi(m)k} - 1, n^{\phi(m)k}\right)$$

is an ABC triple whenever $\frac{m}{\text{rad}(m)} > n$.

- This result extends from Granville and Tucker

Example

When $n = 2$, take $m = k = p$ where p is an odd prime. The $\gcd(n, m) = 1$. Evaluating $\phi(p) = p - 1$.

Theorem (A-S, H)

Let n, m be relatively prime positive integers and $k \in \mathbb{N}$. Let ϕ denote Euler's totient function, then the triple

$$\left(1, n^{\phi(m)k} - 1, n^{\phi(m)k}\right)$$

is an ABC triple whenever $\frac{m}{\text{rad}(m)} > n$.

- This result extends from Granville and Tucker

Example

When $n = 2$, take $m = k = p$ where p is an odd prime. The $\gcd(n, m) = 1$. Evaluating $\phi(p) = p - 1$. Thus, we get $(1, 2^{(p-1)p} - 1, 2^{(p-1)p})$.

Euler's Theorem and Preliminaries

Theorem

If n and a are coprime positive integers, and $\phi(n)$ is Euler's totient function, then a raised to the power $\phi(n)$ is congruent to 1 modulo n, that is

$$a^{\phi(n)} \equiv 1 \mod n$$

Example

Since $\gcd(2,3) = 1$ and $\phi(3) = 2$, then by Euler's Theorem

$$2^{\phi(3)} = 2^2 \equiv 1 \mod 3$$

Proof

Granville-Tucker Generalization

Let the $\gcd(n, m) = 1$,

Proof

Granville-Tucker Generalization

Let the $\gcd(n, m) = 1$, then by Euler's Theorem

$$n^{\phi(m)} \equiv 1 \mod m$$

Therefore

Proof

Granville-Tucker Generalization

Let the $\gcd(n, m) = 1$, then by Euler's Theorem

$$n^{\phi(m)} \equiv 1 \mod m$$

Therefore

$$n^{\phi(m)k} \equiv 1 \mod m$$

Proof

Granville-Tucker Generalization

Let the $\gcd(n, m) = 1$, then by Euler's Theorem

$$n^{\phi(m)} \equiv 1 \mod m$$

Therefore

$$n^{\phi(m)k} \equiv 1 \mod m$$

If

$$n^{\phi(m)k} - \text{rad}\left(n^{\phi(m)k}\left(n^{\phi(m)k} - 1\right)\right) > 0$$

our triple is good.

Example

An Important Property of the Radical

$$\mathrm{rad}(2^3) = \mathrm{rad}(2^2) = \mathrm{rad}(2)$$

Proof II

Proof

$$n^{\phi(m)k} - \text{rad}\left(n^{\phi(m)k}\left(n^{\phi(m)k} - 1\right)\right)$$

Proof II

Proof

$$n^{\phi(m)k} - \text{rad}\left(n^{\phi(m)k}\left(n^{\phi(m)k} - 1\right)\right)$$

$$= n^{\phi(m)k} - \text{rad}\left(n\left(n^{\phi(m)k} - 1\right)\right)$$

Proof II

Proof

$$n^{\phi(m)k} - \operatorname{rad}\left(n^{\phi(m)k}\left(n^{\phi(m)k} - 1\right)\right)$$

$$= n^{\phi(m)k} - \operatorname{rad}\left(n\left(n^{\phi(m)k} - 1\right)\right)$$

$$\geq n^{\phi(m)k} - n\operatorname{rad}\left(\left(n^{\phi(m)k} - 1\right)\right)$$

Proof II

Proof

$$n^{\phi(m)k} - \operatorname{rad}\left(n^{\phi(m)k}\left(n^{\phi(m)k} - 1\right)\right)$$

$$= n^{\phi(m)k} - \operatorname{rad}\left(n\left(n^{\phi(m)k} - 1\right)\right)$$

$$\geq n^{\phi(m)k} - n\operatorname{rad}\left(\left(n^{\phi(m)k} - 1\right)\right)$$

$$= n^{\phi(m)k} - n\operatorname{rad}\left(\frac{n^{\phi(m)k} - 1}{\frac{m}{\operatorname{rad}(m)}}\right)$$

Proof II

Proof

$$n^{\phi(m)k} - \operatorname{rad}\left(n^{\phi(m)k}\left(n^{\phi(m)k} - 1\right)\right)$$

$$= n^{\phi(m)k} - \operatorname{rad}\left(n\left(n^{\phi(m)k} - 1\right)\right)$$

$$\geq n^{\phi(m)k} - n\operatorname{rad}\left(\left(n^{\phi(m)k} - 1\right)\right)$$

$$= n^{\phi(m)k} - n\operatorname{rad}\left(\frac{n^{\phi(m)k} - 1}{\frac{m}{\operatorname{rad}(m)}}\right)$$

$$\geq n^{\phi(m)k} - n\left(\frac{n^{\phi(m)k} - 1}{\frac{m}{\operatorname{rad}(m)}}\right)$$

Proof III

Proof

$$n^{\phi(m)k} - n\left(\frac{n^{\phi(m)k} - 1}{\frac{m}{\text{rad}(m)}}\right)$$

Proof III

Proof

$$n^{\phi(m)k} - n\left(\frac{n^{\phi(m)k}-1}{\frac{m}{\mathrm{rad}(m)}}\right)$$

$$= n^{\phi(m)k}\left(1-\frac{n}{\frac{m}{\mathrm{rad}(m)}}\right)+\frac{n}{\frac{m}{\mathrm{rad}(m)}} > 0$$

whenever $\frac{m}{\mathrm{rad}(m)} > n$. Therefore the triple $(1, n^{\phi(m)k}-1, n^{\phi(m)k})$ is good.

Table of Contents

Definitions

Definition

A **cubic curve** is an implicit function of the form:

$$E : y^2 + a_1xy + a_3y = x_3 + a_2x^2 + a_4x + a_6$$

where all the $a_i \in \mathbb{K}$.

Definition

The following are quantities of the cubic curve:

$$b_2 = a_1^2 + 4a_2 \text{ and } b_4 = 2a_4 + a_1 a_3$$

Definition

The following are quantities of the cubic curve:

$$b_2 = a_1^2 + 4a_2 \text{ and } b_4 = 2a_4 + a_1 a_3$$

$$b_6 = a_3^2 + 4a_6 \text{ and } c_4 = b_2^2 - 24b_4$$

Definition

The following are quantities of the cubic curve:

$$b_2 = a_1^2 + 4a_2 \text{ and } b_4 = 2a_4 + a_1 a_3$$

$$b_6 = a_3^2 + 4a_6 \text{ and } c_4 = b_2^2 - 24 b_4$$

$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6$$

Definition

The following are quantities of the cubic curve:

$$b_2 = a_1^2 + 4a_2 \text{ and } b_4 = 2a_4 + a_1 a_3$$
$$b_6 = a_3^2 + 4a_6 \text{ and } c_4 = b_2^2 - 24 b_4$$
$$c_6 = -b_2^3 + 36 b_2 b_4 - 216 b_6$$

Definition

The discriminant of a cubic curve is $\Delta = \frac{c_4^3 - c_6^2}{1728}$

Singular Cubic Curves

Definition

A function is **smooth** if it is infinitely differentiable.

Singular Cubic Curves

Definition

A function is **smooth** if it is infinitely differentiable.

Definition

Cubic curves are **singular** if the curve has self intersections or is not smooth.

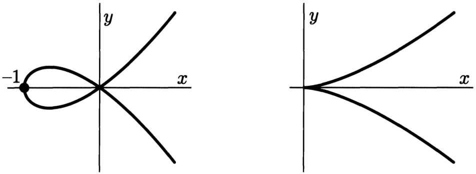
Singular Cubic Curves

Definition

A function is **smooth** if it is infinitely differentiable.

Definition

Cubic curves are **singular** if the curve has self intersections or is not smooth.



A Singular Cubic with Distinct Tangent Directions

A Singular Cubic with A Cusp

Elliptic Curves

Definition

An **elliptic curve**, E, is an implicit cubic function where solutions to E live in the set $E(\mathbb{K})$ where $\mathbb{K}$ is a field.

Elliptic Curves

Definition

An **elliptic curve**, E, is an implicit cubic function where solutions to E live in the set $E(\mathbb{K})$ where $\mathbb{K}$ is a field.

Example

$$y^2 = x^3 - \frac{5999296622651011281514842057388032}{11044276742439206463052992 01}x + \frac{1788539687547948386432785170466755056049496853053 44}{3670336821729412544123021103203366018880 1}$$

Elliptic Curves

Definition

An **elliptic curve**, E, is an implicit cubic function where solutions to E live in the set $E(\mathbb{K})$ where $\mathbb{K}$ is a field.

Example

$$y^2 = x^3 - \frac{5999296622651011281514842057388032}{110442767424392064630529920 1}x + \frac{1788539687547948386432785170466755056049496853053 44}{367033682172941254412302110320336601888 01}$$

Remark

We write this specific elliptic curve as $y^2 = x^3 - Ax + B$ where A and B are equal to the coefficients above.

Example Continued- Invariants

Example

The invariants of the previous example $y^2 = x^3 - Ax + B$ are given below:

$c_4 = 2^{16} \cdot 3^8 \cdot 7^{-32} \cdot 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787$

Example Continued- Invariants

Example

The invariants of the previous example $y^2 = x^3 - Ax + B$ are given below:

$$c_4 = 2^{16} \cdot 3^8 \cdot 7^{-32} \cdot 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787$$

$$c_6 = -1 \cdot 2^{24} \cdot 3^{12} \cdot 7^{-48} \cdot 11 \cdot 23 \cdot 613 \cdot 92831 \cdot 12117817 \cdot$$

$$3838779431 \cdot 25878899155777$$

Example Continued- Invariants

Example

The invariants of the previous example $y^2 = x^3 - Ax + B$ are given below:

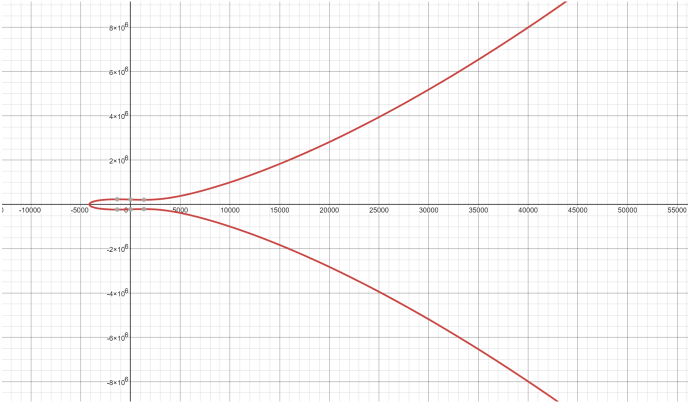
$$c_4 = 2^{16} \cdot 3^8 \cdot 7^{-32} \cdot 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787$$

$$c_6 = -1 \cdot 2^{24} \cdot 3^{12} \cdot 7^{-48} \cdot 11 \cdot 23 \cdot 613 \cdot 92831 \cdot 12117817 \cdot$$

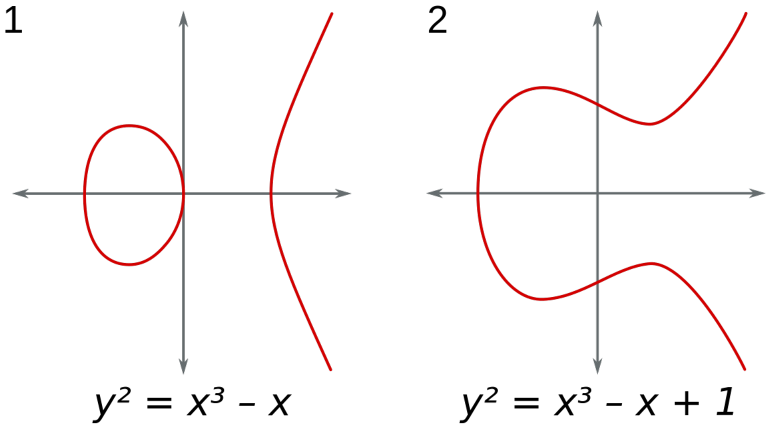
$$3838779431 \cdot 25878899155777$$

$$\Delta = 2^{72} \cdot 3^{30} \cdot 5^6 \cdot 7^{-88} \cdot 37^2 \cdot 47^{12} \cdot 61^2 \cdot 461^6 \cdot 2113^2$$

Picture of the Example



Examples of Nicer Elliptic Curves

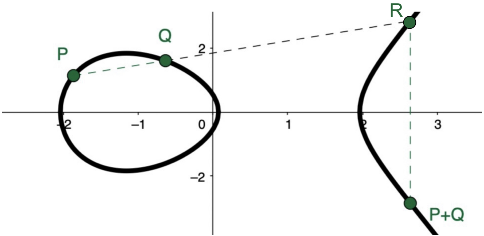


Group Structure on $E(\mathbb{Q})$

The group structure over $E(\mathbb{Q})$ is defined using the following operation:

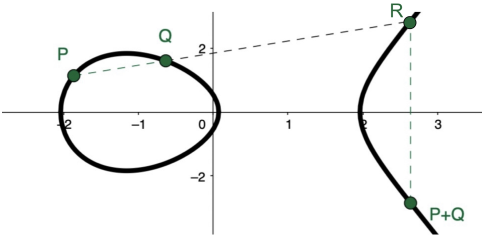
Group Structure on $E(\mathbb{Q})$

The group structure over $E(\mathbb{Q})$ is defined using the following operation:



Group Structure on $E(\mathbb{Q})$

The group structure over $E(\mathbb{Q})$ is defined using the following operation:



Where the point at infinity, $\mathcal{O}$, is the identity of the group.

Isomorphisms Between Elliptic Curves

Definition

We say that E_1 is $\mathbb{Q}$-isomorphic to E_2 if there exists $\phi : E_1 \to E_2$ with the property that $\phi(\mathcal{O}_{E_1}) = \mathcal{O}_{E_2}$ and ϕ is defined as

$$\phi(x, y) = (u^2 x + r, u^3 y + u^2 sx + w)$$

where $u, r, s, w \in \mathbb{Q}$ and $u \neq 0$.

Minimal Models

Definition

Let E be a rational elliptic curve. A **global minimal model** for E is a Weierstrass model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

such that each $a_j \in \mathbb{Z}$ and the discriminant Δ of the equation is minimal over all $\mathbb{Q}$-isomorphic elliptic curves to E.

Minimal Models

Definition

Let E be a rational elliptic curve. A **global minimal model** for E is a Weierstrass model

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$$

such that each $a_j \in \mathbb{Z}$ and the discriminant Δ of the equation is minimal over all $\mathbb{Q}$-isomorphic elliptic curves to E.

Definition

We call the discriminant of a global minimal model the **minimal discriminant of** E, denoted Δ_E^{min}.

Remark

The invariants c_4 and c_6 will now refer to the **invariants associated to a minimal model** of E. In particular,

$$1728\Delta_E^{\min} = c_4^3 - c_6^2.$$

Remark

The invariants c_4 and c_6 will now refer to the **invariants associated to a minimal model** of E. In particular,

$$1728\Delta_E^{\min} = c_4^3 - c_6^2.$$

Definition

If the $\gcd(c_4, \Delta) = 1$, then we say that E is a **semistable** elliptic curve.

Example of Minimal Model

Example

A minimal model of the Elliptic Curve

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

is given by

Example of Minimal Model

Example

A minimal model of the Elliptic Curve

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

is given by

$$y^2 + xy = x^3 - 1395244653077281522587148 0x + 20059662830488694621546896044577294400$$

Example of Minimal Model

Example

A minimal model of the Elliptic Curve

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

is given by

$$y^2 + xy = x^3 - 1395244653077281522587148 0x + \\ 2005966283048869462154689604457729440 0$$

The invariants of both are given by:

Example of Minimal Model

Example

A minimal model of the Elliptic Curve

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

is given by

$$y^2 + xy = x^3 - 139522446530772815225871480x + 20059662830488694621546896044577294400$$

The invariants of both are given by:

$$c_4 = 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787$$

Example of Minimal Model

Example

A minimal model of the Elliptic Curve

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

is given by

$$y^2 + xy = x^3 - 13952446530772815225871480x + 20059662830488694621546896044577294400$$

The invariants of both are given by:

$$c_4 = 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787 \quad c_6 = -11 \cdot 23 \cdot 613 \cdot 92831 \cdot 12117817 \cdot 3838779431 \cdot 25878899155777$$

Example of Minimal Model

Example

A minimal model of the Elliptic Curve

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

is given by

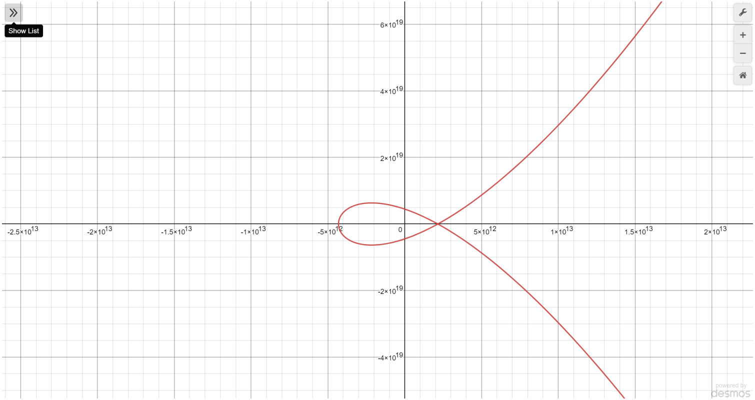
$$y^2 + xy = x^3 - 13952446530772815225871480x + 200596628304886946215468960445772944\,00$$

The invariants of both are given by:

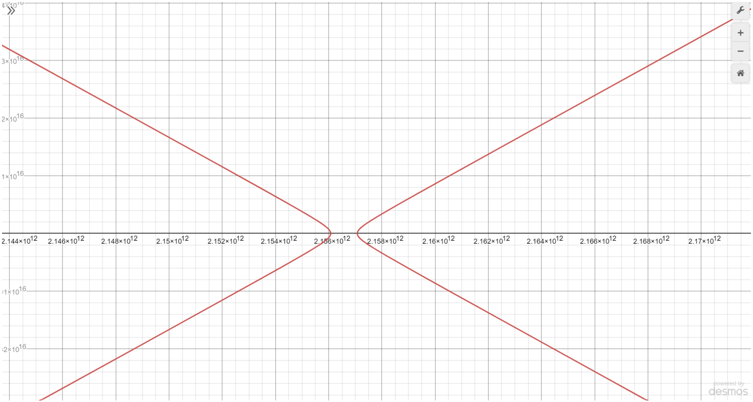
$$c_4 = 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787 \quad c_6 = -11 \cdot 23 \cdot 613 \cdot 92831 \cdot 12117817 \cdot 3838779431 \cdot 25878899155777$$

$$\Delta_E = 2^{24} \cdot 3^6 \cdot 5^6 \cdot 7^8 \cdot 37^2 \cdot 47^{12} \cdot 61^2 \cdot 461^6 \cdot 2113^2$$

Minimal Model Picture



Minimal Model Picture II



Comparison Between Invariants

Example

Invariants of $y^2 = x^3 - Ax + B$:

$$c_4 = 2^{16} \cdot 3^8 \cdot 7^{-32} \cdot 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787$$

$$c_6 = -1 \cdot 2^{24} \cdot 3^{12} \cdot 7^{-48} \cdot 11 \cdot 23 \cdot 613 \cdot 92831 \cdot 12117817 \cdot 3838779431 \cdot 25878899155777$$

$$\Delta = 2^{72} \cdot 3^{30} \cdot 5^6 \cdot 7^{-88} \cdot 37^2 \cdot 47^{12} \cdot 61^2 \cdot 461^6 \cdot 2113^2$$

Comparison Between Invariants

Example

Invariants of $y^2 = x^3 - Ax + B$:

$$c_4 = 2^{16} \cdot 3^8 \cdot 7^{-32} \cdot 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787$$

$$c_6 = -1 \cdot 2^{24} \cdot 3^{12} \cdot 7^{-48} \cdot 11 \cdot 23 \cdot 613 \cdot 92831 \cdot 12117817 \cdot 3838779431 \cdot 25878899155777$$

$$\Delta = 2^{72} \cdot 3^{30} \cdot 5^6 \cdot 7^{-88} \cdot 37^2 \cdot 47^{12} \cdot 61^2 \cdot 461^6 \cdot 2113^2$$

Invariants of Minimal Model

$$c_4 = 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787$$

Comparison Between Invariants

Example

Invariants of $y^2 = x^3 - Ax + B$:

$$c_4 = 2^{16} \cdot 3^8 \cdot 7^{-32} \cdot 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787$$

$$c_6 = -1 \cdot 2^{24} \cdot 3^{12} \cdot 7^{-48} \cdot 11 \cdot 23 \cdot 613 \cdot 92831 \cdot 12117817 \cdot 3838779431 \cdot 25878899155777$$

$$\Delta = 2^{72} \cdot 3^{30} \cdot 5^6 \cdot 7^{-88} \cdot 37^2 \cdot 47^{12} \cdot 61^2 \cdot 461^6 \cdot 2113^2$$

Invariants of Minimal Model

$$c_4 = 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787 \quad c_6 = -1 \cdot 11 \cdot 23 \cdot 613 \cdot 92831 \cdot 12117817 \cdot 3838779431 \cdot 25878899155777$$

Comparison Between Invariants

Example

Invariants of $y^2 = x^3 - Ax + B$:

$$c_4 = 2^{16} \cdot 3^8 \cdot 7^{-32} \cdot 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787$$

$$c_6 = -1 \cdot 2^{24} \cdot 3^{12} \cdot 7^{-48} \cdot 11 \cdot 23 \cdot 613 \cdot 92831 \cdot 12117817 \cdot 3838779431 \cdot 25878899155777$$

$$\Delta = 2^{72} \cdot 3^{30} \cdot 5^6 \cdot 7^{-88} \cdot 37^2 \cdot 47^{12} \cdot 61^2 \cdot 461^6 \cdot 2113^2$$

Invariants of Minimal Model

$$c_4 = 43 \cdot 313 \cdot 379 \cdot 33558163 \cdot 3912383529787 \quad c_6 = -1 \cdot 11 \cdot 23 \cdot 613 \cdot 92831 \cdot 12117817 \cdot 3838779431 \cdot 25878899155777$$

$$\Delta_E = 2^{24} \cdot 3^6 \cdot 5^6 \cdot 7^8 \cdot 37^2 \cdot 47^{12} \cdot 61^2 \cdot 461^6 \cdot 2113^2$$

Definition

For a rational elliptic curve E, the **conductor** N_E of E is denoted as the integer

$$N_E = \prod_{p \mid \Delta_E^{\min}} p^{f_p}$$

where $f_p \geq 1$

Definition

For a rational elliptic curve E, the **conductor** N_E of E is denoted as the integer

$$N_E = \prod_{p|\Delta_E^{\min}} p^{f_p}$$

where $f_p \geq 1$

Remark

If E is a **semistable** elliptic curve, then $N_E = \mathrm{rad}(\Delta_E^{\min})$

Conductor Example

Example

$$\Delta_E = 2^{24} \cdot 3^6 \cdot 5^6 \cdot 7^8 \cdot 37^2 \cdot 47^{12} \cdot 61^2 \cdot 461^6 \cdot 2113^2$$

$$N_E = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 37 \cdot 47 \cdot 61 \cdot 461 \cdot 2113$$

Modified Szpiro Conjecture

Modified Szpiro Conjecture (1988)

For any given $\epsilon > 0$, there are finitely many elliptic curves E over $\mathbb{Q}$ (up to isomorphism) such that

$$N_E^{6+\epsilon} < \max\{|c_4|^3, c_6^2\}$$

where c_4,c_6, and N_E are associated to a minimal model of E.

Modified Szpiro Conjecture

Modified Szpiro Conjecture (1988)

For any given $\epsilon > 0$, there are finitely many elliptic curves E over $\mathbb{Q}$ (up to isomorphism) such that

$$N_E^{6+\epsilon} < \max\{|c_4|^3, c_6^2\}$$

where c_4, c_6, and N_E are associated to a minimal model of E.

Remark

The Modified Szpiro conjecture has been shown to be equivalent to the abc conjecture.

Table of Contents

Good Elliptic Curves

Definition

An elliptic curve is defined to be **good** if

$$N_E^6 < \max\{|c_4|^3, c_6^2\}$$

Good Elliptic Curve Example

Example

The conductor of

$$y^2 + xy = x^3 - 13952446530772815225871480x + 20059662830488694621546896044577294400$$

is given by

Good Elliptic Curve Example

Example

The conductor of

$$y^2 + xy = x^3 - 13952446530772815225871480x + 20059662830488694621546896044577294400$$

is given by

$$N_E = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 37 \cdot 47 \cdot 61 \cdot 461 \cdot 2113$$

Good Elliptic Curve Example

Example

The conductor of

$$y^2 + xy = x^3 - 1395244653077281522587148 0x + 2005966283048869462154689604457729440 0$$

is given by

$$N_E = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 37 \cdot 47 \cdot 61 \cdot 461 \cdot 2113$$

$$|c_4|^3 = 43^3 \cdot 313^3 \cdot 379^3 \cdot 33558163^3 \cdot 3912383529787^3$$

Good Elliptic Curve Example

Example

The conductor of

$$y^2 + xy = x^3 - 139524465307728152258 71480x + 20059662830488694621546896044577294400$$

is given by

$$N_E = 2 \cdot 3 \cdot 5 \cdot 7 \cdot 37 \cdot 47 \cdot 61 \cdot 461 \cdot 2113$$

$$|c_4|^3 = 43^3 \cdot 313^3 \cdot 379^3 \cdot 33558163^3 \cdot 3912383529787^3$$

$$c_4^3 > N_E^6$$

Therefore the elliptic curve above is good.

Current Literature

Question

Are there infinitely many good elliptic curves?

Current Literature

Question

Are there infinitely many good elliptic curves?

- 1990: Masser showed that there were infinitely many good elliptic curves

Current Literature

Question

Are there infinitely many good elliptic curves?

- 1990: Masser showed that there were infinitely many good elliptic curves
- Masser had a non-constructive proof, our project is focused on constructing these good elliptic curves

Current Literature

Question

Are there infinitely many good elliptic curves?

- 1990: Masser showed that there were infinitely many good elliptic curves
- Masser had a non-constructive proof, our project is focused on constructing these good elliptic curves
- Late 1990s: Nitaj used good ABC triples to find good elliptic curves.

Current Literature

Question

Are there infinitely many good elliptic curves?

- 1990: Masser showed that there were infinitely many good elliptic curves
- Masser had a non-constructive proof, our project is focused on constructing these good elliptic curves
- Late 1990s: Nitaj used good ABC triples to find good elliptic curves.
- 2020: Barrios showed constructively that there were infinitely many elliptic curves.

Definitions

Definition

An **isogeny** is a surjective group homomorphism, ϕ, between two elliptic curves E_1 and E_2 such that

$$\phi\left(\mathcal{O}_{E_1}\right) = \mathcal{O}_{E_2}$$

Definitions

Definition

An **isogeny** is a surjective group homomorphism, ϕ, between two elliptic curves E_1 and E_2 such that

$$\phi\left(\mathcal{O}_{E_1}\right) = \mathcal{O}_{E_2}$$

Definition

n-isogeny An **n-isogeny** is an isogeny such that

$$\ker(\phi) = \mathbb{Z}/n\mathbb{Z}$$

Definition

An **isogeny class** of an elliptic curve E defined over $\mathbb{Q}$ is the set of all $\mathbb{Q}$-isomorphism classes of elliptic curves that are isogenous to E.

Definition

An **isogeny class** of an elliptic curve E defined over $\mathbb{Q}$ is the set of all $\mathbb{Q}$-isomorphism classes of elliptic curves that are isogenous to E.

Research Goal

For a given *n*, we study parameterized families of elliptic curves that parameterize all n-isogenous elliptic curves. This is how we construct infinitely many elliptic curves.

Our Research

Question

Does there exist an isogeny class with the property that each elliptic curve in it is good? If they do exist, What conditions, if any, do we need to have to obtain an isogeny class that only contains good elliptic curves?

Our Research

Question

Does there exist an isogeny class with the property that each elliptic curve in it is good? If they do exist, What conditions, if any, do we need to have to obtain an isogeny class that only contains good elliptic curves?

Definition

An isogeny class of E is considered a **good isogeny class** if every elliptic curve isogenous to E is good.

Methods

Theorem (Barrios,2022)

Let $E/\mathbb{Q}$ be an elliptic curve that admits a non-trivial n-isogeny. Then there exists relatively prime integers a, b and a square-free integer d such that the isogeny class of E is given by

$$\{F_{n,i}(a, b, d)\}$$

Methods

Theorem (Barrios,2022)

Let $E/\mathbb{Q}$ be an elliptic curve that admits a non-trivial n-isogeny. Then there exists relatively prime integers a, b and a square-free integer d such that the isogeny class of E is given by

$$\{F_{n,i}(a, b, d)\}$$

- What is this saying? Given an elliptic curve in an isogeny class, we can parameterize its isomorphism class by variables a and b.

Methods

Theorem (Barrios,2022)

Let $E/\mathbb{Q}$ be an elliptic curve that admits a non-trivial n-isogeny. Then there exists relatively prime integers a, b and a square-free integer d such that the isogeny class of E is given by

$$\{F_{n,i}(a, b, d)\}$$

- What is this saying? Given an elliptic curve in an isogeny class, we can parameterize its isomorphism class by variables a and b.
- Our work focuses on finding infinitely many good isogeny classes where each of the curves admits a 12-isogeny

Results

In particular, we study the 8 parameterized elliptic curves

$$F_{12,i}(a, b, 1) \quad \text{with} \quad 1 \leq i \leq 8$$

Results

In particular, we study the 8 parameterized elliptic curves

$$F_{12,i}(a,b,1) \quad \text{with} \quad 1 \leq i \leq 8$$

Remark

Every elliptic curve that admits a 12-isogeny is isomorphic to one of the elliptic curves in our isogeny class, therefore by studying $F_{12,i}$, we are studying all curves with a 12-isogeny.

Results

In particular, we study the 8 parameterized elliptic curves

$$F_{12,i}(a,b,1) \quad \text{with} \quad 1 \leq i \leq 8$$

Remark

Every elliptic curve that admits a 12-isogeny is isomorphic to one of the elliptic curves in our isogeny class, therefore by studying $F_{12,i}$, we are studying all curves with a 12-isogeny.

Example

$F_{12,1}$ is of the form $y^2 = x^3 + A_1 x + B_1$ where $t = \frac{b}{a}$ and

$$A_1 = (-48)(t^2+3)(t^6+225t^4-405t^2+243)$$
$$B_1 = (-128)(t^4+18t^2-27)(t^4-24t^3+18t^2-27)(t^4+24t^3+18t^2-27)$$

Results

Theorem (A-S,H)

Let a, b, c be a good ABC triple such that $b \equiv 0 \mod 6$, then the isogeny class of

$$F_{12,i}(a, b)$$

is good whenever $\frac{b}{a} > 25.4928$.

Remark

By our earlier theorems constructing good ABC triples, we then get infinitely many good isogeny classes.

Results

$F_{12,i}$	Weierstrass Transformation	u	δ	$\max\{\lvert c_4\rvert^3, c_6^2\}$
1	$\frac{24}{(a+b)^4}$	6	3.73205	$\lvert c_4\rvert^3$
2	$\frac{24}{(a+b)^4}$	6	3.73205	$\lvert c_4\rvert^3$
3	$\frac{24}{(a+b)^4}$	6	4.36919	c_6^2
4	$\frac{24}{(a+b)^4}$	6	25.4928	c_6^2
5	$\frac{24}{(a+b)^4}$	6	3.73205	$\lvert c_4\rvert^3$
6	$\frac{24}{(a+b)^4}$	6	3.73205	$\lvert c_4\rvert^3$
7	$\frac{24}{(a+b)^4}$	6	3.73205	$\lvert c_4\rvert^3$
8	$\frac{24}{(a+b)^4}$	6	3.73205	$\lvert c_4\rvert^3$

Acknowledgements

We would like to thank Alex Barrios, Summer Soller, and everyone involved with PRiME for their guidance.

This material is based on work supported by the National Science Foundation under Grant No. DMS-2113782.

This work was supported in part by NSF awards CNS-1730158, ACI-1540112, ACI-1541349, OAC-1826967, OAC-2112167, CNS-2120019, the University of California Office of the President, and the University of California San Diego's California Institute for Telecommunications and Information Technology/Qualcomm Institute. Thanks to CENIC for the 100Gbps networks.