Elliptic Curves and Mordell's Theorem

Aurash Vatan, Andrew Yao

MIT PRIMES

December 16, 2017

Diophantine Equations

Definition (Diophantine Equations)

Diophantine Equations are polynomials of two or more variables with solutions restricted to $\mathbb{Z}$ or $\mathbb{Q}$.

- For two variables, D.E. define plane curves

Diophantine Equations

Definition (Diophantine Equations)

Diophantine Equations are polynomials of two or more variables with solutions restricted to $\mathbb{Z}$ or $\mathbb{Q}$.

- For two variables, D.E. define plane curves
- So rational solutions correspond to points with rational coordinates

Diophantine Equations

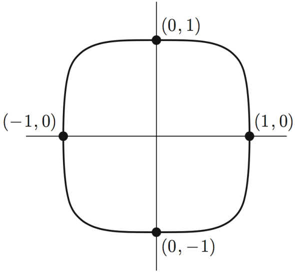
Definition (Diophantine Equations)

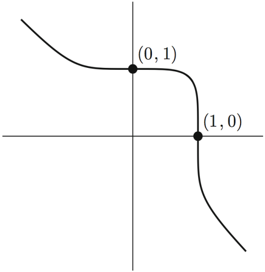
Diophantine Equations are polynomials of two or more variables with solutions restricted to $\mathbb{Z}$ or $\mathbb{Q}$.

- For two variables, D.E. define plane curves
- So rational solutions correspond to points with rational coordinates
- Ex. Fermat's theorem: $x^n + y^n = 1,\ n > 2,\ x, y \in \mathbb{Q}$ equivalent to $x^n + y^n = z^n,\ x, y, z, \in \mathbb{Z}$

The Rational Points on Fermat Curves

Two examples of Diophantine equations with rational solutions marked: $x^4 + y^4 = 1$ and $x^5 + y^5 = 1$.





Diophantine Equations

Definition (Diophantine Equations)

Diophantine Equations are polynomials of two or more variables with solutions restricted to $\mathbb{Z}$ or $\mathbb{Q}$.

- For two variables, D.E. define plane curves
- So rational solutions correspond to points with rational coordinates
- Ex. Fermat's theorem: $x^n + y^n = 1,\ n > 2,\ x, y \in \mathbb{Q}$ equivalent to $x^n + y^n = z^n,\ x, y, z, \in \mathbb{Z}$
- Question: finite or infinite number of rational points?

Diophantine Equations

Definition (Diophantine Equations)

Diophantine Equations are polynomials of two or more variables with solutions restricted to $\mathbb{Z}$ or $\mathbb{Q}$.

- For two variables, D.E. define plane curves
- So rational solutions correspond to points with rational coordinates
- Ex. Fermat's theorem: $x^n + y^n = 1,\ n > 2,\ x, y \in \mathbb{Q}$ equivalent to $x^n + y^n = z^n,\ x, y, z, \in \mathbb{Z}$
- Question: finite or infinite number of rational points?
- Question: given some known rational points on a curve, can we generate more?

Diophantine Equations

Definition (Diophantine Equations)

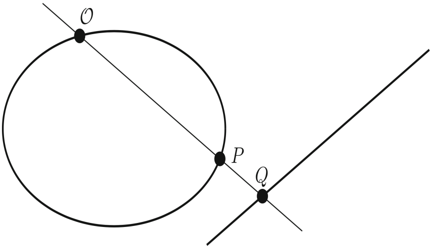
Diophantine Equations are polynomials of two or more variables with solutions restricted to $\mathbb{Z}$ or $\mathbb{Q}$.

- For two variables, D.E. define plane curves
- So rational solutions correspond to points with rational coordinates
- Ex. Fermat's theorem: $x^n + y^n = 1,\ n > 2,\ x, y \in \mathbb{Q}$ equivalent to $x^n + y^n = z^n,\ x, y, z, \in \mathbb{Z}$
- Question: finite or infinite number of rational points?
- Question: given some known rational points on a curve, can we generate more?
- Mordell's Theorem: finite number of rational points generate all rational points for a class of cubic curves (elliptic curves)

Rational Points on Conics

Definition

General Rational Conic: $Ax^2 + Bxy + Cy^2 + Dx + Ey + F = 0$, $A, B, C, D, E, F \in \mathbb{Q}$.



Theorem

Take a general conic with rational coefficients and a rational point $\mathcal{O}$. A point P on the conic is rational if and only if the line through P and $\mathcal{O}$ has rational slope.

- Theorem gives geometric method for generating rational points
- Method can be described algebraically

An Application: Generating Pythagorean Triples

Examples

Take the unit circle with $\mathbb{O} = (-1, 0)$. The line through $\mathbb{O}$ with rational slope t intersects the circle again at $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.

Theorem (Generation of Pythagorean Triples)

(a, b, c) is an in integer solution to $x^2 + y^2 = z^2$ if and only if $(a, b, c) = (n^2 - m^2, 2mn, n^2 + m^2)$ for $n, m \in \mathbb{Z}$.

- Pythagorean triples correspond to rational points on $x^2 + y^2 = 1$

An Application: Generating Pythagorean Triples

Examples

Take the unit circle with $\mathbb{O} = (-1, 0)$. The line through $\mathbb{O}$ with rational slope t intersects the circle again at $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.

Theorem (Generation of Pythagorean Triples)

(a, b, c) is an in integer solution to $x^2 + y^2 = z^2$ if and only if $(a, b, c) = (n^2 - m^2, 2mn, n^2 + m^2)$ for $n, m \in \mathbb{Z}$.

- Pythagorean triples correspond to rational points on $x^2 + y^2 = 1$
- We already have $\frac{a}{c} = \frac{1-t^2}{1+t^2}$ and $\frac{b}{c} = \frac{2t}{1+t^2}$

An Application: Generating Pythagorean Triples

Examples

Take the unit circle with $\mathbb{O} = (-1, 0)$. The line through $\mathbb{O}$ with rational slope t intersects the circle again at $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.

Theorem (Generation of Pythagorean Triples)

(a, b, c) is an in integer solution to $x^2 + y^2 = z^2$ if and only if $(a, b, c) = (n^2 - m^2, 2mn, n^2 + m^2)$ for $n, m \in \mathbb{Z}$.

- Pythagorean triples correspond to rational points on $x^2 + y^2 = 1$
- We already have $\frac{a}{c} = \frac{1-t^2}{1+t^2}$ and $\frac{b}{c} = \frac{2t}{1+t^2}$
- Plugging in $t = \frac{m}{n}$,

$$\frac{a}{c} = \frac{n^2 - m^2}{n^2 + m^2}, \qquad \frac{b}{c} = \frac{2mn}{n^2 + m^2}$$

An Application: Generating Pythagorean Triples

Examples

Take the unit circle with $\mathbb{O} = (-1, 0)$. The line through $\mathbb{O}$ with rational slope t intersects the circle again at $\left(\frac{1-t^2}{1+t^2}, \frac{2t}{1+t^2}\right)$.

Theorem (Generation of Pythagorean Triples)

(a, b, c) is an in integer solution to $x^2 + y^2 = z^2$ if and only if $(a, b, c) = (n^2 - m^2, 2mn, n^2 + m^2)$ for $n, m \in \mathbb{Z}$.

- Pythagorean triples correspond to rational points on $x^2 + y^2 = 1$
- We already have $\frac{a}{c} = \frac{1-t^2}{1+t^2}$ and $\frac{b}{c} = \frac{2t}{1+t^2}$
- Plugging in $t = \frac{m}{n}$,

$$\frac{a}{c} = \frac{n^2 - m^2}{n^2 + m^2}, \qquad \frac{b}{c} = \frac{2mn}{n^2 + m^2}$$

- We see that this implies $c = n^2 + m^2$ and the rest follows

Rational Points on $y^2 = x^3 + c$

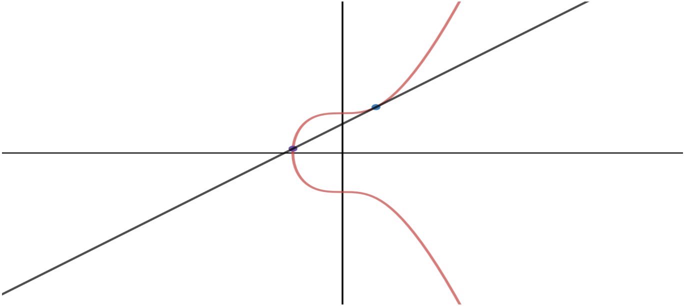
- Moving to cubics, our method for conics fails
- Given one rational point on a cubic curve, can we get more?
- Bachet studied rational solutions to $C : y^2 = x^3 + c$ for $c \in \mathbb{Z}$
- Discovered formula in (1621!) that takes one rational point on C and returns another

Bachet's Formula

Theorem (Bachet's Formula)

Bachet's formula says that for a cubic $C : y^2 = x^3 + c$ with $c \in \mathbb{Z}$, if (x_1, y_1) is a rational solution of C, then so is $\left(\frac{x^4-8cx}{4y^2}, \frac{-x^6-20cx^3+8c^2}{8y^3}\right)$.

There is a geometric procedure equivalent to applying Bachet: find the second intersection of the tangent at (x_1, y_1) and C.



Bachet's Formula

Take the example $C : y^2 = x^3 + 3$. One rational point by inspection is $(1, 2)$. Applying Bachet's formula yields

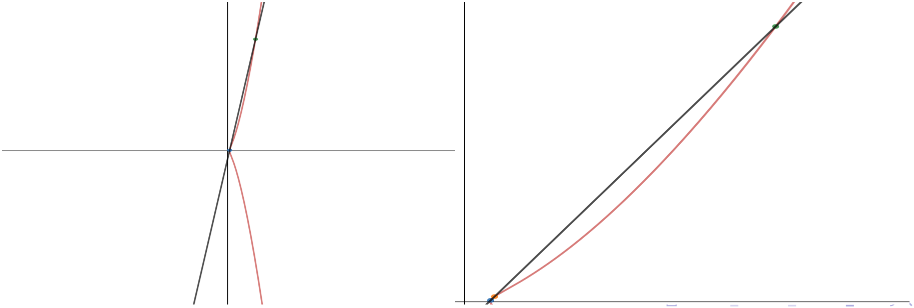
- $(1, 2)$
- $\left(-\frac{23}{16}, -\frac{11}{64}\right)$
- $\left(\frac{2540833}{7744}, -\frac{4050085583}{681472}\right)$
- And so on... This formula almost always generates infinitely many rational points.

Can often find one solution by inspection, so being able to generate infinitely many is a huge improvement.
But Bachet does not generate all solutions.

But! Bachet is Not Enough

$y^2 = x^3 - 26$ has two "easy" rational roots: $(3,1)$ and $(35,207)$. Applying Bachet to each repeatedly:

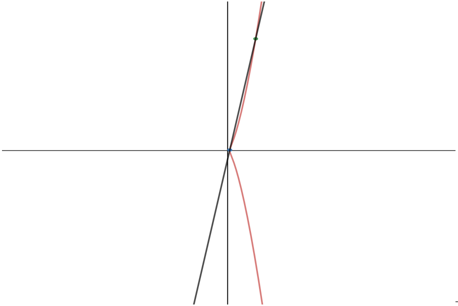
- $(3,1) \to \left(\frac{705}{4}, \frac{18719}{8}\right) \to \left(\frac{247043235585}{5606415376}, \frac{-122770338185379457}{419785957693376}\right) \to \ldots$

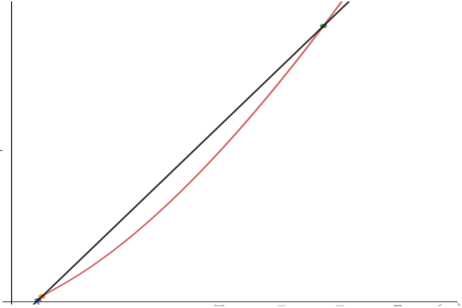


But! Bachet is Not Enough

$y^2 = x^3 - 26$ has two "easy" rational roots: $(3, 1)$ and $(35, 207)$. Applying Bachet to each repeatedly:

- $(3, 1) \to \left(\frac{705}{4}, \frac{18719}{8}\right) \to \left(\frac{247043235585}{5606415376}, \frac{-1227703381853379457}{419785957693376}\right) \to \ldots$
- $(35, 207) \to \left(\frac{167545}{19044}, \frac{-67257971}{2628072}\right) \to \left(\frac{102869565155239795 2865}{344592394091494400016}, \frac{4970551157449683117229613279377}{6396737528620859270011033599936}\right) \to \ldots$

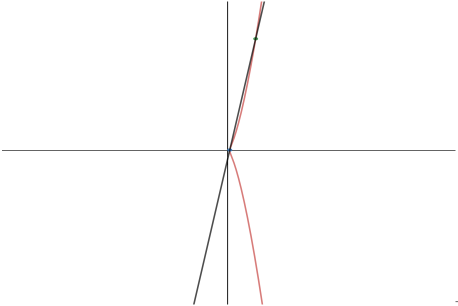


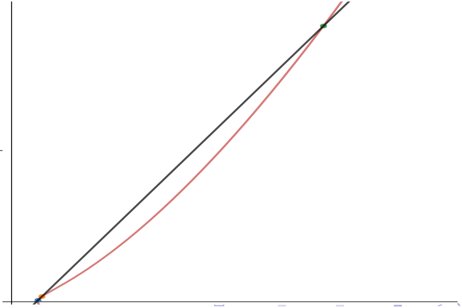


But! Bachet is Not Enough

$y^2 = x^3 - 26$ has two "easy" rational roots: $(3, 1)$ and $(35, 207)$. Applying Bachet to each repeatedly:

- $(3,1) \to \left(\frac{705}{4}, \frac{18719}{8}\right) \to \left(\frac{247043235585}{5606415376}, \frac{-1227703381853794 57}{419785957693376}\right) \to \dots$
- $(35,207) \to \left(\frac{167545}{19044}, \frac{-67257971}{2628072}\right) \to \left(\frac{1028695651552397952865}{344592394091494400016}, \frac{4970551157449683117229613279377}{6396737528620859270011033599936}\right) \to \dots$
- The line through $(3,1)$ (blue) and $(35,207)$ (green) intersects C at $\left(\frac{881}{256}, \frac{15735}{4096}\right)$ (orange).





But! Bachet is Not Enough

- $(3,1) \to \left(\frac{705}{4}, \frac{18719}{8}\right) \to \left(\frac{247043235585}{5606415376}, \frac{-122770338185379457}{419785957693376}\right) \to \dots$
- $(35,207) \to \left(\frac{167545}{19044}, \frac{-67257971}{2628072}\right) \to$
  $\left(\frac{1028695651552397952865}{344592394091494400016}, \frac{4970551157449683117229613279377}{6396737528620859270011033599936}\right) \to \dots$
- $\left(\frac{881}{256}, \frac{15735}{4096}\right)$ does not show up in either sequence

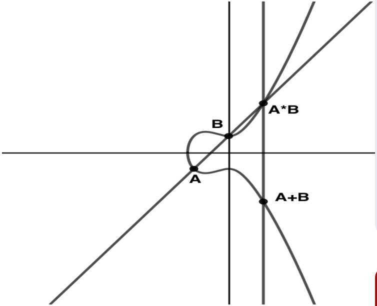
But! Bachet is Not Enough

- $(3, 1) \to \left(\frac{705}{4}, \frac{18719}{8}\right) \to \left(\frac{247043235585}{5606415376}, \frac{-122770338185379457}{419785957693376}\right) \to \dots$
- $(35, 207) \to \left(\frac{167545}{19044}, \frac{-67257971}{2628072}\right) \to \left(\frac{1028695651552397952865}{344592394091494400016}, \frac{4970551157449683117229613279377}{6396737528620859270011033599936}\right) \to \dots$
- $\left(\frac{881}{256}, \frac{15735}{4096}\right)$ does not show up in either sequence
- But it **can** be generated from $(3, 1)$ and $(35, 207)$

But! Bachet is Not Enough

- $(3,1) \to \left(\frac{705}{4}, \frac{18719}{8}\right) \to \left(\frac{247043235585}{5606415376}, \frac{-1227703381853794570}{419785957693376}\right) \to \dots$
- $(35,207) \to \left(\frac{167545}{19044}, \frac{-67257971}{2628072}\right) \to \left(\frac{1028695651552397952865}{3445923940914944000016}, \frac{49705511574496831172296132793770}{6396737528620859270011033599936}\right) \to \dots$
- $\left(\frac{881}{256}, \frac{15735}{4096}\right)$ does not show up in either sequence
- But it **can** be generated from $(3,1)$ and $(35,207)$
- We need a method for generating new rational points from 2 inputs

Group Law



Definition (The Group Law on Rational Points in C)

Let distinct $A, B \in C$ have coordinates in $\mathbb{Q}$. Define $A + B$ as the reflection over the $x - axis$ of the third intersection point, $A * B$, of line $\overline{AB}$ with C. If $A = B$, we define $A + B$ as the reflection of the second intersection point of the tangent line to C at A with C.

The Identity

We define the identity as $\mathcal{O}$. If A and B share a x-coordinate, we say $\overline{AB}$ intersects C "at infinity" at $\mathcal{O}$.

Rational Elliptic Curves

We can generalize Bachet's formula to more general cubics, namely rational elliptic curves.

Definition (Rational Elliptic Curves)

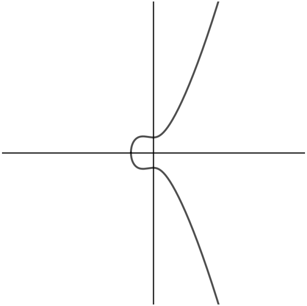
We define rational elliptic curves as non-singular algebraic plane curves described by polynomials of the form $y^2 = x^3 + ax^2 + bx + c,\ a, b, c \in \mathbb{Q}$, plus a "point at infinity" $\mathcal{O}$.

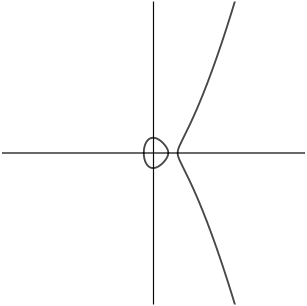
Definition

The group of rational points on an elliptic curve C is denoted by $C(\mathbb{Q})$.

Examples

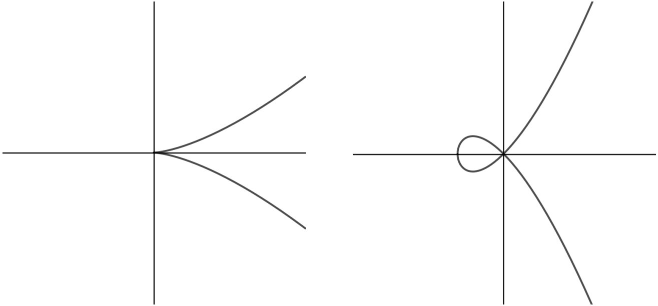
Below are the graphs of two elliptic curves in $\mathbb{R}^2$: $y^2 = x^3 + x^2 + 1$ and $y^2 = x^3 - 2x^2 + 1$.





Non-Examples

These curves are singular and therefore are **not** elliptic curves: $y^2 = x^3$ and $y^2 = x^3 + x^2$. Notice that all have either a cusp, or self-intersection (node).



Finite Generation

We are interested in the *generation* of $C(\mathbb{Q})$.

Definition

A group G is finitely generated if there exists a finite set $\{g_1, g_2, ..., g_n\} \subset G$ such that for all $a \in G$ there exist $\{a_1 ... a_n\} \subset \mathbb{Z}$ such that $a = \sum_{i=0}^{n} g_i a_i$.

Mordell's Theorem

Theorem (Mordell's Theorem)

Let C be a non-singular cubic curve given by an equation

$$C : y^2 = x^3 + ax^2 + bx,$$

with $a, b \in \mathbb{Z}$. Then $C(\mathbb{Q})$, the group of rational points on C, is a finitely generated abelian group.

- Restricted to elliptic curves with a root at $(0, 0)$.
- This means there exists a finite set of points so that all rational points can be obtained by inductively applying the group law.

Proof of Mordell's Theorem:

- Consider the subgroup $2C(\mathbb{Q})$ of $C(\mathbb{Q})$. Then take representatives $A_1, A_2, \ldots$ of its cosets.

Proof of Mordell's Theorem:

- Consider the subgroup $2C(\mathbb{Q})$ of $C(\mathbb{Q})$. Then take representatives $A_1, A_2, \ldots$ of its cosets.
- For any P, there are some points P_1 and A_i such that

$$P = 2P_1 + A_i.$$

Proof of Mordell's Theorem:

- Consider the subgroup $2C(\mathbb{Q})$ of $C(\mathbb{Q})$. Then take representatives $A_1, A_2, \dots$ of its cosets.
- For any P, there are some points P_1 and A_i such that
$$P = 2P_1 + A_i.$$
- Repeat this process for P_1 to find a P_2, and then a P_3, and so forth.

Proof of Mordell's Theorem:

- Consider the subgroup $2C(\mathbb{Q})$ of $C(\mathbb{Q})$. Then take representatives $A_1, A_2, \ldots$ of its cosets.
- For any P, there are some points P_1 and A_i such that

$$P = 2P_1 + A_i.$$

- Repeat this process for P_1 to find a P_2, and then a P_3, and so forth.
-

$$\begin{aligned} P &= 2P_1 + A_{i_1} \\ P_1 &= 2P_2 + A_{i_2} \\ P_2 &= 2P_3 + A_{i_3} \\ P_3 &= 2P_4 + A_{i_4} \end{aligned}$$

Proof of Mordell's Theorem:

- Consider the subgroup $2C(\mathbb{Q})$ of $C(\mathbb{Q})$. Then take representatives $A_1, A_2, \ldots$ of its cosets.
- For any P, there are some points P_1 and A_i such that

$$P = 2P_1 + A_i.$$

- Repeat this process for P_1 to find a P_2, and then a P_3, and so forth.
- $$\begin{aligned} P &= 2P_1 + A_{i_1} \\ P_1 &= 2P_2 + A_{i_2} \\ P_2 &= 2P_3 + A_{i_3} \\ P_3 &= 2P_4 + A_{i_4} \end{aligned}$$
- Repeating m times and back-substituting,

$$P = A_{i_1} + 2A_{i_2} + 4A_{i_3} + \ldots + 2^{m-1}A_{i_m} + 2^m P_m$$

Proof of Mordell's Theorem:

Lemma

$\exists$ *finite* S *independent of* P *such that for large enough* m, $P_m \in S$.

Proof of Mordell's Theorem:

Lemma

$\exists$ finite S independent of P such that for large enough m, $P_m \in S$.

- Take the Elliptic Curve $y^2 = x^3 - 2$. Pick starting point

$$P = \left(\frac{30732610574763}{160280942564521}, \frac{4559771683571581358275}{2029190552145716973931}\right)$$

Proof of Mordell's Theorem:

Lemma

$\exists$ *finite S independent of P such that for large enough m, $P_m \in S$.*

- Take the Elliptic Curve $y^2 = x^3 - 2$. Pick starting point
$$P = \left(\frac{30732610574763}{160280942564521}, \frac{4559771683571581358275}{2029190552145716973931}\right)$$
- $$\begin{aligned} P &= \left(\frac{2340922881}{58675600}, \frac{113259286337279}{449455096000}\right) + (3,5) \\ &= 2\left(\frac{129}{100}, \frac{-383}{1000}\right) + (3,5) \end{aligned}$$

Proof of Mordell's Theorem:

Lemma

$\exists$ *finite* S *independent of* P *such that for large enough* m, $P_m \in S$.

- Take the Elliptic Curve $y^2 = x^3 - 2$. Pick starting point

$$P = \left(\frac{30732610574763}{160280942564521}, \frac{4559771683571581358275}{2029190552145716973931} \right)$$

- $$P = \left(\frac{2340922881}{58675600}, \frac{113259286337279}{449455096000} \right) + (3,5)$$
$$= 2\left(\frac{129}{100}, \frac{-383}{1000} \right) + (3,5)$$

- $$\left(\frac{129}{100}, \frac{-383}{1000} \right) = 2(3,5) + 0$$

Proof of Mordell's Theorem:

Lemma

$\exists$ *finite S independent of P such that for large enough m, $P_m \in S$.*

- Now,

$$P = \left(\frac{30732610574763}{160280942564521}, \frac{4559771683571581358275}{2029190552145716973931}\right)$$

$$P_1 = \left(\frac{129}{100}, \frac{-383}{1000}\right)$$

$$P_2 = (3, 5).$$

Proof of Mordell's Theorem:

Lemma

$\exists$ *finite* S *independent of* P *such that for large enough* m, $P_m \in S$.

- Now,

$$P = \left(\frac{30732610574763}{160280942564521}, \frac{4559771683571581358275}{2029190552145716973931}\right)$$
$$P_1 = \left(\frac{129}{100}, \frac{-383}{1000}\right)$$
$$P_2 = (3, 5).$$

- Notice numerators and denominators decrease as m increases

Proof of Mordell's Theorem:

Lemma

$\exists$ finite S independent of P such that for large enough m, $P_m \in S$.

- Now,

$$P = \left(\frac{30732610574763}{160280942564521}, \frac{4559771683571581358275}{2029190552145716973931}\right)$$

$$P_1 = \left(\frac{129}{100}, \frac{-383}{1000}\right)$$

$$P_2 = (3, 5).$$

- Notice numerators and denominators decrease as m increases
- $\exists K \in \mathbb{Z}$ dependent only on C such that for sufficiently large m, numerator and denominator of x-coordinate of P_m less than K

Proof of Mordell's Theorem:

Lemma

$\exists$ *finite* S *independent of* P *such that for large enough* m, $P_m \in S$.

- Now,

$$P = \left(\frac{30732610574763}{160280942564521}, \frac{4559771683571581358275}{2029190552145716973931}\right)$$
$$P_1 = \left(\frac{129}{100}, \frac{-383}{1000}\right)$$
$$P_2 = (3, 5).$$

- Notice numerators and denominators decrease as m increases
- $\exists K \in \mathbb{Z}$ dependent only on C such that for sufficiently large m, numerator and denominator of x-coordinate of P_m less than K
- S is the set of $P \in C(\mathbb{Q})$ with x-coordinate's with numerator and denominator less than K

Proof of Mordell's Theorem:

Lemma

The number of cosets of $2C(\mathbb{Q})$ in $C(\mathbb{Q})$ is finite.

Proof of Mordell's Theorem:

Lemma

The number of cosets of $2C(\mathbb{Q})$ in $C(\mathbb{Q})$ is finite.

- Equivalent to the index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ being finite.
- This result is known as Weak Mordell's Theorem

Proof of Mordell's Theorem:

Lemma

The number of cosets of $2C(\mathbb{Q})$ in $C(\mathbb{Q})$ is finite.

- Equivalent to the index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ being finite.
- This result is known as Weak Mordell's Theorem

Note that

$$P = A_{i_1} + 2A_{i_2} + 4A_{i_3} + ... + 2^{m-1}A_{i_m} + 2^m P_m.$$

Proof of Mordell's Theorem:

Lemma

The number of cosets of $2C(\mathbb{Q})$ in $C(\mathbb{Q})$ is finite.

- Equivalent to the index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ being finite.
- This result is known as Weak Mordell's Theorem

Note that

$$P = A_{i_1} + 2A_{i_2} + 4A_{i_3} + ... + 2^{m-1}A_{i_m} + 2^m P_m.$$

- Lemma 1 tells us there is a finite set S of P_m.

Proof of Mordell's Theorem:

Lemma

The number of cosets of $2C(\mathbb{Q})$ in $C(\mathbb{Q})$ is finite.

- Equivalent to the index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ being finite.
- This result is known as Weak Mordell's Theorem

Note that

$$P = A_{i_1} + 2A_{i_2} + 4A_{i_3} + ... + 2^{m-1}A_{i_m} + 2^m P_m.$$

- Lemma 1 tells us there is a finite set S of P_m.
- Lemma 2 tells us that there is a finite set of A_i.

Proof of Mordell's Theorem:

Lemma

The number of cosets of $2C(\mathbb{Q})$ in $C(\mathbb{Q})$ is finite.

- Equivalent to the index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ being finite.
- This result is known as Weak Mordell's Theorem

Note that

$$P = A_{i_1} + 2A_{i_2} + 4A_{i_3} + \ldots + 2^{m-1}A_{i_m} + 2^m P_m.$$

- Lemma 1 tells us there is a finite set S of P_m.
- Lemma 2 tells us that there is a finite set of A_i.
- Thus, generating set $G = S \cup \{A_1, A_2, \ldots\}$ is finite.

Generalizations

- Mordell's theorem holds for all rational elliptic curves, not only those with a root at $(0, 0)$.
- Mordell made a conjecture about higher degree curves that was proved in 1983 by Falting.

Theorem

Falting's Theorem] A curve of genus greater than 1 *has only finitely many rational points.*

Definition (Genus)

The genus g of a non-singular curve can be defined in terms of its degree d as $\frac{(d-1)(d-2)}{2}$.

Notice that elliptic curves therefore have genus 1.

Acknowledgements

We would like to thank

- Our mentor, Andrew Senger

We would like to thank

- Our mentor, Andrew Senger
- MIT PRIMES

Acknowledgements

We would like to thank

- Our mentor, Andrew Senger
- MIT PRIMES
- Our parents