Theorem Lemma

Towards Mordell's Theorem: A useful Homomorphism

Sayak Chakrabarti

October 3, 2021

Results until now

- **Height** $h(x) = h(\frac{m}{n}) = \max\{|m|, |n|\}$

Results until now

- **Height** $h(x) = h(\frac{m}{n}) = \max\{|m|, |n|\}$
- Finiteness property of Height

Results until now

- **Height** $h(x) = h(\frac{m}{n}) = \max\{|m|, |n|\}$
- Finiteness property of Height
- Bounds of heights of sums of 2 points

Results until now

Lemma 1

For every $M \in \mathbb{R}$, $|\{P \in C(\mathbb{Q}) | h(P) \leq M\}|$ is finite

Results until now

Lemma 1

For every $M \in \mathbb{R}$, $|\{P \in C(\mathbb{Q}) | h(P) \leq M\}|$ is finite

Lemma 2

Let P_0 be a fixed rational point of C. Then $\exists \kappa_0 \in \mathbb{Q}$ depending on P_0, a, b, c such that

$$h(P + P_0) \leq 2h(P) + \kappa_0 \quad \forall P \in C(\mathbb{Q})$$

Lemma 3

$\exists \kappa \in \mathbb{Q}$ depending on a, b, c such that

$$h(2P) \geq 4h(P) - \kappa \quad \forall P \in C(\mathbb{Q})$$

Results until now

Lemma 1

For every $M \in \mathbb{R}$, $|\{P \in C(\mathbb{Q}) | h(P) \leq M\}|$ is finite

Lemma 2

Let P_0 be a fixed rational point of C. Then $\exists \kappa_0 \in \mathbb{Q}$ depending on P_0, a, b, c such that

$$h(P + P_0) \leq 2h(P) + \kappa_0 \quad \forall P \in C(\mathbb{Q})$$

Lemma 3

$\exists \kappa \in \mathbb{Q}$ depending on a, b, c such that

$$h(2P) \geq 4h(P) - \kappa \quad \forall P \in C(\mathbb{Q})$$

Lemma 4

The index $(C(\mathbb{Q}) : 2C(\mathbb{Q}))$ is finite

Preliminaries

- Already defined: $C(\mathbb{Q})$

Preliminaries

- Already defined: $C(\mathbb{Q})$
- $\Gamma = C(\mathbb{Q})$

Preliminaries

- Already defined: $C(\mathbb{Q})$
- $\Gamma = C(\mathbb{Q})$
- Weierstrass normal form: $C : y^2 = f(x) = x^3 + ax^2 + bx + c$

Preliminaries

- Already defined: $C(\mathbb{Q})$
- $\Gamma = C(\mathbb{Q})$
- Weierstrass normal form: $C : y^2 = f(x) = x^3 + ax^2 + bx + c$
- Suppose $f(x)$ has a rational root, x_0, translate origin to $(x_0, 0)$

Preliminaries

- Already defined: $C(\mathbb{Q})$
- $\Gamma = C(\mathbb{Q})$
- Weierstrass normal form: $C : y^2 = f(x) = x^3 + ax^2 + bx + c$
- Suppose $f(x)$ has a rational root, x_0, translate origin to $(x_0, 0)$
- New curve $C : y^2 = f(x) = x^3 + ax^2 + bx$

Preliminaries

- Already defined: $C(\mathbb{Q})$
- $\Gamma = C(\mathbb{Q})$
- Weierstrass normal form: $C : y^2 = f(x) = x^3 + ax^2 + bx + c$
- Suppose $f(x)$ has a rational root, x_0, translate origin to $(x_0, 0)$
- New curve $C : y^2 = f(x) = x^3 + ax^2 + bx$
- Discriminant $D = b^2(a^2 - 4b)$ (assumption: non-singular curve)

Preliminaries

- Already defined: $C(\mathbb{Q})$
- $\Gamma = C(\mathbb{Q})$
- Weierstrass normal form: $C : y^2 = f(x) = x^3 + ax^2 + bx + c$
- Suppose $f(x)$ has a rational root, x_0, translate origin to $(x_0, 0)$
- New curve $C : y^2 = f(x) = x^3 + ax^2 + bx$
- Discriminant $D = b^2(a^2 - 4b)$ (assumption: non-singular curve)
- Define $T = (0, 0)$, we know $2T = \mathcal{O}$

A Map between Curves

- Want to analyze $(\Gamma : 2\Gamma) \iff$ order of factor group $\Gamma/2\Gamma$

A Map between Curves

- Want to analyze $(\Gamma : 2\Gamma) \iff$ order of factor group $\Gamma/2\Gamma$
- Analyze duplication map $P \to 2P$ (we will write this as a composition of 2 maps of degree 2)

A Map between Curves

$$C : y^2 = x^3 + ax^2 + bx$$
$$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$$

A Map between Curves

$C : y^2 = x^3 + ax^2 + bx$
$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$
Given by $\bar{a} = -2a$; $\bar{b} = a^2 - 4b$

A Map between Curves

$C : y^2 = x^3 + ax^2 + bx$
$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$
Given by $\bar{a} = -2a$; $\bar{b} = a^2 - 4b$

A Map between Curves

$C : y^2 = x^3 + ax^2 + bx$
$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$
Given by $\bar{a} = -2a$; $\bar{b} = a^2 - 4b$
Consider $\bar{\bar{C}} : y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x$

A Map between Curves

$C : y^2 = x^3 + ax^2 + bx$
$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$
Given by $\bar{a} = -2a$; $\bar{b} = a^2 - 4b$
Consider $\bar{\bar{C}} : y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x$
$\bar{\bar{a}} = 4a, \bar{\bar{b}} = 16b$

A Map between Curves

$C : y^2 = x^3 + ax^2 + bx$
$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$
Given by $\bar{a} = -2a$; $\bar{b} = a^2 - 4b$
Consider $\bar{\bar{C}} : y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x$
$\bar{\bar{a}} = 4a, \bar{\bar{b}} = 16b$
Note that $\bar{\bar{C}} \sim C$

A Map between Curves

$C : y^2 = x^3 + ax^2 + bx$
$\bar{C} : y^2 = x^3 + \bar{a}x^2 + \bar{b}x$
Given by $\bar{a} = -2a$; $\bar{b} = a^2 - 4b$
Consider $\bar{\bar{C}} : y^2 = x^3 + \bar{\bar{a}}x^2 + \bar{\bar{b}}x$
$\bar{\bar{a}} = 4a, \bar{\bar{b}} = 16b$
Note that $\bar{\bar{C}} \sim C$
$(x, y) \to (4x, 8y)$

A Homomorphism

Goal: Define map $\phi : C \to \bar{C}$
(This will also give $\Gamma \to \bar{\Gamma}$)

A Homomorphism

Goal: Define map $\phi : C \to \bar{C}$
(This will also give $\Gamma \to \bar{\Gamma}$)
Similarly $\bar{\phi} : \bar{C} \to \bar{\bar{C}}$

A Homomorphism

$$\phi(x,y) = (\bar{x},\bar{y}) = (x + a + \tfrac{b}{x}, y(1 - \tfrac{b}{x^2})) = (\tfrac{y}{x^2}, y(1 - \tfrac{b}{x^2}))$$

A Homomorphism

$$\phi(x,y) = (\bar{x},\bar{y}) = (x + a + \tfrac{b}{x}, y(1 - \tfrac{b}{x^2})) = (\tfrac{y}{x^2}, y(1 - \tfrac{b}{x^2}))$$

(Can be verified easily!)

A Homomorphism

$$\phi(x,y) = (\bar{x},\bar{y}) = (x + a + \frac{b}{x}, y(1 - \frac{b}{x^2})) = (\frac{y}{x^2}, y(1 - \frac{b}{x^2}))$$

(Can be verified easily!)
$\rightarrow$ Is this always defined?

A Homomorphism

$$\phi(x,y) = (\bar{x},\bar{y}) = (x + a + \tfrac{b}{x}, y(1 - \tfrac{b}{x^2})) = (\tfrac{y}{x^2}, y(1 - \tfrac{b}{x^2}))$$

(Can be verified easily!)
$\rightarrow$ Is this always defined?
Define $\phi(T) = \bar{\mathcal{O}}, \phi(\mathcal{O}) = \bar{\mathcal{O}}$

A Homomorphism

Kernel of ϕ?

A Homomorphism

Kernel of ϕ?
Only 2 points T and $\mathcal{O}$ sent to $\bar{\mathcal{O}}$

A Homomorphism

Kernel of ϕ?
Only 2 points T and $\mathcal{O}$ sent to $\bar{\mathcal{O}}$

A Homomorphism

- $\{\mathcal{O}, T\}$ subgroup of C
- C is abelian group

A Homomorphism

- $\{\mathcal{O}, T\}$ subgroup of C
- C is abelian group
- Intuition: $\bar{C}$ is isomorphic the quotient subgroup $C/\{\mathcal{O}, T\}$

Main Proposition

Proposition 1

Let C, $\bar{C}$ be elliptic curves as defined.
(a) There is a homomorphism $\phi : C \to \bar{C}$ as defined before
(b) Same process gives the map $\bar{\phi} : \bar{C} \to \bar{\bar{C}}$ denoted by ψ. Also $\psi \cdot \phi : C \to \bar{\bar{C}}$ given by $(x, y) \to (\frac{x}{4}, \frac{y}{8})$
(c) We have $\psi \cdot \phi : C \to C$ given by

$$\psi \cdot \phi(P) = 2P$$

The "calculative" Proof

(a) Left to prove that $\phi(P+Q) = \phi(P) + \phi(Q)$

The "calculative" Proof

(a) Left to prove that $\phi(P+Q)=\phi(P)+\phi(Q)$
If any one of them is $\mathcal{O}$ then trivial

The "calculative" Proof

(a) Left to prove that $\phi(P+Q) = \phi(P) + \phi(Q)$
If any one of them is $\mathcal{O}$ then trivial
If any one of them is T, we show that $\phi(P+T) = \phi(P)$.
We have $P + T = (x+y) + (0,0) = (\frac{b}{x}, -\frac{by}{x^2})$. Can check from this that $\phi(\frac{b}{x}, -\frac{by}{x^2}) = (x, y)$.
However this is true when $P \neq T$. When $P = Q = T$, we have $\phi(T+T) = \phi(\mathcal{O}) = \bar{\mathcal{O}} = \mathcal{O} + \mathcal{O}$ as expected.

The "calculative" Proof

(a) Left to prove that $\phi(P+Q) = \phi(P) + \phi(Q)$
If any one of them is $\mathcal{O}$ then trivial
If any one of them is T, we show that $\phi(P+T) = \phi(P)$.
We have $P + T = (x+y) + (0,0) = (\frac{b}{x}, -\frac{by}{x^2})$. Can check from this that $\phi(\frac{b}{x}, -\frac{by}{x^2}) = (x, y)$.
However this is true when $P \neq T$. When $P = Q = T$, we have $\phi(T+T) = \phi(\mathcal{O}) = \bar{\mathcal{O}} = \mathcal{O} + \mathcal{O}$ as expected.
Also we show that ϕ is odd, i.e.
$\phi(-P) = \phi(x, -y) = \left(\left(\frac{-y}{x}\right)^2, \frac{-y(x^2-b)}{x^2}\right) = -\phi(x, y) = -\phi(P)$.

The "calculative" Proof

Next we want to show that if $P_1 + P_2 + P_3 = \mathcal{O}$ then we will have $\phi(P_2) + \phi(P_2) + \phi(P_3) = \bar{\mathcal{O}}$.
(If we have this then $\phi(P_1 + P_2) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$ from this)
Also reasonable to assume neither of them are $\mathcal{O}$ or T.

The "calculative" Proof

Next we want to show that if $P_1 + P_2 + P_3 = \mathcal{O}$ then we will have $\phi(P_2) + \phi(P_2) + \phi(P_3) = \bar{\mathcal{O}}$.
(If we have this then $\phi(P_1 + P_2) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$ from this)
Also reasonable to assume neither of them are $\mathcal{O}$ or T.
Note that P_1, P_2, P_3 are collinear (Why?)

The "calculative" Proof

Next we want to show that if $P_1 + P_2 + P_3 = \mathcal{O}$ then we will have $\phi(P_2) + \phi(P_2) + \phi(P_3) = \bar{\mathcal{O}}$.
(If we have this then $\phi(P_1 + P_2) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$ from this)
Also reasonable to assume neither of them are $\mathcal{O}$ or T.
Note that P_1, P_2, P_3 are collinear (Why?)
Let $y = \lambda x + \nu$ be the line through them, with $\nu \neq 0$

The "calculative" Proof

Next we want to show that if $P_1 + P_2 + P_3 = \mathcal{O}$ then we will have $\phi(P_2) + \phi(P_2) + \phi(P_3) = \bar{\mathcal{O}}$.
(If we have this then $\phi(P_1 + P_2) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$ from this)
Also reasonable to assume neither of them are $\mathcal{O}$ or T.
Note that P_1, P_2, P_3 are collinear (Why?)
Let $y = \lambda x + \nu$ be the line through them, with $\nu \neq 0$
The image of this line in $\bar{C}$ is $y = \bar{\lambda} x + \bar{\nu}$ where $\bar{\lambda} = \frac{\nu\lambda - b}{\nu}$, $\bar{\nu} = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu}$

The "calculative" Proof

Next we want to show that if $P_1 + P_2 + P_3 = \mathcal{O}$ then we will have $\phi(P_2) + \phi(P_2) + \phi(P_3) = \bar{\mathcal{O}}$.
(If we have this then $\phi(P_1 + P_2) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$ from this)
Also reasonable to assume neither of them are $\mathcal{O}$ or T.
Note that P_1, P_2, P_3 are collinear (Why?)
Let $y = \lambda x + \nu$ be the line through them, with $\nu \neq 0$
The image of this line in $\bar{C}$ is $y = \bar{\lambda} x + \bar{\nu}$ where $\bar{\lambda} = \frac{\nu\lambda - b}{\nu}$, $\bar{\nu} = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu}$
To check this, verify that $\bar{\lambda}\bar{x}_i + \bar{\nu} = \bar{y}_i$ putting values of $\bar{\lambda}, \bar{\nu}, \bar{x}_i, \bar{y}_i$; for $i = 1, 2, 3$

The "calculative" Proof

Next we want to show that if $P_1 + P_2 + P_3 = \mathcal{O}$ then we will have $\phi(P_2) + \phi(P_2) + \phi(P_3) = \bar{\mathcal{O}}$.
(If we have this then $\phi(P_1 + P_2) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$ from this)
Also reasonable to assume neither of them are $\mathcal{O}$ or T.
Note that P_1, P_2, P_3 are collinear (Why?)
Let $y = \lambda x + \nu$ be the line through them, with $\nu \neq 0$
The image of this line in $\bar{C}$ is $y = \bar{\lambda} x + \bar{\nu}$ where $\bar{\lambda} = \frac{\nu\lambda - b}{\nu}$, $\bar{\nu} = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu}$
To check this, verify that $\bar{\lambda}\bar{x_i} + \bar{\nu} = \bar{y_i}$ putting values of $\bar{\lambda}, \bar{\nu}, \bar{x_i}, \bar{y_i}$; for $i = 1, 2, 3$
Can be shown that $(\lambda x + \nu) = f(x)^2$ has only distinct roots

The "calculative" Proof

Next we want to show that if $P_1 + P_2 + P_3 = \mathcal{O}$ then we will have $\phi(P_2) + \phi(P_2) + \phi(P_3) = \bar{\mathcal{O}}$.
(If we have this then $\phi(P_1 + P_2) = -\phi(P_3) = \phi(P_1) + \phi(P_2)$ from this)
Also reasonable to assume neither of them are $\mathcal{O}$ or T.
Note that P_1, P_2, P_3 are collinear (Why?)
Let $y = \lambda x + \nu$ be the line through them, with $\nu \neq 0$
The image of this line in $\bar{C}$ is $y = \bar{\lambda} x + \bar{\nu}$ where $\bar{\lambda} = \frac{\nu\lambda - b}{\nu}$, $\bar{\nu} = \frac{\nu^2 - a\nu\lambda + b\lambda^2}{\nu}$
To check this, verify that $\bar{\lambda}\bar{x}_i + \bar{\nu} = \bar{y}_i$ putting values of $\bar{\lambda}, \bar{\nu}, \bar{x}_i, \bar{y}_i$; for $i = 1, 2, 3$
Can be shown that $(\lambda x + \nu) = f(x)^2$ has only distinct roots
Same thing can be done for complex numbers as well, showing ϕ is a homomorphism in general.

The "calculative" Proof

(b) We have $\bar{\bar{C}} : y^2 = x^3 + 4ax^2 + 16bx$

The "calculative" Proof

(b) We have $\bar{\bar{C}} : y^2 = x^3 + 4ax^2 + 16bx$
Isomorphism from $\bar{\bar{C}} \to C$ given by $(x, y) \to (\frac{x}{4}, \frac{x}{8})$.

The "calculative" Proof

(b) We have $\bar{\bar{C}} : y^2 = x^3 + 4ax^2 + 16bx$
Isomorphism from $\bar{\bar{C}} \to C$ given by $(x, y) \to (\frac{x}{4}, \frac{x}{8})$.
From (a) there is a homomorphism $\bar{\phi} : \bar{C} \to \bar{\bar{C}}$.

The "calculative" Proof

(b) We have $\bar{\bar{C}} : y^2 = x^3 + 4ax^2 + 16bx$
Isomorphism from $\bar{\bar{C}} \to C$ given by $(x, y) \to (\frac{x}{4}, \frac{x}{8})$.
From (a) there is a homomorphism $\bar{\phi} : \bar{C} \to \bar{\bar{C}}$.
$\psi : \bar{C} \to C$ is given by composition of homomorphism $\bar{\phi}$ and isomorphism $\bar{\bar{C}} \to C$.

The "calculative" Proof

(b) We have $\bar{\bar{C}} : y^2 = x^3 + 4ax^2 + 16bx$
Isomorphism from $\bar{\bar{C}} \to C$ given by $(x, y) \to (\frac{x}{4}, \frac{x}{8})$.
From (a) there is a homomorphism $\bar{\phi} : \bar{C} \to \bar{\bar{C}}$.
$\psi : \bar{C} \to C$ is given by composition of homomorphism $\bar{\phi}$ and isomorphism $\bar{\bar{C}} \to C$.
Required homomorphism from $\bar{C}$ to C

The "calculative" Proof

(c) To show that $\psi \cdot \phi$ is multiplication by 2.

The "calculative" Proof

(c) To show that $\psi \cdot \phi$ is multiplication by 2.
We have

$$2P = 2(x, y) = \left(\frac{(x^2 - b)^2}{4y^2}, \frac{(x^2 - b)(x^4 + 2ax^3 + 6bx^2 + 2abx + b^2)}{8y^3} \right)$$

The "calculative" Proof

(c) To show that $\psi \cdot \phi$ is multiplication by 2.
We have

$$2P = 2(x,y) = \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3} \right)$$

We have $\phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2} \right)$, $\psi(\bar{x},\bar{y}) = \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-b)}{8\bar{x}^2} \right)$

The "calculative" Proof

(c) To show that $\psi \cdot \phi$ is multiplication by 2.
We have

$$2P = 2(x,y) = \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3}\right)$$

We have $\phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2}\right)$, $\psi(\bar{x},\bar{y}) = \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-b)}{8\bar{x}^2}\right)$
Using this and some calculations later, can be shown that

$$\psi(\phi(x,y)) = \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3}\right)$$

The "calculative" Proof

(c) To show that $\psi \cdot \phi$ is multiplication by 2.
We have

$$2P = 2(x,y) = \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3} \right)$$

We have $\phi(x,y) = \left(\frac{y^2}{x^2}, \frac{y(x^2-b)}{x^2} \right)$, $\psi(\bar{x},\bar{y}) = \left(\frac{\bar{y}^2}{4\bar{x}^2}, \frac{\bar{y}(\bar{x}^2-b)}{8\bar{x}^2} \right)$
Using this and some calculations later, can be shown that

$$\psi(\phi(x,y)) = \left(\frac{(x^2-b)^2}{4y^2}, \frac{(x^2-b)(x^4+2ax^3+6bx^2+2abx+b^2)}{8y^3} \right)$$

This gives $\psi \cdot \phi(x,y) = 2(x,y)$

Next Lecture

In next lecture, Lemma 4 will be completely proved using this homomorphism, with the proof of Mordell's Theorem.

Acknowledgements

Most of the content has been taken from Silverman, JH and Tate, T; Rational Points on Elliptic Curves, *Springer*, 2015.