Mordell's Theorem (I/II)

Justin Scarfy

The University of British Columbia

January 31, 2012

Introduction

Background

In the past few lectures we learned the definition of elliptic curves, absorbed the Nagell-Lutz Theorem, were being introduced to the L-functions of elliptic curves, and got spoiled by a few mouth-watering conjectures.

Introduction

Background

In the past few lectures we learned the definition of elliptic curves, absorbed the Nagell-Lutz Theorem, were being introduced to the L-functions of elliptic curves, and got spoiled by a few mouth-watering conjectures.

Lecture Plan

Today we shall start discussing a theorem that L. Mordell proved in 1922:

The group of rational points on a non-singular cubic elliptic curve is finitely generated.

Introduction

Background

In the past few lectures we learned the definition of elliptic curves, absorbed the Nagell-Lutz Theorem, were being introduced to the L-functions of elliptic curves, and got spoiled by a few mouth-watering conjectures.

Lecture Plan

Today we shall start discussing a theorem that L. Mordell proved in 1922:

The group of rational points on a non-singular cubic elliptic curve is finitely generated.

The main source I follow is that of Silverman-Tate, in which they employ a technique called heights, and cheerfully partition the π so I can serve them to you by slices.

Introduction

Background

In the past few lectures we learned the definition of elliptic curves, absorbed the Nagell-Lutz Theorem, were being introduced to the L-functions of elliptic curves, and got spoiled by a few mouth-watering conjectures.

Lecture Plan

Today we shall start discussing a theorem that L. Mordell proved in 1922:

The group of rational points on a non-singular cubic elliptic curve is finitely generated.

The main source I follow is that of Silverman-Tate, in which they employ a technique called heights, and cheerfully partition the π so I can serve them to you by slices.

Disclaimer

I only have time to serve you a finite portion of the π today.

Review

Definition (Non-Singular Cubic Elliptic Curve)

Recall the precise definition of a non-singular cubic elliptic curve E is an equation of the form

$$y^2 = f(x) = x^3 + ax^2 + bx + c \tag{1}$$

with non-zero discrimant:

$$\Delta := -16(4a^3 + 27b^2) \neq 0$$

Review

Definition (Non-Singular Cubic Elliptic Curve)

Recall the precise definition of a non-singular cubic elliptic curve E is an equation of the form

$$y^2 = f(x) = x^3 + ax^2 + bx + c \tag{1}$$

with non-zero discriminant:

$$\Delta := -16(4a^3 + 27b^2) \neq 0$$

Nagell-Lutz Theorem

Let E be a non-singular cubic elliptic curve with the form $y^2 = x^3 + ax + b$, $a, b \in \mathbb{Z}$

If $P \in E(\mathbb{Q})$ is a torsion point of order $m \geq 2$, then,

1) $x(P), y(P) \in \mathbb{Z}$
2) Either $2P = 0$ or $y^2 | \Delta := 4a^2 + 27b^2$

Heights

Definition (Heights)

For all $x \in \mathbb{Q}$ with $x = \frac{m}{n}$ where $(m, n) = 1$, we define $H : \mathbb{Q} \to \mathbb{Z}^+$ by

$$H(x) := \max\{|m|, |n|\}$$

Heights

Definition (Heights)

For all $x \in \mathbb{Q}$ with $x = \frac{m}{n}$ where $(m, n) = 1$, we define $H : \mathbb{Q} \to \mathbb{Z}^+$ by

$$H(x) := \max\{|m|, |n|\}$$

The Finiteness Property of the Height

The set of all rational numbers whose height is less than a fixed number is finite.

Heights

Definition (Heights)

For all $x \in \mathbb{Q}$ with $x = \frac{m}{n}$ where $(m, n) = 1$, we define $H : \mathbb{Q} \to \mathbb{Z}^+$ by

$$H(x) := \max\{|m|, |n|\}$$

The Finiteness Property of the Height

The set of all rational numbers whose height is less than a fixed number is finite.

Heights of Points on Elliptic Curves

For $E : y^2 = f(x) = x^3 + ax^2 + bx + c$ with $a, b, c \in \mathbb{Z}$ and rational point $P = (x, y)$ on E,

$$H(P) := H(x)$$

further we define "small h" height: $h : E \to \mathbb{R}_{\geq 0}$ by:

$$h(P) = \log H(P)$$

and finally define the height of point $\mathcal{O}$ at infinity to be: $H(\mathcal{O}) = 1$ or $h(\mathcal{O}) = 0$

Partitioning the π

Theorem (Modrell 1922)

The group of rational points $E(\mathbb{Q})$ is finitely generated.

Partitioning the π

Theorem (Modrell 1922)

The group of rational points $E(\mathbb{Q})$ is finitely generated.

Slice 1

For every $M \in \mathbb{R}$, the set $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ is finite. □

Partitioning the π

Theorem (Modrell 1922)

The group of rational points $E(\mathbb{Q})$ is finitely generated.

Slice 1

For every $M \in \mathbb{R}$, the set $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ is finite. $\square$

Slice 2

Let $P_0 \in \mathbb{Q}$ on E be fixed, then there exists a constant κ_0 depending on P_0 and a, b, c such that $h(P + P_0) < 2h(P) + \kappa_0$ for all $P \in E(\mathbb{Q})$.

Partitioning the π

Theorem (Modrell 1922)

The group of rational points $E(\mathbb{Q})$ is finitely generated.

Slice 1

For every $M \in \mathbb{R}$, the set $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ is finite. $\square$

Slice 2

Let $P_0 \in \mathbb{Q}$ on E be fixed, then there exists a constant κ_0 depending on P_0 and a, b, c such that $h(P + P_0) < 2h(P) + \kappa_0$ for all $P \in E(\mathbb{Q})$.

Slice 3

There is a constant κ, depending on a, b, c so that $h(2P) \geq 4h(P) - \kappa$ for all $P \in E(\mathbb{Q})$.

Partitioning the π

Theorem (Modrell 1922)

The group of rational points $E(\mathbb{Q})$ is finitely generated.

Slice 1

For every $M \in \mathbb{R}$, the set $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ is finite. □

Slice 2

Let $P_0 \in \mathbb{Q}$ on E be fixed, then there exists a constant κ_0 depending on P_0 and a, b, c such that $h(P + P_0) < 2h(P) + \kappa_0$ for all $P \in E(\mathbb{Q})$.

Slice 3

There is a constant κ, depending on a, b, c so that $h(2P) \geq 4h(P) - \kappa$ for all $P \in E(\mathbb{Q})$.

Slice 4

Not ready yet– will be ready and served next week!

Descent Theorem (1/6)

Descent Theorem

Let Γ be an abelian group, and suppose that there is a function $h : \Gamma \to \mathbb{R}_{\geq 0}$ with the following three properties:

a) For every $M \in \mathbb{R}$, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite.
b) For every $P_0 \in \Gamma$, there is a constant κ_0 with $h(P + P_0) \leq 2h(P) + \kappa_0$.
c) There is a constant κ so that $h(2P) \geq 4h(P) - \kappa$ for all $P \in \Gamma$.

Descent Theorem (1/6)

Descent Theorem

Let Γ be an abelian group, and suppose that there is a function $h : \Gamma \to \mathbb{R}_{\geq 0}$ with the following three properties:

a) For every $M \in \mathbb{R}$, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite.
b) For every $P_0 \in \Gamma$, there is a constant κ_0 with $h(P + P_0) \leq 2h(P) + \kappa_0$.
c) There is a constant κ so that $h(2P) \geq 4h(P) - \kappa$ for all $P \in \Gamma$.

Then, Γ is finitely generated

Descent Theorem (1/6)

Descent Theorem

Let Γ be an abelian group, and suppose that there is a function $h : \Gamma \to \mathbb{R}_{\geq 0}$ with the following three properties:

a) For every $M \in \mathbb{R}$, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite.
b) For every $P_0 \in \Gamma$, there is a constant κ_0 with $h(P + P_0) \leq 2h(P) + \kappa_0$.
c) There is a constant κ so that $h(2P) \geq 4h(P) - \kappa$ for all $P \in \Gamma$.

Oh, and further suppose that:
d) The subgroup 2Γ has finite index in Γ

Then, Γ is finitely generated

Descent Theorem (1/6)

Descent Theorem

Let Γ be an abelian group, and suppose that there is a function $h : \Gamma \to \mathbb{R}_{\geq 0}$ with the following three properties:

a) For every $M \in \mathbb{R}$, the set $\{P \in \Gamma : h(P) \leq M\}$ is finite.
b) For every $P_0 \in \Gamma$, there is a constant κ_0 with $h(P + P_0) \leq 2h(P) + \kappa_0$.
c) There is a constant κ so that $h(2P) \geq 4h(P) - \kappa$ for all $P \in \Gamma$.

Oh, and further suppose that:
d) The subgroup 2Γ has finite index in Γ

Then, Γ is finitely generated

Proof of the Descent Theorem (1/6)

First we take a representative for each coset of 2Γ in Γ, assume there are n of them, and Let $Q_1, Q_2, \ldots, Q_n$ be representative of the cosets (i.e. For any $P \in \Gamma$, there exists an index i_1, depending on P, such that $P - Q_{i_1} \in 2\Gamma$).

Descent Theorem (2/6)

Proof of the Descent Theorem (2/6)

After all, P has to be in one of the cosets (i.e. We can write $P - Q_{i_1} = 2P_1$ for some $P_1 \in \Gamma$).

Descent Theorem (2/6)

Proof of the Descent Theorem (2/6)

After all, P has to be in one of the cosets (i.e. We can write $P - Q_{i_1} = 2P_1$ for some $P_1 \in \Gamma$).

Feeding this into the finite state automata yields:

$$\begin{aligned} P_1 - Q_{i_2} &= 2P_2 \\ P_2 - Q_{i_3} &= 2P_3 \\ &\vdots \\ P_{m-1} - Q_{i_m} &= 2P_m \end{aligned}$$

where $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_m}$ are chosen from the coset representation $Q_1, Q_2, \ldots, Q_n$ and $P_1, P_2, \ldots, P_m$ are elements of Γ.

Descent Theorem (2/6)

Proof of the Descent Theorem (2/6)

After all, P has to be in one of the cosets (i.e. We can write $P - Q_{i_1} = 2P_1$ for some $P_1 \in \Gamma$).

Feeding this into the finite state automata yields:

$$\begin{aligned} P_1 - Q_{i_2} =& 2P_2 \\ P_2 - Q_{i_3} =& 2P_3 \\ &\vdots \\ P_{m-1} - Q_{i_m} =& 2P_m \end{aligned}$$

where $Q_{i_1}, Q_{i_2}, \ldots, Q_{i_m}$ are chosen from the coset representation $Q_1, Q_2, \ldots, Q_n$ and $P_1, P_2, \ldots, P_m$ are elements of Γ.

Moral: P_i is more-or-less equal to $2P_{i+1}$, the height of P_{i+1} is more-or-less one fourth the height of P_i. So the sequence of points $P, P_1, P_2, \ldots$ should have decreasing height, and from property a), the set will be finite.

Descent Theorem (3/6)

Proof of the Descent Theorem (3/6)

From the first equation we see $P = Q_i + 2P_1$, and substituting the second equation $P_1 = Q_{i_2} + 4P_2$ into the first gives $P = Q_{i_1} + 2Q_{i_2} + 4P_2$

Descent Theorem (3/6)

Proof of the Descent Theorem (3/6)

From the first equation we see $P = Q_i + 2P_1$, and substituting the second equation $P_1 = Q_{i_2} + 4P_2$ into the first gives $P = Q_{i_1} + 2Q_{i_2} + 4P_2$

Continuing in this fashion, we obtain

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

In particular, this says that P is in the subgroup of Γ generated by the Q_i's and P_m.

Descent Theorem (3/6)

Proof of the Descent Theorem (3/6)

From the first equation we see $P = Q_i + 2P_1$, and substituting the second equation $P_1 = Q_{i_2} + 4P_2$ into the first gives $P = Q_{i_1} + 2Q_{i_2} + 4P_2$

Continuing in this fashion, we obtain

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

In particular, this says that P is in the subgroup of Γ generated by the Q_i's and P_m.

Next we show that by choosing m large enough, we can force P_m to have height less than a certain fixed bound. Then the finite set of points with height less than that bound, together with the $Q_i's$, will generate Γ.

Descent Theorem (3/6)

Proof of the Descent Theorem (3/6)

From the first equation we see $P = Q_i + 2P_1$, and substituting the second equation $P_1 = Q_{i_2} + 4P_2$ into the first gives $P = Q_{i_1} + 2Q_{i_2} + 4P_2$

Continuing in this fashion, we obtain

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

In particular, this says that P is in the subgroup of Γ generated by the Q_i's and P_m.

Next we show that by choosing m large enough, we can force P_m to have height less than a certain fixed bound. Then the finite set of points with height less than that bound, together with the $Q_i's$, will generate Γ.

Taking one of the $P_j's$ in the sequence of points $P, P_1, P_2, \ldots$ and examine the relation between the height of P_{j-1} and that of P_j. We want to show that the height of P_j is considerably smaller.

Descent Theorem (4/6)

Proof of the Descent Theorem (4/6)

If we apply b) with $-Q_i$ in place of P_0, we obtain a constant κ_i such that $h(P - Q_i) \leq 2h(P) + \kappa_i$ for all $P \in \Gamma$.

Descent Theorem (4/6)

Proof of the Descent Theorem (4/6)

If we apply b) with $-Q_i$ in place of P_0, we obtain a constant κ_i such that $h(P - Q_i) \leq 2h(P) + \kappa_i$ for all $P \in \Gamma$.

Now we do this for each Q_i, $1 \leq i \leq n$.
Let κ' be the largest of the κ_i's, then
$h(P - Q_i) \leq 2h(P) + \kappa'$ for all $P \in \Gamma$ and all $1 \leq i \leq n$, this can be done as there are only $Q_i's$, and is one place where property (d) that 2Γ has finite index in Γ.

Descent Theorem (4/6)

Proof of the Descent Theorem (4/6)

If we apply b) with $-Q_i$ in place of P_0, we obtain a constant κ_i such that $h(P - Q_i) \leq 2h(P) + \kappa_i$ for all $P \in \Gamma$.

Now we do this for each Q_i, $1 \leq i \leq n$.
Let κ' be the largest of the κ_i's, then
$h(P - Q_i) \leq 2h(P) + \kappa'$ for all $P \in \Gamma$ and all $1 \leq i \leq n$, this can be done as there are only $Q_i' s$, and is one place where property (d) that 2Γ has finite index in Γ.

Let κ be the constant from (c), then we deduce:

$$4h(P_j) \leq h(2P_j) + \kappa = h(P_{j-1} - Q_{i_j}) + \kappa \leq 2h(P_{j-1}) + \kappa' + \kappa$$

which can be rewritten as:

$$h(P_j) \leq \frac{1}{2}h(P_{j-1}) + \frac{\kappa' + \kappa}{4} = \frac{3}{4}h(P_{j-1}) - \frac{1}{4}\big(h(P_{j-1}) - (\kappa' + \kappa)\big)$$

Descent Theorem (5/6)

Proof of the Descent Theorem (5/6)

From the previous equation we see that if $h(P_{j-1}) \geq \kappa' + \kappa$, then

$$h(P_j) \leq \frac{3}{4} h(P_{j-1})$$

Descent Theorem (5/6)

Proof of the Descent Theorem (5/6)

From the previous equation we see that if $h(P_{j-1}) \geq \kappa' + \kappa$, then

$$h(P_j) \leq \frac{3}{4} h(P_{j-1})$$

So in the sequence of points $P, P_1, P_2, P_3, \ldots,$ as long as the points P_j satisfies the condition $h(P_j) \geq \kappa' + \kappa$, then the next point in the sequence has much smaller height, namely $h(P_{j+1}) \leq \frac{3}{4} h(P_j)$.

Descent Theorem (5/6)

Proof of the Descent Theorem (5/6)

From the previous equation we see that if $h(P_{j-1}) \geq \kappa' + \kappa$, then

$$h(P_j) \leq \frac{3}{4} h(P_{j-1})$$

So in the sequence of points $P, P_1, P_2, P_3, \ldots,$ as long as the points P_j satisfies the condition $h(P_j) \geq \kappa' + \kappa$, then the next point in the sequence has much smaller height, namely $h(P_{j+1}) \leq \frac{3}{4} h(P_j)$.

N.B. If you start with a number and keep multiplying it by 3/4, it approaches zero. So eventually we will find an index m such that $h(P_m) \leq \kappa' + \kappa$

Descent Theorem (5/6)

Proof of the Descent Theorem (5/6)

From the previous equation we see that if $h(P_{j-1}) \geq \kappa' + \kappa$, then

$$h(P_j) \leq \frac{3}{4} h(P_{j-1})$$

So in the sequence of points $P, P_1, P_2, P_3, \dots,$ as long as the points P_j satisfies the condition $h(P_j) \geq \kappa' + \kappa$, then the next point in the sequence has much smaller height, namely $h(P_{j+1}) \leq \frac{3}{4} h(P_j)$.

N.B. If you start with a number and keep multiplying it by 3/4, it approaches zero. So eventually we will find an index m such that $h(P_m) \leq \kappa' + \kappa$

We have now shown that every element $P \in \Gamma$ can be written in the form:

$$P = a_1 Q_1 + a_2 Q_2 + \cdots + a_n Q_n + 2^m R$$

for certain integers $a_1, \dots, a_n$ and some point $R \in \Gamma$ satisfying the inequality $h(R) \leq \kappa' + \kappa$

Descent Theorem (6/6)

Proof of the Descent Theorem (6/6)

Hence the set

$$\{Q_1, Q_2, \ldots, Q_n\} \cup \{R \in \Gamma : h(R) \leq \kappa' + \kappa\}$$

generates Γ.

Descent Theorem (6/6)

Proof of the Descent Theorem (6/6)

Hence the set

$$\{Q_1, Q_2, \ldots, Q_n\} \cup \{R \in \Gamma : h(R) \leq \kappa' + \kappa\}$$

generates Γ.

From a) and d), this set is finite, which completes the proof that Γ is finitely generated. $\square$

Descent Theorem (6/6)

Proof of the Descent Theorem (6/6)

Hence the set

$$\{Q_1, Q_2, \ldots, Q_n\} \cup \{R \in \Gamma : h(R) \leq \kappa' + \kappa\}$$

generates Γ.

From a) and d), this set is finite, which completes the proof that Γ is finitely generated. $\square$

Remark

This Theorem is called a Descent Theorem as the proof imitates the style of Fermat's method of infinite descent: One starts with an arbitrary point $P \in E(\mathbb{Q})$, and by manipulation descents to a smaller point [in terms of height, of course].

The Height of $P + P_0$ (1/7)

First we recall that if $P = (x, y)$ is a rational point on E, then x and y have the form

$$x = \frac{m}{e^2} \quad \text{and} \quad y = \frac{n}{e^3}$$

for integers m, n, e with $e > 0$ and $\gcd(m, e) = \gcd(n, e) = 1$.
This can be shown by mimicking the steps in the proof of Nagell-Lutz Theorem.

The Height of $P + P_0$ (1/7)

First we recall that if $P = (x, y)$ is a rational point on E, then x and y have the form

$$x = \frac{m}{e^2} \quad \text{and} \quad y = \frac{n}{e^3}$$

for integers m, n, e with $e > 0$ and $\gcd(m, e) = \gcd(n, e) = 1$.
This can be shown by mimicking the steps in the proof of Nagell-Lutz Theorem.

Now suppose we write

$$x = \frac{m}{M} \quad \text{and} \quad y = \frac{n}{N}$$

in lowest terms with $M > 0$ and $N > 0$.

The Height of $P + P_0$ (1/7)

First we recall that if $P = (x, y)$ is a rational point on E, then x and y have the form

$$x = \frac{m}{e^2} \quad \text{and} \quad y = \frac{n}{e^3}$$

for integers m, n, e with $e > 0$ and $\gcd(m, e) = \gcd(n, e) = 1$.
This can be shown by mimicking the steps in the proof of Nagell-Lutz Theorem.

Now suppose we write

$$x = \frac{m}{M} \quad \text{and} \quad y = \frac{n}{N}$$

in lowest terms with $M > 0$ and $N > 0$.

Substituting into the equation (1) of E yields:

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M} + c$$

The Height of $P + P_0$ (1/7)

First we recall that if $P = (x, y)$ is a rational point on E, then x and y have the form

$$x = \frac{m}{e^2} \quad \text{and} \quad y = \frac{n}{e^3}$$

for integers m, n, e with $e > 0$ and $\gcd(m, e) = \gcd(n, e) = 1$.
This can be shown by mimicking the steps in the proof of Nagell-Lutz Theorem.

Now suppose we write

$$x = \frac{m}{M} \quad \text{and} \quad y = \frac{n}{N}$$

in lowest terms with $M > 0$ and $N > 0$.

Substituting into the equation (1) of E yields:

$$\frac{n^2}{N^2} = \frac{m^3}{M^3} + a\frac{m^2}{M^2} + b\frac{m}{M} + c$$

Clearing the denominators gives:

$$M^3 n^2 = N^2 m^3 + aN^2 M m^2 + bN^2 M^2 m + cN^2 M^3 \tag{2}$$

The Height of $P + P_0$ (2/7)

Since N^2 is a factor of all terms on the R.H.S. of (2), it follows that $N^2 | M^3 n^2$. But $\gcd(n, N) = 1$, so $N^2 | M^3$.

The Height of $P + P_0$ (2/7)

Since N^2 is a factor of all terms on the R.H.S. of (2), it follows that $N^2 | M^3 n^2$. But $\gcd(n, N) = 1$, so $N^2 | M^3$.

Conversely, we show $M^3 | N^2$, in three steps:

The Height of $P + P_0$ (2/7)

Since N^2 is a factor of all terms on the R.H.S. of (2), it follows that $N^2 | M^3 n^2$. But $\gcd(n, N) = 1$, so $N^2 | M^3$.

Conversely, we show $M^3 | N^2$, in three steps:

- From (2) we immediately see that $M | N^2 m^3$, and since $\gcd(m, M) = 1$, we find $M | N^2$.

The Height of $P + P_0$ (2/7)

Since N^2 is a factor of all terms on the R.H.S. of (2), it follows that $N^2 | M^3 n^2$. But $\gcd(n, N) = 1$, so $N^2 | M^3$.

Conversely, we show $M^3 | N^2$, in three steps:

- From (2) we immediately see that $M | N^2 m^3$, and since $\gcd(m, M) = 1$, we find $M | N^2$.
- Using the above back to (2), we find $M^2 | N^2 m^3$, so $M | N$.

The Height of $P + P_0$ (2/7)

Since N^2 is a factor of all terms on the R.H.S. of (2), it follows that $N^2 | M^3 n^2$. But $\gcd(n, N) = 1$, so $N^2 | M^3$.

Conversely, we show $M^3 | N^2$, in three steps:

- From (2) we immediately see that $M | N^2 m^3$, and since $\gcd(m, M) = 1$, we find $M | N^2$.
- Using the above back to (2), we find $M^2 | N^2 m^3$, so $M | N$.
- Again by (2), we see that this implies $M^3 | N^2 m^3$, so $M^3 | N^2$.

The Height of $P + P_0$ (2/7)

Since N^2 is a factor of all terms on the R.H.S. of (2), it follows that $N^2|M^3n^2$. But $\gcd(n, N) = 1$, so $N^2|M^3$.

Conversely, we show $M^3|N^2$, in three steps:

- From (2) we immediately see that $M|N^2m^3$, and since $\gcd(m, M) = 1$, we find $M|N^2$.
- Using the above back to (2), we find $M^2|N^2m^3$, so $M|N$.
- Again by (2), we see that this implies $M^3|N^2m^3$, so $M^3|N^2$.

Therefore, $M^3 = N^2$.

Further, during the proof we showed that $M|N$.

The Height of $P + P_0$ (2/7)

Since N^2 is a factor of all terms on the R.H.S. of (2), it follows that $N^2 | M^3 n^2$. But $\gcd(n, N) = 1$, so $N^2 | M^3$.

Conversely, we show $M^3 | N^2$, in three steps:

- From (2) we immediately see that $M | N^2 m^3$, and since $\gcd(m, M) = 1$, we find $M | N^2$.
- Using the above back to (2), we find $M^2 | N^2 m^3$, so $M | N$.
- Again by (2), we see that this implies $M^3 | N^2 m^3$, so $M^3 | N^2$.

Therefore, $M^3 = N^2$.

Further, during the proof we showed that $M | N$.

So if we let $e = \frac{N}{M}$,we find that

$$e^2 = \frac{N^2}{M^2} = \frac{M^3}{M^2} = M, \quad \text{and} \quad e^3 = \frac{N^2}{M^3} = \frac{N^3}{N^2} = N.$$

Therefore $x = \dfrac{m}{e^2}$ and $y = \dfrac{n}{e^3}$ have the desired form.

The Height of $P + P_0$ (3/7)

If the point P is given in lowest terms as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, then $|e^2| \leq H(P)$ and $|m| \leq H(P)$, and we claim there is a constant $K > 0$, depending on a, b, c such that

$$|n| \leq KH(P)^{3/2}$$

The Height of $P + P_0$ (3/7)

If the point P is given in lowest terms as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, then $|e^2| \leq H(P)$ and $|m| \leq H(P)$, and we claim there is a constant $K > 0$, depending on a, b, c such that

$$|n| \leq KH(P)^{3/2}$$

To prove this we just use the fact that the point satisfies the equation: substituting into equation (1) and multiplying by e^6 to clear denominator:

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6$$

The Height of $P + P_0$ (3/7)

If the point P is given in lowest terms as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, then $|e^2| \leq H(P)$ and $|m| \leq H(P)$, and we claim there is a constant $K > 0$, depending on a, b, c such that

$$|n| \leq KH(P)^{3/2}$$

To prove this we just use the fact that the point satisfies the equation: substituting into equation (1) and multiplying by e^6 to clear denominator:

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6$$

Taking the absolute value and using the triangle inequality yields:

$$\begin{aligned} |n^2| &\leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6| \\ &\leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3 \end{aligned}$$

So we can take $K = \sqrt{1 + |a| + |b| + |c|}$

The Height of $P + P_0$ (3/7)

If the point P is given in lowest terms as $P = \left(\frac{m}{e^2}, \frac{n}{e^3}\right)$, then $|e^2| \leq H(P)$ and $|m| \leq H(P)$, and we claim there is a constant $K > 0$, depending on a, b, c such that

$$|n| \leq KH(P)^{3/2}$$

To prove this we just use the fact that the point satisfies the equation: substituting into equation (1) and multiplying by e^6 to clear denominator:

$$n^2 = m^3 + ae^2m^2 + be^4m + ce^6$$

Taking the absolute value and using the triangle inequality yields:

$$\begin{aligned} |n^2| &\leq |m^3| + |ae^2m^2| + |be^4m| + |ce^6| \\ &\leq H(P)^3 + |a|H(P)^3 + |b|H(P)^3 + |c|H(P)^3 \end{aligned}$$

So we can take $K = \sqrt{1 + |a| + |b| + |c|}$

Now we are ready to have Slice 2.

The Height of $P + P_0$ (4/7)

Slice 2

For P_0 a fixed rational point on E, there is a constant κ_0, depending on P_0 and on a, b, c such that $h(P + P_0) \leq 2h(P) + \kappa_0$ for all $P \in E(\mathbb{Q})$

The Height of $P + P_0$ (4/7)

Slice 2

For P_0 a fixed rational point on E, there is a constant κ_0, depending on P_0 and on a, b, c such that $h(P + P_0) \leq 2h(P) + \kappa_0$ for all $P \in E(\mathbb{Q})$

Serving Slice 2 (1/4)

First we remark that if $P_0 = \mathcal{O}$, the slice is trivial.
So we take $P_0 \neq \mathcal{O}$, say $P_0 = (x_0, y_0)$.

The Height of $P + P_0$ (4/7)

Slice 2

For P_0 a fixed rational point on E, there is a constant κ_0, depending on P_0 and on a, b, c such that $h(P + P_0) \leq 2h(P) + \kappa_0$ for all $P \in E(\mathbb{Q})$

Serving Slice 2 (1/4)

First we remark that if $P_0 = \mathcal{O}$, the slice is trivial.
So we take $P_0 \neq \mathcal{O}$, say $P_0 = (x_0, y_0)$.

To prove the existence of κ_0, it suffices to prove that the inequality holds for all P except those in a some fixed set; this holds because, for any finite number of P, we just looking at the difference $h(P + P_0) - 2h(P)$ and take κ_0 larger than the finite number of values that occur. Hence, it suffices to prove for all points P with $P \notin \{P_0, -P_0, \mathcal{O}\}$.

The Height of $P + P_0$ (4/7)

Slice 2

For P_0 a fixed rational point on E, there is a constant κ_0, depending on P_0 and on a, b, c such that $h(P + P_0) \leq 2h(P) + \kappa_0$ for all $P \in E(\mathbb{Q})$

Serving Slice 2 (1/4)

First we remark that if $P_0 = \mathcal{O}$, the slice is trivial.
So we take $P_0 \neq \mathcal{O}$, say $P_0 = (x_0, y_0)$.

To prove the existence of κ_0, it suffices to prove that the inequality holds for all P except those in a some fixed set; this holds because, for any finite number of P, we just looking at the difference $h(P + P_0) - 2h(P)$ and take κ_0 larger than the finite number of values that occur. Hence, it suffices to prove for all points P with $P \notin \{P_0, -P_0, \mathcal{O}\}$.

We write $P = (x, y)$, the reason for avoiding both P_0 and $-P_0$ is to have $x \neq x_0$.

We also denote

$$P + P_0 = (\xi, \eta)$$

The Height of $P + P_0$ (5/7)

Serving Slice 2 (2/4)

Now $H(P + P_0) = \xi$, so we need a formula for ξ in terms of (x, y) and (x_0, y_0):

$$\xi + x + x_0 = \lambda^2 - a, \qquad \lambda = \frac{y - y_0}{x - x_0}.$$

The Height of $P + P_0$ (5/7)

Serving Slice 2 (2/4)

Now $H(P + P_0) = \xi$, so we need a formula for ξ in terms of (x, y) and (x_0, y_0):

$$\xi + x + x_0 = \lambda^2 - a, \qquad \lambda = \frac{y - y_0}{x - x_0}.$$

After writing out this a little bit:

$$\begin{aligned} \xi &= \frac{(y - y_0)^2}{(x - x_0)^2} - a - x - x_0 \\ &= \frac{(y - y_0)^2 - (x - x_0)^2(x + x_0 + a)}{(x - x_0)^2} \end{aligned}$$

The Height of $P + P_0$ (5/7)

Serving Slice 2 (2/4)

Now $H(P + P_0) = \xi$, so we need a formula for ξ in terms of (x, y) and (x_0, y_0):

$$\xi + x + x_0 = \lambda^2 - a, \qquad \lambda = \frac{y - y_0}{x - x_0}.$$

After writing out this a little bit:

$$\begin{aligned}
\xi &= \frac{(y - y_0)^2}{(x - x_0)^2} - a - x - x_0 \\
&= \frac{(y - y_0)^2 - (x - x_0)^2(x + x_0 + a)}{(x - x_0)^2} \\
&= \frac{Ay + Bx^2 + Cx + D}{Ex^2 + Fx + G}
\end{aligned}$$

where A, B, C, D, E, F, G are certain rational numbers which can be expressed in terms of a, b, c and (x_0, y_0).

The Height of $P + P_0$ (6/7)

Serving Slice 2 (3/4)

Further, we are able to multiply the numerator and denominator by the l.c.d. of $A, \ldots, G$, and hence we may assume that $A, \ldots, G \in \mathbb{Z}$, which depend only on a, b, c and (x_0, y_0), After substituting $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ and clearing out the denominators by multiplying the numerator and denominator by e^4, we find:

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}$$

The Height of $P + P_0$ (6/7)

Serving Slice 2 (3/4)

Further, we are able to multiply the numerator and denominator by the l.c.d. of $A, \ldots, G$, and hence we may assume that $A, \ldots, G \in \mathbb{Z}$, which depend only on a, b, c and (x_0, y_0), After substituting $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ and clearing out the denominators by multiplying the numerator and denominator by e^4, we find:

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}$$

Notice we have an expression for ξ as an integer divided by an integer: although we are uncertain that it is in the lowest terms, but cancellation will only make the height smaller:

$$H(\xi) \leq \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}$$

The Height of $P + P_0$ (6/7)

Serving Slice 2 (3/4)

Further, we are able to multiply the numerator and denominator by the l.c.d. of $A, \ldots, G$, and hence we may assume that $A, \ldots, G \in \mathbb{Z}$, which depend only on a, b, c and (x_0, y_0), After substituting $x = \frac{m}{e^2}$ and $y = \frac{n}{e^3}$ and clearing out the denominators by multiplying the numerator and denominator by e^4, we find:

$$\xi = \frac{Ane + Bm^2 + Cme^2 + De^4}{Em^2 + Fme^2 + Ge^4}$$

Notice we have an expression for ξ as an integer divided by an integer: although we are uncertain that it is in the lowest terms, but cancellation will only make the height smaller:

$$H(\xi) \leq \max\{|Ane + Bm^2 + Cme^2 + De^4|, |Em^2 + Fme^2 + Ge^4|\}$$

Further, from above we have the estimates

$$e \leq H(P)^{1/2}, \quad n \leq KH(P)^{3/2}, \quad m \leq H(P)$$

where K depends on only a, b, c.

The Height of $P + P_0$ (7/7)

Serving Slice 2 (4/4)

Using the above and triangle inequality gives

$$\begin{aligned}
|Ane + Bm^2 + Cme^2 + De^4| &\leq |Ane| + |Bm^2| + |Cme^2| + |De^4| \\
&\leq (|AK| + |B| + |C| + |D|)H(P)^2 \\
|Em^2 + Fme^2 + Ge^4| &\leq |Em^2| + |Fme^2| + |Ge^4| \\
&\leq (|E| + |F| + |G|)H(P)^2
\end{aligned}$$

The Height of $P + P_0$ (7/7)

Serving Slice 2 (4/4)

Using the above and triangle inequality gives

$$\begin{aligned} |Ane + Bm^2 + Cme^2 + De^4| &\leq |Ane| + |Bm^2| + |Cme^2| + |De^4| \\ &\leq (|AK| + |B| + |C| + |D|)H(P)^2 \\ |Em^2 + Fme^2 + Ge^4| &\leq |Em^2| + |Fme^2| + |Ge^4| \\ &\leq (|E| + |F| + |G|)H(P)^2 \end{aligned}$$

It follows

$$H(P + P_0) = H(\xi) \leq \max\{|AK| + |B| + |C| + |D|,\ \ |E| + |F| + |G|\}H(P)^2$$

The Height of $P + P_0$ (7/7)

Serving Slice 2 (4/4)

Using the above and triangle inequality gives

$$\begin{aligned}
|Ane + Bm^2 + Cme^2 + De^4| &\leq |Ane| + |Bm^2| + |Cme^2| + |De^4| \\
&\leq (|AK| + |B| + |C| + |D|)H(P)^2 \\
|Em^2 + Fme^2 + Ge^4| &\leq |Em^2| + |Fme^2| + |Ge^4| \\
&\leq (|E| + |F| + |G|)H(P)^2
\end{aligned}$$

It follows

$$H(P + P_0) = H(\xi) \leq \max\{|AK| + |B| + |C| + |D|,\ \ |E| + |F| + |G|\}H(P)^2$$

Taking the logarithm of both sides yields

$$h(P + P_0) \leq 2h(P) + \kappa_0$$

where the constant $\kappa_0 = \log \max\{|AK| + |B| + |C| + |D|,\ \ |E| + |F| + |G|\}$ depends only on a, b, c and (x_0, y_0) and does NOT depend on $P = (x, y)$. $\square$

The Height of $2P$ (1/10)

Slice 3

There is a constant κ, depending on a, b, c so that

$$h(2P) \geq 4h(P) - \kappa \quad \text{for all} \;\; P \in E(\mathbb{Q})$$

The Height of $2P$ (1/10)

Slice 3

There is a constant κ, depending on a, b, c so that

$$h(2P) \geq 4h(P) - \kappa \quad \text{for all } \ P \in E(\mathbb{Q})$$

Serving Slice 3 (1/2)

Mimicking the Serving of Slice 2, we ignore the finite set of points satisfying $2P = \mathcal{O}$ since we can always take κ larger than $4h(P)$ for all points in that finite set.

The Height of $2P$ (1/10)

Slice 3

There is a constant κ, depending on a, b, c so that

$$h(2P) \geq 4h(P) - \kappa \quad \text{for all} \;\; P \in E(\mathbb{Q})$$

Serving Slice 3 (1/2)

Mimicking the Serving of Slice 2, we ignore the finite set of points satisfying $2P = \mathcal{O}$ since we can always take κ larger than $4h(P)$ for all points in that finite set.

Let $P = (x, y)$ and write $2P = (\xi, \eta)$.
The duplication formula we derived earlier states that

$$\xi + 2x = \lambda^2 - a, \qquad \text{where} \;\; \lambda = \frac{f'(x)}{2y}$$

The Height of $2P$ (2/10)

Serving Slice 3 (2/2)

Using $y^2 = f(x)$, we obtain an explicit formula for ξ in terms of x :

$$\xi = \frac{(f'(x))^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 + \cdots}{4x^3 + \cdots}$$

Note that $f(x) \neq 0$ because $2P \neq \mathcal{O}$.

The Height of $2P$ (2/10)

Serving Slice 3 (2/2)

Using $y^2 = f(x)$, we obtain an explicit formula for ξ in terms of x :

$$\xi = \frac{(f'(x))^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 + \cdots}{4x^3 + \cdots}$$

Note that $f(x) \neq 0$ because $2P \neq \mathcal{O}$.

Thus, ξ is the quotient of two polynomials in x with integer coefficients. Since the cubic $y^2 = f(x)$ is non-singular by assumption, we know that $f(x)$ and $f'(x)$ have NO common (complex) roots, and thus the polynomials in the numerator and the denominator of ξ also have NO common roots.

The Height of $2P$ (2/10)

Serving Slice 3 (2/2)

Using $y^2 = f(x)$, we obtain an explicit formula for ξ in terms of x :

$$\xi = \frac{(f'(x))^2 - (8x + 4a)f(x)}{4f(x)} = \frac{x^4 + \cdots}{4x^3 + \cdots}$$

Note that $f(x) \neq 0$ because $2P \neq \mathcal{O}$.

Thus, ξ is the quotient of two polynomials in x with integer coefficients. Since the cubic $y^2 = f(x)$ is non-singular by assumption, we know that $f(x)$ and $f'(x)$ have NO common (complex) roots, and thus the polynomials in the numerator and the denominator of ξ also have NO common roots.

Since $h(P) = h(x)$ and $h(2P) = h(\xi)$, we are trying to prove that

$$h(\xi) \geq 4h(x) - \kappa$$

Hence we reduced our task to proving the following slice about heights and quotients of polynomials:

The Height of $2P$ (3/10)

Slice $3i$

Let $\phi(X)$ and $\psi(X)$ be polynomials with integer coefficients and NO common (complex) roots. Let $d = \max\{\deg(\phi), \deg(\psi)\}$

a) There is an integer $R \geq 1$, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$,

$$\gcd\left(n^d\phi\Big(\frac{m}{n}\Big), n^d\psi\Big(\frac{m}{n}\Big)\right) \quad \text{divides } \ R$$

b) There are constants κ_1 and κ_2, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$ which are NOT roots of ψ,

$$dh\Big(\frac{m}{n}\Big) - \kappa_1 \leq h\Big(\frac{\phi(m/n)}{\psi(m/n)}\Big) \leq dh\Big(\frac{m}{n}\Big) + \kappa_2$$

The Height of $2P$ (3/10)

Slice $3i$

Let $\phi(X)$ and $\psi(X)$ be polynomials with integer coefficients and NO common (complex) roots. Let $d = \max\{\deg(\phi), \deg(\psi)\}$

a) There is an integer $R \geq 1$, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$,

$$\gcd\left(n^d\phi\left(\frac{m}{n}\right), n^d\psi\left(\frac{m}{n}\right)\right) \quad \text{divides} \;\; R$$

b) There are constants κ_1 and κ_2, depending on ϕ and ψ, so that for all rational numbers $\frac{m}{n}$ which are NOT roots of ψ,

$$dh\left(\frac{m}{n}\right) - \kappa_1 \leq h\left(\frac{\phi(m/n)}{\psi(m/n)}\right) \leq dh\left(\frac{m}{n}\right) + \kappa_2$$

Serving Slice $3i$ (1/8)

a) First we observe that since ϕ and ψ have degree at most d, both $n^d\phi\left(\frac{m}{n}\right)$ and $n^d\psi\left(\frac{m}{n}\right)$ are integers, so their g.c.d. makes sense.

The Height of $2P$ (4/10)

Serving Slice $3i$ (2/8)

Next we note that ϕ and ψ are interchangeable, so for correctness, we will take $\deg(\phi) := d$ and $\deg(\psi) := e \leq d$.

The Height of $2P$ (4/10)

Serving Slice $3i$ (2/8)

Next we note that ϕ and ψ are interchangeable, so for correctness, we will take deg(ϕ) $:= d$ and deg(ψ)$:= e \leq d$.

Then we can write:

$$\Phi(m,n) := n^d \phi\Big(\frac{m}{n}\Big) = a_0 m^d + a_1 m^{d-1} + \cdots + a_d n^d,$$
$$\Psi(m,n) := n^d \psi\Big(\frac{m}{n}\Big) = b_0 m^e n^{d-e} + b_1 m^{e-1} n^{d-n+1} + \cdots + b_e n^d$$

So we need to find an estimate for $\gcd(\Phi(m,n), \Psi(m,n))$ which does NOT depend on m OR n.

The Height of $2P$ (4/10)

Serving Slice $3i$ (2/8)

Next we note that ϕ and ψ are interchangeable, so for correctness, we will take deg(ϕ) $:= d$ and deg(ψ)$:=e \leq d$.

Then we can write:

$$\Phi(m,n) := n^d \phi\Big(\frac{m}{n}\Big) = a_0 m^d + a_1 m^{d-1} + \cdots + a_d n^d,$$
$$\Psi(m,n) := n^d \psi\Big(\frac{m}{n}\Big) = b_0 m^e n^{d-e} + b_1 m^{e-1} n^{d-n+1} + \cdots + b_e n^d$$

So we need to find an estimate for $\gcd(\Phi(m,n), \Psi(m,n))$ which does NOT depend on m OR n.

Since $\phi(X)$ and $\psi(X)$ have NO common roots, they are relative prime in the Euclidean ring $\mathbb{Q}[X]$, so they generate the unit ideal:

The Height of $2P$ (4/10)

Serving Slice $3i$ (2/8)

Next we note that ϕ and ψ are interchangeable, so for correctness, we will take deg(ϕ) $:= d$ and deg(ψ)$:=e \leq d$.

Then we can write:

$$\Phi(m,n) := n^d \phi\left(\frac{m}{n}\right) = a_0 m^d + a_1 m^{d-1} + \cdots + a_d n^d,$$
$$\Psi(m,n) := n^d \psi\left(\frac{m}{n}\right) = b_0 m^e n^{d-e} + b_1 m^{e-1} n^{d-n+1} + \cdots + b_e n^d$$

So we need to find an estimate for $\gcd(\Phi(m,n), \Psi(m,n))$ which does NOT depend on m OR n.

Since $\phi(X)$ and $\psi(X)$ have NO common roots, they are relative prime in the Euclidean ring $\mathbb{Q}[X]$, so they generate the unit ideal:

So we can find polynomials $F(X)$ and $G(X)$ with rational coefficients satisfying

$$F(X)\phi(X) + G(X)\psi(X) = 1 \tag{3}$$

The Height of $2P$ (5/10)

Servicing Slice $3i$ (3/8)

Now let A be a large enough integer so that $AF(X)$ and $AG(X)$ have integer coefficients, and let $D = \max\{\deg(F), \deg(G)\}$.
N.B. A and D do NOT depend on m or n.

The Height of $2P$ (5/10)

Servicing Slice $3i$ (3/8)

Now let A be a large enough integer so that $AF(X)$ and $AG(X)$ have integer coefficients, and let $D = \max\{\deg(F), \deg(G)\}$.
N.B. A and D do NOT depend on m or n.

Now we evaluate the identity (3) at $X = \frac{m}{n}$ and multiply both sides by An^{D+d}.

$$n^D AF\Big(\frac{m}{n}\Big) \cdot n^d \phi\Big(\frac{m}{n}\Big) + n^D AG\Big(\frac{m}{n}\Big) \cdot n^d \psi\Big(\frac{m}{n}\Big) = An^{D+d}$$

The Height of $2P$ (5/10)

Servicing Slice $3i$ (3/8)

Now let A be a large enough integer so that $AF(X)$ and $AG(X)$ have integer coefficients, and let $D = \max\{\deg(F), \deg(G)\}$.
N.B. A and D do NOT depend on m or n.

Now we evaluate the identity (3) at $X = \frac{m}{n}$ and multiply both sides by An^{D+d}.

$$n^D AF\Big(\frac{m}{n}\Big) \cdot n^d \phi\Big(\frac{m}{n}\Big) + n^D AG\Big(\frac{m}{n}\Big) \cdot n^d \psi\Big(\frac{m}{n}\Big) = An^{D+d}$$

Let $\gamma = \gamma(m,n) := \gcd\Big(\Phi(m,n), \Psi(m,n)\Big)$

We have:

$$\Big\{n^D AF\Big(\frac{m}{n}\Big)\Big\}\Phi(m,n) + \Big\{n^D AG\Big(\frac{m}{n}\Big)\Big\}\Psi(m,n) = An^{D+d}$$

Since the quantities in braces are integers, we see that $\gamma | An^{D+d}$

The Height of $2P$ (6/10)

Serving Slice $3i$ (4/8)

We also need to show $\gamma | Aa_0^{D+d}$, where a_0 is the leading coefficient of $\phi(X)$. We observe that since γ divides $\Phi(m,n)$, it certainly divides:

$$An^{D+d-1}\Phi(m,n) = Aa_0 m^d n^{D+d-1} + Aa_1 m^{d-1} n^{D+d} + \cdots + Aa_d n^{D+2d-1}.$$

The Height of $2P$ (6/10)

Serving Slice $3i$ (4/8)

We also need to show $\gamma | Aa_0^{D+d}$, where a_0 is the leading coefficient of $\phi(X)$. We observe that since γ divides $\Phi(m,n)$, it certainly divides:

$$An^{D+d-1}\Phi(m,n) = Aa_0 m^d n^{D+d-1} + Aa_1 m^{d-1} n^{D+d} + \cdots + Aa_d n^{D+2d-1}.$$

But in the sum, every term after the first one contains An^{D+d} as a factor; and we just proved that γ divides An^{D+d}.

The Height of $2P$ (6/10)

Serving Slice 3i (4/8)

We also need to show $\gamma | A a_0^{D+d}$, where a_0 is the leading coefficient of $\phi(X)$. We observe that since γ divides $\Phi(m,n)$, it certainly divides:

$$An^{D+d-1}\Phi(m,n) = Aa_0 m^d n^{D+d-1} + Aa_1 m^{d-1} n^{D+d} + \cdots + Aa_d n^{D+2d-1}.$$

But in the sum, every term after the first one contains An^{D+d} as a factor; and we just proved that γ divides An^{D+d}.

It follows that γ also divides the first term $Aa_0 m^d n^{D+d-1}$. Thus, γ divides $\gcd(An^{D+d}, Aa_0 m^d n^{D+d-1})$; and because $(m,n)=1$, we conclude that γ divides $Aa_0 n^{D+d-1}$

The Height of $2P$ (6/10)

Serving Slice $3i$ (4/8)

We also need to show $\gamma | Aa_0^{D+d}$, where a_0 is the leading coefficient of $\phi(X)$. We observe that since γ divides $\Phi(m,n)$, it certainly divides:

$$An^{D+d-1}\Phi(m,n) = Aa_0m^dn^{D+d-1} + Aa_1m^{d-1}n^{D+d} + \cdots + Aa_dn^{D+2d-1}.$$

But in the sum, every term after the first one contains An^{D+d} as a factor; and we just proved that γ divides An^{D+d}.

It follows that γ also divides the first term $Aa_0m^dn^{D+d-1}$. Thus, γ divides $\gcd(An^{D+d}, Aa_0m^dn^{D+d-1})$; and because $(m,n) = 1$, we conclude that γ divides Aa_0n^{D+d-1}

Now using the fact that γ divides $Aa_0n^{D+d-2}\Phi(m,n)$ and repeating the above argument shows that γ divides $Aa_0^2n^{D+d-2}$; eventually, we reach the conclusion that γ divides Aa_0^{D+d}, finishing the serving of a).

The Height of $2P$ (7/10)

Serving Slice $3i$ (5/8)

b) Two inequalities to be proven:

- The upper bound is similar to Slice 2 so it is left as an exercise.
- For the lower bound: as usual, we are cool to exclude some finite set of rational numbers when we prove prove the inequality of this sort: so we assume that the rational number $\frac{m}{n}$ is NOT a root of ϕ.

The Height of $2P$ (7/10)

Serving Slice $3i$ (5/8)

b) Two inequalities to be proven:

- The upper bound is similar to Slice 2 so it is left as an exercise.
- For the lower bound: as usual, we are cool to exclude some finite set of rational numbers when we prove prove the inequality of this sort: so we assume that the rational number $\frac{m}{n}$ is NOT a root of ϕ.

For $0 \neq r \in \mathbb{Q}$, it is clear from the definition that $h(r) = h\left(\frac{1}{r}\right)$. So reverting the role of ϕ and ψ if necessary, we may assume that $\deg(\phi) = d$ and $\deg(\psi) = e$ with $e \leq d$.

The Height of $2P$ (7/10)

Serving Slice $3i$ (5/8)

b) Two inequalities to be proven:
- The upper bound is similar to Slice 2 so it is left as an exercise.
- For the lower bound: as usual, we are cool to exclude some finite set of rational numbers when we prove prove the inequality of this sort: so we assume that the rational number $\frac{m}{n}$ is NOT a root of ϕ.

For $0 \neq r \in \mathbb{Q}$, it is clear from the definition that $h(r) = h\Big(\frac{1}{r}\Big)$. So reverting the role of ϕ and ψ if necessary, we may assume that $\deg(\phi) = d$ and $\deg(\psi) = e$ with $e \leq d$.

Continuing from a), the rational number whose height we want to estimate is

$$\xi = \frac{\phi\left(\frac{m}{n}\right)}{\psi\left(\frac{m}{n}\right)} = \frac{n^d\phi\left(\frac{m}{n}\right)}{n^d\psi\left(\frac{m}{n}\right)} = \frac{\Phi(m,n)}{\Psi(m,n)}$$

except when $|\Phi(m,n)|$ and $|\Psi(m,n)|$ have common factors.

The Height of $2P$ (8/10)

Serving Slice $3i$ (6/8)

We showed in a) that there is some $R \geq 1$, independent of m and n, so that the g.c.d. of $\Phi(m,n)$ and $\Psi(m,n)$ divides R.

The Height of $2P$ (8/10)

Serving Slice $3i$ (6/8)

We showed in a) that there is some $R \geq 1$, independent of m and n, so that the g.c.d. of $\Phi(m,n)$ and $\Psi(m,n)$ divides R.

This bounds the possible cancellation, and we find that

$$\begin{aligned} H(\xi) &\geq \frac{1}{R} \max\{|\Phi(m,n)|, |\Psi(m,n)|\} \\ &= \frac{1}{R} \max\left\{\left|n^d \phi\left(\frac{m}{n}\right)\right|, \left|n^d \psi\left(\frac{m}{n}\right)\right|\right\} \\ &\geq \frac{1}{2R}\left(\left|n^d \phi\left(\frac{m}{n}\right)\right| + \left|n^d \psi\left(\frac{m}{n}\right)\right|\right) \end{aligned}$$

The Height of $2P$ (8/10)

Serving Slice $3i$ (6/8)

We showed in a) that there is some $R \geq 1$, independent of m and n, so that the g.c.d. of $\Phi(m,n)$ and $\Psi(m,n)$ divides R.

This bounds the possible cancellation, and we find that

$$\begin{aligned} H(\xi) &\geq \frac{1}{R} \max\{|\Phi(m,n)|, |\Psi(m,n)|\} \\ &= \frac{1}{R} \max\left\{\left|n^d \phi\left(\frac{m}{n}\right)\right|, \left|n^d \psi\left(\frac{m}{n}\right)\right|\right\} \\ &\geq \frac{1}{2R}\left(\left|n^d \phi\left(\frac{m}{n}\right)\right| + \left|n^d \psi\left(\frac{m}{n}\right)\right|\right) \end{aligned}$$

In terms of multiplicative notation, we want to compare $H(\xi)$ to $H\left(\frac{m}{n}\right)^d = \max\{|m|^d, |n|^d\}$, so we consider the quotient:

The Height of $2P$ (9/10)

Serving Slice $3i$ (7/8)

$$
\begin{aligned}
\frac{H(\xi)}{H(m/n)^d} &\geq \frac{1}{2R} \cdot \frac{\left(\left|n^d \phi\left(\frac{m}{n}\right)\right| + \left|n^d \psi\left(\frac{m}{n}\right)\right|\right)}{\max\{|m|^d, |n|^d\}} \\
&= \frac{1}{2R} \cdot \frac{\left(\left|\phi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|\right)}{\max\left\{\left|\frac{m}{n}\right|^d, 1\right\}}
\end{aligned}
$$

The Height of $2P$ (9/10)

Serving Slice $3i$ (7/8)

$$\frac{H(\xi)}{H(m/n)^d} \geq \frac{1}{2R} \cdot \frac{\left(\left|n^d\phi\left(\frac{m}{n}\right)\right| + \left|n^d\psi\left(\frac{m}{n}\right)\right|\right)}{\max\{|m|^d, |n|^d\}}$$

$$= \frac{1}{2R} \cdot \frac{\left(\left|\phi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|\right)}{\max\left\{\left|\frac{m}{n}\right|^d, 1\right\}}$$

This suggests that we look at the function p of a real variable t defined by

$$p(t) = \frac{\left|\phi(t)\right| + \left|\psi(t)\right|}{\max\left\{|t|^d, 1\right\}}$$

The Height of $2P$ (9/10)

Serving Slice $3i$ (7/8)

$$\frac{H(\xi)}{H(m/n)^d} \geq \frac{1}{2R} \cdot \frac{\left(\left|n^d \phi\left(\frac{m}{n}\right)\right| + \left|n^d \psi\left(\frac{m}{n}\right)\right|\right)}{\max\{|m|^d, |n|^d\}}$$

$$= \frac{1}{2R} \cdot \frac{\left(\left|\phi\left(\frac{m}{n}\right)\right| + \left|\psi\left(\frac{m}{n}\right)\right|\right)}{\max\left\{\left|\frac{m}{n}\right|^d, 1\right\}}$$

This suggests that we look at the function p of a real variable t defined by

$$p(t) = \frac{\left|\phi(t)\right| + \left|\psi(t)\right|}{\max\left\{|t|^d, 1\right\}}$$

Since $\max\{\deg(\phi), \deg(\psi)\} \leq d$, we see that $\lim_{|t|\to\infty} p(t) \neq 0$ and

$$\lim_{|t|\to\infty} p(t) = \begin{cases} |a_0| & \text{if } \deg(\phi) < d \\ |a_0| + |b_0| & \text{if } \deg(\phi) = d \end{cases}$$

The Height of $2P$ (10/10)

Serving Slice $3i$ (8/8)

So there is a constant $C > 0$ so that $p(t) > C$ for all $t \in \mathbb{R}$

Use the fact in the inequality we derived above, we find that

$$H(\xi) \geq \frac{C}{2R} H\left(\frac{m}{n}\right)^{d}$$

The Height of $2P$ (10/10)

Serving Slice $3i$ (8/8)

So there is a constant $C > 0$ so that $p(t) > C$ for all $t \in \mathbb{R}$

Use the fact in the inequality we derived above, we find that

$$H(\xi) \geq \frac{C}{2R} H\left(\frac{m}{n}\right)^d$$

Finally we see that the constants C and R do NOT depend on m and n, so taking logarithms gives the desired inequality:

$h(\xi) \geq dh\left(\frac{m}{n}\right) - \kappa_1$ with $\kappa_1 = \log(2R/C)$. $\square$

The Height of $2P$ (10/10)

Serving Slice $3i$ (8/8)

So there is a constant $C > 0$ so that $p(t) > C$ for all $t \in \mathbb{R}$

Use the fact in the inequality we derived above, we find that

$$H(\xi) \geq \frac{C}{2R} H\left(\frac{m}{n}\right)^d$$

Finally we see that the constants C and R do NOT depend on m and n, so taking logarithms gives the desired inequality:

$h(\xi) \geq dh\left(\frac{m}{n}\right) - \kappa_1$ with $\kappa_1 = \log(2R/C)$. □

Remarks

Notice that there are two ideas in the above proof:
1) to bound the amount of cancellation;
2) to look at $\frac{H(\phi(x)/\psi(x))}{H(x)^d}$ as a function on something compact.

Summary

Today we initiated the proof of Modrell's Theorem by partitioning the π into four slices, picked up the definition of heights on the road, and proved the Descend Theorem which connects the π to Modrell.

Summary

Today we initiated the proof of Modrell's Theorem by partitioning the π into four slices, picked up the definition of heights on the road, and proved the Descend Theorem which connects the π to Modrell.

Slice 1

For every $M \in \mathbb{R}$, the set $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ is finite.

Summary

Today we initiated the proof of Modrell's Theorem by partitioning the π into four slices, picked up the definition of heights on the road, and proved the Descend Theorem which connects the π to Modrell.

Slice 1

For every $M \in \mathbb{R}$, the set $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ is finite.

Slice 2

Let $P_0 \in \mathbb{Q}$ on E be fixed, then there exists a constant κ_0 depending on P_0 and a, b, c such that $h(P + P_0) < 2h(P) + \kappa_0$ for all $P \in E(\mathbb{Q})$.

Summary

Today we initiated the proof of Modrell's Theorem by partitioning the π into four slices, picked up the definition of heights on the road, and proved the Descend Theorem which connects the π to Modrell.

Slice 1

For every $M \in \mathbb{R}$, the set $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ is finite.

Slice 2

Let $P_0 \in \mathbb{Q}$ on E be fixed, then there exists a constant κ_0 depending on P_0 and a, b, c such that $h(P + P_0) < 2h(P) + \kappa_0$ for all $P \in E(\mathbb{Q})$.

Slice 3

There is a constant κ, depending on a, b, c so that $h(2P) \geq 4h(P) - \kappa$ for all $P \in E(\mathbb{Q})$.

Summary

Today we initiated the proof of Modrell's Theorem by partitioning the π into four slices, picked up the definition of heights on the road, and proved the Descend Theorem which connects the π to Modrell.

Slice 1

For every $M \in \mathbb{R}$, the set $\{P \in E(\mathbb{Q}) : h(P) \leq M\}$ is finite.

Slice 2

Let $P_0 \in \mathbb{Q}$ on E be fixed, then there exists a constant κ_0 depending on P_0 and a, b, c such that $h(P + P_0) < 2h(P) + \kappa_0$ for all $P \in E(\mathbb{Q})$.

Slice 3

There is a constant κ, depending on a, b, c so that $h(2P) \geq 4h(P) - \kappa$ for all $P \in E(\mathbb{Q})$.

Slice 4 (SPOILER)

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