Torsion, Rank and Integer Points on Elliptic Curves

Gary Walsh, University of Ottawa

June 2011

Overview

0. Introductory Remarks

Overview

0. Introductory Remarks

I. Torsion

Overview

0. Introductory Remarks

I. Torsion

II. Rank

Overview

0. Introductory Remarks

I. Torsion

II. Rank

III. Integer Points

Generalities

An *elliptic curve defined over* $\mathbb{Q}$:

Generalities

An *elliptic curve defined over* $\mathbb{Q}$:

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

$A, B \in \mathbb{Z}$, $x^3 + Ax + B$ has only simple roots.

(short Weierstrass model)

Other Models of Elliptic Curves

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
(general Weierstrass equation)

Other Models of Elliptic Curves

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
(general Weierstrass equation)

$ax^3 + by^3 = c$ (general taxicab equation)

Other Models of Elliptic Curves

$y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$
(general Weierstrass equation)

$ax^3 + by^3 = c$ (general taxicab equation)

$aX^4 - bY^2 = c$ (quartic equations)

Other Models of Elliptic Curves

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
(general Weierstrass equation)

$ax^3 + by^3 = c$ (general taxicab equation)

$aX^4 - bY^2 = c$ (quartic equations)

$ax^2 - by^2 = c, dx^2 - ez^2 = f$
(simultaneous Pell equations)

Other Models of Elliptic Curves

$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6$
(general Weierstrass equation)

$ax^3 + by^3 = c$ (general taxicab equation)

$aX^4 - bY^2 = c$ (quartic equations)

$ax^2 - by^2 = c, dx^2 - ez^2 = f$
(simultaneous Pell equations)

$x^2 + y^2 = c^2(1 + dx^2y^2)$ (Edwards Curves)

$F(x, y) = 0$ ($F = 0$ is a curve of genus 1)

Primary Objects of Study

$E(\mathbb{Q}) = \{(x, y) \in (Q)^2; y^2 = x^3 + Ax + B\} \bigcup \{\infty\}$,

the group of rational points on E.

Primary Objects of Study

$\bullet E(\mathbb{Q}) = \{(x, y) \in Q^2; y^2 = x^3 + Ax + B\} \cup \{\infty\}$, the group of rational points on E.

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r.$$

Primary Objects of Study

• $E(\mathbb{Q}) = \{(x, y) \in Q^2; y^2 = x^3 + Ax + B\} \cup \{\infty\}$, the group of rational points on E.

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r.$$

T is the *torsion subgroup* of $E(\mathbb{Q})$, consisting of the points on E of finite order, and $r = Rank(E)$.

Primary Objects of Study

$\bullet E(\mathbb{Q}) = \{(x, y) \in Q^2; y^2 = x^3 + Ax + B\} \cup \{\infty\}$, the group of rational points on E.

$$E(\mathbb{Q}) \cong T \oplus \mathbb{Z}^r.$$

T is the *torsion subgroup* of $E(\mathbb{Q})$, consisting of the points on E of finite order, and $r = Rank(E)$.

$\bullet E(\mathbb{Z}) = \{(x, y) \in \mathbb{Z}^2; F(x, y) = 0\}$,

where $F(x, y) = 0$ is a curve of genus 1.

Effective Results

Wishlist:

Effective Results

Wishlist:

Torsion: description of all possible groups, an algorithm to compute torsion, specific values for families of curves

Effective Results

Wishlist:

Torsion: description of all possible groups, an algorithm to compute torsion, specific values for families of curves

Rank: finiteness, boundedness, upper bounds, computational algorithm, connection to L-functions (BSD)

Effective Results

Wishlist:

Torsion: description of all possible groups, an algorithm to compute torsion, specific values for families of curves

Rank: finiteness, boundedness, upper bounds, computational algorithm, connection to L-functions (BSD)

Integral Points: finiteness, upper bounds, algorithm to compute all points, specific results for families of curves

I.1 Torsion - group structure

I.1 Torsion - group structure

Mazur's Theorem

I.1 Torsion - group structure

Mazur's Theorem

Let E be an elliptic curve defined over $\mathbb{Q}$, and let T denote the subgroup of $E(\mathbb{Q})$ consisting of the points of finite order.

Then T has one of the following two forms

I.1 Torsion - group structure

Mazur's Theorem

Let E be an elliptic curve defined over $\mathbb{Q}$, and let T denote the subgroup of $E(\mathbb{Q})$ consisting of the points of finite order.

Then T has one of the following two forms

i. A cyclic group of order N with $1 \leq N \leq 10$ or $N = 12$.

ii. The product of a cyclic group of order 2 and a cyclic group of order $2N$, with $1 \leq N \leq 4$.

I.1 Torsion - group structure

Kamienny's Theorem

I.1 Torsion - group structure

Kamienny's Theorem

Let K be a quadratic field, and let E be an elliptic curve defined over K. Let $\mathcal{T}$ denote the subgroup of $E(K)$ consisting of the points of finite order.

Then $\mathcal{T}$ has one of the following forms

I.1 Torsion - group structure

Kamienny's Theorem

Let K be a quadratic field, and let E be an elliptic curve defined over K. Let $\mathcal{T}$ denote the subgroup of $E(K)$ consisting of the points of finite order. Then $\mathcal{T}$ has one of the following forms

i. A cyclic group of order N with $1 \leq N \leq 16$ or $N = 18$.

ii. The product of a cyclic group of order 2 and a cyclic group of order $2N$, with $1 \leq N \leq 6$.

iii. The product of a cyclic group of order 3 and a cyclic group of order $2N$, with $1 \leq N \leq 2$.

iv. The product of two cyclic groups of order 4.

I.1 Torsion - group structure

Merel's Theorem

I.1 Torsion - group structure

Merel's Theorem

Let K be a number field of degree $d > 1$, and let E be an elliptic curve defined over K. Let $\mathcal{T}$ denote the subgroup of $E(K)$ consisting of the points of finite order.

If $\mathcal{T}$ contains a point of prime order p, then

$$p < d^{3d^2}.$$

I.1 Torsion - group structure

Merel's Theorem

Let K be a number field of degree $d > 1$, and let E be an elliptic curve defined over K. Let $\mathcal{T}$ denote the subgroup of $E(K)$ consisting of the points of finite order.

If $\mathcal{T}$ contains a point of prime order p, then

$$p < d^{3d^2}$$

Corollary Let d be a positive integer. There is a real number $B(d)$ with the property that for any elliptic curves E, defined over any number field K of degree d, every torsion point in $E(K)$ has order bounded by $B(d)$.

I.2 Torsion - computation

Theorem (Nagell-1936,Lutz-1937)

I.2 Torsion - computation

Theorem (Nagell-1936,Lutz-1937)

Let E be the elliptic curve defined by

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

where $f(x)$ is a nonsingular cubic curve with integer coefficients a, b, c, and let

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

represent the discrimininant of f.

I.2 Torsion - computation

Theorem (Nagell-1936,Lutz-1937)

Let E be the elliptic curve defined by

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

where $f(x)$ is a nonsingular cubic curve with integer coefficients a, b, c, and let

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

represent the discrimininant of f.

If $P = (x, y)$ is a point of finite order on E, then x and y are integers, and either

i. $y = 0$ (in which case P has order 2), or
ii. y divides D. (in fact y^2 divides D)

I.2 Torsion - computation

Theorem (Nagell-1936,Lutz-1937)

Let E be the elliptic curve defined by

$$y^2 = f(x) = x^3 + ax^2 + bx + c,$$

where $f(x)$ is a nonsingular cubic curve with integer coefficients a, b, c, and let

$$D = -4a^3c + a^2b^2 + 18abc - 4b^3 - 27c^2$$

represent the discrimininant of f.

If $P = (x, y)$ is a point of finite order on E, then x and y are integers, and either

i. $y = 0$ (in which case P has order 2), or
ii. y divides D. (in fact y^2 divides D)

This is an **extremely** useful computational tool.

Computing Rational Torsion

Computing Rational Torsion

- Put E into Weierstrass form:

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

Computing Rational Torsion

- Put E into Weierstrass form:

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

- Compute all possible torsion points $P = (x, y)$ by $y^2 \mid D(E)$, and Cardano's formula for x.

Computing Rational Torsion

• Put E into Weierstrass form:

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

• Compute all possible torsion points $P = (x, y)$ by $y^2 \mid D(E)$, and Cardano's formula for x.

• Compute mP for $m \leq 12$ to determine finiteness of the order of P, and list off all torsion points.

Computing Rational Torsion

- Put E into Weierstrass form:

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

- Compute all possible torsion points $P = (x, y)$ by $y^2 \mid D(E)$, and Cardano's formula for x.

- Compute mP for $m \leq 12$ to determine finiteness of the order of P, and list off all torsion points.

- Finally, determine cyclicity of the case $|T| = 4k$ by

Computing Rational Torsion

- Put E into Weierstrass form:

$$E : y^2 = f(x) = x^3 + ax^2 + bx + c.$$

- Compute all possible torsion points $P = (x, y)$ by $y^2 \mid D(E)$, and Cardano's formula for x.

- Compute mP for $m \leq 12$ to determine finiteness of the order of P, and list off all torsion points.

- Finally, determine cyclicity of the case $|T| = 4k$ by

$T = C_{4k}$ iff $f(x) = 0$ has 3 integer roots
$T = C_2 \times C_{2k}$ iff $f(x) = 0$ has 1 integer root.

A Simple Example

A Simple Example

$$E : y^2 = x^3 + 1$$

A Simple Example

$$E : y^2 = x^3 + 1$$

$D(E) = 27$, and so for $(x, y) \in T(E)$, N-L implies $y \in \{0, \pm 1, \pm, 3\}$, and

A Simple Example

$$E : y^2 = x^3 + 1$$

$D(E) = 27$, and so for $(x, y) \in T(E)$, N-L implies $y \in \{0, \pm 1, \pm, 3\}$, and

$T(E) \subseteq \{\infty, (-1, 0), (0, 1), (0, -1), (2, 3), (2, -3)\}$.

A Simple Example

$$E : y^2 = x^3 + 1$$

$D(E) = 27$, and so for $(x, y) \in T(E)$, N-L implies $y \in \{0, \pm 1, \pm, 3\}$, and

$T(E) \subseteq \{\infty, (-1, 0), (0, 1), (0, -1), (2, 3), (2, -3)\}$.

Let $P = (2, 3)$, then

$$2P = (0, 1), 3P = (-1, 0), 2(-1, 0) = \infty,$$

and so

A Simple Example

$$E : y^2 = x^3 + 1$$

$D(E) = 27$, and so for $(x, y) \in T(E)$, N-L implies $y \in \{0, \pm 1, \pm, 3\}$, and

$T(E) \subseteq \{\infty, (-1, 0), (0, 1), (0, -1), (2, 3), (2, -3)\}$.

Let $P = (2, 3)$, then

$$2P = (0, 1), 3P = (-1, 0), 2(-1, 0) = \infty,$$

and so

$$T(E) \cong C_6.$$

A Family of Curves

$$E_k : y^2 = x^3 + k, \quad p^6 \nmid k$$

A Family of Curves

$$E_k : y^2 = x^3 + k, \quad p^6 \nmid k$$

All nontrivial torsion points are as follows:

1. If $k = C^2$, then $(0, \pm C)$ are of order 3.
2. If $k = D^3$, then $(-D, 0)$ is of order 2.
3. If $k = 1$, then $(2, \pm 3)$ are of order 6.
4. If $k = -432$, then $(12, \pm 36)$ are of order 3.

A Family of Curves

$$E_k : y^2 = x^3 + k, \quad p^6 \not| k$$

All nontrivial torsion points are as follows:

1. If $k = C^2$, then $(0, \pm C)$ are of order 3.
2. If $k = D^3$, then $(-D, 0)$ is of order 2.
3. If $k = 1$, then $(2, \pm 3)$ are of order 6.
4. If $k = -432$, then $(12, \pm 36)$ are of order 3.

Proof: First observe that $x_{2P} = (w - 2)x_P$, where $w = 9x_P^3/4y_P^2$. Then use the Nagell-Lutz theorem to show that $w \in \mathbb{Z}$, and that for $|w - 2| > 1$, P cannot have odd order.

Another Family of Curves

$$E_A : y^2 = x^3 + Ax, \quad p^4 \nmid A$$

Another Family of Curves

$$E_A : y^2 = x^3 + Ax, \quad p^4 \not| A$$

Remark. E_A is related to Diophantine equations of the form $u^2 - dy^4 = k$ with $A = kd$.

Another Family of Curves

$$E_A : y^2 = x^3 + Ax, \quad p^4 \nmid A$$

Remark. E_A is related to Diophantine equations of the form $u^2 - dy^4 = k$ with $A = kd$.

The nontrivial torsion points on E_A are:

1. $(0, 0)$ is a point of order 2.
2. If $A = 4$, then $(2, \pm 4)$ are of order 4.
3. If $A = -C^2$, then $(\pm C, 0)$ is of order 2.

Another Family of Curves

$$E_A : y^2 = x^3 + Ax, \quad p^4 \nmid A$$

Remark. E_A is related to Diophantine equations of the form $u^2 - dy^4 = k$ with $A = kd$.

The nontrivial torsion points on E_A are:

1. $(0,0)$ is a point of order 2.
2. If $A = 4$, then $(2, \pm 4)$ are of order 4.
3. If $A = -C^2$, then $(\pm C, 0)$ is of order 2.

Proof. First observe that $x_{2P} = (x_P^2 - A)^2/4y_P^2$, then a detailed elementary 2-adic analysis shows that if P is of odd order, then 2^4 divides A.

Williams Curves

$$E_m : y^2 = x^3 - (3m^4 + 24m)x + (-2m^6 + 40m^3 + 16)$$

Williams Curves

$$E_m : y^2 = x^3 - (3m^4 + 24m)x + (-2m^6 + 40m^3 + 16)$$

Remark. E_m is related to the existence of a pure cubic unit with rational summand $x = m$. $((x + yD^{1/3} + zD^{2/3})/3$.

Williams Curves

$$E_m : y^2 = x^3 - (3m^4 + 24m)x + (-2m^6 + 40m^3 + 16)$$

Remark. E_m is related to the existence of a pure cubic unit with rational summand $x = m$. $((x + yD^{1/3} + zD^{2/3})/3$.

Remark $P_m = (3m^2, 4(m^3 - 1))$ is of order 3 on E_m.

Williams Curves

$$E_m : y^2 = x^3 - (3m^4 + 24m)x + (-2m^6 + 40m^3 + 16)$$

Remark. E_m is related to the existence of a pure cubic unit with rational summand $x = m$. $((x + yD^{1/3} + zD^{2/3})/3$.

Remark $P_m = (3m^2, 4(m^3 - 1))$ is of order 3 on E_m.

Theorem (Herrmann-W, 2003)
For all integers $m \neq 1$,

$$T(E_m) \cong C_3.$$

Note: E_1 is singular

(Start of) Proof. Because E_m has a point of order 3, Mazur's theorem implies $T(E_m)$ is one of

$$C_3, C_6, C_9, C_{12}, C_2 \times C_6.$$

(Start of) Proof. Because E_m has a point of order 3, Mazur's theorem implies $T(E_m)$ is one of

$$C_3, C_6, C_9, C_{12}, C_2 \times C_6.$$

Point: need to rule out the existence of points of order 2 and 9.

(Start of) Proof. Because E_m has a point of order 3, Mazur's theorem implies $T(E_m)$ is one of

$$C_3, C_6, C_9, C_{12}, C_2 \times C_6.$$

Point: need to rule out the existence of points of order 2 and 9.

$P = (x, y)$ of order 2 on E_m satisfies

$$F(x, m) = 0, \quad x, m \in \mathbb{Z}$$

where

(Start of) Proof. Because E_m has a point of order 3, Mazur's theorem implies $T(E_m)$ is one of

$$C_3, C_6, C_9, C_{12}, C_2 \times C_6.$$

Point: need to rule out the existence of points of order 2 and 9.

$P = (x, y)$ of order 2 on E_m satisfies

$$F(x, m) = 0, \quad x, m \in \mathbb{Z}$$

where

$$F(X, Y) = X^3 - (3Y^4 + 24Y)X + (-2Y^6 + 40Y^3 + 16).$$

(Start of) Proof. Because E_m has a point of order 3, Mazur's theorem implies $T(E_m)$ is one of

$$C_3, C_6, C_9, C_{12}, C_2 \times C_6.$$

Point: need to rule out the existence of points of order 2 and 9.

$P = (x, y)$ of order 2 on E_m satisfies

$$F(x, m) = 0, \quad x, m \in \mathbb{Z}$$

where

$$F(X, Y) = X^3 - (3Y^4 + 24Y)X + (-2Y^6 + 40Y^3 + 16).$$

$F = 0$ is a curve of genus 0, leading to

$$t(t^2 - 3m) = 2, \quad t \in \mathbb{Z}$$

and eventually to $m = 1$.

If there is a point $P = (x, y)$ on E_m of order 9, then there is such a point which satisfies

$$3P = P_m = (3m^2, 4(m^3 - 1)),$$

If there is a point $P = (x, y)$ on E_m of order 9, then there is such a point which satisfies

$$3P = P_m = (3m^2, 4(m^3 - 1)),$$

which translates into

$$f(x, m) = 0, \quad x, m \in \mathbb{Z}$$

where

$$f(X, Y) = X^9 + a_8(Y)X^8 + \cdots + a_0(Y),$$

with

If there is a point $P = (x, y)$ on E_m of order 9, then there is such a point which satisfies

$$3P = P_m = (3m^2, 4(m^3 - 1)),$$

which translates into

$$f(x, m) = 0, \quad x, m \in \mathbb{Z}$$

where

$$f(X, Y) = X^9 + a_8(Y)X^8 + \cdots + a_0(Y),$$

with

$a_8 = -27Y^2$

$a_7 = 36Y^4 + 288Y$

$a_6 = 516Y^6 - 1248Y^3 - 1536$

$a_5 = 702Y^8 - 4320Y^5 + 13284Y^2$

$a_4 = -954Y^{10} - 11232Y^7 - 27648Y^4 + 9216Y$

$a_3 = -3372Y^{12} + 96Y^9 + 322560Y^6 - 270336Y^3 + 12288$

$a_2 = -3564Y^{14} + 49248Y^{11} - 622080Y^8 + 165888Y^5 + 331776Y^2$

$a_1 = -1719Y^{16} + 65376Y^{13} + 548352Y^{10} - 589824Y^7 + 626688Y^4 - 589824Y$

$a_0 = -323Y^{18} + 24672Y^{15} - 823296Y^{12} + 1586176Y^9 - 1265664Y^6 + 196608Y^3 + 26214$

Part II: The Rank of E

Part II: The Rank of E

The Mordell-Weil Theorem The group $E(\mathbb{Q})$ is finitely generated.

Part II: The Rank of E

The Mordell-Weil Theorem The group $E(\mathbb{Q})$ is finitely generated.

Proof

- properties of *height* functions on E
- $[E : 2E]$ is finite
- *Descent* theorem

Computing the Rank of $y^2 = x^3 + Ax$

Computing the Rank of $y^2 = x^3 + Ax$

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \cdots \times \mathbb{Z} \times \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}$$

r is the number of copies of $\mathbb{Z}$.

Computing the Rank of $y^2 = x^3 + Ax$

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \cdots \times \mathbb{Z} \times \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}$$

r is the number of copies of $\mathbb{Z}$.

If $G = \mathbb{Z}/p_i^{n_i}\mathbb{Z}$, then

$$[G : 2G] = \begin{cases} 2 & \text{if } p = 2, \\ 1 & \text{otherwise,} \end{cases}$$

Computing the Rank of $y^2 = x^3 + Ax$

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \cdots \times \mathbb{Z} \times \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}$$

r is the number of copies of $\mathbb{Z}$.

If $G = \mathbb{Z}/p_i^{n_i}\mathbb{Z}$, then

$$[G : 2G] = \begin{cases} 2 & \text{if } p = 2, \\ 1 & \text{otherwise,} \end{cases}$$

therefore

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = 2^r \cdot 2^q,$$

where q is the number of i with $p_i = 2$.

Computing the Rank of $y^2 = x^3 + Ax$

$$E(\mathbb{Q}) \cong \mathbb{Z} \times \cdots \times \mathbb{Z} \times \mathbb{Z}/p_1^{n_1}\mathbb{Z} \times \mathbb{Z}/p_k^{n_k}\mathbb{Z}$$

r is the number of copies of $\mathbb{Z}$.

If $G = \mathbb{Z}/p_i^{n_i}\mathbb{Z}$, then

$$[G : 2G] = \begin{cases} 2 & \text{if } p = 2, \\ 1 & \text{otherwise,} \end{cases}$$

therefore

$$[E(\mathbb{Q}) : 2E(\mathbb{Q})] = 2^r \cdot 2^q,$$

where q is the number of i with $p_i = 2$.

Need to understand $[2] : E \to E$.

Some Maps

Some Maps

Given $E : y^2 = x^3 + Ax$, define

$$\overline{E} : y^2 = x^3 - 4Ax.$$

Notice that $\overline{\overline{E}}$ is given by $y^2 = x^3 + 2^4 Ax$, and $\psi : \overline{\overline{E}} \to E$, given by

$$\psi(x, y) = (x/4, y/8),$$

is an isomorphism.

Some Maps

Given $E : y^2 = x^3 + Ax$, define

$$\overline{E} : y^2 = x^3 - 4Ax.$$

Notice that $\overline{\overline{E}}$ is given by $y^2 = x^3 + 2^4 Ax$, and $\psi : \overline{\overline{E}} \to E$, given by

$$\psi(x, y) = (x/4, y/8),$$

is an isomorphism.

Lemma For $P = (x, y) \in E$, define

$$\phi(P) = \begin{cases} \mathcal{O}_{\overline{E}} & \text{if } P = \mathcal{O}, P = (0,0 \\ (x + A/x, y/x(x - A/x)) & \text{otherwise.} \end{cases}$$

Then ϕ is a homomorphism from E to $\overline{E}$ with $Ker(\phi) = \{\mathcal{O}, (0,0)\}$.

Some Maps

Given $E : y^2 = x^3 + Ax$, define

$$\overline{E} : y^2 = x^3 - 4Ax.$$

Notice that $\overline{\overline{E}}$ is given by $y^2 = x^3 + 2^4 Ax$, and $\psi : \overline{\overline{E}} \to E$, given by

$$\psi(x, y) = (x/4, y/8),$$

is an isomorphism.

Lemma For $P = (x, y) \in E$, define

$$\phi(P) = \begin{cases} \mathcal{O}_{\overline{E}} & \text{if } P = \mathcal{O}, P = (0,0 \\ (x + A/x, y/x(x - A/x)) & \text{otherwise.} \end{cases}$$

Then ϕ is a homomorphism from E to $\overline{E}$ with $Ker(\phi) = \{\mathcal{O}, (0, 0)\}$.

$\overline{\phi} : \overline{E} \to \overline{\overline{E}}$ is similarly defined.

Factoring [2]

Lemma For all $P \in E$,

$$[2]P = \psi\overline{\phi}\phi(P).$$

Factoring [2]

Lemma For all $P \in E$,

$$[2]P = \psi\overline{\phi}\phi(P).$$

Lemma

$$2^{r+2} = [E(\mathbb{Q}) : \overline{\phi}(\overline{E}(\mathbb{Q}))] \cdot [\overline{E}(\mathbb{Q}) : \phi(E(\mathbb{Q}))]$$

One More Map

One More Map

For $x \in \mathbb{Q}^*$, let $[x]$ denote the coset of x in $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

For example $[9/8] = 1/2$.

One More Map

For $x \in \mathbb{Q}^*$, let $[x]$ denote the coset of x in $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

For example $[9/8] = 1/2$.

Define $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ by

$$\alpha(O) = 1, \alpha((0,0)) = [A],$$

and for $P = (x, y)$ with $x \neq 0$,

$$\alpha(P) = [x].$$

One More Map

For $x \in \mathbb{Q}^*$, let $[x]$ denote the coset of x in $\mathbb{Q}^*/\mathbb{Q}^{*2}$.

For example $[9/8] = 1/2$.

Define $\alpha : E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^{*2}$ by

$$\alpha(O) = 1, \alpha((0,0)) = [A],$$

and for $P = (x, y)$ with $x \neq 0$,

$$\alpha(P) = [x].$$

Lemma $\alpha(E(\mathbb{Q})) \cong E(\mathbb{Q})/\overline{\phi}(\overline{E}(\mathbb{Q}))$.

A Computational Tool for the Rank

$$E = E_A : y^2 = x^3 + Ax$$

A Computational Tool for the Rank

$$E = E_A : y^2 = x^3 + Ax$$

Corollary $2^{r+2} = |\alpha(E(\mathbb{Q}))| \cdot |\overline{\alpha}(\overline{E}(\mathbb{Q}))|.$

A Computational Tool for the Rank

$$E = E_A : y^2 = x^3 + Ax$$

Corollary $2^{r+2} = |\alpha(E(\mathbb{Q}))| \cdot |\overline{\alpha}(\overline{E}(\mathbb{Q}))|$.

Theorem The group $\alpha(E)$ consists of $1, [A], \pm[x]$ (if $-A = x^2$ for some $x \in \mathbb{N}$), and those $[d]$ such that d is a (positive or negative) divisor of A ($d \neq 1, A$) with the property that

$$dS^4 + (A/d)T^4 = U^2$$

is solvable in positive integers S, T, U, with gcd$(A/d, S)$ 1.
A similar statement holds for $\overline{\alpha}(\overline{E})$.

An Example:

$E : y^2 = x^3 - 17x$ and $\overline{E} : y^2 = x^3 + 68x$.

An Example:

$E : y^2 = x^3 - 17x$ and $\overline{E} : y^2 = x^3 + 68x$.

$1, -17 \in \alpha(E)$, and we need only check $-1, 17$:

An Example:

$E : y^2 = x^3 - 17x$ and $\overline{E} : y^2 = x^3 + 68x$.

$1, -17 \in \alpha(E)$, and we need only check $-1, 17$:

$$-S^4 + 17T^4 = U^2, \quad 17S^4 - T^4 = U^2$$

are solvable in positive integers, so

$$|\alpha(E)| = 4.$$

An Example:

$E : y^2 = x^3 - 17x$ and $\overline{E} : y^2 = x^3 + 68x$.

$1, -17 \in \alpha(E)$, and we need only check $-1, 17$:

$$-S^4 + 17T^4 = U^2, \quad 17S^4 - T^4 = U^2$$

are solvable in positive integers, so

$$|\alpha(E)| = 4.$$

$1, 17 \in \overline{\alpha}(\overline{E})$, and we need only check $2, 34$:

An Example:

$E : y^2 = x^3 - 17x$ and $\overline{E} : y^2 = x^3 + 68x$.

$1, -17 \in \alpha(E)$, and we need only check $-1, 17$:

$$-S^4 + 17T^4 = U^2, \quad 17S^4 - T^4 = U^2$$

are solvable in positive integers, so

$$|\alpha(E)| = 4.$$

$1, 17 \in \overline{\alpha}(\overline{E})$, and we need only check $2, 34$:

$$2S^4 + 34T^4 = U^2, \quad 34S^4 + 2T^4 = U^2$$

are solvable in positive integers, so

$$|\overline{\alpha}(\overline{E})| = 4.$$

An Example:

$E : y^2 = x^3 - 17x$ and $\overline{E} : y^2 = x^3 + 68x$.

$1, -17 \in \alpha(E)$, and we need only check $-1, 17$:

$$-S^4 + 17T^4 = U^2, \quad 17S^4 - T^4 = U^2$$

are solvable in positive integers, so

$$|\alpha(E)| = 4.$$

$1, 17 \in \overline{\alpha}(\overline{E})$, and we need only check $2, 34$:

$$2S^4 + 34T^4 = U^2, \quad 34S^4 + 2T^4 = U^2$$

are solvable in positive integers, so

$$|\overline{\alpha}(\overline{E})| = 4.$$

Therefore, $2^{r+2} = 4 \cdot 4 = 16$, hence $r = 2$.

A Theorem of Blair Spearman

A Theorem of Blair Spearman

Theorem If p is a rational prime of the form $p = u^4 + v^4$, then the rank over $\mathbb{Q}$ of

$$E_p : y^2 = x^3 - px$$

is equal to 2.

A Theorem of Blair Spearman

Theorem If p is a rational prime of the form $p = u^4 + v^4$, then the rank over $\mathbb{Q}$ of

$$E_p : y^2 = x^3 - px$$

is equal to 2.

Proof Compute $|\alpha(E_p)|$ and $|\overline{\alpha}(\overline{E_p})|$.

A Theorem of Blair Spearman

Theorem If p is a rational prime of the form $p = u^4 + v^4$, then the rank over $\mathbb{Q}$ of

$$E_p : y^2 = x^3 - px$$

is equal to 2.

Proof Compute $|\alpha(E_p)|$ and $|\overline{\alpha}(\overline{E_p})|$.

We automatically have $1, -p \in \alpha(E_p)$, so we just need to show $-1, p \in \alpha(E_p)$, which means showing that

$$-S^4 + pT^4 = U^2$$

is solvable with $\gcd(S, p) = 1$, and that

$$pS^4 - T^4 = U^2$$

is solvable with $\gcd(S, -1) = 1$.

Put $(S, T, U) = (u, 1, v^2)$ in the first case and $(S, T, U) = (1, u, v^2)$ in the second case.
It follows that $|\alpha(E_p)| = 4$.

Put $(S, T, U) = (u, 1, v^2)$ in the first case and $(S, T, U) = (1, u, v^2)$ in the second case.
It follows that $|\alpha(E_p)| = 4$.

Similarly we have $1, p \in \overline{\alpha}(\overline{E_p})$, so we just need to show $2, 2p \in \overline{\alpha}(\overline{E_p})$, which means showing that

$$2S^4 + 2pT^4 = U^2$$

is solvable with $\gcd(S, 2p) = 1$ and

$$2pS^4 + 2T^4 = U^2$$

is solvable with $\gcd(S, 2) = 1$.

Put $(S,T,U) = (u,1,v^2)$ in the first case and $(S,T,U) = (1,u,v^2)$ in the second case.
It follows that $|\alpha(E_p)| = 4$.

Similarly we have $1, p \in \overline{\alpha}(\overline{E_p})$, so we just need to show $2, 2p \in \overline{\alpha}(\overline{E_p})$, which means showing that

$$2S^4 + 2pT^4 = U^2$$

is solvable with $\gcd(S, 2p) = 1$ and

$$2pS^4 + 2T^4 = U^2$$

is solvable with $\gcd(S, 2) = 1$.

Put $(S,T,U) = (u-v, 1, 2(u^2 - uv + v^2))$.

$(p = u^4 + v^4 \Rightarrow \gcd(S, 2p) = (u - v, 2p) = 1)$

Put $(S,T,U) = (u, 1, v^2)$ in the first case and $(S,T,U) = (1, u, v^2)$ in the second case.
It follows that $|\alpha(E_p)| = 4$.

Similarly we have $1, p \in \overline{\alpha}(\overline{E_p})$, so we just need to show $2, 2p \in \overline{\alpha}(\overline{E_p})$, which means showing that

$$2S^4 + 2pT^4 = U^2$$

is solvable with $\gcd(S, 2p) = 1$ and

$$2pS^4 + 2T^4 = U^2$$

is solvable with $\gcd(S, 2) = 1$.

Put $(S,T,U) = (u - v, 1, 2(u^2 - uv + v^2))$.

$(p = u^4 + v^4 \Rightarrow \gcd(S, 2p) = (u - v, 2p) = 1)$

Thus, $|\overline{\alpha}(\overline{E_p})| = 4$, and $2^{r+2} = 4 \cdot 4 = 16$, and

$$rank_{E_p} = 2.$$

III. Integer Points on Elliptic Curves

Theorem (Siegel, 1929) Let $F \in \mathbb{Z}[X, Y]$. If the curve $F(X, Y) = 0$ represents a curve of genus 1, then there are only finitely many integers x, y for which $F(x, y) = 0$.

III. Integer Points on Elliptic Curves

Theorem (Siegel, 1929) Let $F \in \mathbb{Z}[X,Y]$. If the curve $F(X,Y) = 0$ represents a curve of genus 1, then there are only finitely many integers x, y for which $F(x,y) = 0$.

Theorem (Baker and Coates, 1970) Let $F \in \mathbb{Z}[X,Y]$ of total degree n and height H. If the curve $F(X,Y) = 0$ represents a curve of genus 1, and x, y are integers satisfying $F(x,y) = 0$, then

$$\max(|x|,|y|) < \exp\exp\exp((2H)^{10^{n^{10}}}.$$

Computing All Integer Points on a Curve

Computing All Integer Points on a Curve

• Packages exist which have programs to compute **all** integer points on an elliptic curve: MAGMA, PARI, KASH, SIMATH.

Computing All Integer Points on a Curve

• Packages exist which have programs to compute **all** integer points on an elliptic curve: MAGMA, PARI, KASH, SIMATH.

Elliptic Method

Computing All Integer Points on a Curve

• Packages exist which have programs to compute **all** integer points on an elliptic curve: MAGMA, PARI, KASH, SIMATH.

Elliptic Method

1. Compute generators for

$$E(\mathbb{Q}) \cong T \oplus < P_1 > \oplus \cdots \oplus < P_r > .$$

Computing All Integer Points on a Curve

• Packages exist which have programs to compute **all** integer points on an elliptic curve: MAGMA, PARI, KASH, SIMATH.

Elliptic Method

1. Compute generators for

$$E(\mathbb{Q}) \cong T \oplus < P_1 > \oplus \cdots \oplus < P_r > .$$

2. S. David's bound for linear forms in elliptic logarithms to get a (large) bound for M:

$$P = P_T + k_1 P_1 + \cdots + k_r P_r$$

and $P \in E(\mathbb{Z})$ implies $k_i < M$.

Computing All Integer Points on a Curve

• Packages exist which have programs to compute **all** integer points on an elliptic curve: MAGMA, PARI, KASH, SIMATH.

Elliptic Method

1. Compute generators for

$$E(\mathbb{Q}) \cong T \oplus < P_1 > \oplus \cdots \oplus < P_r > .$$

2. S. David's bound for linear forms in elliptic logarithms to get a (large) bound for M:

$$P = P_T + k_1 P_1 + \cdots + k_r P_r$$

and $P \in E(\mathbb{Z})$ implies $k_i < M$.

3. De Weger's reduction procedure to reduce M: $M \to \log(M)$.

Computing All Integer Points on a Curve

• Packages exist which have programs to compute **all** integer points on an elliptic curve: MAGMA, PARI, KASH, SIMATH.

Elliptic Method

1. Compute generators for

$$E(\mathbb{Q}) \cong T \oplus < P_1 > \oplus \cdots \oplus < P_r > .$$

2. S. David's bound for linear forms in elliptic logarithms to get a (large) bound for M:

$$P = P_T + k_1 P_1 + \cdots + k_r P_r$$

and $P \in E(\mathbb{Z})$ implies $k_i < M$.

3. De Weger's reduction procedure to reduce M: $M \to \log(M)$.

4. Enumerate the remaining cases.

Computing All Integer Points on a Curve

• Packages exist which have programs to compute **all** integer points on an elliptic curve: MAGMA, PARI, KASH, SIMATH.

Elliptic Method

1. Compute generators for

$$E(\mathbb{Q}) \cong T \oplus < P_1 > \oplus \cdots \oplus < P_r > .$$

2. S. David's bound for linear forms in elliptic logarithms to get a (large) bound for M:

$$P = P_T + k_1 P_1 + \cdots + k_r P_r$$

and $P \in E(\mathbb{Z})$ implies $k_i < M$.

3. De Weger's reduction procedure to reduce M: $M \to \log(M)$.

4. Enumerate the remaining cases.

Let $E : y^2 = x^3 + 877x$. $E(\mathbb{Q}) =< P_2, (u, v) >$

Computing All Integer Points on a Curve

• Packages exist which have programs to compute **all** integer points on an elliptic curve: MAGMA, PARI, KASH, SIMATH.

Elliptic Method

1. Compute generators for

$$E(\mathbb{Q}) \cong T \oplus < P_1 > \oplus \cdots \oplus < P_r > .$$

2. S. David's bound for linear forms in elliptic logarithms to get a (large) bound for M:

$$P = P_T + k_1 P_1 + \cdots + k_r P_r$$

and $P \in E(\mathbb{Z})$ implies $k_i < M$.

3. De Weger's reduction procedure to reduce M: $M \to \log(M)$.

4. Enumerate the remaining cases.

Let $E : y^2 = x^3 + 877x$. $E(\mathbb{Q}) =< P_2, (u, v) >$
$u = \frac{375494528127162193105504069942092792346201}{62159877768644257535639389356838044100}$

A Hybrid Theorem

Theorem (W, 2010) Let N denote a square-free positive integer, and let

$$E : y^2 = x^3 - Nx.$$

Then there are at most

$$48 \cdot 3^{\omega(N)}$$

integer points (X, Y) on E with

$$|X| > \max_{D|N, D>1} \frac{6|N/D|^{20}\epsilon_D^{23}}{D^6},$$

where $\omega(D)$ is the number of prime factors of D and ϵ_D is the fundamental unit in $\mathbb{Q}(\sqrt{D})$.

A Hybrid Theorem

Theorem (W, 2010) Let N denote a square-free positive integer, and let

$$E : y^2 = x^3 - Nx.$$

Then there are at most

$$48 \cdot 3^{\omega(N)}$$

integer points (X, Y) on E with

$$|X| > \max_{D|N, D>1} \frac{6|N/D|^{20}\epsilon_D^{23}}{D^6},$$

where $\omega(D)$ is the number of prime factors of D and ϵ_D is the fundamental unit in $\mathbb{Q}(\sqrt{D})$.

Main Tool Siegel's method for irrationality measure in Diophantine Approximation applied to algebraic numbers of degree 4.

Integral Points on Spearman's Curves

Integral Points on Spearman's Curves

Theorem (W,2009) Let p be an odd prime and $E_p : y^2 = x^3 - px$. There exist at most 4 integral points (x, y) on E_p with $y > 0$, and a complete description of those integral points is as follows.

Integral Points on Spearman's Curves

Theorem (W,2009) Let p be an odd prime and $E_p : y^2 = x^3 - px$. There exist at most 4 integral points (x, y) on E_p with $y > 0$, and a complete description of those integral points is as follows.

1. If $p = 2u^2 - 1$ for some integer u, then $(x, y) = (u^2, u(u^2 - 1)) \in E_p$.

2. If $p = u^4 + v^2$ for some integers u, v, then $(x, y) = (-u^2, uv) \in E_p$.

3. If $\epsilon_p = T + U\sqrt{p}$ satisfies $Norm(\epsilon_p) = -1$ and $U = u^2$ for some integer u, then $(x, y) = (pu^2, puT) \in E_p$.

Integral Points on Spearman's Curves

Theorem (W,2009) Let p be an odd prime and $E_p : y^2 = x^3 - px$. There exist at most 4 integral points (x, y) on E_p with $y > 0$, and a complete description of those integral points is as follows.

1. If $p = 2u^2 - 1$ for some integer u, then $(x, y) = (u^2, u(u^2 - 1)) \in E_p$.

2. If $p = u^4 + v^2$ for some integers u, v, then $(x, y) = (-u^2, uv) \in E_p$.

3. If $\epsilon_p = T + U\sqrt{p}$ satisfies $Norm(\epsilon_p) = -1$ and $U = u^2$ for some integer u, then $(x, y) = (pu^2, puT) \in E_p$.

Proof Relies on an irrationality measure for a class of algebraic numbers of degree 4 following Thue's method (Chen and Voutier, 1997).

Integral Points on Spearman's Curves

Theorem (W,2009) Let p be an odd prime and $E_p : y^2 = x^3 - px$. There exist at most 4 integral points (x, y) on E_p with $y > 0$, and a complete description of those integral points is as follows.

1. If $p = 2u^2 - 1$ for some integer u, then $(x, y) = (u^2, u(u^2 - 1)) \in E_p$.

2. If $p = u^4 + v^2$ for some integers u, v, then $(x, y) = (-u^2, uv) \in E_p$.

3. If $\epsilon_p = T + U\sqrt{p}$ satisfies $Norm(\epsilon_p) = -1$ and $U = u^2$ for some integer u, then $(x, y) = (pu^2, puT) \in E_p$.

Proof Relies on an irrationality measure for a class of algebraic numbers of degree 4 following Thue's method (Chen and Voutier, 1997).
Exercise The maximum of 4 is attained!!

An Extension of Spearman's Theorem

Theorem (W,2010) Let p denote an odd prime, and let $E_p : y^2 = x^3 - px$. Classify the integer points (x, y) on E_p with $y > 0$ as follows:

An Extension of Spearman's Theorem

Theorem (W,2010) Let p denote an odd prime, and let $E_p : y^2 = x^3 - px$. Classify the integer points (x, y) on E_p with $y > 0$ as follows:

i. If $p = 2u^2 - 1$ for some integer u, then $(x, y) = (u^2, u(u^2 - 1)) \in E_p$.
ii. If $p = u^4 + v^2$ for some integers u, v, then $(x, y) = (-u^2, uv) \in E_p$.
iii. If $\epsilon_p = T + U\sqrt{p}$ satisfies $Norm(\epsilon_p) = -1$ and $U = u^2$ for some integer u, then $(x, y) = (pu^2, puT) \in E_p$.

An Extension of Spearman's Theorem

Theorem (W,2010) Let p denote an odd prime, and let $E_p : y^2 = x^3 - px$. Classify the integer points (x, y) on E_p with $y > 0$ as follows:

i. If $p = 2u^2 - 1$ for some integer u, then $(x, y) = (u^2, u(u^2 - 1)) \in E_p$.
ii. If $p = u^4 + v^2$ for some integers u, v, then $(x, y) = (-u^2, uv) \in E_p$.
iii. If $\epsilon_p = T + U\sqrt{p}$ satisfies $Norm(\epsilon_p) = -1$ and $U = u^2$ for some integer u, then $(x, y) = (pu^2, puT) \in E_p$.

If E_p contains two integer points (x, y) with $y > 0$, then the rank of E_p is 2 except possibly if the two integer points are of type *ii.* and *iii.*

An Extension of Spearman's Theorem

Theorem (W,2010) Let p denote an odd prime, and let $E_p : y^2 = x^3 - px$. Classify the integer points (x, y) on E_p with $y > 0$ as follows:

i. If $p = 2u^2 - 1$ for some integer u, then $(x, y) = (u^2, u(u^2 - 1)) \in E_p$.
ii. If $p = u^4 + v^2$ for some integers u, v, then $(x, y) = (-u^2, uv) \in E_p$.
iii. If $\epsilon_p = T + U\sqrt{p}$ satisfies $Norm(\epsilon_p) = -1$ and $U = u^2$ for some integer u, then $(x, y) = (pu^2, puT) \in E_p$.

If E_p contains two integer points (x, y) with $y > 0$, then the rank of E_p is 2 except possibly if the two integer points are of type *ii.* and *iii.*

Example Spearman's curves have two points of type *ii.* If $p = 577$, E_p has one point of each type and by the Theorem, $rank(E_{577}) = 2$.

Reduction to a Thue Equation

All integer solutions (x, y) to

$$x^2 - (2^{2m} + 1)y^2 = -2^{2m} \quad (*)$$

arise from

$$x+y\sqrt{2^{2m}+1} = \pm(\pm 1+\sqrt{2^{2m}+1})(2^m+\sqrt{2^{2m}+1})^{2i}$$

for some $i \geq 0$.

Put $\quad T_k + U_k\sqrt{2^{2m}+1} = (2^m + \sqrt{2^{2m}+1})^k$

A solution (x, y) to $(*)$ with $y = Y^2$
is equivalent to

$$\mathbf{Y^2 = T_{2k} \pm U_{2k}} = (T_k \pm U_k)^2 + (2aU_k)^2.$$

$$Y^2 = (T_k \pm U_k)^2 + (2aU_k)^2,$$

hence there are coprime positive integers r, s such that

$$Y = r^2 + s^2,\ T_k \pm U_k = r^2 - s^2,\ 2aU_k = 2rs,$$

with r even and s odd. Put $R = r/a$.

$$Y^2 = (T_k \pm U_k)^2 + (2aU_k)^2,$$

hence there are coprime positive integers r, s such that

$$Y = r^2 + s^2,\ T_k \pm U_k = r^2 - s^2,\ 2aU_k = 2rs,$$

with r even and s odd. Put $R = r/a$.

Solve for T_k, U_k, substitute $(x, y) = (T_k, U_k)$ into $x^2 - (2^{2m} + 1)y^2 = \pm 1$ **:**

Thue equation:

$$Y^2 = (T_k \pm U_k)^2 + (2aU_k)^2,$$

hence there are coprime positive integers r, s such that

$$Y = r^2 + s^2,\ T_k \pm U_k = r^2 - s^2,\ 2aU_k = 2rs,$$

with r even and s odd. Put $R = r/a$.

Solve for T_k, U_k, substitute $(x, y) = (T_k, U_k)$ into $x^2 - (2^{2m} + 1)y^2 = \pm 1$ **:**

Thue equation:

$$s^4 - 2s^3R - 6a^2s^2R^2 + 2a^2sR^3 + a^4R^4 = \pm 1$$

$(R = r/a$ and $a = 2^{m-1})$.

Akhtari's Theorem (to appear in Acta Arithmetica)

Let $F(x, y)$ be an irreducible binary quartic form with integer coefficients that splits in $\mathbb{R}$. If $J_F = 0$, then the inequality

$$|F(x, y)| = 1$$

has at most 12 positive integer solutions (x, y).

Akhtari's Theorem (to appear in Acta Arithmetica)

Let $F(x, y)$ be an irreducible binary quartic form with integer coefficients that splits in $\mathbb{R}$. If $J_F = 0$, then the inequality

$$|F(x, y)| = 1$$

has at most 12 positive integer solutions (x, y).

Proof Siegel's method (1929), elaborated by Evertse (1983).

Akhtari's Theorem (to appear in Acta Arithmetica)

Let $F(x, y)$ be an irreducible binary quartic form with integer coefficients that splits in $\mathbb{R}$. If $J_F = 0$, then the inequality

$$|F(x, y)| = 1$$

has at most 12 positive integer solutions (x, y).

Proof Siegel's method (1929), elaborated by Evertse (1983).

Corollary*

For all $m \geq 0$, the equation

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m}$$

has at most $\mathbf{3}$ solutions in coprime positive integers $(X, Y) \neq (1, 1)$.

Yuan's Theorem

Let $A > 0$, B and N be rational integers, and

$F(X, Y) = BX^4 - AX^3Y - 6BX^2Y^2 + AXY^3 + BY^4.$

If $A > 308B^4$, then all coprime integer solutions (x, y) to the inequality

$$|F(x, y)| \leq N$$

satisfy

$$x^2 + y^2 \leq \max\left(\frac{25A^2}{64B^2}, \frac{4N^2}{A}\right).$$

Yuan's Theorem

Let $A > 0$, B and N be rational integers, and

$F(X,Y) = BX^4 - AX^3Y - 6BX^2Y^2 + AXY^3 + BY^4$.

If $A > 308B^4$, then all coprime integer solutions (x,y) to the inequality

$$|F(x,y)| \leq N$$

satisfy

$$x^2 + y^2 \leq \max\left(\frac{25A^2}{64B^2}, \frac{4N^2}{A}\right).$$

Proof The hypergeometric method is used to obtain an irrationality measure for a class of algebraic numbers, for approximations p/q with p, q in an imaginary quadratic field.

Observation 1

If $(X, Y) \neq (1, 1)$ is a solution in coprime positive integers to

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m},$$

with $Y = r^2 + s^2$, $r > s > 0$, and $a = 2^{m-1}$, then

$$\pm X \pm 2ai = (1 + 2ai)(s \pm ri)^4.$$

Observation 1

If $(X, Y) \neq (1, 1)$ is a solution in coprime positive integers to

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m},$$

with $Y = r^2 + s^2$, $r > s > 0$, and $a = 2^{m-1}$, then

$$\pm X \pm 2ai = (1 + 2ai)(s \pm ri)^4.$$

proof Recall

$$s^4 - 2s^3R - 6a^2s^2R^2 + 2a^2sR^3 + a^4R^4 = \pm 1.$$

Diagonalize this over the Gaussian integers:

$$(1 + 2ai)(s + ri)^4 - (1 - 2ai)(s - ri)^4 = \pm 4ai.$$

Observation 1

If $(X,Y) \neq (1,1)$ is a solution in coprime positive integers to

$$X^2 - (2^{2m}+1)Y^4 = -2^{2m},$$

with $Y = r^2 + s^2$, $r > s > 0$, and $a = 2^{m-1}$, then

$$\pm X \pm 2ai = (1+2ai)(s \pm ri)^4.$$

proof Recall

$$s^4 - 2s^3R - 6a^2s^2R^2 + 2a^2sR^3 + a^4R^4 = \pm 1.$$

Diagonalize this over the Gaussian integers:

$$(1+2ai)(s+ri)^4 - (1-2ai)(s-ri)^4 = \pm 4ai.$$

Put $X_0 = (1+2ai)(s+ri)^4 + (1-2ai)(s-ri)^4$, the result follows from $X_0 = X$.

Observation 2 (The Gap Principle)

If $(X_1, Y_1), (X_2, Y_2)$ sre two coprime positive integer solutions to

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m},$$

with $Y_2 > Y_1 > 1$, then $Y_2 > 2Y_1^3$.

Observation 2 (The Gap Principle)

If $(X_1, Y_1), (X_2, Y_2)$ sre two coprime positive integer solutions to

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m},$$

with $Y_2 > Y_1 > 1$, then $Y_2 > 2Y_1^3$.

proof For $j = 1, 2$ and $Y_j = s_j^2 + r_j^2$, we have

$$(1+2ai)(s_j+r_ji)^4-(1-2ai)(s_j-r_ji)^4 = \pm 4ai.$$

Observation 2 (The Gap Principle)

If $(X_1, Y_1), (X_2, Y_2)$ sre two coprime positive integer solutions to

$$X^2 - (2^{2m}+1)Y^4 = -2^{2m},$$

with $Y_2 > Y_1 > 1$, then $Y_2 > 2Y_1^3$.

proof For $j = 1, 2$ and $Y_j = s_j^2 + r_j^2$, we have

$$(1+2ai)(s_j+r_ji)^4 - (1-2ai)(s_j-r_ji)^4 = \pm 4ai.$$

Let $\omega = \frac{1-2ai}{1+2ai}$, use the fact that

$$\mid \omega - \left(\frac{s_j + r_j i}{s_j - r_j i}\right)^4 \mid = \frac{4a}{\sqrt{1+4a^2Y_j^2}}$$

is very small for both $j = 1, 2$.

The Main Argument

Suppose that $(X_1, Y_1), (X_2, Y_2), (X_3, Y_3)$ are co-prime positive integer solutions to

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m},$$

with $Y_3 > Y_2 > Y_1 > 1$, $Y_j = s_j^2 + r_j^2$ $(j = 1, 2, 3)$.

The Main Argument

Suppose that $(X_1, Y_1), (X_2, Y_2), (X_3, Y_3)$ are coprime positive integer solutions to

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m},$$

with $Y_3 > Y_2 > Y_1 > 1$, $Y_j = s_j^2 + r_j^2$ $(j = 1, 2, 3)$. Then

$$X_1 \pm 2ai = (1 \pm 2ai)(s_1 \pm r_1 i)^4,$$

$$X_3 \pm 2ai = (1 \pm 2ai)(s_3 \pm r_3 i)^4,$$

The Main Argument

Suppose that $(X_1, Y_1), (X_2, Y_2), (X_3, Y_3)$ are coprime positive integer solutions to

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m},$$

with $Y_3 > Y_2 > Y_1 > 1$, $Y_j = s_j^2 + r_j^2$ $(j = 1, 2, 3)$. Then

$$X_1 \pm 2ai = (1 \pm 2ai)(s_1 \pm r_1 i)^4,$$

$$X_3 \pm 2ai = (1 \pm 2ai)(s_3 \pm r_3 i)^4,$$

giving

$$(1+2ai)(s_1+r_1 i)^4-(1-2ai)(s_1-r_1 i)^4 = \pm 4ai,$$

$$(1+2ai)(s_3+r_3 i)^4-(1-2ai)(s_3-r_3 i)^4 = \pm 4ai.$$

The Main Argument

Suppose that $(X_1, Y_1), (X_2, Y_2), (X_3, Y_3)$ are coprime positive integer solutions to

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m},$$

with $Y_3 > Y_2 > Y_1 > 1$, $Y_j = s_j^2 + r_j^2$ $(j = 1, 2, 3)$. Then

$$X_1 \pm 2ai = (1 \pm 2ai)(s_1 \pm r_1 i)^4,$$

$$X_3 \pm 2ai = (1 \pm 2ai)(s_3 \pm r_3 i)^4,$$

giving

$$(1+2ai)(s_1+r_1 i)^4 - (1-2ai)(s_1 - r_1 i)^4 = \pm 4ai,$$

$$(1+2ai)(s_3+r_3 i)^4 - (1-2ai)(s_3 - r_3 i)^4 = \pm 4ai.$$

Using the above, the following is easy to show:

$$\gamma - \overline{\gamma} = \pm 4 Y_1^4 a i,$$

with

$$\gamma = (X_1 \pm 2ai)(s_1 - r_1 i)^4 (s_3 + r_3 i)^4.$$

$$\gamma - \overline{\gamma} = \pm 4Y_1^4 ai,$$

with

$$\gamma = (X_1 \pm 2ai)(s_1 - r_1 i)^4 (s_3 + r_3 i)^4.$$

Define (x, y) by

$$x + yi = (s_1 - r_1 i)(s_3 + r_3 i),$$

then

$$\mid (X_1 \pm 2ai)(x+yi)^4 - (X_1 \mp 2ai)(x-yi)^4 \mid = 4aY_1^4,$$

$$\gamma - \overline{\gamma} = \pm 4Y_1^4 ai,$$

with

$$\gamma = (X_1 \pm 2ai)(s_1 - r_1 i)^4 (s_3 + r_3 i)^4.$$

Define (x, y) by

$$x + yi = (s_1 - r_1 i)(s_3 + r_3 i),$$

then

$$\mid (X_1 \pm 2ai)(x+yi)^4 - (X_1 \mp 2ai)(x-yi)^4 \mid = 4aY_1^4,$$

i.e.

$$\mid \mp ax^4 - 2X_1 x^3 y \pm 6ax^2 y^2 + 2X_1 xy^3 \mp ay^4 \mid = aY_1^4.$$

$$\gamma - \overline{\gamma} = \pm 4 Y_1^4 ai,$$

with

$$\gamma = (X_1 \pm 2ai)(s_1 - r_1 i)^4 (s_3 + r_3 i)^4.$$

Define (x, y) by

$$x + yi = (s_1 - r_1 i)(s_3 + r_3 i),$$

then

$$\mid (X_1 \pm 2ai)(x+yi)^4 - (X_1 \mp 2ai)(x-yi)^4 \mid = 4aY_1^4,$$

i.e.

$$\mid \mp ax^4 - 2X_1 x^3 y \pm 6ax^2y^2 + 2X_1 xy^3 \mp ay^4 \mid = aY_1^4.$$

This is a Thue equation of the form in Yuan's theorem with

$$B = \pm a, A = 2X_1, N = aY_1^4.$$

The hypothesis in Yuan's theorem:

$$A > 308B^4$$

The hypothesis in Yuan's theorem:

$$A > 308B^4$$

Recall

$$Y_1^2 = T_{2k} \pm U_{2k}.$$

Similarly

$$X_1 = (1 + 4a^2)U_{2k} \pm T_{2k}.$$

The hypothesis in Yuan's theorem:

$$A > 308B^4$$

Recall

$$Y_1^2 = T_{2k} \pm U_{2k}.$$

Similarly

$$X_1 = (1 + 4a^2)U_{2k} \pm T_{2k}.$$

Assume $k > 1$ (regard $k = 1$ as an exercise).

Then

$$A = 2X_1 \geq 2(4a^2 + 1)U_4 - 2T_4 =$$

$$16a(4a^2+1)(8a^2+1) - 4(8a^2+1)^2 > 308a^4 = 308B^4.$$

The conclusion of Yuan's theorem gives

$$x^2 + y^2 \leq \max\left(\frac{100X_1^2}{64a^2}, \frac{4a^2Y_1^8}{2X_1}\right),$$

The conclusion of Yuan's theorem gives

$$x^2 + y^2 \leq \max\left(\frac{100X_1^2}{64a^2}, \frac{4a^2Y_1^8}{2X_1}\right),$$

whereas the Gap Principle gives

$$x^2 + y^2 = (r_1^2 + s_1^2)(r_3^2 + s_3^2) = Y_1Y_3 \geq 16Y_1^{10}.$$

The conclusion of Yuan's theorem gives

$$x^2 + y^2 \leq \max\left(\frac{100X_1^2}{64a^2}, \frac{4a^2Y_1^8}{2X_1}\right),$$

whereas the Gap Principle gives

$$x^2 + y^2 = (r_1^2 + s_1^2)(r_3^2 + s_3^2) = Y_1Y_3 \geq 16Y_1^{10}.$$

The inequality $X_1^2 < (4a^2 + 1)Y_1^4$ is used to derive a contradiction from these two inequalities.

Theorem For all $m \geq 0$, there are at most $\mathbf{2}$ solutions in coprime positive integers $(X, Y) \neq (1, 1)$ to the equation

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m}.$$

Theorem For all $m \geq 0$, there are at most $\mathbf{2}$ solutions in coprime positive integers $(X, Y) \neq (1, 1)$ to the equation

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m}.$$

Conjecture For all $m \geq 3$, there are NO solutions in coprime positive integers (X, Y) to the equation

$$X^2 - (2^{2m} + 1)Y^4 = -2^{2m}$$

other than $(X, Y) = (1, 1)$.