

On the simplest cubic fields and related Thue equations

Akinari Hoshi

Rikkyo University

January 25th 2012

§0 fun

§0 fun

§1 Introduction: Brief history

§1 Introduction:
Brief history

§2 Results

§2 Results

§3 Theorem C: Correspondence

§3 Theorem C:
Correspondence

§4 Theorem O_1, O_2 : Okazaki's Theorem

§4 Theorem O_1, O_2 :
Okazaki's
Theorem

§5 Theorem S: Solutions

§5 Theorem S:
Solutions

- ▶ On correspondence between solutions of a family of cubic Thue equations and isomorphism classes of the simplest cubic fields, J. Number Theory **131** (2011) 2135–2150.

Diophantine Approximation

Approximating $\alpha \in \mathbb{R}$ by $\frac{p}{q} \in \mathbb{Q}$.

Example

▶ $\alpha = \sqrt{2}$.

$$1, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \frac{14142}{10000}, \frac{141421}{100000}, \frac{1414213}{1000000}, \frac{14142135}{10000000},$$

$$\frac{141421356}{100000000}, \frac{1414213562}{1000000000}, \frac{14142135623}{10000000000}, \frac{141421356237}{100000000000}, \dots$$

▶ $\alpha = \pi$.

$$3, \frac{31}{10}, \frac{314}{100}, \frac{3141}{1000}, \frac{31415}{10000}, \frac{314159}{100000}, \frac{3141592}{1000000}, \frac{31415926}{10000000},$$

$$\frac{314159265}{100000000}, \frac{3141592653}{1000000000}, \frac{31415926535}{10000000000}, \frac{314159265358}{100000000000}, \dots$$

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence§4 Theorem O₁,
O₂: Okazaki's
Theorem§5 Theorem S:
Solutions

Diophantine approximation

- ▶ $\alpha = \sqrt{2} \approx 1.4142135623730950488$.
 $1, \frac{14}{10}, \frac{141}{100}, \frac{1414}{1000}, \frac{14142}{10000}, \frac{141421}{100000}, \frac{1414213}{1000000}, \frac{14142135}{10000000},$
 $\frac{141421356}{100000000}, \frac{1414213562}{1000000000}, \frac{14142135623}{10000000000}, \frac{141421356237}{100000000000}, \dots$
- ▶ $\frac{3}{2} = 1.5, \frac{7}{5} = 1.4, \frac{17}{12} \approx 1.4166, \frac{41}{29} \approx 1.4139$
- ▶ $\frac{99}{70} \approx 1.4128, \frac{239}{169} \approx 1.414201, \frac{577}{408} \approx 1.414215$
- ▶ $\frac{1393}{985} \approx 1.4142131, \frac{3363}{2378} \approx 1.4142136$
- ▶ $\frac{8119}{5741} \approx 1.41421355, \frac{19601}{13860} \approx 1.414213564$
- ▶ $\frac{47321}{33461} \approx 1.4142135620, \frac{114243}{80782} \approx 1.4142135624$
- ▶ $\frac{275807}{195025} \approx 1.41421356236, \frac{665857}{470832} \approx 1.414213562374$
- ▶ $\frac{1607521}{1136689} \approx 1.414213562372, \frac{3880899}{2744210} \approx 1.4142135623731$
- ▶ $\frac{9369319}{6625109} \approx 1.41421356237308$
- ▶ $\frac{22619537}{15994428} \approx 1.414213562373096$
- ▶ $\frac{54608393}{38613965} \approx 1.4142135623730948$

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

Diophantine approximation

- ▶ $\alpha = \pi \approx 3.1415926535897932384626$.
- ▶ $3, \frac{31}{10}, \frac{314}{100}, \frac{3141}{1000}, \frac{31415}{10000}, \frac{314159}{100000}, \frac{3141592}{1000000}, \frac{31415926}{10000000}, \frac{314159265}{100000000}, \frac{3141592653}{1000000000}, \frac{31415926535}{10000000000}, \frac{314159265358}{100000000000}, \dots$
- ▶ $\frac{22}{7} \approx 3.142, \frac{333}{106} \approx 3.14150, \frac{355}{113} \approx 3.1415929$
- ▶ $\frac{103993}{33102} \approx 3.1415926530, \frac{104348}{33215} \approx 3.1415926539$
- ▶ $\frac{208341}{66317} \approx 3.1415926534, \frac{312689}{99532} \approx 3.1415926536$
- ▶ $\frac{833719}{265381} \approx 3.141592653581, \frac{1146408}{364913} \approx 3.141592653591$
- ▶ $\frac{4272943}{1360120} \approx 3.1415926535893$
- ▶ $\frac{5419351}{1725033} \approx 3.1415926535898$
- ▶ $\frac{80143857}{25510582} \approx 3.141592653589792$
- ▶ $\frac{165707065}{52746197} \approx 3.1415926535897934$
- ▶ $\frac{245850922}{78256779} \approx 3.1415926535897931$
- ▶ $\frac{411557987}{131002976} \approx 3.14159265358979325$
- ▶ $\frac{1068966896}{340262731} \approx 3.141592653589793235$

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

Dirichlet's theorem

Theorem (Dirichlet 1842)

Let $\alpha, Q \in \mathbb{R}$ ($Q > 1$).

$\exists p, q \in \mathbb{Z}$ s.t. $\gcd(p, q) = 1$, $1 \leq q \leq Q$ and $|q\alpha - p| < \frac{1}{Q}$.

$$\blacktriangleright \left| \alpha - \frac{p}{q} \right| \leq \frac{1}{qQ} < \frac{1}{q^2}.$$

Corollary (Dirichlet 1842)

If α is irrational, then $\exists \infty \frac{p}{q} \in \mathbb{Q}$ s.t. $\left| \alpha - \frac{p}{q} \right| < \frac{1}{q^2}$.

How to construct such a “good” $\frac{p}{q}$?

- ▶ Continued fractions.

Definition (Continued fractions)

A finite or infinite expression of the form

$$[a_0; a_1, a_2, \dots] = a_0 + \frac{1}{a_1 + \frac{1}{a_2 + \dots}}$$

where $a_i > 0$, is called a **continued fraction**.

- ▶ $\sqrt{2} = [1; 2, 2, 2, 2, \dots]$, $\sqrt{3} = [1; 1, 2, 1, 2, 1, 2, \dots]$,
 $\pi = [3; 7, 15, 1, 292, 1, 1, 1, 2, 1, 3, 1, 14, 2, 1, 1, 2, 2, \dots]$.

Definition (Convergents)

Let $\alpha = [a_0; a_1, a_2, \dots]$ be a continued fraction.

The i -th convergent of α is $C_i = [a_0; a_1, \dots, a_i]$.

$[a_0; a_1, \dots]$ is called convergent if $\lim_{i \rightarrow \infty} C_i = \exists \alpha \in \mathbb{R}$.

- ▶ For any $a_i \in \mathbb{Z}_{>0}$, $[a_0; a_1, a_2, \dots]$ is convergent.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence§4 Theorem O₁,
O₂: Okazaki's
Theorem§5 Theorem S:
Solutions

Let $\alpha = [a_0; a_1, \dots]$ be a simple c.f. (i.e. $a_i \in \mathbb{Z}_{>0}$).
Let $C_i = [a_0; a_1, \dots, a_i]$ be the i -th convergent to α .

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence§4 Theorem O₁,
O₂: Okazaki's
Theorem§5 Theorem S:
Solutions

Lemma

C_i is given by $C_i = p_i/q_i$ for $i \geq 0$ where

$$\begin{cases} p_{-1} = 1, q_{-1} = 0, \\ p_0 = a_0, q_0 = 1, \\ p_i = a_i p_{i-1} + p_{i-2}, q_i = a_i q_{i-1} + q_{i-2} \quad (i \geq 1). \end{cases}$$

Lemma

- (1) $p_i q_{i-1} - p_{i-1} q_i = (-1)^i$ for $i \geq 0$;
- (2) $(p_i, q_i) = 1$;
- (3) $1 = q_0 \leq q_1 < q_2 < q_3 < \dots$;
- (4) $C_0 < C_2 < C_4 < \dots < \alpha < \dots < C_5 < C_3 < C_1$;
- (5) $|C_i - C_{i+1}| = 1/(q_i q_{i+1})$ for $i \geq 0$.

Let $\alpha = [a_0; a_1, \dots]$ be a simple c.f. (i.e. $a_i \in \mathbb{Z}_{>0}$).

Let $C_i = [a_0; a_1, \dots, a_i]$ be the i -th convergent to α .

Theorem

(1) Any convergent $C_i = p_i/q_i$ satisfies

$$\left| \alpha - \frac{p_i}{q_i} \right| < \frac{1}{q_i q_{i+1}} < \frac{1}{q_i^2};$$

(2) Conversely, if $p/q \in \mathbb{Q}$ satisfy

$$\left| \alpha - \frac{p}{q} \right| < \frac{1}{2q^2},$$

then $\frac{p}{q}$ is one of the convergents of α (i.e. $\frac{p}{q} = C_i = \frac{p_i}{q_i}$).

▶ [Jump to Dirichlet's Theorem](#)

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

§1 Introduction: Brief history of Thue equations

Definition (Thue equations)

Let $F(x, y) \in \mathbb{Z}[x, y]$ be an irreducible binary form of degree $n \geq 3$. A Diophantine equation

$$F(x, y) = a_n x^n + a_{n-1} x^{n-1} y + \cdots + a_1 x y^{n-1} + a_0 y^n = \lambda$$

where $\lambda \in \mathbb{Z}$ ($\lambda \neq 0$), is called a **Thue equation**.

Theorem (Thue 1909)

A Thue equation has finitely many solutions $(x, y) \in \mathbb{Z}^2$.

Example

The equation $F(x, y) = x^3 - 3xy^2 - y^3 = 1$ has only 6 integer solutions:

$$(x, y) = (0, -1), (-1, 1), (1, 0), (2, 1), (1, -3), (-3, 2).$$

Let α be an algebraic number of degree $n \geq 2$,
i.e. $f(\alpha) = 0$ with $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Z}$.

Theorem (Liouville 1844)

$$\exists c_1 = c_1(\alpha) > 0 \quad \text{s.t.} \quad \left| \alpha - \frac{x}{y} \right| > \frac{c_1}{y^n} \quad \text{for } \forall x, y (y > 0)$$

This theorem is **effective**, i.e. can compute c_1 explicitly.
Indeed, we may take

$$c_1(\alpha) = \min(1, 1/C), \quad C = \max_{[\alpha-1, \alpha+1]} |f'(x)|.$$

Example

- ▶ $\alpha = \sqrt{2}$, $c_1 = \frac{1}{2(\alpha+1)} \approx 0.20717$
- ▶ $\alpha = \sqrt[3]{2}$, $c_1 = \frac{1}{3(\alpha+1)^2} \approx 0.0652668$

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence§4 Theorem O₁,
O₂: Okazaki's
Theorem§5 Theorem S:
Solutions

Let α be an algebraic number of degree $n \geq 2$,
i.e. $f(\alpha) = 0$ with $f(x) = a_n x^n + \cdots + a_1 x + a_0$, $a_i \in \mathbb{Z}$.

Theorem (Thue 1909)

$$\exists c_2 = c_2(\alpha) > 0 \quad \text{s.t.} \quad \left| \alpha - \frac{x}{y} \right| > \frac{c_2}{y^{\frac{n}{2}+1}} \quad \text{for } \forall x, y \ (y > 0).$$

- ▶ This theorem is **not effective** (cannot compute c_2).

Corollary (Thue 1909)

$$\left| \alpha - \frac{x}{y} \right| < \frac{1}{y^{\frac{n}{2}+1+\varepsilon}} \quad \text{has only finitely many solutions } \frac{x}{y} \in \mathbb{Q}.$$

Through many mathematicians' efforts, Roth proved:

Theorem (Roth 1955)

$$\left| \alpha - \frac{x}{y} \right| < \frac{1}{y^{2+\varepsilon}} \quad \text{has only finitely many solutions } \frac{x}{y} \in \mathbb{Q}.$$

Proof of Thue's theorem :

$F(x, y) = \lambda$ has only finitely many solutions

By contradiction. Suppose not.

Let $F(x, 1) = f(x) = a_n(x - \alpha_1) \cdots (x - \alpha_n)$.

Define $\gamma = \min_{i \neq j} |\alpha_i - \alpha_j|$.

Claim 1 $\exists i \exists \infty(x, y)$ with $F(x, y) = \lambda$ and $|\alpha_i - \frac{x}{y}| < \frac{\gamma}{2}$.

\therefore If not, $\exists \infty(x, y)$ s.t. $|\lambda| = |F(x, y)| = |y^n f(\frac{x}{y})| = |a_n y^n| \prod_{i=1}^n |\frac{x}{y} - \alpha_i| \geq |a_n y^n| (\frac{\gamma}{2})^n \rightarrow \infty (|y| \rightarrow \infty)$.

Fix $\alpha = \alpha_1$ with $\exists \infty(x, y)$ s.t. $|\alpha - \frac{x}{y}| < \frac{\gamma}{2}$ (WLOG).

Claim 2 For $i = 2, \dots, n$, $|\frac{x}{y} - \alpha_i| > \frac{\gamma}{2}$.

$\therefore \gamma \leq |\alpha - \alpha_i| \leq |\alpha - \frac{x}{y}| + |\frac{x}{y} - \alpha_i| < \frac{\gamma}{2} + |\frac{x}{y} - \alpha_i|$.

$$\frac{\exists c_2}{|y|^{\frac{n}{2}+1}} < \left| \alpha - \frac{x}{y} \right| = \left| \frac{F(x, y)}{a_n y^n \prod_{i=2}^n (\frac{x}{y} - \alpha_i)} \right| < \frac{|\lambda|}{|a_n| |y^n| (\frac{\gamma}{2})^{n-1}}.$$

(↑ by **Thue's Theorem**) (↑ by **Claim 2**)

Hence $|y| < \left(\frac{\lambda}{c_2 |a_n| (\frac{\gamma}{2})^{n-1}} \right)^{1/(n-\frac{n}{2}-1)}$. Contradiction. \square

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence§4 Theorem O₁,
O₂: Okazaki's
Theorem§5 Theorem S:
Solutions

Theorem (Baker 1967)

Let $n \geq 2$. Let $\alpha_1, \dots, \alpha_n$ be non-zero algebraic numbers s.t. $\log \alpha_1, \dots, \log \alpha_n$ are linearly independent over \mathbb{Q} .

Suppose $\kappa > 2n + 1$ and $d \in \mathbb{Z}_{>0}$.

Then $\exists C = C(n, \alpha_1, \dots, \alpha_n, \kappa, d) > 0$; effectively computable number s.t.

\forall algebraic numbers β_1, \dots, β_n not all zero with $\deg \beta_i \leq d$,

$$|\beta_1 \log \alpha_1 + \dots + \beta_n \log \alpha_n| > C e^{-(\log H)^\kappa}$$

where $H = \max\{H(\beta_1), \dots, H(\beta_n)\}$ and $H(\beta_i)$; height of β_i .

Theorem (Baker 1968)

Suppose $\kappa > n + 1 \geq 4$.

All solutions $(x, y) \in \mathbb{Z}^2$ of Thue eq. $F(x, y) = \lambda$ satisfy

$$\max\{|x|, |y|\} < C e^{(\log \lambda)^\kappa}$$

where $C = C(n, \kappa, a_0, \dots, a_n)$ is effectively computable.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

Thomas' theorem for a family of Thue equations

Family of cubic
Thue equations

Akinari Hoshi

$$F_m^{(3)}(X, Y) = X^3 - mX^2Y - (m+3)XY^2 - Y^3 = 1$$

By using Baker's theory, Thomas proved

Theorem (Thomas 1990)

If $-1 \leq m \leq 10^3$ or $1.365 \times 10^7 \leq m$, then all solutions of $F_m^{(3)}(x, y) = 1$ are given by trivial solutions $(x, y) = (0, -1), (-1, 1), (1, 0)$ for $\forall m$ and additionally

$$(x, y) = (-1, -1), (-1, 2), (2, -1) \quad \text{for } m = -1,$$

$$(x, y) = (5, 4), (4, -9), (-9, 5) \quad \text{for } m = -1,$$

$$(x, y) = (2, 1), (1, -3), (-3, 2) \quad \text{for } m = 0,$$

$$(x, y) = (-7, -2), (-2, 9), (9, -7) \quad \text{for } m = 2.$$

Theorem (Mignotte 1993)

For the remaining case, \exists only trivial solutions.

► Theorem C

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

§2 Results

We consider Thomas' family of cubic Thue equations

$$F_m^{(3)}(X, Y) := X^3 - mX^2Y - (m+3)XY^2 - Y^3 = \lambda$$

for $m \in \mathbb{Z}$ and general $\lambda \in \mathbb{Z}$ ($\lambda \neq 0$).

- ▶ We may assume that $-1 \leq m$ and $0 < \lambda$ because

$$\begin{aligned}F_{-m-3}^{(3)}(X, Y) &= F_m^{(3)}(-Y, -X), \\ -F_m^{(3)}(X, Y) &= F_m^{(3)}(-X, -Y).\end{aligned}$$

- ▶ $\lambda = a^3$ for some $a \in \mathbb{Z}$, $F_m^{(3)}(x, y) = a^3$ has three **trivial solutions** $(a, 0)$, $(0, -a)$, $(-a, a)$, i.e. $xy(x+y) = 0$.
- ▶ If $(x, y) \in \mathbb{Z}^2$ is solution, then $(y, -x-y)$, $(-x-y, x)$ are also solutions because $F_m^{(3)}(x, y)$ is invariant under the action $x \mapsto y \mapsto -x-y \mapsto x$ of order three.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

Mignotte-Pethö-Lemmermeyer (1996)

Family of cubic
Thue equations

Akinari Hoshi

$$F_m^{(3)}(X, Y) = X^3 - mX^2Y - (m+3)XY^2 - Y^3 = \lambda$$

By using Baker's theory, they proved:

Theorem Mignotte-Pethö-Lemmermeyer (1996)

Let $m \geq 1649$ and $\lambda > 1$. If $F_m^{(3)}(x, y) = \lambda$, then

$$\log |y| < c_1 \log^2(m+3) + c_2 \log(m+1) \log \lambda$$

where

$$c_1 = 700 + 476.4 \left(1 - \frac{1432.1}{m+1}\right)^{-1} \left(1.501 - \frac{1902}{m+1}\right) < 1956.4,$$

$$c_2 = 29.82 + \left(1 - \frac{1432.1}{m+1}\right)^{-1} \frac{1432}{(m+1) \log(m+1)} < 30.71.$$

Example (much smaller than previous bounds)

- ▶ If $m = 1649$ and $\lambda = 10^9$, then $|y| < 10^{48698}$.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

$$F_m^{(3)}(X, Y) = X^3 - mX^2Y - (m+3)XY^2 - Y^3 = \lambda$$

By using Baker's theory, they proved:

Theorem Mignotte-Pethö-Lemmermeyer (1996)

For $-1 \leq m$ and $1 < \lambda \leq 2m + 3$, all solutions to $F_m^{(3)}(x, y) = \lambda$ are given by trivial solutions for $\lambda = a^3$ and

$$(x, y) \in \{(-1, 2), (2, -1), (-1, -1), \\ (-1, m+2), (m+2, -m-1), (-m-1, -1)\}$$

for $\lambda = 2m + 3$,

except for $m = 1$ in which case \exists extra solutions:

$$(x, y) \in \{(1, -4), (-4, 3), (3, 1), (3, -11), (-11, 8), (8, 3)\}$$

for $\lambda = 5 (= 2m + 3)$.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

Lettl-Pethö-Voutier (1999)

Let θ_2 be a root of $f_m(X) := F_m(X, 1)$ with $-\frac{1}{2} < \theta_2 < 0$.

By using hypergeometric method, they proved:

Theorem Lettl-Pethö-Voutier (1999)

Let $m \geq 1$ and assume that $(x, y) \in \mathbb{Z}^2$ is a primitive solution to $|F_m^{(3)}(x, y)| \leq \lambda(m)$ with $-\frac{y}{2} < x \leq y$ and $\frac{8\lambda(m)}{2m+3} \leq y$ where $\lambda(m) : \mathbb{Z} \rightarrow \mathbb{N}$. Then

(i) x/y is a convergent to θ_2 , and we have either $y = 1$ or

$$\left| \frac{x}{y} - \theta_2 \right| < \frac{\lambda(m)}{y^3(m+1)} \quad \text{and} \quad y \geq m + 2.$$

(ii) Define

$$\kappa = \frac{\log(\sqrt{m^2 + 3m + 9}) + 0.83}{\log(m + \frac{3}{2}) - 1.3}.$$

If $m \geq 30$, then $y^{2-\kappa} < 17.78 \cdot 2.59^\kappa \lambda(m)$.

Example (comparing with MPL (1996))

► For $m = 1649$, $|y| < 635\lambda(m)^{1.54}$ instead of $|y| < 10^{46649}\lambda(m)^{288}$.

$$f_m^{(3)}(X) := F_m^{(3)}(X, 1), \quad L_m^{(3)} := \text{Spl}_{\mathbb{Q}} f_m^{(3)}(X)$$

- ▶ The splitting fields $L_m^{(3)}$ are totally real cyclic cubic fields which are called **Shanks' simplest cubic** fields.
- ▶ $L_m^{(3)} = L_{-m-3}^{(3)}$ for $m \in \mathbb{Z}$. $\text{disc}_X f_m^{(3)} = (m^2 + 3m + 9)^2$.

Theorem C (Correspondence)

For a given $m \in \mathbb{Z}$,

$\exists (x, y) \in \mathbb{Z}^2$ with $xy(x+y) \neq 0$ s.t. $F_m^{(3)}(x, y) = \lambda$

for some $\lambda \in \mathbb{N}$ with $\lambda \mid m^2 + 3m + 9$

$\iff \exists n \in \mathbb{Z} \setminus \{m, -m-3\}$ s.t. $L_m^{(3)} = L_n^{(3)}$.

Moreover integers n, m and $(x, y) \in \mathbb{Z}^2$ satisfy

$$N = m + \frac{(m^2 + 3m + 9)xy(x+y)}{F_m^{(3)}(x, y)}$$

where N is either n or $-n-3$.

▶ Thomas' theorem

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

For a fixed $m \in \mathbb{Z}$, we obtain the correspondence

$$\boxed{\exists n \in \mathbb{Z} \setminus \{m, -m - 3\} \text{ s.t. } L_m^{(3)} = L_n^{(3)}} \quad (I)$$

1 : 3 \Updownarrow Theorem C

$$\boxed{\begin{array}{l} \exists (x, y) \in \mathbb{Z}^2 \text{ with } xy(x + y) \neq 0 \\ \text{s.t. } F_m^{(3)}(x, y) = \lambda |m^2 + 3m + 9 \end{array}} \quad (II)$$

► $\text{disc}(F_m^{(3)}(X, Y)) = (m^2 + 3m + 9)^2$.

Corollary

For a fixed $m \geq -1$,

$$\#\{n \geq -1 \mid (I)\} = \frac{\#\{(x, y) \mid (II) \ \& \ \gcd(x, y) = 1\}}{3}.$$

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence§4 Theorem O₁,
O₂: Okazaki's
Theorem§5 Theorem S:
Solutions

R. Okazaki's theorems O_1 , O_2

Okazaki announced the following theorems in 2002.

He use his result on gaps between sol's (2002) which is based on Baker's theory: Laurent-Mignotte-Nesterenko (1995).

Theorem O_1 (Okazaki 2002+ α)

For $-1 \leq m < n \in \mathbb{Z}$, if $L_m^{(3)} = L_n^{(3)}$ then $m \leq 35731$.

Theorem O_2 (Okazaki unpublished)

For $-1 \leq m < n \in \mathbb{Z}$, if $L_m^{(3)} = L_n^{(3)}$ then
 $m, n \in \{-1, 0, 1, 2, 3, 5, 12, 54, 66, 1259, 2389\}$.

In particular, we get

$$\begin{aligned} L_{-1}^{(3)} = L_5^{(3)} = L_{12}^{(3)} = L_{1259}^{(3)}, \\ L_0^{(3)} = L_3^{(3)} = L_{54}^{(3)}, \quad L_1^{(3)} = L_{66}^{(3)}, \quad L_2^{(3)} = L_{2389}^{(3)}. \end{aligned}$$

A brief sketch of the proof (slide) is available at

<http://www1.doshisha.ac.jp/~rokazaki/papers.html>

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O_1 ,
 O_2 : Okazaki's
Theorem

§5 Theorem S:
Solutions

Thomas' $4 \times 3 = 12$ non-trivial solutions for $\lambda = 1$

$$(x, y) = (-1, -1), (-1, 2), (2, -1) \quad \text{for } m = -1,$$

$$(x, y) = (5, 4), (4, -9), (-9, 5) \quad \text{for } m = -1,$$

$$(x, y) = (2, 1), (1, -3), (-3, 2) \quad \text{for } m = 0,$$

$$(x, y) = (-7, -2), (-2, 9), (9, -7) \quad \text{for } m = 2$$

correspond to

$$L_{-1}^{(3)} = L_{12}^{(3)}, \quad L_{-1}^{(3)} = L_{1259}^{(3)}, \quad L_0^{(3)} = L_{54}^{(3)}, \quad L_2^{(3)} = L_{2389}^{(3)}.$$

$$L_{-1}^{(3)} = L_5^{(3)}, \quad L_0^{(3)} = L_3^{(3)}, \quad L_1^{(3)} = L_{66}^{(3)}, \quad L_3^{(3)} = L_{54}^{(3)}, \\ L_5^{(3)} = L_{12}^{(3)}, \quad L_5^{(3)} = L_{1259}^{(3)}, \quad L_{12}^{(3)} = L_{1259}^{(3)}$$

correspond to $7 \times 3 = \exists 21$ (non-trivial) solutions for $\lambda > 1$.

$$L_m^{(3)} = L_n^{(3)} \text{ (33 solutions), } L_n^{(3)} = L_m^{(3)} \text{ (33 solutions)}$$

Conclusion: in total $\exists 66$ solutions.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

Theorem S: Solutions

$$F_m^{(3)}(X, Y) = X^3 - mX^2Y - (m+3)XY^2 - Y^3 = \lambda$$

By [Theorem C](#) and [Theorems O₁](#), [O₂](#), we get:

Theorem S

For $m \geq -1$,

all integer solutions $(x, y) \in \mathbb{Z}^2$ with $xy(x+y) \neq 0$
to $F_m^{(3)}(x, y) = \lambda$ with $\lambda \in \mathbb{N}$ and $\lambda \mid m^2 + 3m + 9$
are given in Table 1. (66 solutions)

Corollary

For $m \geq -1$, all solutions to $F_m^{(3)}(x, y) = m^2 + 3m + 9$ are
given in Table 1 and $(x, y) = (3, 0), (0, -3), (-3, 3)$.

- ▶ \therefore the elliptic curve $y^2 + 3y = x^3 - 9$ over \mathbb{Q} has only
two integral points $(x, y) = (3, -6), (3, 3)$.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

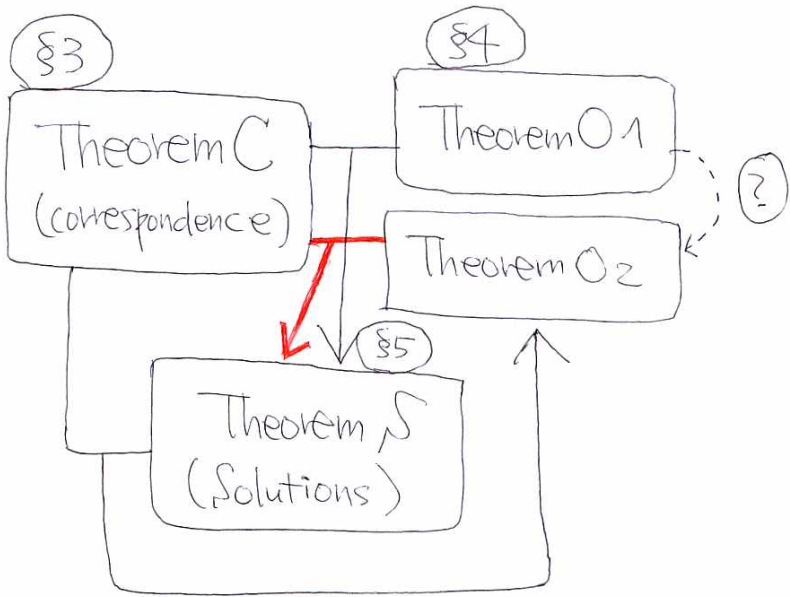
§5 Theorem S:
Solutions

Table 1

| m | n | $-n - 3$ | $2m + 3$ | λ | $m^2 + 3m + 9$ | (x, y) |
|------|-------|----------|----------|------------------|------------------|----------------------------------|
| -1 | -15 | 12 | 1 | 1 | 7 | $(-1, 2), (2, -1), (-1, -1)$ |
| -1 | 1259 | -1262 | 1 | 1 | 7 | $(4, -9), (-9, 5), (5, 4)$ |
| -1 | 5 | -8 | 1 | 7 | 7 | $(1, -3), (-3, 2), (2, 1)$ |
| 0 | 54 | -57 | 3 | 1 | 9 | $(1, -3), (-3, 2), (2, 1)$ |
| 0 | -6 | 3 | 3 | 3 | 9 | $(-1, 2), (2, -1), (-1, -1)$ |
| 1 | -69 | 66 | 5 | 13 | 13 | $(-2, 7), (7, -5), (-5, -2)$ |
| 2 | -2392 | 2389 | 7 | 1 | 19 | $(-2, 9), (9, -7), (-7, -2)$ |
| 3 | -3 | 0 | 9 | 9 | 27 | $(-1, 2), (2, -1), (-1, -1)$ |
| 3 | -57 | 54 | 9 | 9 | 27 | $(-1, 5), (5, -4), (-4, -1)$ |
| 5 | 1259 | -1262 | 13 | 49 | 49 | $(3, -22), (-22, 19), (19, 3)$ |
| 5 | -15 | 12 | 13 | 49 | 49 | $(-1, 5), (5, -4), (-4, -1)$ |
| 5 | -1 | -2 | 13 | 49 | 49 | $(-1, -2), (-2, 3), (3, -1)$ |
| 12 | -2 | -1 | 27 | 27 | $3^3 \cdot 7$ | $(-1, 2), (2, -1), (-1, -1)$ |
| 12 | -1262 | 1259 | 27 | 27 | $3^3 \cdot 7$ | $(-1, 14), (14, -13), (-13, -1)$ |
| 12 | -8 | 5 | 27 | $3^3 \cdot 7$ | $3^3 \cdot 7$ | $(-1, 5), (5, -4), (-4, -1)$ |
| 54 | 0 | -3 | 111 | 7^3 | $3^2 \cdot 7^3$ | $(-1, -2), (-2, 3), (3, -1)$ |
| 54 | -6 | 3 | 111 | $3 \cdot 7^3$ | $3^2 \cdot 7^3$ | $(-1, 5), (5, -4), (-4, -1)$ |
| 66 | -4 | 1 | 135 | $3^3 \cdot 13^2$ | $3^3 \cdot 13^2$ | $(-2, 7), (7, -5), (-5, -2)$ |
| 1259 | -1 | -2 | 2521 | 61^3 | $7 \cdot 61^3$ | $(-4, -5), (-5, 9), (9, -4)$ |
| 1259 | -15 | 12 | 2521 | 61^3 | $7 \cdot 61^3$ | $(-1, 14), (14, -13), (-13, -1)$ |
| 1259 | 5 | -8 | 2521 | $7 \cdot 61^3$ | $7 \cdot 61^3$ | $(-3, -19), (-19, 22), (22, -3)$ |
| 2389 | -5 | 2 | 4781 | 67^3 | $19 \cdot 67^3$ | $(-2, 9), (9, -7), (-7, -2)$ |

Table 1

| m | n | $-n - 3$ | $2m + 3$ | λ | $m^2 + 3m + 9$ | (x, y) |
|------|-------|----------|----------|------------------|------------------|----------------------------------|
| -1 | -15 | 12 | 1 | 1 | 7 | $(-1, 2), (2, -1), (-1, -1)$ |
| -1 | 1259 | -1262 | 1 | 1 | 7 | $(4, -9), (-9, 5), (5, 4)$ |
| -1 | 5 | -8 | 1 | 7 | 7 | $(1, -3), (-3, 2), (2, 1)$ |
| 0 | 54 | -57 | 3 | 1 | 9 | $(1, -3), (-3, 2), (2, 1)$ |
| 0 | -6 | 3 | 3 | 3 | 9 | $(-1, 2), (2, -1), (-1, -1)$ |
| 1 | -69 | 66 | 5 | 13 | 13 | $(-2, 7), (7, -5), (-5, -2)$ |
| 2 | -2392 | 2389 | 7 | 1 | 19 | $(-2, 9), (9, -7), (-7, -2)$ |
| 3 | -3 | 0 | 9 | 9 | 27 | $(-1, 2), (2, -1), (-1, -1)$ |
| 3 | -57 | 54 | 9 | 9 | 27 | $(-1, 5), (5, -4), (-4, -1)$ |
| 5 | 1259 | -1262 | 13 | 49 | 49 | $(3, -22), (-22, 19), (19, 3)$ |
| 5 | -15 | 12 | 13 | 49 | 49 | $(-1, 5), (5, -4), (-4, -1)$ |
| 5 | -1 | -2 | 13 | 49 | 49 | $(-1, -2), (-2, 3), (3, -1)$ |
| 12 | -2 | -1 | 27 | 27 | $3^3 \cdot 7$ | $(-1, 2), (2, -1), (-1, -1)$ |
| 12 | -1262 | 1259 | 27 | 27 | $3^3 \cdot 7$ | $(-1, 14), (14, -13), (-13, -1)$ |
| 12 | -8 | 5 | 27 | $3^3 \cdot 7$ | $3^3 \cdot 7$ | $(-1, 5), (5, -4), (-4, -1)$ |
| 54 | 0 | -3 | 111 | 7^3 | $3^2 \cdot 7^3$ | $(-1, -2), (-2, 3), (3, -1)$ |
| 54 | -6 | 3 | 111 | $3 \cdot 7^3$ | $3^2 \cdot 7^3$ | $(-1, 5), (5, -4), (-4, -1)$ |
| 66 | -4 | 1 | 135 | $3^3 \cdot 13^2$ | $3^3 \cdot 13^2$ | $(-2, 7), (7, -5), (-5, -2)$ |
| 1259 | -1 | -2 | 2521 | 61^3 | $7 \cdot 61^3$ | $(-4, -5), (-5, 9), (9, -4)$ |
| 1259 | -15 | 12 | 2521 | 61^3 | $7 \cdot 61^3$ | $(-1, 14), (14, -13), (-13, -1)$ |
| 1259 | 5 | -8 | 2521 | $7 \cdot 61^3$ | $7 \cdot 61^3$ | $(-3, -19), (-19, 22), (22, -3)$ |
| 2389 | -5 | 2 | 4781 | 67^3 | $19 \cdot 67^3$ | $(-2, 9), (9, -7), (-7, -2)$ |



§3 Theorem C: Correspondence

$$F_m^{(3)}(X, Y) = X^3 - mX^2Y - (m+3)XY^2 - Y^3,$$
$$f_m^{(3)}(X) := F_m^{(3)}(X, 1), \quad L_m^{(3)} := \text{Spl}_{\mathbb{Q}} f_m^{(3)}(X)$$

- ▶ $f_m^{(3)}(X)$ is a generic polynomial for C_3 over any field k .

Definition (generic polynomial) $\mathbf{t} = (t_1, \dots, t_n)$.

A polynomial $f(\mathbf{t}, X) \in k(\mathbf{t})[X]$ is called **generic** over k if

- (1) $\text{Gal}(f/k(\mathbf{t})) \simeq G$;
- (2) $\forall M/K \supset k$ with $\text{Gal}(M/K) \simeq G$,
 $\exists \mathbf{a} \in K^n$ s.t. $M = \text{Spl}_K f(\mathbf{a}, X)$.

- ▶ related to Inverse Galois Problem.
- ▶ When $L_m^{(3)} = L_n^{(3)}$?

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

§3 Theorem C: Correspondence

$$F_m^{(3)}(X, Y) = X^3 - mX^2Y - (m+3)XY^2 - Y^3,$$
$$f_m^{(3)}(X) := F_m^{(3)}(X, 1), \quad L_m^{(3)} := \text{Spl}_{\mathbb{Q}} f_m^{(3)}(X)$$

Theorem (Morton 1994, Chapman 1996, Hoshi-Miyake 2009)

Assume that $\text{char } k \neq 2$.

For $m, n \in k$, $L_m^{(3)} = L_n^{(3)}$

$$\iff \exists u \in k \text{ s.t. either } n = m + \frac{(m^2 + 3m + 9)u(u+1)}{f_m(u)}$$

or $n = -m - 3 - \frac{(m^2 + 3m + 9)u(u+1)}{f_m(u)}$.

- ▶ using multi-resolvent polynomial.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

Proof of Theorem C

By above [Theorem](#), $L_n^{(3)} = L_m^{(3)} \iff \exists u \in \mathbb{Q}$ s.t. either $n = m + \frac{(m^2+3m+9)u(u+1)}{f_m^{(3)}(u)}$ or $n = -m - 3 - \frac{(m^2+3m+9)u(u+1)}{f_m^{(3)}(u)}$.

Write $u = x/y$ with $\gcd(x, y) = 1$ then we have

$$n = m + \frac{(m^2+3m+9)xy(x+y)}{F_m^{(3)}(x,y)} \text{ or } n = -m - 3 - \frac{(m^2+3m+9)xy(x+y)}{F_m^{(3)}(x,y)}.$$

- ▶ If $\exists x, y \in \mathbb{Z}$ s.t. $F_m^{(3)}(x, y) =: \lambda \mid m^2 + 3m + 9$ and $xy(x+y) \neq 0$, then $\exists n \in \mathbb{Z} \setminus \{m, -m-3\}$ s.t.

$$L_n^{(3)} = L_m^{(3)}.$$

- ▶ We should show that **the converse also holds**, namely $L_n^{(3)} = L_m^{(3)}, (n \neq m, -m-3) \implies \lambda \mid m^2 + 3m + 9$.

Define $h(u) := (m^2 + 3m + 9)u(u+1)$. Then

$$\frac{h(u)}{f_m^{(3)}(u)} \in \mathbb{Z} \text{ where } u = x/y \text{ with } \gcd(x, y) = 1.$$

[§0 fun](#)[§1 Introduction:
Brief history](#)[§2 Results](#)[§3 Theorem C:
Correspondence](#)[§4 Theorem O₁,
O₂: Okazaki's
Theorem](#)[§5 Theorem S:
Solutions](#)

Take the resultant $R := \text{Res}_u(h(u), f_m^{(3)}(u))$

$$R = \begin{vmatrix} m^2 + 3m + 9 & m^2 + 3m + 9 & 0 & 0 & 0 \\ 0 & m^2 + 3m + 9 & m^2 + 3m + 9 & 0 & 0 \\ 0 & 0 & m^2 + 3m + 9 & m^2 + 3m + 9 & 0 \\ 1 & m + 3 & m & -1 & 0 \\ 0 & 1 & m + 3 & m & -1 \end{vmatrix}$$

$$= -(m^2 + 3m + 9)^3.$$

We also see

$$R = \begin{vmatrix} m^2 + 3m + 9 & m^2 + 3m + 9 & 0 & 0 & h(u)u^2 \\ 0 & m^2 + 3m + 9 & m^2 + 3m + 9 & 0 & h(u)u \\ 0 & 0 & m^2 + 3m + 9 & m^2 + 3m + 9 & h(u) \\ 1 & m + 3 & m & -1 & f_m^{(3)}(u)u \\ 0 & 1 & m + 3 & m & f_m^{(3)}(u) \end{vmatrix}$$

$$= -(m^2 + 3m + 9)^2 \left(h(u)p(u) + f_m^{(3)}(u)q(u) \right) \text{ where}$$

$$p(u) = 2u^2 - (2m+1)u - m - 5, \quad q(u) = -(m^2 + 3m + 9)(2u + 1).$$

Hence we have

$$h(u)p(u) + f_m^{(3)}(u)q(u) = (m^2 + 3m + 9).$$

Take the homogeneous form

$$H(x, y) := y^3 \cdot h(x/y), \quad P(x, y) := y^2 \cdot p(x/y),$$

$$Q(x, y) := y^2 \cdot p(x/y), \quad F_m^{(3)}(x, y) = y^3 \cdot f_m^{(3)}(x/y).$$

Then

$$H(x, y)P(x, y) + F_m^{(3)}(x, y)Q(x, y) = (m^2 + 3m + 9)y^5.$$

Hence

$$\frac{H(x, y)P(x, y)}{F_m^{(3)}(x, y)} + Q(x, y) = \frac{(m^2 + 3m + 9)y^5}{F_m^{(3)}(x, y)} \in \mathbb{Z}.$$

We also see

$$\frac{H(x, y)P(x, y)\sigma^2}{F_m^{(3)}(x, y)} + Q(x, y)\sigma^2 = \frac{(m^2 + 3m + 9)x^5}{F_m^{(3)}(x, y)} \in \mathbb{Z}.$$

where $\sigma^2 : y \mapsto x \mapsto -x - y$

because $F_m^{(3)}(x, y)$ and $H(x, y)$ are σ -invariants.

Since $\gcd(x, y) = 1$, $\lambda = F_m^{(3)}(x, y) \mid m^2 + 3m + 9$.

► Theorem C



§4 Theorem O_1 : Okazaki's Theorem

For $m \in \mathbb{Z}$, we take

$$F_m^{(3)}(X, Y) = (X - \theta_1^{(m)}Y)(X - \theta_2^{(m)}Y)(X - \theta_3^{(m)}Y),$$

and $L_m = \mathbb{Q}(\theta_1^{(m)})$. We see

$$-2 < \theta_3^{(m)} < -1, \quad -\frac{1}{2} < \theta_2^{(m)} < 0, \quad 1 < \theta_1^{(m)}.$$

Take the exterior product

$$\boldsymbol{\delta} = {}^t(\delta_1, \delta_2, \delta_3) := \mathbf{1} \times \boldsymbol{\theta} = {}^t(\theta_2 - \theta_3, \theta_3 - \theta_1, \theta_1 - \theta_2)$$

where $\mathbf{1} = {}^t(1, 1, 1)$, $\boldsymbol{\theta} = {}^t(\theta_1, \theta_2, \theta_3) \in \mathbb{R}^3$.

The norm $N(\boldsymbol{\delta}) = \delta_1 \delta_2 \delta_3 = -\sqrt{D}$ where
 $D = ((\theta_1 - \theta_2)(\theta_1 - \theta_3)(\theta_2 - \theta_3))^2$.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O_1 ,
 O_2 : Okazaki's
Theorem

§5 Theorem S:
Solutions

The canonical lattice

$$\mathcal{L}^{\natural} = \delta(\mathbb{Z}\mathbf{1} + \mathbb{Z}\theta)$$

of F is orthogonal to $\mathbf{1}$, where the product of vectors is the component-wise product. We consider the curve \mathcal{H}

$$\mathcal{H} : z_1 + z_2 + z_3 = 0, \quad z_1 z_2 z_3 = \sqrt{D}.$$

on the plane $\Pi = \{ {}^t(z_1, z_2, z_3) \in \mathbb{R}^3 \mid z_1 + z_2 + z_3 = 0 \}$.

For (x, y) with $F_m^{(3)}(x, y) = 1$, we see $x\mathbf{1} - y\theta \in (\mathcal{O}_{L_m}^{\times})^3$ because $N(x\mathbf{1} - y\theta) = 1$. Then we get a bijection

$$(x, y) \longleftrightarrow z = \delta(-x\mathbf{1} + y\theta) \in \mathcal{L}^{\natural} \cap \mathcal{H}$$

via $N(z) = N(\delta)N(-x\mathbf{1} + y\theta) = (-\sqrt{D})(-1) = \sqrt{D}$. Let

$\log : (\mathbb{R}^{\times})^3 \ni {}^t(z_1, z_2, z_3) \mapsto {}^t(\log |z_1|, \log |z_2|, \log |z_3|) \in \mathbb{R}^3$

be the logarithmic map. By Dirichlet's unit theorem, the set

$$\mathcal{E}(L_m) := \{ \log \varepsilon \mid \varepsilon = {}^t(\varepsilon, \varepsilon^{\sigma}, \varepsilon^{\sigma^2}), \varepsilon \in \mathcal{O}_{L_m}^{\times} \}$$

is a lattice of rank 2 on the plane

$$\Pi_{\log} := \{ {}^t(u_1, u_2, u_3) \in \mathbb{R}^3 \mid u_1 + u_2 + u_3 = 0 \}.$$

We use the modified logarithmic map

$$\phi : (\mathbb{R}^\times)^3 \ni \mathbf{z} \mapsto \mathbf{u} = {}^t(u_1, u_2, u_3) = \log(D^{-1/6} \mathbf{z}) \in \mathbb{R}^3.$$

For (x, y) with $F_m^{(3)}(x, y) = 1$ and

$$\mathbf{z} = \delta(-x\mathbf{1} + y\boldsymbol{\theta}) \in \mathcal{L}^{\natural} \cap \mathcal{H},$$

$\mathbf{u} = \phi(\mathbf{z}) = \phi(\delta(-x\mathbf{1} + y\boldsymbol{\theta})) \in \phi(\delta) + \mathcal{E}(L_m) \subset \Pi_{\log}$; the displaced lattice, since $-x\mathbf{1} + y\boldsymbol{\theta} \in (\mathcal{O}_{L_m}^\times)^3$. We can show

$$\blacktriangleright 3\phi(\delta) \in \mathcal{E}(L_m).$$

We now assume that $L_m = L_n$ for $-1 \leq m < n$ and take a common trivial solution $(x, y) = (1, 0)$. Then

$$\mathbf{u}^{(m)}, \mathbf{u}^{(n)} \in \mathcal{M} = \mathbb{Z}\phi(\delta^{(m)}) + \mathbb{Z}\phi(\delta^{(n)}) + \mathcal{E}(L_m) \subset \Pi_{\log}$$

where \mathcal{M} is a lattice with discriminant

$d(\mathcal{M}) = d(\mathcal{E}(L_m))$, $\frac{1}{3}d(\mathcal{E}(L_m))$ or $\frac{1}{9}d(\mathcal{E}(L_m))$. We may get:

$$\blacktriangleright d(\mathcal{M}) = d(\mathcal{E}(L_m)) \text{ or } \frac{1}{3}d(\mathcal{E}(L_m)).$$

We adopt local coordinates for $\mathcal{C} := \phi(\mathcal{H}) \subset \Pi_{\log}$ by

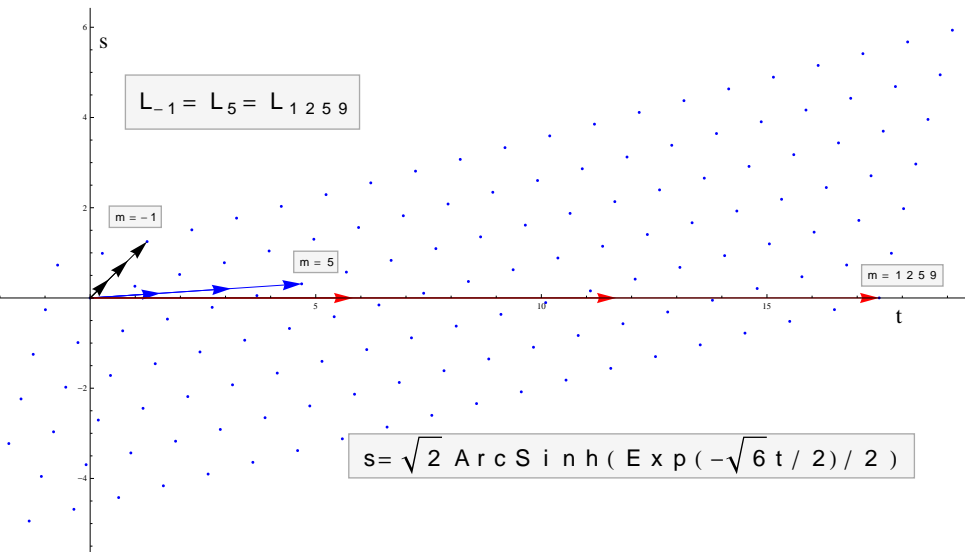
$$s = s(\mathbf{u}) := \frac{u_2 - u_3}{\sqrt{2}}, \quad t = t(\mathbf{u}) := -\frac{\sqrt{6}u_1}{2}.$$

Then

$$s = \sqrt{2} \operatorname{arcsinh} \left(\exp \left(-\sqrt{6}t/2 \right) / 2 \right), \quad 0 \leq s \leq \sqrt{3}t.$$

Example

| m | -1 | 0 | 1 | 2 | 3 | 4 | 5 |
|-----|--------|--------|--------|--------|--------|--------|--------|
| s | 0.4163 | 0.3016 | 0.2263 | 0.1773 | 0.1444 | 0.1212 | 0.1042 |
| t | 0.4206 | 0.6893 | 0.9267 | 1.1269 | 1.2952 | 1.4385 | 1.5624 |



Using a result of Laurent-Mignotte-Nesterenko (1995) in Baker's theory, Okazaki gave:

Theorem (Okazaki 2002)

Assume distinct points $\mathbf{u} = \mathbf{u}^{(m)}$ and $\mathbf{u}' = \mathbf{u}^{(n)}$ of \mathcal{M} on \mathcal{C} . Assume $t' = t(\mathbf{u}') \geq t = t(\mathbf{u})$. Then

$$\frac{\sqrt{2} d(\mathcal{M}) \exp(\sqrt{6}t/2)}{1 + \exp(-2(t' - t)/\sqrt{6} \log 2)} \leq t'.$$

Theorem (Okazaki 2002)

For $\mathbf{z}' \in \mathcal{L}^{\natural} \cap \mathcal{H}$ and $t' = t(\mathbf{z}')$, we have

$$\frac{t'}{d(\mathbb{Z}\phi(\boldsymbol{\delta}) + \mathcal{E}(L_m))} \leq 5.04 \times 10^4.$$

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence§4 Theorem O₁,
O₂: Okazaki's
Theorem§5 Theorem S:
Solutions

We can show

$$0.14 \exp(\sqrt{6}t/2) - t < t' - t.$$

Then it follows

$$\begin{aligned} & \frac{\sqrt{2} \exp(\sqrt{6}t/2)}{1 + \exp(-2(0.14 \exp(\sqrt{6}t/2) - t)/\sqrt{6} \log 2)} \\ & < \frac{\sqrt{2} \exp(\sqrt{6}t/2)}{1 + \exp(-2(t' - t)/\sqrt{6} \log 2)} \leq \frac{t'}{d(\mathcal{M})} \leq 5.04 \times 10^4. \end{aligned}$$

We get $t \leq 8.56$ and hence $m \leq 35731$. □

§5 Theorem S: Solutions

Theorem C + Theorem O₁ ⇒ Theorem S

▶ Theorem S

Let θ_2 be a root of $f_m^{(3)}(X)$ with $-\frac{1}{2} < \theta_2 < 0$. For $m \geq 18$,

$$-\frac{1}{m} + \frac{2}{m^2} - \frac{3}{m^3} - \frac{3}{m^4} + \frac{17}{m^5} - \frac{28}{m^6} < \theta_2 < -\frac{1}{m} + \frac{2}{m^2} - \frac{3}{m^3} - \frac{3}{m^4} + \frac{17}{m^5} - \frac{27}{m^6}.$$

The continued fraction expansion of the root θ_2 of $f_m^{(3)}(X)$ is given as follows:

When m is even,

$$\theta_2 = \begin{cases} [-1; 1, m+1, \frac{m}{2}, 1, 3, \frac{m-14}{14}, 1, 6, [\frac{m}{6}], \dots], & \text{if } m = 14k \geq 28, \\ [-1; 1, m+1, \frac{m}{2}, 1, 3, \frac{m-2}{14}, [\frac{49m+72}{6}], \dots], & \text{if } m = 14k+2 \geq 156, \\ [-1; 1, m+1, \frac{m}{2}, 1, 3, \frac{m-4}{14}, 6, 1, [\frac{m-4}{6}], \dots], & \text{if } m = 14k+4 \geq 18, \\ [-1; 1, m+1, \frac{m}{2}, 1, 3, \frac{m-6}{14}, 3, 2, [\frac{m-2}{6}], \dots], & \text{if } m = 14k+6 \geq 20, \\ [-1; 1, m+1, \frac{m}{2}, 1, 3, \frac{m-8}{14}, 2, 3, [\frac{m-2}{6}], \dots], & \text{if } m = 14k+8 \geq 22, \\ [-1; 1, m+1, \frac{m}{2}, 1, 3, \frac{m-10}{14}, 1, 1, 2, 1, [\frac{m-4}{6}], \dots], & \text{if } m = 14k+10 \geq 24, \\ [-1; 1, m+1, \frac{m}{2}, 1, 3, \frac{m-12}{14}, 1, 2, 1, 1, [\frac{m-2}{6}], \dots], & \text{if } m = 14k+12 \geq 68. \end{cases}$$

When m is odd,

$$\theta_2 = \begin{cases} [-1; 1, m+1, \frac{m+1}{2}, 3, 1, \frac{m-15}{14}, 2, 3, [\frac{m-1}{6}], \dots], & \text{if } m = 14k + 1 \geq 29, \\ [-1; 1, m+1, \frac{m+1}{2}, 3, 1, \frac{m-17}{14}, 1, 1, 2, 1, [\frac{m-3}{6}], \dots], & \text{if } m = 14k + 3 \geq 31, \\ [-1; 1, m+1, \frac{m+1}{2}, 3, 1, \frac{m-19}{14}, 1, 2, 1, 1, [\frac{m-3}{6}], \dots], & \text{if } m = 14k + 5 \geq 33, \\ [-1; 1, m+1, \frac{m+1}{2}, 3, 1, \frac{m-21}{14}, 1, 6, [\frac{m-1}{6}], \dots], & \text{if } m = 14k + 7 \geq 35, \\ [-1; 1, m+1, \frac{m+1}{2}, 3, 1, \frac{m-9}{14}, 2, 3, [\frac{49m+73}{6}], \dots], & \text{if } m = 14k + 9 \geq 65, \\ [-1; 1, m+1, \frac{m+1}{2}, 3, 1, \frac{m-11}{14}, 6, 1, [\frac{m-5}{6}], \dots], & \text{if } m = 14k + 11 \geq 25, \\ [-1; 1, m+1, \frac{m+1}{2}, 3, 1, \frac{m-13}{14}, 3, 2, [\frac{m-3}{6}], \dots], & \text{if } m = 14k + 13 \geq 27. \end{cases}$$

It is enough to find all non-trivial solutions $(x, y) \in \mathbb{Z}^2$ to $F_m^{(3)}(x, y) = \lambda \mid m^2 + 3m + 9$ for $-1 \leq m \leq 35731$.

Indeed if there exists a non-trivial solution $(x, y) \in \mathbb{Z}^2$ to $F_n^{(3)}(x, y) = \lambda \mid n^2 + 3n + 9$ for $n \geq 35732$ then there exists $-1 \leq m \leq 35731$ such that $L_m = L_n$.

(i) $-1 \leq m \leq 2407$. For small m , we can use MAGMA (Bilu-Hanrot).

(ii) $2408 \leq m \leq 35731$ and $2(2m + 3 + \frac{27}{2m+3}) \leq y$. We consider $|F_m^{(3)}(x, y)| \leq m^2 + 3m + 9$. Applying Lettel-Pethö-Voutier Theorem [Theorem](#)

$$\lambda(m) = m^2 + 3m + 9, \quad \frac{8\lambda(m)}{2m+3} = 2 \left(2m + 3 + \frac{27}{2m+3} \right),$$

x/y is a convergent to θ_2 . But this is impossible.

(iii) $2408 \leq m \leq 35731$ and $y < 2(2m + 3 + \frac{27}{2m+3})$. The bound is small enough to reach using a computer.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence

§4 Theorem O₁,
O₂: Okazaki's
Theorem

§5 Theorem S:
Solutions

$$F_m^{(6)}(x, y) = x^6 - 2mx^5y - (5m + 15)x^4y^2 - 20x^3y^3 + 5mx^2y^4 + (2m + 6)xy^5 + y^6 = \lambda$$

- ▶ $f_m^{(6)}(X) := F_m^{(6)}(X, 1)$.
- ▶ $f_m^{(6)}(X)$ is irreducible/ \mathbb{Q} for $m \in \mathbb{Z} \setminus \{-8, -3, 0, 5\}$.
- ▶ $L_m^{(6)} := \text{Spl}_{\mathbb{Q}} f_m^{(6)}(X)$, then $L_m^{(6)} = L_{-m-3}^{(6)}$; the simplest sextic fields.
- ▶ $L_m^{(3)} \subset L_m^{(6)}$ for $\forall m \in \mathbb{Z}$.

Theorem

For a given $m \in \mathbb{Z}$, $\exists n \in \mathbb{Z} \setminus \{m, -m - 3\}$ s.t. $L_m^{(6)} = L_n^{(6)}$
 $\iff \exists (x, y) \in \mathbb{Z}^2$ with
 $xy(x + y)(x - y)(x + 2y)(2x + y) \neq 0$ s.t. $F_m^{(6)}(x, y) = \lambda$
for some $\lambda \in \mathbb{N}$ with $\lambda \mid 27(m^2 + 3m + 9)$.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence§4 Theorem O₁,
O₂: Okazaki's
Theorem§5 Theorem S:
Solutions

Moreover integers n, m and $(x, y) \in \mathbb{Z}^2$ satisfy

$$N = m + \frac{(m^2 + 3m + 9)xy(x+y)(x-y)(x+2y)(2x+y)}{F_m^{(6)}(x, y)}$$

where N is either n or $-n - 3$.

By Okazaki's theorem and the fact $L_m^{(3)} \subset L_m^{(6)}$, we get:

Theorem

For $m, n \in \mathbb{Z}$, $L_m^{(6)} = L_n^{(6)} \iff m = n$ or $m = -n - 3$.

Theorem

For $m \in \mathbb{Z}$, $F_m^{(6)}(x, y) = \lambda$ with $\lambda \mid 27(m^2 + 3m + 9)$ has only trivial solutions, i.e. $xy(x+y)(x-y)(x+2y)(2x+y) = 0$.

§0 fun

§1 Introduction:
Brief history

§2 Results

§3 Theorem C:
Correspondence§4 Theorem O₁,
O₂: Okazaki's
Theorem§5 Theorem S:
Solutions