A Note on the Field Isomorphism Problem
of $X^3 + sX + s$ and Related Cubic Thue Equations

Akinari HOSHI$^{1,*}$ and Katsuya MIYAKE$^{2,*}$

$^1$Department of Mathematics, Rikkyo University, 3-34-1 Nishi-Ikebukuro, Toshima-ku, Tokyo 171-8501, Japan
$^2$Department of Mathematics, School of Fundamental Science and Engineering, Waseda University, 3-4-1 Ohkubo, Shinjuku-ku, Tokyo 169-8555, Japan

Received January 30, 2009; final version accepted April 22, 2009.

We study the field isomorphism problem of cubic generic polynomial $X^3 + sX + s$ over the field of rational numbers with the specialization of the parameter $s$ to nonzero rational integers $m$ via primitive solutions to the family of cubic Thue equations $x^3 - 2m^2y - 9mxy^2 - m(2m+27)y^3 = \lambda$ where $\lambda^2$ is a divisor of $m^3(4m+27)^3$.

KEYWORDS: Field isomorphism problem, generic polynomial, cubic Thue equations

1. Introduction

Let $K$ be an arbitrary field and $K(s)$ the rational function field over $K$ with indeterminate $s$. Let $S_n$ and $C_n$ denote the symmetric group of degree $n$ and the cyclic group of order $n$ respectively. We take the cubic polynomial

$$f_s(X) = X^3 + sX + s \in K(s)[X].$$

The polynomial $f_s(X)$ is known as a generic polynomial for $S_3$ over $K$. Namely the Galois group $\text{Gal}_{K(s)}f_s(X)$ of $f_s(X)$ over $K(s)$ is isomorphic to $S_3$ and every Galois extension $L/M$ over an arbitrary field $M \supset K$ with Galois group $S_3$ can be obtained as $L = \text{Spl}_Mf_s(X)$, the splitting field of $f_s(X)$ over $M$, for some $a \in M$ (cf. [7, Section 2.1]).

Because the generic polynomial $f_s(X) = X^3 + sX + s$ supplies us all Galois extensions with Galois group $S_3$ over the base field $K$ by specializing the parameter $s$ to elements $a \in K$, it is natural to ask the following problem:

Field isomorphism problem. For $a, b \in K$, determine whether $\text{Spl}_Kf_a(X)$ and $\text{Spl}_Kf_b(X)$ are isomorphic over $K$ or not.

In the cyclic cubic case, Morton [10] gave an explicit answer to this problem for the generic polynomial $X^3 + sX^2 - (s + 3)X + 1$ for $C_3$ over a field $K$ with char $K \neq 2$ (see also [1] and [3]). In [2], the authors investigated the field isomorphism problem of $f_s(X)$ over a field $K$ with char $K \neq 3$ and gave the following theorem:

**Theorem 1 ([2, Corollary 8]).** Assume that char $K \neq 3$. For $a, b \in K \setminus \{0,-27/4\}$ with $a \neq b$, the splitting fields of $f_a(X)$ and of $f_b(X)$ over $K$ coincide if and only if there exists $u \in K$ such that

$$b = \frac{a(u^2 + 9u - 3a)^2}{(u^3 - 2au^2 - 9au - 2a^2 - 27a)^2}.$$

For the polynomial $f_s(X)$, we assume that $a \neq 0, -27/4$ since the discriminant of $f_s(X)$ is given by $-a^3(4a + 27)$. As a consequence of Theorem 1, we see that for an infinite field $K$ and a fixed element $a \in K$, there exist infinitely many elements $b \in K$ such that the field overlap $\text{Spl}_Kf_a(X) = \text{Spl}_Kf_b(X)$ occurs.

For $m \in \mathbb{Z}$, we define the cubic form $F_m(X,Y) \in \mathbb{Z}[X,Y]$ by

$$F_m(X,Y) := X^3 - 2mX^2Y - 9mXY^2 - m(2m+27)Y^3.$$

The aim of this paper is to study the field isomorphism problem of $f_s(X)$ over the field $\mathbb{Q}$ of rational numbers with the specialization $s \mapsto m \in \mathbb{Z}$ in more detail by Theorem 1 via certain integral solutions $(x,y) \in \mathbb{Z}^2$ to the family of cubic Thue equations

$$F_m(x,y) = \lambda \in \mathbb{Z}.$$
The main result of this paper is as follows:

**Theorem 2.** Let \( m \in \mathbb{Z} \setminus \{0\} \) and \( f_m(X) = X^3 + mX + m \in \mathbb{Z}[X] \). If there exists \( n \in \mathbb{Z} \setminus \{0\} \) with \( n \neq m \) such that the splitting fields of \( f_n(X) \) and of \( f_m(X) \) over \( \mathbb{Q} \) coincide then there exists a primitive solution \( (x, y) \in \mathbb{Z}^2 \) with \( y > 0 \) to

\[
F_m(x, y) = x^3 - 2mx^2y - 9mxy^2 - m(2m + 27)y^3 = \lambda
\]

for such a \( \lambda \in \mathbb{Z} \) as \( \lambda^2 \) is a divisor of \( m^3(4m + 27)^5 \). In particular, the primitive solution \( (x, y) \in \mathbb{Z}^2 \) to (*) can be chosen to satisfy the relation

\[
n = m + \frac{m(4m + 27)y(x^2 + 9xy + 27y^2 + my^2)(x^2 - mx^2y - m^2y^3)}{F_m(x, y)^2}.
\]

Conversely if there exists a primitive solution \( (x, y) \in \mathbb{Z}^2 \) to (*) with a \( \lambda \in \mathbb{Z} \) such that \( \lambda^2 \) is a divisor of \( m^3(4m + 27)^5 \), then for the rational number \( n \in \mathbb{Q} \) determined by (1) the splitting fields of \( f_n(X) \) and of \( f_m(X) \) over \( \mathbb{Q} \) coincide, except for the cases of \( n = 0 \) and of \( n = -27/4 \). For a fixed \( m \in \mathbb{Z} \setminus \{0\} \), furthermore, there exist only finitely many \( n \in \mathbb{Z} \) such that the splitting field of \( f_m(X) \) and of \( f_n(X) \) over \( \mathbb{Q} \) coincide.

We should consider only primitive solutions \( (x, y) \in \mathbb{Z}^2 \) (i.e. \( \gcd(x, y) = 1 \)) because \( (x, y) \) and \( (cx, cy) \) for \( c \in \mathbb{Z} \setminus \{0\} \) give the same \( n \in \mathbb{Z} \) by (1). For \( (x, y) \in \mathbb{Z}^2 \) with \( y \neq 0 \), we may assume that \( y > 0 \) because, if \( y \) is a solution to (*) for \( \lambda \), then \((-x, -y)\) becomes a solution to (*) for \(-\lambda\). For \((x, 0) \in \mathbb{Z}^2\), we may assume that \( x > 0 \).

For this reason, we exclude \((-1, 0) \in \mathbb{Z}^2 \) from primitive solutions. Then the trivial primitive solution \((1, 0) \in \mathbb{Z}^2 \setminus \{(-1, 0)\} \) to (*) for \( \lambda = 1 \) implies the trivial equality \( n = m \) by (1). The converse also holds if \( \text{Gal}_{\mathbb{Q}} f_m(X) \cong S_3 \). In general, we may follow the following assertion which complements Theorem 2:

**Theorem 3.** For \( m, n \in \mathbb{Z} \setminus \{0\} \), we assume that the splitting fields of \( f_m(X) \) and of \( f_n(X) \) over \( \mathbb{Q} \) coincide. Then we have:

(i) If \( \text{Gal}_{\mathbb{Q}} f_m(X) \cong S_3 \) then there exists only one primitive solution \( (x, y) \in \mathbb{Z}^2 \setminus \{(-1, 0)\} \) with \( y \geq 0 \) to (*) which satisfies the condition (1) with respect to \( m \) and \( n \). In particular, for \( m = n \) such primitive solution is \((1, 0) \in \mathbb{Z}^2 \);

(ii) If \( \text{Gal}_{\mathbb{Q}} f_m(X) \cong C_3 \) then \( m = -b^2 - b - 7 \) for some \( b \in \mathbb{Z} \) and there are exactly three primitive solutions \( (x, y) \in \mathbb{Z}^2 \setminus \{(-1, 0)\} \) with \( y \geq 0 \) to (*) which satisfy the condition (1) with respect to \( m \) and \( n \). In particular, for \( m = n \) such solutions are given by \((1, 0), (b - 4, 1), (-b - 5, 1) \in \mathbb{Z}^2 \) with \( \lambda = 1, -(2b + 1)^3, (2b + 1)^3 \) respectively;

(iii) If \( \text{Gal}_{\mathbb{Q}} f_m(X) \cong C_2 \) then \( m = n = -8 \) and the corresponding primitive solutions \( (x, y) \in \mathbb{Z}^2 \setminus \{(-1, 0)\} \) with \( y \geq 0 \) to (*) which satisfy the condition (1) are given by \((1, 0), (-4, 1) \in \mathbb{Z}^2 \) with \( \lambda = 1, -8 \) respectively.

By Theorem 3, we get the following corollary:

**Corollary 4.** For \( m \in \mathbb{Z} \setminus \{0\} \), let \( N \) be the number of all primitive solutions \( (x, y) \in \mathbb{Z}^2 \setminus \{(-1, 0)\} \) with \( y \geq 0 \) to (*) for \( \lambda \in \mathbb{Z} \) varying under the condition that \( \lambda^2 \) divides \( m^3(4m + 27)^5 \). Then we have

\[
\#\{n \in \mathbb{Z} \mid \text{Spl}_{\mathbb{Q}} f_n(X) = \text{Spl}_{\mathbb{Q}} f_m(X)\} \leq \frac{1}{\mu} \cdot N
\]

with \( \mu = 1, 3, 2 \) according to \( \text{Gal}_{\mathbb{Q}} f_m(X) \cong S_3, C_3, C_2 \), respectively.

In Section 2, we prepare some lemmas and recall the result in [3] which gives a generalization of Theorem 1 (cf. also the survey paper [5, Theorem 5.1]). In Section 3, we prove Theorem 2 and Theorem 3. We note that for fixed \( m, n \in \mathbb{Z} \) with \( \text{Spl}_{\mathbb{Q}} f_n(X) = \text{Spl}_{\mathbb{Q}} f_m(X) \), the corresponding primitive solutions to (*) can be obtained by (1) explicitly. In Sections 4 and 5, we will give some numerical examples of Theorem 2 via integral solutions to the family \( F_m(Y) = \lambda \) of cubic Thue equations. This computation was achieved by using PARI/GP [11] and we checked it by Mathematica [13]. For instance, we will give the following numerical example (cf. Table 2 in Section 4):

**Corollary 5.** For \( m \in \mathbb{Z} \setminus \{0\} \) in the range \(-10 \leq m \leq 5 \), an integer \( n \in \mathbb{Z} \setminus \{0, m\} \) satisfies that \( \text{Spl}_{\mathbb{Q}} f_n(X) = \text{Spl}_{\mathbb{Q}} f_m(X) \) if and only if \((m, n)\) is one of the following 17 pairs:

\[
\begin{align*}
(-10, -106480), & (-10, -400), (-9, -3087), (-9, -27), (-7, -1588867), \\
(-7, -189), & (-7, -49), (-6, 12), (-6, 54), (-6, 48000), (-5, 625), \\
(-4, 128), & (-3, 27), (-2, 3456), (1, 300763), (2, 208974222), (4, 3456000).
\end{align*}
\]

2. Preliminaries

We take the cubic generic polynomial

\[
f_s(X) = X^3 + sX + s \in K(s)[X]
\]
Lemma 7. For \( m \in \mathbb{Z} \setminus \{0\} \), the splitting field \( \text{Sp}_4 f_m(X) \) is totally real (resp. totally imaginary) if \( m \leq -7 \) (resp. \(-6 \leq m \)).

Lemma 8. For \( m \in \mathbb{Z} \setminus \{0\} \), the polynomial \( f_m(X) \) is irreducible over \( \mathbb{Q} \) except for \( m = -8 \). In the case of \( m = -8 \), \( f_m(X) \) splits as \( f_m(X) \) splits as \( f_m(X) = (X+2)(X^2-2X-4) \) over \( \mathbb{Q} \), and hence \( \text{Sp}_4 f_m(X) = \mathbb{Q}(\sqrt{5}) \).

Proof. If \( f_m(X) \) is reducible over \( \mathbb{Q} \) for \( m \in \mathbb{Z} \) then \( f_m(X) \) has a linear factor. Hence there exist \( a, b, c \in \mathbb{Z} \) such that \( f_m(X) = X^3 + mX + m = (X-a)(X^2 + bX + c) \). By comparing the coefficients, we have

\[
\begin{align*}
b &= a, \\
c &= \frac{-a^2}{a+1} = a - 1 + \frac{1}{a+1}, \\
m &= -\frac{a^3}{a+1} = -a^2 + a - 1 + \frac{1}{a+1}.
\end{align*}
\]

Hence we see \( a \in \{-2, 0\} \). According to \( a = -2 \) and \( a = 0 \), we have \( (a, b, c, m) = (-2, -2, -4, -8) \) and \((0, 0, 0, 0)\), respectively.

Field isomorphism problem of \( X^3 + sX + s \) and related Thue equations

For \( S \) over the base field \( K \). The discriminant of \( f_m(X) \) is \(-s^2(4s + 27)\). Hence the quadratic subfield of \( \text{Sp}_4 f_m(X) \) is given by \( K(\sqrt{-4s - 27}) \) unless char \( K = 2 \). We treat the case where \( K = \mathbb{Q} \) and take the specialization \( s \mapsto m \in \mathbb{Z} \setminus \{0\} \). Then we first see the following lemmas:

Lemma 7. \( \text{Sp}_4 f_m(X) \) is irreducible over \( \mathbb{Q} \) except for \( m = -8 \). In the case of \( m = -8 \), \( f_m(X) \) splits as \( f_m(X) = (X+2)(X^2-2X-4) \) over \( \mathbb{Q} \), and hence \( \text{Sp}_4 f_m(X) = \mathbb{Q}(\sqrt{5}) \).

Proof. If \( f_m(X) \) is reducible over \( \mathbb{Q} \) for \( m \in \mathbb{Z} \) then \( f_m(X) \) has a linear factor. Hence there exist \( a, b, c \in \mathbb{Z} \) such that \( f_m(X) = X^3 + mX + m = (X-a)(X^2 + bX + c) \). By comparing the coefficients, we have

\[
\begin{align*}
b &= a, \\
c &= \frac{-a^2}{a+1} = a - 1 + \frac{1}{a+1}, \\
m &= -\frac{a^3}{a+1} = -a^2 + a - 1 + \frac{1}{a+1}.
\end{align*}
\]

Hence we see \( a \in \{-2, 0\} \). According to \( a = -2 \) and \( a = 0 \), we have \( (a, b, c, m) = (-2, -2, -4, -8) \) and \((0, 0, 0, 0)\), respectively.

Lemma 8. For \( m \in \mathbb{Z} \setminus \{0\} \), the Galois group \( \text{Gal}_4 f_m(X) \) of \( f_m(X) \) over \( \mathbb{Q} \) is isomorphic to \( C_3 \) if and only if there exists \( b \in \mathbb{Z} \) such that \( m = -b^2 - b - 7 \).

Proof. If \( \text{Gal}_4 f_m(X) \cong C_3 \) then there exists \( a \in \mathbb{Z} \) such that \( a^2 = -(4m + 27) \) because the discriminant \( \text{disc}(f_m(X)) \) of \( f_m(X) \) is \(-m^2(4m + 27) \). In this case, \( m = -(a^2 + 27)/4 \in \mathbb{Z} \) and hence \( a = 2b + 1 \) for some \( b \in \mathbb{Z} \). Thus we get \( m = -b^2 - b - 7 \). Conversely if \( m = -b^2 - b - 7 \) with \( b \in \mathbb{Z} \) then we have \( \text{Gal}_4 f_m(X) \cong C_3 \) because \( \text{disc}(f_m(X)) = (2b + 1)^2(b^2 + b + 7)^2 \).
Table 1.

<table>
<thead>
<tr>
<th>$G_m$</th>
<th>$G_3$</th>
<th>$G_{m3}$</th>
<th>DT$(R_{m3})$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$S_1$</td>
<td>$S_1 \times S_1$</td>
<td>$L_m \cap L_n = \mathbb{Q}$</td>
<td>6</td>
</tr>
<tr>
<td>$S_1 \times C_3$</td>
<td>$L_m \cap L_n = \mathbb{Q}$</td>
<td>3, 3</td>
<td></td>
</tr>
<tr>
<td>$S_1 \times C_2$</td>
<td>$L_m \cap L_n = \mathbb{Q}$</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>$C_1$</td>
<td>$S_1 \times C_1$</td>
<td>$L_m \cap L_n = \mathbb{Q}$</td>
<td>3, 2, 1</td>
</tr>
<tr>
<td>$C_1 \times C_1$</td>
<td>$L_m \cap L_n = \mathbb{Q}$</td>
<td>3, 3</td>
<td></td>
</tr>
<tr>
<td>$C_1 \times C_2$</td>
<td>$L_m \cap L_n = \mathbb{Q}$</td>
<td>4, 2</td>
<td></td>
</tr>
<tr>
<td>$C_2$</td>
<td>$C_2 \times C_2$</td>
<td>$L_m \cap L_n = \mathbb{Q}$</td>
<td>3, 1, 1, 1</td>
</tr>
<tr>
<td>$C_2$</td>
<td>$C_2$</td>
<td>$L_m = L_n$</td>
<td>2, 2, 1, 1</td>
</tr>
</tbody>
</table>

Lemma 10. For $m \in \mathbb{Z} \setminus \{0\}$, the decomposition type $\text{DT}(R_{m3})$ of $R_{m3}(X)$ is given by

$$\text{DT}(R_{m3}) = \begin{cases} 3, 2, & \text{if } G_m \cong S_3, \\ 3, 1, 1, & \text{if } G_m \cong C_3, \\ 2, 2, 1, & \text{if } G_m \cong C_2. \end{cases}$$

Next we consider the cases of $n = 0$ and $n = -27/4$. By (2), the sextic polynomials $R_{m,0}(X)$ and $R_{m,-27/4}(X)$ have multiple roots. Indeed we have $R_{m,0}(X) = m(X^2 + 9X - 3m)^3$ and $R_{m,-27/4}(X) = (4m + 27)(X^3 + 9mX + 27m^2)^2/4$.

Lemma 11. (i) For $m \in \mathbb{Z} \setminus \{0\}$, there exists $u \in \mathbb{Q}$ such that $R_{m,0}(u) = 0$ if and only if there exists $c \in \mathbb{Z}$ such that $m = 3(c + 3)$;

(ii) For $m \in \mathbb{Z} \setminus \{0\}$, there exists $u \in \mathbb{Q}$ such that $R_{m,-27/4}(u) = 0$ if and only if $m = -8$.

Proof. (i) If there exists $u \in \mathbb{Q}$ such that $R_{m,0}(u) = m(u^2 + 9u - 3m)^3 = 0$, then there exist integers $a, b \in \mathbb{Z}$ such that $u^2 + 9u - 3m = (a - b)(a - b)$. In this case, we see $m = b(b + 9)/3$ and $a = -b - 9$. Thus, $b = 3c$ for some $c \in \mathbb{Z}$, and hence $m = 3(c + 3)$. Conversely if $m = 3(c + 3)$, then we have $R_{3(c+3),0}(X) = 3(c + 3)(X^3 - 3c)^3(X^3 + 9c^2)$. (ii) If there exists $u \in \mathbb{Q}$ such that $R_{m,-27/4}(u) = (4m + 27)(u^3 + 9mu + 27m)^2/4 = 0$, then there exist integers $a, b, c \in \mathbb{Z}$ such that $u^3 + 9mu + 27m = (a - b)(a^2 + bu + c)$. By comparing the coefficients, we obtain

$$b = a, \quad c = \frac{3a^2}{a + 3}, \quad m = -\frac{a^3}{9(a + 3)}.$$

Thus $a = 3d$ for some $d \in \mathbb{Z}$, and

$$m = -\frac{d^3}{d + 1} = -d^2 + d - \frac{1}{d + 1}.$$

Hence we have $d \in \{-2, 0\}$. According to $d = -2$ and $d = 0$, we get $(a, b, c, m) = (-6, -6, -36, -8)$ and $(0, 0, 0, 0)$, respectively.

As an application, by using the sextic polynomial $R_{m,0}(X)$ for $u = x = 0$, we get the following example of the overlap $\text{Spl}_Q f_m(X) = \text{Spl}_Q f_n(X)$ of the splitting fields.

Proposition 12. If $(m, n) \in \mathbb{Z}^2$ is one of the 8 pairs

$$(-54, -12), (-18, -108), (-15, -675), (-14, -5292),$$

$$(-13, -4563), (-12, -432), (-9, -27), (27, -3),$$

then $\text{Spl}_Q f_m(X) = \text{Spl}_Q f_n(X)$.

Proof. If $m$ and $n$ satisfy the equation

$$4m^2n + 27m^2 + 108mn + 729n = 0, \quad (3)$$

then $\text{Spl}_Q f_m(X) = \text{Spl}_Q f_n(X)$ because the constant term of $R_{m,n}(X)$ is $-m^2(4m^2n + 27m^2 + 108mn + 729n)$. By (3), we have

$$n = -\frac{27m^2}{(2m + 27)^2} = -\frac{1}{3} \left( \frac{9m}{2m + 27} \right)^2 = -\frac{1}{3} \left( \frac{1}{2} \left( \frac{9 - 243}{2m + 27} \right) \right)^2.$$
Hence if \( n \in \mathbb{Z} \), then we have \( 243/(2m + 27) \in \mathbb{Z} \). Then we finally see \( m = -135, -54, -27, -18, -15, -14, -13, -12, -9, 0, 27, 108 \). We exclude the cases \( m = -135, -27, 0, 108 \) because we obtain \( (m, n) = (-135, -25/3), (-27, -27), (0, 0), (108, -16/3) \), respectively, in these cases.

Next we put
\[
F_m(X, Y) := X^3 - 2mX^2Y - 9mXY^2 - m(2m + 27)Y^3 \in \mathbb{Z}[X, Y]
\]
as in Theorem 2 and study the cubic polynomial
\[
F_m(X, 1) = X^3 - 2mX^2 - 9mX - m(2m + 27) \in \mathbb{Z}[X].
\]
The discriminant of \( F_m(X, 1) \) is \(-m^2(4m + 27)^3\).

**Lemma 13.** For \( m \in \mathbb{Z} \setminus \{0\} \), the splitting fields of \( f_m(X) = X^3 + mX + m \) and of \( F_m(X, 1) = X^3 - 2mX^2 - 9mX - m(2m + 27) \) over \( \mathbb{Q} \) coincide. In particular, the polynomial \( F_m(X, 1) \) is reducible over \( \mathbb{Q} \) only for \( m = -8 \), and \( F_{-8}(X, 1) = (X + 2)(X^2 + 14X + 44) \).

**Proof.** The assertion follows directly from the fact that \( f_m(X) \) can be transformed to \( F_m(Z, 1) \) by the following Tschirnhausen transformation:
\[
F_m(Z, 1) = \text{Resultant}_X(f_m(X), Z - (2X^2 - 3X + 2m)).
\]
The inverse transformation is also given as
\[
f_m(X) = \text{Resultant}_X(F_m(Z, 1), X - \frac{2Z^3 - (4m + 9)Z - 6m}{4m + 27}).
\]
It follows from Lemma 7 that for \( m \in \mathbb{Z} \setminus \{0\} \), the polynomial \( F_m(X, 1) \) is reducible over \( \mathbb{Q} \) if and only if \( m = -8 \).

\section{3. Proof of Theorem 2 and of Theorem 3}

We use Theorem 1 in the case where \( K = \mathbb{Q} \). Take
\[
F_m(X, Y) = X^3 - 2mX^2Y - 9mXY^2 - m(2m + 27)Y^3 \in \mathbb{Z}[X, Y].
\]
For \( m \in \mathbb{Z} \setminus \{0\} \), we assume that there exists \( n \in \mathbb{Z} \setminus \{0\}, n \neq m \), such that \( \text{Spl}_{\mathbb{Q}} f_m(X) = \text{Spl}_{\mathbb{Q}} f_n(X) \). By Theorem 1, there exists \( u \in \mathbb{Q} \) such that
\[
n = \frac{m(u^2 + 9u - 3m)}{F_m(u, 1)^2}
\]
which is equivalent to the condition that \( R_{m,n}(u) = m(u^2 + 9u - 3m)^3 - nF_m(u, 1)^2 = 0 \).

We write \( u = x/y \) as a quotient of relatively prime integers \( x, y \in \mathbb{Z} \) with \( y > 0 \). Then we have
\[
n = \frac{m(x^2 + 9xy - 3y^2)^3}{F_m(x, y)^2}
\]
\[
= m + \frac{m(4m + 27)y(x^2 + 9xy + 27y^2 + my^2)(x^3 - mx^2y - m^2y^3)}{F_m(x, y)^2} \in \mathbb{Z}.
\]
We put
\[
\lambda := F_m(x, y).
\]
Then \( \lambda^3 \) divides \( m(4m + 27)y(x^2 + 9xy + 27y^2 + my^2)(x^3 - mx^2y - m^2y^3) \).

**Proof of Theorem 2.** In order to prove Theorem 2, we should show that \( \lambda^3 \) divides \( m^3(4m + 27)^3 \). Then it follows by Thue’s theorem that for a fixed \( m \in \mathbb{Z} \), there exist only finitely many \( n \in \mathbb{Z} \) such that \( \text{Spl}_{\mathbb{Q}} f_m(X) = \text{Spl}_{\mathbb{Q}} f_n(X) \) because \( \lambda \) runs over a finite number of integers.

We will use the standard method via resultant and the Sylvester matrix (cf. [8, Theorem 6.1], [9, Chapter 8, Section 5] and [12, Section 1.3]). Put
\[
g(u) := m(u^2 + 9u - 3m)^3, \quad h(u) := F_m(u, 1)^2.
\]
We take the resultant
\[
r_m := \text{Resultant}_u(g(u), h(u)) = m^{18}(4m + 27)^{18} \in \mathbb{Z}
\]
of \( g(u) \) and \( h(u) \) with respect to \( u \).
Now we expand the polynomials $g(u)$ and $h(u)$ with respect to $u$ as

$$g(u) = \sum_{i=0}^{6} a_i u^{6-i} = mu^6 + 27mu^5 - 9(m - 27)mu^4 - 81m(2m - 9)u^3$$
$$+ 27(m - 27)m^2 u^2 + 243m^3 u - 27m^4,$$

$$h(u) = \sum_{i=0}^{6} b_i u^{6-i} = u^6 - 4mu^5 + 2m(2m - 9)u^4 + 2m(16m - 27)u^3$$
$$+ m^2(8m + 189)u^2 + 18m^2(2m + 27)u + m^2(2m + 27)^2.$$

Then the resultant $r_m$ is also given as the following determinant:

$$r_m = \begin{vmatrix}
  a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & 0 & 0 & 0 & 0 & g(u)u^5 & \\
  0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & 0 & 0 & 0 & g(u)u^4 & \\
  0 & 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & 0 & 0 & g(u)u^3 & \\
  0 & 0 & 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & a_6 & 0 & g(u)u^2 & \\
  0 & 0 & 0 & 0 & a_0 & a_1 & a_2 & a_3 & a_4 & a_5 & g(u)u & \\
  b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & 0 & 0 & 0 & 0 & h(u)^2 & \\
  0 & b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & 0 & 0 & 0 & h(u)^2 & \\
  0 & 0 & b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & 0 & h(u)u^2 & \\
  0 & 0 & 0 & b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & b_6 & h(u)u & \\
  0 & 0 & 0 & 0 & b_0 & b_1 & b_2 & b_3 & b_4 & b_5 & h(u) & \\
\end{vmatrix};$$

hence we have

$$r_m = m^6(4m + 27)^3 g(u)p(u) + h(u)q(u) \quad \text{(6)}$$

where

$$p(u) = -15u^5 + 3(19m + 9)u^4 - (48m^2 - 176m + 27)u^3 - 3m(4m^2 + 125m - 135)u^2$$
$$- 6m(26m^2 + 339m + 162)u - m(28m^3 + 636m^2 + 3591m - 1458),$$

$$q(u) = m(15u^5 + 3(m + 126)u^4 - (68m - 2943)u^3 - (26m^2 + 1809m - 5103)u^2$$
$$+ 9(5m^2 - 810m - 1458)u + 67m^3 + 2538m^2 + 11664m + 19683).$$

By (5) and (6), we have

$$g(u)p(u) + h(u)q(u) = m^3(4m + 27)^5.$$

Put

$$G(x, y) := y^6 \cdot g(x/y), \quad P(x, y) := y^5 \cdot p(x/y), \quad Q(x, y) := y^5 \cdot q(x/y).$$

Then

$$G(x, y)P(x, y) + F_m(x, y)^2 Q(x, y) = m^3(4m + 27)^5y^{11}.$$

Hence we get

$$\frac{G(x, y)P(x, y)}{\lambda^2} + \frac{Q(x, y)}{\lambda^2} = \frac{m^3(4m + 27)^5y^{11}}{\lambda^2} \in \mathbb{Z}.$$
Field isomorphism problem of $X^3 + sX + s$ and related Thue equations

<table>
<thead>
<tr>
<th>$m$</th>
<th>$a$</th>
<th>$F_m(x, y) = a$</th>
<th>$n$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$-10$</td>
<td>$1$</td>
<td>$(1, 0)$</td>
<td>$-10$</td>
</tr>
<tr>
<td></td>
<td>$-1$</td>
<td>$(-1, 1)$</td>
<td>$-106480$</td>
</tr>
<tr>
<td></td>
<td>$-5$</td>
<td>$(-5, 1)$</td>
<td>$-400$</td>
</tr>
<tr>
<td></td>
<td>$13^2$</td>
<td>$(-11, 1)$</td>
<td>$-640/13$</td>
</tr>
<tr>
<td></td>
<td>$-13^2$</td>
<td>$(-9, 2)$</td>
<td>$-270/13$</td>
</tr>
<tr>
<td></td>
<td>$2 \cdot 13^2$</td>
<td>$(2, 1)$</td>
<td>$-160/13$</td>
</tr>
<tr>
<td></td>
<td>$-5 \cdot 13^2$</td>
<td>$(-125, 9)$</td>
<td>$-6072400/13$</td>
</tr>
<tr>
<td></td>
<td>$-5 \cdot 13^2$</td>
<td>$(5, 4)$</td>
<td>$-6250/13$</td>
</tr>
<tr>
<td></td>
<td>$2 \cdot 5 \cdot 13^2$</td>
<td>$(-20, 3)$</td>
<td>$-100/13$</td>
</tr>
<tr>
<td>$-9$</td>
<td>$1$</td>
<td>$(1, 0)$</td>
<td>$-9$</td>
</tr>
<tr>
<td></td>
<td>$1$</td>
<td>$(5, 1)$</td>
<td>$-3087$</td>
</tr>
<tr>
<td></td>
<td>$3^3$</td>
<td>$(-6, 1)$</td>
<td>$-9$</td>
</tr>
<tr>
<td></td>
<td>$-3^3$</td>
<td>$(-3, 1)$</td>
<td>$-9$</td>
</tr>
<tr>
<td></td>
<td>$-3^3$</td>
<td>$(-12, 1)$</td>
<td>$-3087$</td>
</tr>
<tr>
<td></td>
<td>$-3^3$</td>
<td>$(-3, 2)$</td>
<td>$-3087$</td>
</tr>
<tr>
<td></td>
<td>$3^3$</td>
<td>$(0, 1)$</td>
<td>$-27$</td>
</tr>
<tr>
<td></td>
<td>$3^3$</td>
<td>$(-9, 1)$</td>
<td>$-27$</td>
</tr>
<tr>
<td></td>
<td>$-3^3$</td>
<td>$(-9, 2)$</td>
<td>$-27$</td>
</tr>
<tr>
<td></td>
<td>$1$</td>
<td>$(1, 0)$</td>
<td>$-8$</td>
</tr>
<tr>
<td></td>
<td>$-2^3$</td>
<td>$(-4, 1)$</td>
<td>$-8$</td>
</tr>
<tr>
<td></td>
<td>$2^3$</td>
<td>$(-6, 1)$</td>
<td>$-2274/4$</td>
</tr>
<tr>
<td></td>
<td>$5^3$</td>
<td>$(-7, 1)$</td>
<td>$-64/5$</td>
</tr>
<tr>
<td></td>
<td>$-5^3$</td>
<td>$(-9, 2)$</td>
<td>$-216/5$</td>
</tr>
<tr>
<td></td>
<td>$2^3 \cdot 5^3$</td>
<td>$(-16, 3)$</td>
<td>$-64/5$</td>
</tr>
<tr>
<td></td>
<td>$-2^3 \cdot 5^3$</td>
<td>$(-12, 1)$</td>
<td>$-216/5$</td>
</tr>
<tr>
<td></td>
<td>$2^3 \cdot 5^3$</td>
<td>$(-26, 3)$</td>
<td>$-6859/20$</td>
</tr>
<tr>
<td></td>
<td>$2^3 \cdot 5^3$</td>
<td>$(-34, 7)$</td>
<td>$-6859/20$</td>
</tr>
<tr>
<td>$-7$</td>
<td>$1$</td>
<td>$(1, 0)$</td>
<td>$-7$</td>
</tr>
<tr>
<td></td>
<td>$1$</td>
<td>$(-3, 1)$</td>
<td>$-189$</td>
</tr>
<tr>
<td></td>
<td>$1$</td>
<td>$(-5, 1)$</td>
<td>$-7$</td>
</tr>
<tr>
<td></td>
<td>$1$</td>
<td>$(-6, 1)$</td>
<td>$-189$</td>
</tr>
<tr>
<td></td>
<td>$1$</td>
<td>$(41, 9)$</td>
<td>$-1588867$</td>
</tr>
<tr>
<td></td>
<td>$-1$</td>
<td>$(-4, 1)$</td>
<td>$-7$</td>
</tr>
<tr>
<td></td>
<td>$-1$</td>
<td>$(-9, 2)$</td>
<td>$-189$</td>
</tr>
<tr>
<td></td>
<td>$-1$</td>
<td>$(-25, 4)$</td>
<td>$-1588867$</td>
</tr>
<tr>
<td></td>
<td>$-1$</td>
<td>$(-16, 5)$</td>
<td>$-1588867$</td>
</tr>
<tr>
<td></td>
<td>$7$</td>
<td>$(-14, 3)$</td>
<td>$-49$</td>
</tr>
<tr>
<td></td>
<td>$-7$</td>
<td>$(-7, 1)$</td>
<td>$-49$</td>
</tr>
<tr>
<td></td>
<td>$-7$</td>
<td>$(-7, 2)$</td>
<td>$-49$</td>
</tr>
<tr>
<td></td>
<td>$1$</td>
<td>$(1, 0)$</td>
<td>$-6$</td>
</tr>
<tr>
<td></td>
<td>$1$</td>
<td>$(-13, 3)$</td>
<td>$48000$</td>
</tr>
<tr>
<td></td>
<td>$2$</td>
<td>$(-4, 1)$</td>
<td>$12$</td>
</tr>
<tr>
<td></td>
<td>$3^3$</td>
<td>$(-3, 1)$</td>
<td>$[0]$</td>
</tr>
<tr>
<td></td>
<td>$-9^2$</td>
<td>$(-9, 2)$</td>
<td>$54$</td>
</tr>
<tr>
<td></td>
<td>$-2 \cdot 3^3$</td>
<td>$(-8, 1)$</td>
<td>$[0]$</td>
</tr>
<tr>
<td>$-6$</td>
<td>$1$</td>
<td>$(1, 0)$</td>
<td>$-5$</td>
</tr>
<tr>
<td></td>
<td>$1$</td>
<td>$(-4, 1)$</td>
<td>$625$</td>
</tr>
<tr>
<td></td>
<td>$7^3$</td>
<td>$(-1, 1)$</td>
<td>$-57$</td>
</tr>
<tr>
<td></td>
<td>$-7^3$</td>
<td>$(-9, 2)$</td>
<td>$135/7$</td>
</tr>
<tr>
<td></td>
<td>$5 \cdot 7^3$</td>
<td>$(-10, 3)$</td>
<td>$257$</td>
</tr>
<tr>
<td>$-5$</td>
<td>$1$</td>
<td>$(1, 0)$</td>
<td>$-4$</td>
</tr>
<tr>
<td></td>
<td>$-2^7$</td>
<td>$(-4, 1)$</td>
<td>$128$</td>
</tr>
<tr>
<td>$11^2$</td>
<td>$(1, 1)$</td>
<td>$-32/11$</td>
<td></td>
</tr>
</tbody>
</table>

$3m^3 - nF_m(u, 1)^2 = 0$. We write $u = x/y$ with $x, y \in \mathbb{Z}$, $y > 0$ and $\gcd(x, y) = 1$. Then, by (4), $R_{m,n}(u) = 0$ if and only if $(x, y) \in \mathbb{Z}^2$ satisfies the condition (1).

We note that the sextic polynomial $R_{m,n}(X)$ has no multiple roots by (2). Hence it follows from Theorem 9 that the number of the set $\{ u \in \mathbb{Q} \mid R_{m,n}(u) = 0 \}$ equals exactly $\mu$ where $\mu = 1, 3, 2$ according to $\text{Gal}_{\mathbb{Q}} f_m(X) \cong S_3, C_3, C_2,$
Table 3.

<table>
<thead>
<tr>
<th>m</th>
<th>n</th>
<th>(F_m(x, y) = \lambda)</th>
<th>(\lambda)</th>
<th>(F_m(x, y) = \lambda')</th>
<th>(\lambda')</th>
</tr>
</thead>
<tbody>
<tr>
<td>52</td>
<td>48000</td>
<td>((-13, 3))</td>
<td>(-1)</td>
<td>((-140, 3))</td>
<td>(-2^6 \cdot 5^3 \cdot 11^3 \cdot 23^3)</td>
</tr>
<tr>
<td>54</td>
<td>48000</td>
<td>((28, 1))</td>
<td>(-2^2 \cdot 5^3)</td>
<td>((1640, 1))</td>
<td>(-2^7 \cdot 5^3 \cdot 11^3 \cdot 23^3)</td>
</tr>
<tr>
<td>3456</td>
<td></td>
<td>((-3, 1))</td>
<td>(3^3)</td>
<td>((0, 1))</td>
<td>(3^3)</td>
</tr>
<tr>
<td>12</td>
<td>54</td>
<td>((18, 1))</td>
<td>(-2^2 \cdot 5^3 \cdot 5^3)</td>
<td>((36, 1))</td>
<td>(-2 \cdot 3^{10})</td>
</tr>
</tbody>
</table>

respectively (see the number of 1’s in \(DT(R_{m,n})\) as on Table 1).

We also see that by the assumption \(m \neq n\), \((1, 0) \in \mathbb{Z}^2\) does not hold the condition (1). Thus the number of the primitive solutions \((x, y) \in \mathbb{Z}^2 \setminus \{(-1, 0)\}\) with \(y \geq 0\) to (1) which satisfies (1) is exactly \(m\) and the assertion follows when \(m \neq n\).

In the case where \(n = m\), we recall that \(R_{m,n}(X)\) becomes quintic and \((1, 0) \in \mathbb{Z}^2\) corresponds to the vanishing root. By Lemma 10, the number of the set \(\{u \in \mathbb{Q} \mid R_{m,n}(u) = 0\}\) equals exactly \(m - 1\) and \((1, 0) \in \mathbb{Z}^2\) satisfies the condition (1). Hence the number of the primitive solutions \((x, y) \in \mathbb{Z}^2 \setminus \{(-1, 0)\}\) with \(y \geq 0\) to (1) which satisfies (1) also equals \(m\).

For \(m = n\), the corresponding primitive solutions \((x, y) \in \mathbb{Z}^2 \setminus \{(-1, 0)\}\) satisfy

\[
\phi_m(x, y) := y(x^2 + 9xy + 27y^2 + m^2y^2)(x^3 - mx^2y - m^2y^3) = 0.
\]

If \(\text{Gal}_{\mathbb{Q}}(f_m) \cong C_3\) then by Lemma 8 there exists \(b \in \mathbb{Z}\) such that \(m = -b^2 - b - 7\), and hence we have

\[
\psi_{-b^2-b-7}(x, y) = y(x - (b - 4)y)(x + (b + 5)y)(x^3 + (b^2 + b + 7)x^2y - (b^2 + b + 7)y^3).
\]

Thus, the corresponding three primitive solutions are \((1, 0), (-b - 4, 1), (-b - 5, 1) \in \mathbb{Z}^2\). If \(\text{Gal}_{\mathbb{Q}}(f_m) \cong C_2\) then \(m = -8\) by Lemma 7. We see

\[
\psi_{-8}(x, y) = y(x + 4y)(x^2 + 9xy + 19y^2)(x^2 + 4xy - 16y^2).
\]

Hence the corresponding two primitive solutions are given by \((1, 0)\) and \((-4, 1)\).

\[\square\]

4. Numerical example 1

We give some numerical examples of Theorem 2, Theorem 3 and Corollary 4. By using PARI/GP [11], we computed for \(m \in \mathbb{Z} \setminus \{0\}\) in the range \(-10 \leq m \leq 5\), all primitive solutions \((x, y) \in \mathbb{Z}^2 \setminus \{(-1, 0)\}\) with \(y \geq 0\) to \(F_m(x, y) = \lambda\) where \(\lambda^2\) is a divisor of \(m^3(4m + 27)^5\) as on Table 2. We checked Table 2 by Mathematica [13]. By the result on Table 2, we get Corollary 5 which we stated in Section 1, because all integers \(n \in \mathbb{Z}\) which satisfy \(\text{Spl}_{\mathbb{Q}}(f_m) = \text{Spl}_{\mathbb{Q}}(f_n)\) appear on Table 2.

5. Numerical example 2

By Theorem 1, we evaluated those integers \(m, n \in \mathbb{Z} \setminus \{0\}\) in the range

(i) \(-6 \leq m < n \leq 2 \times 10^5\), i.e. \(\text{Spl}_{\mathbb{Q}}(f_m)\) is totally imaginary, 

(ii) \(-2 \times 10^5 \leq n < m \leq -7\), i.e. \(\text{Spl}_{\mathbb{Q}}(f_m)\) is totally real

for which \(R_{m,n}(X)\) has a linear factor over \(\mathbb{Q}\), namely, \(\text{Spl}_{\mathbb{Q}}(f_m) = \text{Spl}_{\mathbb{Q}}(f_n)\). Note that we should check only for \(m, n \in \mathbb{Z} \setminus \{0\}\) which satisfy that \((4m + 27)(4n + 27)\) is square. We also computed the corresponding primitive solutions \((x, y) \in \mathbb{Z}^2\) to \(F_m(x, y) = \lambda\) and to \(F_n(x, y) = \lambda'\) with respect to \([m, n]\) and to \([n, m]\) respectively. The result of the case (i) (resp. (ii)) is given on Table 3 (resp. on Table 4).

Acknowledgments

The authors would like to thank anonymous referees for reading the original manuscript very carefully and for suggesting improvements and corrections.
Table 4.

<table>
<thead>
<tr>
<th>$m$</th>
<th>$n$</th>
<th>$P_{o}(s,y) = 1$</th>
<th>$s$</th>
<th>$P_{o}(s,y) = 3$</th>
<th>$y$</th>
</tr>
</thead>
<tbody>
<tr>
<td>7</td>
<td>49</td>
<td>(7, 1)</td>
<td>7</td>
<td>(35, 2)</td>
<td>$7^2 \cdot 13^3$</td>
</tr>
<tr>
<td>7</td>
<td>49</td>
<td>(7, 2)</td>
<td>7</td>
<td>(28, 1)</td>
<td>$7^2 \cdot 13^3$</td>
</tr>
<tr>
<td>7</td>
<td>49</td>
<td>(14, 3)</td>
<td>7</td>
<td>(7, 3)</td>
<td>$7^2 \cdot 13^3$</td>
</tr>
<tr>
<td>7</td>
<td>107</td>
<td>(3, 1)</td>
<td>1</td>
<td>(36, 1)</td>
<td>$3^10$</td>
</tr>
<tr>
<td>7</td>
<td>107</td>
<td>(3, 2)</td>
<td>1</td>
<td>(36, 1)</td>
<td>$3^10$</td>
</tr>
<tr>
<td>7</td>
<td>107</td>
<td>(3, 3)</td>
<td>1</td>
<td>(36, 1)</td>
<td>$3^10$</td>
</tr>
<tr>
<td>7</td>
<td>107</td>
<td>(3, 4)</td>
<td>1</td>
<td>(36, 1)</td>
<td>$3^10$</td>
</tr>
<tr>
<td>7</td>
<td>107</td>
<td>(3, 5)</td>
<td>1</td>
<td>(36, 1)</td>
<td>$3^10$</td>
</tr>
<tr>
<td>7</td>
<td>107</td>
<td>(3, 6)</td>
<td>1</td>
<td>(36, 1)</td>
<td>$3^10$</td>
</tr>
<tr>
<td>7</td>
<td>107</td>
<td>(3, 7)</td>
<td>1</td>
<td>(36, 1)</td>
<td>$3^10$</td>
</tr>
<tr>
<td>7</td>
<td>107</td>
<td>(3, 8)</td>
<td>1</td>
<td>(36, 1)</td>
<td>$3^10$</td>
</tr>
<tr>
<td>7</td>
<td>107</td>
<td>(3, 9)</td>
<td>1</td>
<td>(36, 1)</td>
<td>$3^10$</td>
</tr>
</tbody>
</table>

Table continues...
REFERENCES


