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 $x^3 - 2mx^2y - 9mxy^2 - m(2m + 27)y^3 = \lambda$ where λ^2 is a divisor of $m^3(4m + 27)^5$.

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 $L = \text{Spl}_M f_a(X)$, the splitting field of $f_a(X)$ 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 $\text{Spl}_K f_a(X)$ and $\text{Spl}_K f_b(X)$ 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 $\text{char } K \neq 2$ (see also [1] and [3]). In [2], the authors investigated the field isomorphism problem of $f_s(X)$ over a field K with $\text{char } K \neq 3$ and gave the following theorem:

Theorem 1 ([2, Corollary 8]). Assume that $\text{char } K \neq 3$. 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

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

For the polynomial $f_a(X)$, we assume that $a \neq 0, -27/4$ since the discriminant of $f_a(X)$ is given by $-a^2(4a + 27)$. 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 $\text{Spl}_K f_b(X) = \text{Spl}_K f_a(X)$ 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*

$$F_m(x, y) = x^3 - 2mx^2y - 9mxy^2 - m(2m + 27)y^3 = \lambda \quad (*)$$

for such a $\lambda \in \mathbb{Z}$ as λ^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

$$n = m + \frac{m(4m + 27)y(x^2 + 9xy + 27y^2 + my^2)(x^3 - mx^2y - m^2y^3)}{F_m(x, y)^2}. \quad (1)$$

Conversely if there exists a primitive solution $(x, y) \in \mathbb{Z}^2$ to $(*)$ with a $\lambda \in \mathbb{Z}$ such that λ^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 (x, y) is a solution to $(*)$ for λ , 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 obtain 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 $\mathcal{N}$ 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 λ^2 divides $m^3(4m + 27)^5$. Then we have*

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

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 $\text{Spl}_{\mathbb{Q}} f_m(X) = \text{Spl}_{\mathbb{Q}} f_n(X)$, the corresponding primitive solutions to $(*)$ can be obtained by (1) explicitly. In Sections 4 and 5, we give some numerical examples of Theorem 2 via integral solutions to the family $F_m(X, Y) = \lambda$ 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:*

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

2. Preliminaries

We take the cubic generic polynomial

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

for S_3 over the base field K . The discriminant of $f_s(X)$ is $-s^2(4s + 27)$. Hence the quadratic subfield of $\text{Spl}_{K(s)}f_s(X)$ is given by $K(s)(\sqrt{-4s - 27})$ unless $\text{char } K = 2$. 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 6. *For $m \in \mathbb{Z} \setminus \{0\}$, the splitting field $\text{Spl}_{\mathbb{Q}}f_m(X)$ is totally real (resp. totally imaginary) if $m \leq -7$ (resp. $-6 \leq m$).*

Lemma 7. *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 $m = -8$, $f_{-8}(X)$ splits as $f_{-8}(X) = (X + 2)(X^2 - 2X - 4)$ over $\mathbb{Q}$, and hence $\text{Spl}_{\mathbb{Q}}f_{-8}(X) = \mathbb{Q}(\sqrt{5})$.*

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

$$b = a, \quad c = \frac{a^2}{a+1} = a - 1 + \frac{1}{a+1}, \quad m = -\frac{a^3}{a+1} = -a^2 + a - 1 + \frac{1}{a+1}.$$

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. $\square$

Lemma 8. *For $m \in \mathbb{Z} \setminus \{0\}$, the Galois group $\text{Gal}_{\mathbb{Q}}f_m(X)$ 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 $\text{Gal}_{\mathbb{Q}}f_m(X) \cong C_3$ 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 $\text{Gal}_{\mathbb{Q}}f_m(X) \cong C_3$ because $\text{disc}(f_m(X)) = (2b + 1)^2(b^2 + b + 7)^2$. $\square$

For $m, n \in \mathbb{Z}$, we define a sextic polynomial $R_{m,n}(X) \in \mathbb{Z}[X]$ by

$$\begin{aligned} R_{m,n}(X) &:= m(X^2 + 9X - 3m)^3 - n(X^3 - 2mX^2 - 9mX - 2m^2 - 27m)^2 \\ &= (m - n)X^6 + m(4n + 27)X^5 - m(4mn + 9m - 18n - 243)X^4 \\ &\quad - m(32mn + 162m - 54n - 729)X^3 - m^2(8mn - 27m + 189n + 729)X^2 \\ &\quad - 9m^2(4mn - 27m + 54n)X - m^2(4m^2n + 27m^2 + 108mn + 729n). \end{aligned}$$

The discriminant of $R_{m,n}(X)$ with respect to X is given by

$$\text{disc}(R_{m,n}(X)) = m^{10}(4m + 27)^{15}n^4(4n + 27)^3 \in \mathbb{Z}. \quad (2)$$

It follows from Theorem 1 that for $m, n \in \mathbb{Z} \setminus \{0\}$ with $m \neq n$, there exists $u \in \mathbb{Q}$ such that $R_{m,n}(u) = 0$ if and only if $\text{Spl}_{\mathbb{Q}}f_m(X) = \text{Spl}_{\mathbb{Q}}f_n(X)$.

We define the *decomposition type* $\text{DT}(R)$ of the polynomial $R(X)$ of degree l by the partition of l induced by the degrees of the irreducible factors of $R(X)$ over $\mathbb{Q}$. For $m, n \in \mathbb{Z} \setminus \{0\}$, we put

$$L_m := \text{Spl}_{\mathbb{Q}}f_m(X), \quad G_m := \text{Gal}_{\mathbb{Q}}f_m(X), \quad G_{m,n} := \text{Gal}_{\mathbb{Q}}(f_m(X)f_n(X)).$$

In [3] and [4], the authors gave the following theorem for a field K with $\text{char } K \neq 3$ as a generalization of Theorem 1 (cf. also [2, Theorem 7] and [5, Theorem 5.1]). Here we state the theorem only for the case where $K = \mathbb{Q}$ and $m, n \in \mathbb{Z}$.

Theorem 9. *For $m, n \in \mathbb{Z} \setminus \{0\}$ with $m \neq n$, we assume that $\#G_m \geq \#G_n$. Then the Galois group $G_{m,n} = \text{Gal}_{\mathbb{Q}}(f_m(X)f_n(X))$ and the intersection field $L_m \cap L_n = \text{Spl}_{\mathbb{Q}}f_m(X) \cap \text{Spl}_{\mathbb{Q}}f_n(X)$ are given by the decomposition type $\text{DT}(R_{m,n})$ of $R_{m,n}(X)$ as Table 1 shows.*

We did not exclude the case $G_{m,n} \cong C_2 \times C_2$ from Table 1 although it does not occur for $m, n \in \mathbb{Z} \setminus \{0\}$ as we see from Lemma 7. This is because the table shows all cases for $m, n \in \mathbb{Q} \setminus \{0, -27/4\}$ with $m \neq n$.

For $u \in \mathbb{Q}$ with $R_{m,n}(u) = 0$, we write $u = x/y$ as a quotient of relatively prime integers $x, y \in \mathbb{Z}$ with $y > 0$. Put $z := 1/u = y/x$ unless $u = 0$. We take

$$\begin{aligned} R'_{m,n}(X) &= X^6 \cdot R_{m,n}(1/X) \\ &= m(1 + 9X - 3mX^2)^3 - n(1 - 2mX - 9mX^2 - 2m^2X^3 - 27mX^3)^2. \end{aligned}$$

Then $R_{m,n}(u) = 0$ if and only if $R'_{m,n}(z) = 0$. We now consider the case of $m = n$. We easily see that $m = n$ if and only if $R'_{m,n}(0) = 0$ because the constant term of $R'_{m,n}(X)$ is $m - n$. Note that Theorem 9 is valid not only for $R_{m,n}(X)$ but also for $R'_{m,n}(X)$ (cf. for example, [3], [4], [5] and [6]). For $n = m$, we see

$$R'_{m,m}(X) = -m(4m + 27)X(mX^2 + 27X^2 + 9X + 1)(m^2X^3 + mX - 1).$$

This means that, in the case of $n = m$, the polynomial $R_{m,m}(X)$ becomes quintic, and the vanishing root corresponds to the point at infinity (i.e. $[x, y] = [1, 0]$).

Table 1.

G_m	G_n	$G_{m,n}$	$DT(R_{m,n})$
S_3	S_3	$S_3 \times S_3$	$L_m \cap L_n = \mathbb{Q}$
		$(C_3 \times C_3) \rtimes C_2$	$[L_m \cap L_n : \mathbb{Q}] = 2$
		S_3	$L_m = L_n$
	C_3	$S_3 \times C_3$	$L_m \cap L_n = \mathbb{Q}$
	C_2	$S_3 \times C_2$	$L_m \not\supset L_n$
		S_3	$L_m \supset L_n$
C_3	C_3	$C_3 \times C_3$	$L_m \neq L_n$
		C_3	$L_m = L_n$
	C_2	C_6	$L_m \cap L_n = \mathbb{Q}$
	C_2	$C_2 \times C_2$	$L_m \neq L_n$
C_2	C_2	C_2	$L_m = L_n$
		C_2	$L_m = L_n$

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

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

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

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 $m = 3c(c + 3)$;

(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 $u^2 + 9u - 3m = (u - a)(u - b)$. 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 $m = 3c(c + 3)$. Conversely if $m = 3c(c + 3)$, then we have $R_{3c(c+3),0}(X) = 3c(c + 3)(X - 3c)^3(X + 3c + 9)^3$. (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 $u^3 + 9mu + 27m = (u - a)(u^2 + bu + c)$. 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

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

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. $\square$

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

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

$$\begin{aligned} &(-54, -12), (-18, -108), (-15, -675), (-14, -5292), \\ &(-13, -4563), (-12, -432), (-9, -27), (27, -3), \end{aligned}$$

then $\text{Spl}_{\mathbb{Q}} f_m(X) = \text{Spl}_{\mathbb{Q}} f_n(X)$.

Proof. If m and n satisfy the equation

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

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

$$n = -\frac{27m^2}{(2m + 27)^2} = -\frac{1}{3} \left(\frac{9m}{2m + 27} \right)^2 = -\frac{1}{3} \left(\frac{1}{2} \left(9 - \frac{243}{2m + 27} \right) \right)^2.$$

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. $\square$

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

$$f_m(X) = \text{Resultant}_Z\left(F_m(Z, 1), X - \frac{2Z^2 - (4m + 9)Z - 6m}{4m + 27}\right).$$

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 $m = -8$. $\square$

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 $\text{Spl}_{\mathbb{Q}} f_n(X) = \text{Spl}_{\mathbb{Q}} f_m(X)$. By Theorem 1, there exists $u \in \mathbb{Q}$ such that

$$n = \frac{m(u^2 + 9u - 3m)^3}{F_m(u, 1)^2}$$

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

$$\begin{aligned} n &= \frac{m(x^2 + 9xy - 3my^2)^3}{F_m(x, y)^2} \\ &= m + \frac{m(4m + 27)y(x^2 + 9xy + 27y^2 + my^2)(x^3 - mx^2y - m^2y^3)}{F_m(x, y)^2} \in \mathbb{Z}. \end{aligned} \tag{4}$$

We put

$$\lambda := F_m(x, y).$$

Then λ^2 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 λ^2 divides $m^3(4m + 27)^5$. 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 λ 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

$$r_m := \text{Resultant}_u(g(u), h(u)) = m^{12}(4m + 27)^{18} \in \mathbb{Z} \tag{5}$$

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

$$\begin{aligned} g(u) &= \sum_{i=0}^6 a_i u^{6-i} = mu^6 + 27mu^5 - 9(m-27)mu^4 - 81m(2m-9)u^3 \\ &\quad + 27(m-27)m^2u^2 + 243m^3u - 27m^4, \\ h(u) &= \sum_{i=0}^6 b_i u^{6-i} = u^6 - 4mu^5 + 2m(2m-9)u^4 + 2m(16m-27)u^3 \\ &\quad + m^2(8m+189)u^2 + 18m^2(2m+27)u + m^2(2m+27)^2. \end{aligned}$$

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

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

hence we have

$$r_m = m^9(4m+27)^{13}(g(u)p(u) + h(u)q(u)) \quad (6)$$

where

$$\begin{aligned} p(u) &= -15u^5 + 3(19m+9)u^4 - (48m^2 - 176m + 27)u^3 - 3m(4m^2 + 125m - 135)u^2 \\ &\quad - 6m(26m^2 + 339m + 162)u - m(28m^3 + 636m^2 + 3591m - 1458), \\ q(u) &= m(15u^5 + 3(m+126)u^4 - (68m-2943)u^3 - (26m^2 + 1809m - 5103)u^2 \\ &\quad + 9(5m^2 - 810m - 1458)u + 67m^3 + 2538m^2 + 11664m + 19683). \end{aligned}$$

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

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

Hence we get

$$\frac{G(x, y)P(x, y)}{\lambda^2} + Q(x, y) = \frac{m^3(4m+27)^5y^{11}}{\lambda^2} \in \mathbb{Z}.$$

It follows from $\gcd(x, y) = 1$ and $\lambda = x^3 - 2mx^2y - 9mxy^2 - m(2m+27)y^3$ that $\gcd(\lambda, y) = 1$. Hence we conclude that $\lambda^2 = F_m(x, y)^2$ divides $m^3(4m+27)^5$.

Conversely if $n \in \mathbb{Q}$ is given by (1) in Theorem 2 then, by (4), the sextic polynomial $R_{m,n}(X) = m(X^2 + 9X - 3m)^3 - nF_m(X, 1)^2$ has a root $u \in \mathbb{Q}$, and hence $\text{Spl}_{\mathbb{Q}}f_m(X) = \text{Spl}_{\mathbb{Q}}f_n(X)$ except for the cases of $n = 0$ and of $n = -27/4$. We note that for $m \in \mathbb{Z} \setminus \{0\}$ if $m \neq 3c(c+3)$ for any $c \in \mathbb{Z}$ (resp. $m \neq -8$) then $n \neq 0$ (resp. $n \neq -27/4$) by Lemma 11. $\square$

Proof of Theorem 3. We give a proof of Theorem 3 by using Theorem 2, Theorem 9 and Lemmas 7, 8 and 10 in the previous section.

We first treat the case where $m \neq n$. From the assumption, there exists $u \in \mathbb{Q}$ such that $R_{m,n}(u) = m(u^2 + 9u -$

Table 2.

m	λ	$F_m(x, y) = \lambda$	n	m	λ	$F_m(x, y) = \lambda$	n
-10	1	(1, 0)	-10	-4	-11^2	(-9, 2)	108/11
	-1	(-1, 1)	-106480		$2^2 \cdot 11^2$	(-8, 3)	16/11
	-5	(-5, 1)	-400		$2^2 \cdot 11^2$	(-26, 7)	9826/11
	13^2	(-11, 1)	-640/13		$-2^2 \cdot 11^2$	(-10, 1)	-2/11
	-13^2	(-9, 2)	-270/13		$-2^2 \cdot 11^2$	(-1384, 365)	206613902738896/11
	$2 \cdot 13^2$	(2, 1)	-160/13	-3	1	(1, 0)	-3
	$-5 \cdot 13^2$	(-125, 9)	-90792400/13		3^2	(-3, 1)	27
	$-5 \cdot 13^2$	(-5, 4)	-6250/13		5^2	(-2, 1)	3/5
-9	$2 \cdot 5 \cdot 13^2$	(-20, 3)	-100/13		$3^2 \cdot 5^2$	(3, 1)	-27/5
	1	(1, 0)	-9		$3^2 \cdot 5^2$	(-24, 7)	35937/5
	1	(-5, 1)	-3087		$-3^2 \cdot 5^2$	(-9, 2)	27/5
	3^3	(-6, 1)	-9	-2	1	(1, 0)	-2
	-3^3	(-3, 1)	-9		1	(-3, 1)	3456
	-3^3	(-12, 1)	-3087		19^2	(5, 1)	-128/19
	-3^3	(-3, 2)	-3087		19^2	(-259, 85)	196710433792/19
	3^4	(0, 1)	-27		-19^2	(-9, 2)	54/19
-8	3^4	(-9, 1)	-27	-1	$2 \cdot 19^2$	(-4, 3)	4/19
	-3^4	(-9, 2)	-27		$-2 \cdot 19^2$	(-22, 7)	16384/19
	1	(1, 0)	-8		1	(1, 0)	-1
	-2^3	(-4, 1)	-8		23^2	(7, 1)	-125/23
	2^4	(-6, 1)	[-27/4]		23^2	(-2, 3)	1/23
	5^2	(-7, 1)	-64/5		23^2	(-11, 5)	2197/23
	-5^2	(-9, 2)	-216/5		-23^2	(-9, 2)	27/23
	$2^3 \cdot 5^2$	(-16, 3)	-64/5	1	-23^2	(-42, 17)	4492125/23
-7	$-2^3 \cdot 5^2$	(-12, 1)	-216/5		1	(1, 0)	1
	$2^4 \cdot 5^2$	(-26, 3)	-6859/20		1	(5, 1)	300763
	$2^4 \cdot 5^2$	(-34, 7)	-6859/20		31^2	(11, 1)	343/31
	1	(1, 0)	-7		-31^2	(-9, 2)	-27/31
	1	(-3, 1)	-189		-31^2	(2, 3)	1/31
	1	(-5, 1)	-7	2	-31^2	(24, 5)	132651/31
	1	(-6, 1)	-189		1	(1, 0)	2
	1	(-41, 9)	-1588867		-1	(15, 2)	208974222
-6	-1	(-4, 1)	-7		-7^2	(-1, 1)	-16/7
	-1	(-9, 2)	-189		$2 \cdot 5^2$	(8, 1)	8788/5
	-1	(-25, 4)	-1588867		$-2 \cdot 5^2$	(-2, 1)	-32/5
	-1	(-16, 5)	-1588867		$-2 \cdot 7^2$	(6, 1)	864/7
	7	(-14, 3)	-49		$5^2 \cdot 7^2$	(13, 1)	1024/35
	-7	(-7, 1)	-49		$-5^2 \cdot 7^2$	(-9, 2)	-54/35
	-7	(-7, 2)	-49		$-2 \cdot 5^2 \cdot 7^2$	(4, 3)	4/35
	1	(1, 0)	-6	3	1	(1, 0)	3
-5	-1	(-13, 3)	48000		13^2	(49, 5)	114818259/13
	2	(-4, 1)	12		-13^2	(2, 1)	3/13
	3^2	(-3, 1)	[0]		$3^2 \cdot 13^2$	(15, 1)	729/13
	-3^2	(-9, 2)	54		$-3^2 \cdot 13^2$	(-9, 2)	-27/13
	$-2 \cdot 3^2$	(-6, 1)	[0]	4	1	(1, 0)	4
-4	1	(1, 0)	-5		2^2	(12, 1)	3456000
	1	(-4, 1)	625		43^2	(17, 1)	4000/43
	7^2	(-1, 1)	-5/7		-43^2	(-9, 2)	-108/43
	-7^2	(-9, 2)	135/7		$-2^2 \cdot 43^2$	(8, 3)	16/43
	$5 \cdot 7^2$	(-10, 3)	25/7	5	1	(1, 0)	5
-3	1	(1, 0)	-4		47^2	(19, 1)	6655/47
	-2^2	(-4, 1)	128		-47^2	(-9, 2)	-135/47
	11^2	(1, 1)	-32/11		$-5 \cdot 47^2$	(10, 3)	25/47

$3m)^3 - nF_m(u, 1)^2 = 0$. 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 μ where $\mu = 1, 3, 2$ according to $\text{Gal}_{\mathbb{Q}} f_m(X) \cong S_3, C_3, C_2$,

Table 3.

m	n	$F_m(x, y) = \lambda$	λ	$F_n(x, y) = \lambda'$	λ'
-6	12	$(-4, 1)$	2	$(-2, 1)$	$-2^2 \cdot 5^3$
-6	54	$(-9, 2)$	-3^2	$(-9, 2)$	-3^{10}
-6	48000	$(-13, 3)$	-1	$(-140, 3)$	$-2^6 \cdot 5^3 \cdot 11^3 \cdot 23^3$
-5	625	$(-4, 1)$	1	$(5, 1)$	$-5^3 \cdot 19^3$
-4	128	$(-4, 1)$	-2^2	$(-8, 1)$	$-2^7 \cdot 7^3$
-3	27	$(-3, 1)$	3^2	$(0, 1)$	-3^7
-2	3456	$(-3, 1)$	1	$(36, 1)$	$-2^6 \cdot 3^{12}$
12	54	$(18, 1)$	$-2^2 \cdot 3^2 \cdot 5^3$	$(36, 1)$	$-2 \cdot 3^{10}$
12	48000	$(28, 1)$	$-2^2 \cdot 5^3$	$(1640, 1)$	$-2^7 \cdot 5^3 \cdot 11^3 \cdot 23^3$
54	48000	$(117, 1)$	3^{10}	$(-3420, 1)$	$-2^6 \cdot 3^2 \cdot 5^3 \cdot 11^3 \cdot 23^3$

respectively (see the number of 1's in $\text{DT}(R_{m,n})$ 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 (*) which satisfies (1) is exactly μ and the assertion follows when $m \neq n$.

In the case where $n = m$, we recall that $R_{m,m}(X)$ 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 $\mu - 1$ 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 (*) which satisfies (1) also equals μ .

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

$$\varphi_m(x, y) := y(x^2 + 9xy + 27y^2 + my^2)(x^3 - mx^2y - m^2y^3) = 0.$$

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

$$\begin{aligned} \varphi_{-b^2-b-7}(x, y) \\ = y(x - (b - 4)y)(x + (b + 5)y)(x^3 + (b^2 + b + 7)x^2y - (b^2 + b + 7)^2y^3). \end{aligned}$$

Thus, the corresponding three primitive solutions are $(1, 0)$, $(b - 4, 1)$, $(-b - 5, 1) \in \mathbb{Z}^2$.

If $\text{Gal}_{\mathbb{Q}} f_m(X) \cong C_2$ then $m = -8$ by Lemma 7. We see

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

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

for which $R_{m,n}(X)$ has a linear factor over $\mathbb{Q}$, namely, $\text{Spl}_{\mathbb{Q}} f_m(X) = \text{Spl}_{\mathbb{Q}} f_n(X)$. 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.

m	n	$F_m(x, y) = \lambda$	λ	$F_n(x, y) = \lambda'$	λ'
-7	-49	$(-7, 1)$	-7	$(-35, 2)$	$7^2 \cdot 13^3$
-7	-49	$(-7, 2)$	-7	$(28, 1)$	$7^2 \cdot 13^3$
-7	-49	$(-14, 3)$	7	$(-7, 3)$	$-7^2 \cdot 13^3$
-7	-189	$(-3, 1)$	1	$(36, 1)$	3^{12}
-7	-189	$(-6, 1)$	1	$(-45, 1)$	3^{12}
-7	-189	$(-9, 2)$	-1	$(-9, 2)$	-3^{12}
-9	-27	$(0, 1)$	3^4	$(9, 1)$	3^8
-9	-27	$(-9, 1)$	3^4	$(-18, 1)$	3^8
-9	-27	$(-9, 2)$	-3^4	$(-9, 2)$	-3^8
-9	-3087	$(-5, 1)$	1	$(14, 1)$	$7^3 \cdot 37^3$
-9	-3087	$(-12, 1)$	-3^3	$(-231, 2)$	$-3^3 \cdot 7^3 \cdot 37^3$
-9	-3087	$(-3, 2)$	-3^3	$(273, 1)$	$3^3 \cdot 7^3 \cdot 37^3$
-10	-400	$(-5, 1)$	-5	$(-10, 1)$	$-2^3 \cdot 5^2 \cdot 11^3$
-10	-106480	$(-1, 1)$	-1	$(-638, 1)$	$2^3 \cdot 11^3 \cdot 181^3$
-12	-54	$(-6, 1)$	$2^2 \cdot 3^2$	$(0, 1)$	$2 \cdot 3^7$
-12	-432	$(0, 1)$	$2^2 \cdot 3^2$	$(36, 1)$	$2^4 \cdot 3^{10}$
-12	-71874	$(-18, 1)$	$2^2 \cdot 3^2$	$(-1584, 1)$	$2 \cdot 3^{10} \cdot 11^3 \cdot 13^3$
-13	-4563	$(0, 1)$	13	$(117, 1)$	$3^{12} \cdot 13^2$
-13	-4563	$(-39, 2)$	$5^3 \cdot 13$	$(-819, 2)$	$3^{12} \cdot 5^3 \cdot 13^2$
-13	-4563	$(-39, 7)$	$-5^3 \cdot 13$	$(-234, 7)$	$-3^{12} \cdot 5^3 \cdot 13^2$
-14	-5292	$(0, 1)$	$-2 \cdot 7$	$(-126, 1)$	$-2^2 \cdot 3^{12} \cdot 7^2$
-15	-675	$(0, 1)$	$-3^2 \cdot 5$	$(-45, 1)$	$3^{10} \cdot 5^2$
-15	-3645	$(-6, 1)$	3^2	$(27, 1)$	$-3^{10} \cdot 7^3$
-16	-6750	$(-6, 1)$	-2^3	$(-45, 1)$	$-3^{12} \cdot 5^3$
-18	-108	$(0, 1)$	$-2 \cdot 3^4$	$(-18, 1)$	$2^2 \cdot 3^8$
-18	-288	$(-6, 1)$	$-2 \cdot 3^3$	$(-12, 1)$	$-2^5 \cdot 3^3 \cdot 5^3$
-27	-3087	$(-45, 1)$	3^8	$(-504, 1)$	$3^4 \cdot 7^3 \cdot 37^3$
-27	-3087	$(9, 4)$	3^8	$(315, 4)$	$3^4 \cdot 7^3 \cdot 37^3$
-27	-3087	$(-36, 5)$	-3^8	$(-189, 5)$	$-3^4 \cdot 7^3 \cdot 37^3$
-36	-147456	$(3, 1)$	3^3	$(528, 1)$	$2^{12} \cdot 3^3 \cdot 71^3$
-38	-8208	$(3, 1)$	-5^3	$(-126, 1)$	$2^3 \cdot 3^{15}$
-45	-16875	$(-9, 1)$	3^4	$(90, 1)$	$-3^8 \cdot 5^3 \cdot 7^3$
-49	-189	$(-63, 1)$	$7^2 \cdot 13^3$	$(-126, 1)$	$3^{12} \cdot 7$
-49	-189	$(-42, 5)$	$-7^2 \cdot 13^3$	$(-63, 5)$	$-3^{12} \cdot 7$
-49	-189	$(21, 4)$	$7^2 \cdot 13^3$	$(63, 4)$	$3^{12} \cdot 7$
-54	-71874	$(9, 2)$	3^6	$(693, 2)$	$3^9 \cdot 11^3 \cdot 13^3$
-54	-432	$(-9, 1)$	-3^6	$(-18, 1)$	$-2^3 \cdot 3^9$
-68	-918	$(6, 1)$	$2^2 \cdot 7^3$	$(36, 1)$	$2 \cdot 3^{12}$
-88	-2376	$(-12, 1)$	$2^3 \cdot 5^3$	$(36, 1)$	$-2^3 \cdot 3^{12}$
-96	-39366	$(-12, 1)$	$-2^5 \cdot 3^2$	$(-162, 1)$	$-2 \cdot 3^{13} \cdot 7^3$
-108	-288	$(9, 1)$	3^8	$(18, 1)$	$2^3 \cdot 3^4 \cdot 5^3$
-135	-46305	$(9, 1)$	3^6	$(252, 1)$	$3^6 \cdot 7^3 \cdot 19^3$
-270	-1440	$(-18, 1)$	$-2 \cdot 3^8$	$(-36, 1)$	$-2^5 \cdot 3^4 \cdot 7^3$
-363	-4125	$(-22, 1)$	$5^3 \cdot 11^2$	$(55, 1)$	$-5^3 \cdot 11 \cdot 17^3$
-368	-1058	$(46, 3)$	$-2^3 \cdot 17^3 \cdot 23$	$(-115, 3)$	$23^2 \cdot 29^3$
-400	-106480	$(35, 2)$	$5^2 \cdot 11^3$	$(715, 2)$	$5 \cdot 11^3 \cdot 181^3$
-432	-71874	$(18, 1)$	$-2^3 \cdot 3^6$	$(-297, 1)$	$3^6 \cdot 11^3 \cdot 13^3$
-675	-3645	$(45, 2)$	$-3^9 \cdot 5^2$	$(-135, 2)$	$3^9 \cdot 5 \cdot 7^3$
-1404	-4992	$(36, 1)$	$2^2 \cdot 3^{10}$	$(72, 1)$	$2^7 \cdot 3^2 \cdot 17^3$
-1890	-8400	$(-45, 1)$	$-3^{10} \cdot 5$	$(-90, 1)$	$-2^3 \cdot 3^2 \cdot 5^2 \cdot 19^3$
-2784	-45414	$(348, 7)$	$-2^5 \cdot 3^2 \cdot 23^3 \cdot 29$	$(-1566, 7)$	$2 \cdot 3^7 \cdot 29^2 \cdot 31^3$
-4913	-103823	$(68, 1)$	$5^3 \cdot 17^3$	$(329, 1)$	$23^3 \cdot 47^3$
-14040	-54080	$(117, 1)$	$3^{12} \cdot 13$	$(234, 1)$	$2^3 \cdot 13^2 \cdot 53^3$
-15498	-64288	$(-126, 1)$	$-2 \cdot 3^{12} \cdot 7$	$(-252, 1)$	$-2^5 \cdot 5^3 \cdot 7^2 \cdot 11^3$

REFERENCES

- [1] Chapman, R. J., “Automorphism polynomials in cyclic cubic extensions,” *J. Number Theory*, **61**: 283–291 (1996).
- [2] Hoshi, A., and Miyake, K., “Tschirnhausen transformation of a cubic generic polynomial and a 2-dimensional involutive Cremona transformation,” *Proc. Japan Acad. Ser. A*, **83**: 21–26 (2007).
- [3] Hoshi, A., and Miyake, K., “A geometric framework for the subfield problem of generic polynomials via Tschirnhausen transformation,” *Number Theory and Applications: Proceedings of the International Conferences on Number Theory and Cryptography*, 65–104. Edited by S. D. Adhikari and B. Ramakrishnan. Hindustan Book Agency (2009).
- [4] Hoshi, A., and Miyake, K., On the field intersection problem of solvable quintic generic polynomials, preprint. arXiv:0804.4875v1 [math.NT]
- [5] Hoshi, A., and Miyake, K., “On the field intersection problem of generic polynomials: a survey,” *RIMS Kôkyûroku Bessatsu*, **B12**: 231–247 (2009).
- [6] Hoshi, A., and Miyake, K., “On the field intersection problem of quartic generic polynomials via formal Tschirnhausen transformation,” *Comment. Math. Univ. St. Pauli*, **58**: 51–86 (2009).
- [7] Jensen, C. U., Ledet, A., and Yui, N., *Generic polynomials. Constructive aspects of the inverse Galois problem*, Mathematical Sciences Research Institute Publications, 45. Cambridge University Press (2002).
- [8] Lang, S., *Elliptic curves: Diophantine analysis*, Grundlehren der Mathematischen Wissenschaften 231, Springer-Verlag, Berlin-New York (1978).
- [9] Lang, S., *Fundamentals of Diophantine geometry*, Springer-Verlag, New York (1983).
- [10] Morton, P., “Characterizing cyclic cubic extensions by automorphism polynomials,” *J. Number Theory*, **49**: 183–208 (1994).
- [11] PARI/GP, version 2.3.4, Bordeaux, 2008, <http://pari.math.u-bordeaux.fr/>.
- [12] Sendra, J. R., Winkler, F., and Pérez-Díaz, S., *Rational algebraic curves. A computer algebra approach*, Algorithms and Computation in Mathematics, 22. Springer-Verlag, Berlin (2008).
- [13] Wolfram Research, Inc., *Mathematica*, Version 6.0, Champaign, IL.