

On reducible trinomials, IV

By ANDRZEJ SCHINZEL (Warszawa)

*To Kálmán Győry, Attila Pethő, János Pintz and András Sárközy
 for their anniversary*

Abstract. Let $n > m$ be positive integers, $d = (n, m)$, $n = dn_1$, $m = dm_1$ and $T(x) = x^n + Ax^m + B$ defined over a field K be such that $x_1^n + Ax_1^m + B$ has a linear or quadratic factor f in $K[x]$. The paper deals with reducibility over K of $T(x)/f(x^d)$ and supplements earlier papers of this series.

The present paper supplements part II and III of the series. We shall use the same notation. In particular, n and m are positive integers, $n_1 = n/(n, m)$, $m_1 = m/(n, m)$, K is a field, $\text{char } K \nmid nm(n - m)$. There is some overlap with [1] indicated in the Remarks after the proofs of Theorem 2, 4 and 5. We shall prove

Theorem 1. Let $n \geq 2m$, $A, B \in K(\mathbf{y})^*$, $A^{-n}B^{n-m} \notin K$. Assume that $x^{n_1} + Ax^{m_1} + B$ has over $K(\mathbf{y})$ a linear factor $x - C$, but not a quadratic factor. Then $(x^n + Ax^m + B)/(x^{(n,m)} - C)$ is reducible over $K(\mathbf{y})$ if and only if for an integer l : $n = 8l$, $m = 2l$ and $A = A_{8,2}^1(C, D)$, $B = -C^4 - AC$, where $D \in K(\mathbf{y})^*$ and

$$A_{8,2}^1(v, w) = \frac{-w^8 - 4vw^6 + 2v^2w^4 - 52v^3w^2 - 9v^4}{64w^2}.$$

Theorem 2. Let $n \geq 2m$, L be a finite separable extension of $K(y)$ such that $\overline{KL}$ is of genus $g > 0$. Assume that $A, B \in L^*$, $A^{-n}B^{n-m} \notin K$ and $x^{n_1} + Ax^{m_1} + B$ has over L a linear factor $x - C$, but not a quadratic factor. For

Mathematics Subject Classification: 11R09.

Key words and phrases: reducibility, trinomials.

$g = 1$, $(x^n + Ax^m + B)/(x^{(n,m)} - C)$ is reducible over L if and only if there exists an integer l such that either $n = 8l$, $m = 2l$ and $A = A_{8,2}^1(C, D)$, $B = -C^4 - AC$, where $D \in L$, or $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in S_2 = \{\langle 10, 2 \rangle, \langle 12, 3 \rangle\}$ and

$$A = A_{\nu,\mu}^1(v, w)u^{\nu-\mu}, \quad B = -C^{n_1} - AC^{m_1}, \quad C = C_{\nu,\mu}(v, w)u^{(\nu,\mu)},$$

where

$$\langle v, w \rangle \in E_{\nu,\mu}^1(L), \quad u \in L$$

and $E_{\nu,\mu}^1$ is an elliptic curve given by

$$E_{10,2}^1: w^2 = v^3 - 2v + 4, \quad C_{10,2} = 20(1 - 2v) \text{ or } -40,$$

$$A_{10,2}^1 = 200^2(22 - 8v + 3v^2 + 10w)^2 - 20^4(1 - 2v)^4 \text{ or } -2200000, \text{ respectively;}$$

$$E_{12,3}^1: w^2 = v^3 - 891v + 9558, \quad C_{12,3} = 18(3v + w - 57) \text{ or } 18,$$

$$A_{12,3}^1 = 6^3(15v + w + 189)^3 - 18^3(3v + w - 57)^3 \text{ or } -5616, \text{ respectively.}$$

For $g > 1$, $(x^n + Ax^n + B)/(x^{(n,m)} - C)$ is reducible over L if and only if there exists an integer l such that $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in \mathbb{Z}^2$, $\nu < \max\{8g, 17\}$ and $(x^\nu + Ax^\mu + B)/(x^{(\mu,\nu)} - C)$ is reducible over L .

Theorem 3. Let $n \geq 2m$, K be an algebraic number field and $a, b \in K^*$. Assume that trinomial $x^{n_1} + ax^{m_1} + b$ has over K a linear factor $x - c$, but not a quadratic factor. Then $(x^n + ax^m + b)/(x^{(n,m)} - c)$ is reducible over K if and only if at least one of the following conditions is satisfied:

- (i) there exist an integer l such that $n = 8l$, $m = 2l$ and $d \in K$ such that $a = A_{8,2}^1(c, d)$, $b = c^4 - ac$;
- ii) there exist an integer l such that $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in S_2$ and $a = A_{\nu,\mu}^1(v, w)u^{\nu-\mu}$, $b = -c^{n_1} - Ac^{m_1}$ and $c = C_{\nu,\mu}(v, w)u^{(\nu,\mu)}$, where $\langle v, w \rangle \in E_{\nu,\mu}^1(K)$, $u \in K$;
- (iii) there exists an integer l such that $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in \mathbb{Z}^2$ and $\langle a_0, b_0, c_0 \rangle \in F_{\nu,\mu}(K)$, where $F_{\nu,\mu}(K)$ is a finite set, possibly empty.

Theorem 4. Let $n \geq 2m$, $A, B \in K(\mathbf{y})^*$, $A^{-n}B^{n-m} \notin K$. Assume that $x^{n_1} + Ax^{m_1} + B$ has over $K(\mathbf{y})$ a quadratic factor $F(x) = x^2 - Px + Q$. Then $(x^n + Ax^m + B)/F(x^{(n,m)})$ is reducible over $K(\mathbf{y})$ if and only if at least one of the following conditions is satisfied:

- (iv) $n = 3m$ and there exist $U_1, U_2 \in K(\mathbf{y})$ such that either $P = -U_1^l$, $l \mid m$, l prime or $P = 4U_2^4$, $4 \mid m$;

- (v) $n = 4m$ and there exist $U_3, \dots, U_7 \in K(\mathbf{y})$ such that either $4Q - 3P^2 = U_3^2$ or $\frac{-P + \sqrt{4Q - 3P^2}}{2} = (U_4 + U_5\sqrt{4Q - 3P^2})$, $l \mid m$, l prime, or $\frac{-P + \sqrt{4Q - 3P^2}}{2} = -4(U_6 + U_7\sqrt{4Q - 3P^2})^4$, $4 \mid m$;
- (vi) $n = 5m$ and there exists $U_8 \in K(\mathbf{y}) \setminus \{1, \zeta_4, -\zeta_4\}$ such that

$$\frac{P^2}{Q} = \frac{U_8 - 2}{U_8^3 - U_8^2 + U_8 - 1}$$

Theorem 5. Let $n \geq 2m$, L be a finite separable extension of $K(y)$ such that $\overline{KL}$ is of genus $g > 0$. Assume that $A, B \in L^*$, $A^{-n}B^{n-m} \notin K$ and $x^{n_1} + Ax^{m_1} + B$ has over L a quadratic factor $F(x) = x^2 - Px + Q$. For $g = 1$, $(x^n + Ax^m + B)/F(x^{(n,m)})$ is reducible over L if and only if either (iv), (v) or (vi) of Theorem 4 hold with $U_1, \dots, U_8$ in L , or (vii) there exists an integer l such that $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in S_3 = \{\langle 5, 2 \rangle, \langle 6, 1 \rangle, \langle 10, 2 \rangle\}$ and $P = P_{\nu, \mu}(v, w)u^{(\nu, \mu)}$, $Q = Q_{\nu, \mu}(v, w)u^{2(\nu, \mu)}$, where $\langle v, w \rangle \in E_{\nu, \mu}^2(L)$, $u \in L$ and $E_{\nu, \mu}^2$ is an elliptic curve given by

$$\begin{aligned} E_{5,2}^2 : w^2 &= v^3 + 5v^2 + 8v + 16, & P_{5,2} &= v + 4, & Q_{5,2} &= v^2 + 6v + 8 - 2w, \\ E_{6,1}^2 : w^2 &= v^3 + 3v + 1, & P_{6,1} &= v + 1, & Q_{6,1} &= v^2 + 2v + 3 - 2w, \\ E_{10,2}^2 : w^2 &= v^3 - 52v + 144, & P_{10,2} &= 2v - 8, & Q_{10,2} &= 3v^2 + 4v + 8w - 68. \end{aligned}$$

For $g > 1$, $(x^n + Ax^m + B)/F(x^{(n,m)})$ is reducible over L if and only if either (iv) or (v) of Theorem 4 hold with $K(\mathbf{y})$ replaced by L or (viii) there exists an integer l such that $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in \mathbb{Z}^2$, $\nu < \max\{\frac{24}{5}g, 16\}$ and $\frac{x^\nu + Ax^\mu + B}{F(x^{(n,m)})}$ is reducible over L .

Corollary 1. Let L be a finite separable extensions of $K(y)$ with $\overline{KL}$ of genus g and $A, B \in L^*$, $A^{-n}B^{n-m} \notin K$ and let F be a linear factor of $x^{n_1} + Ax^{m_1} + B$ in $K(y)[x]$ of maximal possible degree $d \leq 2$. If $n_1 > d + 2$, then $(x^{n_1} + Ax^{m_1} + B)F(x^{(n,m)})^{-1}$ is reducible over L , if and only if there exists an integer l such that $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in \mathbb{N}^2$, $\nu < \max\{17 - (d - 1)^2, \frac{24g}{2d+1}\}$ and $(x^\nu + Ax^\mu + B)F(x^{(\nu, \mu)})^{-1}$ is reducible over L .

Remark 1. This is a minor improvement on Theorem 2 of [4] in which $9d^2 - 8d + 16$ is replaced by $17 - (d - 1)^2$.

Theorem 6. Let $n \geq 2m$, K be an algebraic number field and $a, b \in K^*$. Assume that $x^{n_1} + ax^{m_1} + b$ has over K a quadratic factor $f(x) = x^2 - px + q$. Then $(x^n + ax^m + b)/f(x^{(n,m)})$ is reducible over K if and only if at least one of the following conditions is satisfied:

(ix) $n = 3m$ and there exist $u_1, u_2 \in K$ such that either $p = -u_1^l$, $l|m$, l prime or $p = 4u_2^4$, $4|m$;

(x) $n = 4m$ and there exist $u_3, \dots, u_7$ in K such that either $4q - 3p^2 = u_3^2$ or

$$\frac{-p + \sqrt{4q - 3p^2}}{2} = (u_4 + u_5 \sqrt{4q - 3p^2})^l, \quad l|m, \quad l \text{ prime}$$

or

$$\frac{-p + \sqrt{4q - 3p^2}}{2} = -4(u_6 + u_7 \sqrt{4q - 3p^2})^4, \quad 4|m;$$

(xi) $n = 5m$ and there exists $u_8 \in K \setminus \{1, \zeta_4, -\zeta_4\}$ such that

$$\frac{p^2}{q} = \frac{u_8 - 2}{u_8^3 - u_8^2 + u_8 - 1};$$

(xii) there exists an integer l and $u \in K$ such that $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in S_3$ and $p = P_{\nu, \mu}(v, w)u^{(\nu, \mu)}$, $q = Q_{\nu, \mu}(v, w)u^{2(\nu, \mu)}$, where $\langle v, w \rangle \in E_{\nu, \mu}^2(K)$, $u \in K$;

(xiii) there exists an integer l such that $\langle n/l, m/l \rangle =: \langle \nu, \mu \rangle \in \mathbb{Z}^2$ and $\langle a, b \rangle \in F_{\nu, \mu}(K)$, where $F_{\nu, \mu}(K)$ is a certain finite, possibly empty, set.

The proofs of all six theorems will be performed according to the same scheme: first the condition for reducibility given in the theorem will be shown necessary, then sufficient.

Lemma 1. In the notation of [3] we have for $n \geq 2m > 0$, $(m, n) = 1$, $q > 1$

$$g_{1*}(m, n, q) \begin{cases} \geq 0 & \text{if } \langle m, n, q \rangle = \langle 1, 4, 2 \rangle, \\ \geq 1 & \text{if } \langle m, n, q \rangle = \langle 1, 4, 3 \rangle, \langle 1, 5, 2 \rangle, \\ \geq 2 & \text{if } \langle m, n, q \rangle = \langle 1, 4, 4 \rangle, \\ > \frac{nq}{8} & \text{otherwise.} \end{cases}$$

PROOF. $g_{1*}(m, n, q)$ is the genus of the field $M_{1*}(m, n, q)$. By Lemma 2(a) and Lemmas 13–15 of [2] we have

$$g_{1*}(m, n, q) \geq 1 + \frac{1}{2} \left(\frac{q^{n-2} - q^{n-3}}{2} (n-2) - \left\lfloor \frac{q^{\max(n-3, m-1)}}{m} \left(1 + \frac{m-1}{q^{\varphi(qm)/\varphi(q)}} \right) \right\rfloor \right. \\ \left. - \left\lfloor \frac{q^{\max(n-3, n-m-1)}}{n-m} \left(1 + \frac{n-m-1}{q^{\varphi(q(n-m))/\varphi(q)}} \right) \right\rfloor \right) =: b(m, n, q).$$

Now, we find

$$b(1, 4, 3) = 1 = b(1, 5, 2), \quad b(1, 4, 4) = 2 = b(2, 5, 2)$$

and it remains to consider

$$n = 4, q \geq 5 \quad \text{or} \quad n = 5, q \geq 3 \quad (1)$$

or $n \geq 6$. By a formula on p. 596 of [3].

$$g_{1*}(m, n, q) \geq 1 + \frac{q^{n-3}}{2} \gamma_1(q, m, n),$$

where

$$\gamma_1(q, m, n) = \begin{cases} \frac{q-1}{2}(n-2) - 1 - \frac{q+1}{n-1} & \text{if } m = 1, \\ \frac{q-1}{2}(n-2) - \left(\frac{1}{m} + \frac{1}{n-m} \right) \left(1 + \frac{1}{q} \right) & \text{otherwise} \end{cases}$$

and in the case (1) $\gamma_1(q, n, m) \geq 1$,

$$\frac{q^{n-3}}{2} \gamma_1(q, n, m) \geq \frac{qn}{8}.$$

For $n \geq 6$ the inequality $g_{1*}(m, n, q) > \frac{qn}{8}$ has been proved on p. 596 of [3]. $\square$

PROOF OF THEOREM 1. *Necessity.* Let

$$Q(x; A, B) = \frac{x^{n_1} + Ax^{m_1} + B}{x - C}.$$

If $(x^n + Ax^m + B)/(x^{(m,n)} - C)$ is reducible over $K(\mathbf{y})$, then by Capelli's lemma either $Q(x; A, B)$ is reducible over $K(\mathbf{y})$ or $x^{(n,m)} - \xi$ is reducible over $K(\mathbf{y}, \xi)$, where ξ is a zero of $Q(x; A, B)$. Following the proof of Theorem 1 in [3] we find that either $g_1^*(k, m_1, n_1) = 0$ for a certain $k \in [2, \frac{n_1-1}{2}]$ or $g_{1*}(m_1, n_1, q) = 0$ for a certain $q \mid (m, n)$, $q > 1$, respectively. In the former case, by Lemma 8 of [3], $n_1 \geq 5$ and reducibility of $Q(x; A, B)$ contradicts the assumption that $x^{n_1} + Ax^{m_1} + B$ has no quadratic factor over $K(\mathbf{y})$. In the latter case, by Lemma 1, $\langle m_1, n_1, q \rangle = \langle 1, 4, 2 \rangle$, hence $\langle n, m \rangle = \langle 8, 2 \rangle$. By Lemma 29 of [2] we have

$$\frac{x^4 + Ax - (C^4 + AC)}{x - C} = xf(x)^2 - g(x)^2; \quad f, g \in K(\mathbf{y})[x],$$

hence for $a, b, c \in K(\mathbf{y})$:

$$\begin{aligned} x^3 + Cx^2 + C^2x + C^3 + A &= x(x+a)^2 - (bx+c)^2 \\ &= x^3 + (2a-b^2)x^2 + (a^2-2bc)x - c^2; \end{aligned}$$

$$2a - b^2 = C, \quad a^2 - 2bc = C^2, \quad ad - c^2 = C^3 + A \quad \text{and if } b \neq 0$$

$$(C + b^2)^2 - 8bc = 4C^2; \quad c = \frac{(C + b^2)^2 - 4C^2}{8b},$$

$$A = -c^2 - C^3 = A_{8,2}^1(C, b), \quad B = -C^4 - AC.$$

If $b = 0$ it follows that $C = 0$, hence $B = 0$, contrary to the assumption.

Sufficiency. If $n = 8l$, $m = 2l$, $A = A_{8,2}^1(C, D)$, $B = -C^4 - AC$ where $C \in K(\mathbf{y})$, $D \in K(\mathbf{y})^*$, then

$$\begin{aligned} \frac{x^{8l} + Ax^{2l} + B}{x^{2l} - C} &= \left(x^{3l} + Dx^{2l} + \frac{C + D^2}{2}x^l + \frac{-3C^2 + 2CD^2 + D^4}{8D} \right) \\ &\quad \times \left(x^{3l} - Dx^{2l} + \frac{C + D^2}{2}x^l - \frac{-3C^2 + 2CD^2 + D^4}{8D} \right). \quad (2) \end{aligned}$$

□

PROOF OF THEOREM 2. For $g > 1$ the assertion has already been proved in [3], thus we consider only the case $g = 1$.

Necessity. Arguing as in the Proof of Theorem 1 we find that either $g_{1*}(k, m_1, n_1) \leq 1$ for a certain $k \in [2, \frac{n_1-1}{2}]$ or $Q(x, A, B)$ is irreducible over L and $g_{1*}(m_1, n_1, q) \leq 1$ for a certain $q \mid (m, n)$, $q > 1$. In the former case, by Lemma 8 of [3], $n_1 \leq 6$ and reducibility of $Q(x, A, B)$ contradicts the assumption that $x^{n_1} + Ax^{m_1} + B$ has no quadratic factor over L . In the latter case, by Lemma 1, $\langle m_1, n_1, q \rangle = \langle 1, 4, 2 \rangle$, $\langle 1, 4, 3 \rangle$, or $\langle 1, 5, 2 \rangle$. If $\langle m_1, n_1, q \rangle = \langle 1, 4, 2 \rangle$ it follows, as in the proof of Theorem 1, that $A = A_{8,2}^1(C, D)$, where $D \in L^*$. If $\langle m_1, n_1, q \rangle = \langle 1, 4, 3 \rangle$ and $Q(x, A, B)$ is irreducible over L , then by Lemma 29 of [2], we have

$$\frac{x^4 + Ax - (C^4 + AC)}{x - C} = f(x)^3 + xg(x)^3 + x^2h(x)^3 - 3xf(x)g(x)h(x);$$

$$f, g, h \in L(x).$$

Hence for $a, b, c \in L$:

$$\begin{aligned} x^3 + Cx^2 + C^2x + C^3 + A &= (x + a)^3 + xb^3 + x^2c^3 - 3x(x + a)bc; \\ 3a + c^3 - 3bc &= C, \quad 3a^2 + b^3 - 3abc = C^2, \quad a^3 = C^3 + A, \\ a &= \frac{C - c^3 + 3bc}{3}, \quad \frac{(C - c^3 + 3bc)^2}{3} + b^3 - (C - c^3 + 3bc)bc = C^2. \quad (3) \end{aligned}$$

If $c = 0$ we obtain $a = C/3$, $b^3 = \frac{2}{3}C^2$, $b = \frac{2}{3}(\frac{C}{b})^2$ and taking $\frac{C}{3b} = u$ we have $b = 6u^2$, $C = 18u^3$, $A = a^3 - C^3 = (6^3 - 18^3)u^9 = -5616u^9$.

If $c \neq 0$ we put $\frac{C}{c^3} = \gamma$, $\frac{b}{c^2} = \beta$ and obtain from (3)

$$24\beta^3 + 9\beta^2 - 36\beta + 12 = (3\beta - 2)^2 + 8(3\beta^3 - 3\beta + 1) = (4\gamma - 3\beta + 2)^2.$$

Taking

$$u = \frac{c}{12}, \quad v = 24\beta + 3, \quad w = 24(4\gamma - 3\beta + 2),$$

we have

$$v^3 - 891v + 9558 = w^2$$

and

$$A = A_{18,3}^1(v, w)u^9, \quad C = C_{12,3}(v, w)u^3.$$

If $\langle m_1, n_1, q \rangle = \langle 1, 5, 2 \rangle$ and $Q(x, A, B)$ is irreducible over L , then, by Lemma 29 of [2], we have

$$\frac{x^5 + Ax - (C^5 + AC)}{x - C} = f(x)^2 - xg(x)^2, \quad f, g \in L(x),$$

hence for $a, b, c, d \in L$:

$$\begin{aligned} x^4 + Cx^3 + C^2x^2 + C^3x + C^4 + A &= (x^2 + ax + b)^2 - x(cx + d)^2; \\ 2a - c^2 &= C, \quad 2b + a^2 - 2cd = C^2, \quad 2ab - d^2 = C^3, \quad b^2 = C^4 + A, \\ a &= \frac{C + c^2}{2} \quad b = \frac{1}{8}(3C^2 - 2Cc^2 - c^4 + 8cd), \\ (C + c^2)(3C^2 - 2Cc^2 - c^4 + 8cd) - 8d^2 &= 8C^3. \end{aligned} \quad (4)$$

If $c = 0$ we obtain $-8d^2 = 5C^3$, $C = -\frac{8}{5}\left(\frac{d}{C}\right)^2$ and taking $\frac{d}{5C} = u$ we have $C = -40u^2$, $a = -20u^2$, $b = 600u^4$, $A = b^2 - C^4 = -2200000u^8$.

If $c \neq 0$ we put $\frac{C}{c^2} = \gamma$, $\frac{d}{c^3} = \delta$ and obtain from (4)

$$4(\gamma + 1)^2 - 2(5\gamma^3 - \gamma^2 + 3\gamma + 1) = (4\delta - 2\gamma - 2)^2.$$

Taking $2v = -5\gamma + 1$, $2w = 5(2\delta - \gamma - 1)$, $u = \frac{c}{10}$ we have

$$v^3 - 2v + 4 = w^2$$

and

$$A = A_{18,2}^1(v, w)u^8, \quad C = C_{12,2}(v, w)u^2.$$

Sufficiency. If $n = 8l$, $m = 2l$, $A = A_{8,2}^1(C, D)$, $B = -C^4 - AC$ where $C \in L$, $D \in L$, then $\frac{x^{8l} + Ax^{2l} + B}{x^{2l} - C}$ is reducible over L by (2).

If $n = 10l$, $m = 2l$ and $A = A_{10,2}^1(v, w)u^8$, $B = -C^5 - AC$, $C = C_{10,2}(v, w)u^2$ then

$$\begin{aligned} \frac{x^{10l} + Ax^{2l} + B}{x^{2l} - C} &= (x^{4l} + 10ux^{3l} + 20(3 - v)u^2x^{2l} + 200(w - v + 3)u^3x^l \\ &\quad + 200(22 - 8v + 3v^2 + 10w)u^4)(x^{4l} - 10ux^{3l} + 20(3 - v)u^2x^{2l} \\ &\quad - 200(w - v + 3)u^3x^l + 200(22 - 8v + 3v^2 + 10w)u^4). \end{aligned}$$

If $n = 10l$, $m = 2l$ and $A = -2200000u^8$, $B = -C^5 - AC$, $C = -40u^2$ then

$$\frac{x^{10l} + Ax^{2l} + B}{x^{2l} - C} = (x^{4l} - 20u^2x^{2l} - 200u^3x^l + 600u^4) \\ \times (x^{4l} - 20u^2x^{2l} + 200u^3x^l + 600u^4).$$

If $n = 12l$, $m = 3l$ and $A = A_{12,3}^1(v, w)u^9$, $B = -C^4 - AC$, $C = C_{12,3}(v, w)u^3$ then

$$\frac{x^{12l} + Ax^{3l} + B}{x^{3l} - C} = (x^{3l} + 12ux^{2l} + 6(v-3)u^2x^l + 6(15v+w-189)u^3) \\ \times (x^{6l} - 12ux^{5l} + 6(27-v)u^2x^{4l} + 12(9v+w-171)u^3x^{3l} \\ + 36(v^2 - 36v - 30w + 387)u^4x^{2l} \\ - 36(v-3)(15v+w-189)u^5x^l + 6^2(15v+w-189)u^6).$$

If $n = 12l$, $m = 3l$ and $A = -5616u^9$, $B = -C^4 - AC$, $C = 18u^3$, then

$$\frac{x^{12l} + Ax^{3l} + B}{x^{3l} - C} = (x^{3l} + 6u^2x^l + 6u^3) \\ \times (x^{6l} - 6u^2x^{4l} + 12u^3x^{3l} + 36u^4x^{2l} - 36u^5x^l + 36u^6). \quad \square$$

Remark. The calculations performed in the case $\langle m_1, n_1, q \rangle = \langle 1, 4, 3 \rangle$ are similar to those in the Proof of Theorem 6.5 of [1].

PROOF OF THEOREM 3. In view of Theorem 2 the proof does not differ essentially from the proof of Theorem 3 in [3]. The finiteness of the set $F_{\nu, \mu}(K)$ is a consequence of the Faltings theorem. $\square$

Lemma 2. For $n \geq 2m$, $(m, n) = 1$, $n \geq 2k + 2$ we have the following inequalities

$$g_2^*(k, m, n) \begin{cases} \geq 0 & \text{if } \langle k, m, n \rangle = \langle 1, 1, 5 \rangle, \\ \geq 1 & \text{if } \langle k, m, n \rangle = \langle 1, 2, 5 \rangle, \langle 1, 1, 6 \rangle, \\ \geq \frac{5n}{24} & \text{otherwise.} \end{cases}$$

PROOF. Except for $\langle k, m, n \rangle = \langle 2, 1, 6 \rangle$ this follows from the inequalities

$$g_2^*(k, m, n) \geq \binom{2k}{k} \left(\frac{k(n-2)}{8} - 1 \right) + 1 \quad \text{for } k > 1, \\ *g_2^*(1, m, n) \geq \frac{1}{2} \binom{n-2}{2} + \frac{1}{2} \zeta - (n-2) + 1$$

shown in the proof of Lemma 15 of [4], where ζ is given by the formula (9) there, namely

$$\zeta = \begin{cases} (n+m-4)/2 & \text{if } n \equiv m \equiv 1 \pmod{2}, \\ (2n-m-4)/2 & \text{if } n \equiv 1, m \equiv 0 \pmod{2}, \\ (n-2)/2 & \text{if } n \equiv 0, m \equiv 1 \pmod{2}. \end{cases}$$

For $\langle k, m, n \rangle = \langle 2, 1, 6 \rangle$ we profit by the result of [1] that $g_2^*(2, 1, 6) = 2$. $\square$

Lemma 3. *The number of vectors $\langle \alpha_1, \dots, \alpha_i, \dots, \alpha_a \rangle \in \mathbb{Z}/q\mathbb{Z}$ such that*

$$\sum_{\substack{i=1 \\ i \notin \mathcal{A}}}^a \zeta_q^{\alpha_i} \zeta_{aq}^i = 0, \quad \mathcal{A} \text{ a proper subset of } \{1, \dots, a\} \quad (5)$$

does not exceed

$$q^{a-|\mathcal{A}|-\min\{\min \mathcal{A}-1, \varphi(aq)/\varphi(q)\}},$$

where $\min \emptyset = \infty$.

PROOF. Let $\varrho = [\mathbb{Q}(\zeta_{aq}) : \mathbb{Q}(\zeta_q)] = \varphi(aq)/\varphi(q)$ and let $\zeta_{aq}^{r_j}$ ($1 \leq j \leq \varrho$) be all the conjugates of ζ_{aq} over $\mathbb{Q}(\zeta_q)$. The equation (5) gives

$$\sum_{i=1}^{\min\{\min \mathcal{A}-1, \varrho\}} \zeta_q^{\alpha_i} \zeta_{aq}^{ir_j} = - \sum_{\substack{i=\min\{\min \mathcal{A}-1, \varrho\}+1 \\ i \notin \mathcal{A}}}^a \zeta_q^{\alpha_i} \zeta_{aq}^{ir_j} \quad (1 \leq j \leq \min\{\min \mathcal{A}-1, \varrho\}).$$

The Vandermonde determinant $\det(\zeta_{aq}^{ir_j}) \neq 0$, hence α_i ($1 \leq i \leq \min\{\min \mathcal{A}-1, \varrho\}$) are determined uniquely by α_i ($\min\{\min \mathcal{A}-1, \varrho\} < i \leq a$, $i \notin \mathcal{A}$). The number of vectors formed by the latter is just the bound given in the lemma. $\square$

Lemma 4. *Let $x(t)$ be an algebraic function of t given in the neighbourhood of $t = 0$ by the Puiseux expansions*

$$\begin{aligned} x_i(t) &= \zeta_a^i t^{l_1/m_1} P_i(\zeta_a^i t^{1/m_1}) & (1 \leq i \leq a, i \notin \mathcal{A}), \\ x_{a+j}(t) &= \zeta_b^j t^{l_2/m_2} P_{a+j}(\zeta_b^j t^{1/m_2}) & (1 \leq j \leq b, j \notin \mathcal{B}), \end{aligned}$$

where $l_1, l_2 \in \mathbb{Z}$; $a, b, m_1, m_2 \in \mathbb{N}$, $\mathcal{A}, \mathcal{B}$ subsets of $\{1, \dots, a\}$, $\{1, \dots, b\}$, respectively and P_i, P_{a+j} ordinary power series with non-zero constant term. If

$$l_1 m_2 - l_2 m_1 = 1, \quad q \text{ is a positive integer} \quad (6)$$

and

$$y(t) = \left(\sum_{\substack{i=1 \\ i \notin \mathcal{A} \cup \mathcal{B} + a}}^{a+b} x_i(t)^{1/q} \right)^q, \quad (7)$$

then the number of distinct prime factors of the denominator of t in the field $\overline{K}(t, y(t))$ does not exceed

$$M_1 = \begin{cases} \frac{q^{a+b-|\mathcal{A}|-|\mathcal{B}|-2}}{m_1 m_2} \left(1 + \frac{m_1 - 1}{q^{\min\{\min \mathcal{A}-1, \varphi(aq)/\varphi(q)\}}} \right) \\ \quad \times \left(1 + \frac{m_2 - 1}{q^{\min\{\min \mathcal{B}-1, \varphi(bq)/\varphi(q)\}}} \right) & \text{if } |\mathcal{A}| < a, |\mathcal{B}| < b, \\ \frac{q^{a-|\mathcal{A}|-1}}{m_1} \left(1 + \frac{m_1 - 1}{q^{\min\{\min \mathcal{A}-1, \varphi(aq)/\varphi(q)\}}} \right) & \text{if } |\mathcal{A}| < a, |\mathcal{B}| = b, \\ \frac{q^{b-|\mathcal{B}|-1}}{m_2} \left(1 + \frac{m_2 - 1}{q^{\min\{\min \mathcal{B}-1, \varphi(bq)/\varphi(q)\}}} \right) & \text{if } |\mathcal{A}| = a, |\mathcal{B}| < b, \end{cases} \quad (8)$$

Remark. This lemma generalizes the arguments used in the proof of Lemma 22 and 23 of [2], Lemma 14 of [3].

PROOF. By (7) the Puiseux expansions of $y(t)$ at $t = 0$ are

$$\left(\sum_{\substack{i=1 \\ i \notin \mathcal{A}}}^a \zeta_q^{\alpha_i} \zeta_{aq}^i t^{l_1/m_1 q} P_i(\zeta_a^i t^{1/m_1})^{1/q} + \sum_{\substack{j=1 \\ j \notin \mathcal{B}}}^b \zeta_q^{\alpha_{a+j}} \zeta_{bq}^j t^{l_2/m_2 q} P_{a+j}(\zeta_b^j t^{1/m_2})^{1/q} \right)^q \quad (9)$$

where α_i, α_{a+j} run through $\mathbb{Z}/q\mathbb{Z}$.

Let $\mathcal{S}, \mathcal{T}$ be the sets of vector $\langle \alpha_1, \dots, \alpha_i, \dots, \alpha_a \rangle$ ($i \notin \mathcal{A}, |\mathcal{A}| < a$) and $\langle \alpha_{a+1}, \dots, \alpha_{a+j}, \dots, \alpha_{a+b} \rangle$ ($j \notin \mathcal{B}, |\mathcal{B}| < b$) such that

$$\sum_{\substack{i=1 \\ i \notin \mathcal{A}}}^a \zeta_q^{\alpha_i} \zeta_{aq}^i = 0 \quad \text{and} \quad \sum_{\substack{j=1 \\ j \notin \mathcal{B}}}^b \zeta_q^{\alpha_{a+j}} \zeta_{bq}^j = 0, \quad \text{respectively.}$$

By Lemma 3 we have

$$|\mathcal{S}| \leq q^{a-|\mathcal{A}|-\min\{\min \mathcal{A}-1, \varphi(aq)/\varphi(q)\}} \quad \text{if } |\mathcal{A}| < a, \quad (10)$$

and

$$|\mathcal{T}| \leq q^{b-|\mathcal{B}|-\min\{\min \mathcal{B}-1, \varphi(bq)/\varphi(q)\}} \quad \text{if } |\mathcal{B}| < b. \quad (11)$$

On the other hand, if $|\mathcal{A}| < a, |\mathcal{B}| < b$ and $\langle \alpha_1, \dots, \alpha_a \rangle \notin \mathcal{S}$ and $\langle \alpha_{a+1}, \dots, \alpha_{a+b} \rangle \notin \mathcal{T}$ the parenthesis in (9) contains $t^{l_1/m_1 q}$ and $t^{l_2/m_2 q}$ with non-zero coefficients.

We assert that the q -th power of the parenthesis contains with non-zero coefficients both monomials

$$t^{(q-1)\frac{l_1}{m_1} + \frac{l_2}{m_2q}} \quad \text{and} \quad t^{\frac{l_1}{m_1q} + (q-1)\frac{l_2}{m_2q}}. \quad (12)$$

Indeed, if for $i = 1$ or 2

$$(q-1)\frac{l_i}{m_iq} + \frac{l_{3-i}}{m_{3-i}q} = \sum_{\mu=0}^{\infty} a_{\mu} \left(\frac{l_1}{m_1q} + \frac{\mu}{m_1} \right) + \sum_{\mu=0}^{\infty} b_{\mu} \left(\frac{l_2}{m_2q} + \frac{\mu}{m_2} \right), \quad (13)$$

where a_{μ}, b_{μ} are non-negative integers and

$$\sum_{\mu=0}^{\infty} a_{\mu} + \sum_{\mu=0}^{\infty} b_{\mu} = q, \quad (14)$$

then multiplying both sides of (13) by m_1m_2q we obtain

$$l_{3-i}m_i - l_im_{3-i} \equiv l_1m_2 \sum_{\mu=0}^{\infty} a_{\mu} + l_2m_1 \sum_{\mu=0}^{\infty} b_{\mu} \pmod{q},$$

hence by (6) and (14)

$$(-1)^i \equiv \sum_{\mu=0}^{\infty} a_{\mu} \pmod{q}$$

and for $i = 1$: $\sum_{\mu=0}^{\infty} a_{\mu} = q - 1$, $\sum_{\mu=0}^{\infty} b_{\mu} = 1$; for $i = 2$: $\sum_{\mu=0}^{\infty} a_{\mu} = 1$, $\sum_{\mu=0}^{\infty} b_{\mu} = q - 1$.

Now, (13) gives in both cases

$$\sum_{\mu=0}^{\infty} a_{\mu}\mu = 0 = \sum_{\mu=0}^{\infty} b_{\mu}\mu$$

and, since $a_{\mu} \geq 0$, $b_{\mu} \geq 0$, $a_{\mu} = 0 = b_{\mu}$ for $\mu > 0$, thus for $i = 0$: $a_0 = q - 1$, $b_0 = 1$; for $i = 2$: $a_0 = 1$, $b_0 = q - 1$. Therefore, there is no cancellation and both monomials (12) occur with non-zero coefficients in the Puiseux expansion of $y(t)$ at $t = 0$. Now, by (6),

$$(q-1)\frac{l_i}{m_iq} + \frac{l_{3-i}}{m_{3-i}q} = \frac{ql_im_{3-i} + l_{3-i}m_i - l_im_{3-i}}{m_1m_2q} = \frac{ql_im_{3-i} + (-1)^i}{m_1m_2q},$$

hence the reduced denominator is divisible by qm_{3-i} and, since $(m_1, m_2) = 1$ we have l.c.m. $[qm_2, qm_1] = qm_1m_2$. Thus we obtain for $y(t)$ at $t = 0$

$$\frac{(q^{a-|A|} - |\mathcal{S}|)(q^{b-|B|} - |\mathcal{T}|)}{q^2m_1m_2} \text{ cycles of length } qm_1m_2.$$

If $|\mathcal{A}| < a$, $|\mathcal{B}| < b$, $\langle \alpha_1, \dots, \alpha_a \rangle \notin \mathcal{S}$ and $\langle \alpha_{a+1}, \dots, \alpha_{a+b} \rangle \in \mathcal{T}$, then the parenthesis in (9) contains $t^{\frac{l_1}{m_1q}}$ and $t^{\frac{l_2}{m_2q} + \frac{\nu}{m_2}}$ (we take the least possible $\nu \in \mathbb{N}$) with non-zero coefficients, hence the q -th power of the parenthesis contains with a non-zero coefficient

$$t^{\frac{l_1}{m_1q} + (q-1)\left(\frac{l_2}{m_2q} + \frac{\nu}{m_2}\right)},$$

(the proof is similar to the one given above). However, by (6),

$$\frac{l_1}{m_1q} + (q-1)\left(\frac{l_2}{m_2q} + \frac{\nu}{m_2}\right) = \frac{m_1q(l_2 + \nu(q-1)) + 1}{m_1m_2q},$$

hence the reduced denominator is divisible by m_1q and we obtain for $y(t)$ at $t = 0$ at most

$$\frac{(q^{a-|\mathcal{A}|} - |\mathcal{S}|)|\mathcal{T}|}{q^2m_1}$$

cycles.

If $|\mathcal{A}| < a$, $|\mathcal{B}| < b$, $\langle \alpha_1, \dots, \alpha_a \rangle \in \mathcal{S}$ and $\langle \alpha_{a+1}, \dots, \alpha_{a+b} \rangle \notin \mathcal{T}$ we obtain similarly for $y(t)$ at $t = 0$ at most

$$\frac{|\mathcal{S}|(q^{b-|\mathcal{B}|} - |\mathcal{T}|)}{q^2m_2}$$

cycles.

Finally, if $|\mathcal{A}| < a$, $|\mathcal{B}| < b$, $\langle \alpha_1, \dots, \alpha_a \rangle \in \mathcal{S}$ and $\langle \alpha_{a+1}, \dots, \alpha_{a+b} \rangle \in \mathcal{T}$ the parenthesis in (9) contains with non-zero coefficients

$$t^{\frac{l_1}{m_1q} + \frac{\nu_1}{m_1}} \quad \text{and} \quad t^{\frac{l_2}{m_2q} + \frac{\nu_2}{m_2}}$$

(we take the least possible ν_1, ν_2 in $\mathbb{N}$), hence the q -th power of the parenthesis contains with a non-zero coefficient

$$t^{(q-1)\left(\frac{l_1}{m_1q} + \frac{\nu_1}{m_1}\right) + \frac{l_2}{m_2q} + \frac{\nu_2}{m_2}}. \quad (15)$$

Indeed, if

$$(q-1)\left(\frac{l_1}{m_1q} + \frac{\nu_1}{m_1}\right) + \frac{l_2}{m_2q} + \frac{\nu_2}{m_2} = \sum_{\mu=\nu_1}^{\infty} a_{\mu} \left(\frac{l_1}{m_1q} + \frac{\mu}{m_1}\right) + \sum_{\mu=\nu_2}^{\infty} b_{\mu} \left(\frac{l_2}{m_2q} + \frac{\mu}{m_2}\right), \quad (16)$$

where a_{μ}, b_{μ} are non-negative integers and

$$\sum_{\mu=\nu_1}^{\infty} a_{\mu} + \sum_{\mu=\nu_2}^{\infty} b_{\mu} = q, \quad (17)$$

then multiplying both sides of (16) by $m_1 m_2 q$ we obtain

$$-1 \equiv l_1 m_2 \sum_{\mu=\nu_1}^{\infty} a_{\mu} + l_2 m_1 \sum_{\mu=\nu_2}^{\infty} b_{\mu} \pmod{q},$$

hence by (6) and (17)

$$-1 \equiv \sum_{\mu=\nu_1}^{\infty} a_{\mu} \pmod{q}$$

and $\sum_{\mu=\nu_1}^{\infty} a_{\mu} = q - 1$, $\sum_{\mu=\nu_2}^{\infty} b_{\mu} = 1$. Now (16) gives

$$m_2 \sum_{\mu=\nu_1}^{\infty} a_{\mu} \mu + m_1 \sum_{\mu=\nu_2}^{\infty} b_{\mu} \mu = m_2 (q - 1) \nu_1 + m_1 \nu_2,$$

hence $a_{\mu} = 0$ for $\mu > \nu_1$ and $b_{\mu} = 0$ for $\mu > \nu_2$, $a_{\nu_1} = q - 1$, $b_{\nu_2} = 1$. Therefore, there is no cancellation and the monomial (15) occurs with a non-zero coefficients in the Puiseux expansions of $y(t)$ at $t = 0$. Now,

$$(q - 1) \left(\frac{l_1}{m_1 q} + \frac{\nu_1}{m_1} \right) + \frac{l_2}{m_2 q} + \frac{\nu_2}{m_2} = \frac{q(m_2 l_1 + m_2 \nu_1 (q - 1) + m_1 \nu_2 q) - 1}{m_1 m_2 q},$$

hence the reduced denominator is divisible by q and we obtain for $y(t)$ at most

$$\frac{|\mathcal{S}| |\mathcal{T}|}{q^2}$$

cycles. The total number of cycles does not exceed

$$\begin{aligned} & \frac{(q^{a-|\mathcal{A}|} - |\mathcal{S}|)(q^{b-|\mathcal{B}|} - |\mathcal{T}|)}{q^2 m_1 m_2} + \frac{(q^{a-|\mathcal{A}|} - |\mathcal{S}|) |\mathcal{T}|}{q^2 m_1} + \frac{|\mathcal{S}| (q^{b-|\mathcal{B}|} - |\mathcal{T}|)}{q^2 m_2} + \frac{|\mathcal{S}| |\mathcal{T}|}{q^2} \\ &= \frac{q^{a+b-|\mathcal{A}|-|\mathcal{B}|}}{q^2 m_1 m_2} + |\mathcal{S}| \frac{q^{b-|\mathcal{B}|}}{q^2 m_2} \left(1 - \frac{1}{m_1} \right) + |\mathcal{T}| \frac{q^{a-|\mathcal{A}|}}{q^2 m_1} \left(1 - \frac{1}{m_2} \right) \\ & \quad + \frac{|\mathcal{S}| |\mathcal{T}|}{q^2} \left(1 - \frac{1}{m_1} \right) \left(1 - \frac{1}{m_2} \right). \end{aligned}$$

Using the inequalities (10) and (11) we obtain for the number of cycles the bound M_1 given by (8). $\square$

Consider now the case $|\mathcal{A}| < a$, $|\mathcal{B}| = b$. Then, if $\langle \alpha_1, \dots, \alpha_a \rangle \notin \mathcal{S}$, the monomial of the least degree occurring with a non-zero coefficient in the parenthesis of (9) is $t^{1/m_1 q}$ and the q -th power of the parenthesis contains with a non-zero

coefficient t^{1/m_1} . It follows by (10) that the number of cycles for $y(t)$ at $t = 0$ is at most

$$\begin{aligned} \frac{q^{a-|\mathcal{A}|} - |\mathcal{S}|}{qm_1} + \frac{|\mathcal{S}|}{q} &= \frac{q^{a-|\mathcal{A}|-1}}{m_1} + \frac{|\mathcal{S}|}{q} \left(1 - \frac{1}{m_1}\right) \\ &\leq \frac{q^{a-|\mathcal{A}|-1}}{m_1} \left(1 + \frac{m_1 - 1}{q^{\min\{\min \mathcal{A} - 1, \varphi(aq)/\varphi(q)\}}}\right) = M_1. \end{aligned}$$

The case $|\mathcal{A}| = a$, $|\mathcal{B}| < b$ is treated similarly.

Lemma 5. *Let $x(t)$ be an algebraic function of t given in the neighbourhood of $t = \infty$ by the Puiseux expansion*

$$\begin{aligned} x_i(t) &= \zeta_c^i t^{l_3/m_3} Q_i(\zeta_c^i t^{1/m_3}) & (1 \leq i \leq c, i \notin \mathcal{C}), \\ x_{c+j}(t) &= \zeta_d^j t^{l_4/m_4} Q_{c+j}(\zeta_d^j t^{1/m_4}) & (1 \leq j \leq d, j \notin \mathcal{D}), \end{aligned}$$

where $l_3, l_4 \in \mathbb{Z}$; $c, d, m_3, m_4 \in \mathbb{N}$, $\mathcal{C}, \mathcal{D}$ are proper subsets of $\{1, \dots, a\}$, $\{1, \dots, b\}$, respectively and Q_i, Q_{c+j} ordinary power series with non-zero constant terms. If $l_3 m_4 - l_4 m_3 = 1$, q is a positive integer and

$$y(t) = \left(\sum_{\substack{i=1 \\ i \notin \mathcal{C} \cup \mathcal{D} + c}}^{c+d} x_i(t)^{1/q} \right)^q,$$

then the number of distinct prime factors of the denominator of t in the field $\overline{K}(t, y(t))$ does not exceed

$$M_2 = \begin{cases} \frac{q^{c+d-|\mathcal{C}|-|\mathcal{D}|-2}}{m_3 m_4} \left(1 + \frac{m_3 - 1}{q^{\min\{\min \mathcal{C} - 1, \varphi(cq)/\varphi(q)\}}}\right) \\ \quad \times \left(1 + \frac{m_4 - 1}{q^{\min\{\min \mathcal{D} - 1, \varphi(dq)/\varphi(q)\}}}\right) & \text{if } |\mathcal{C}| < c, |\mathcal{D}| < d, \\ \frac{q^{c-|\mathcal{C}|-1}}{m_3} \left(1 + \frac{m_3 - 1}{q^{\min\{\min \mathcal{C} - 1, \varphi(cq)/\varphi(q)\}}}\right) & \text{if } |\mathcal{C}| < c, |\mathcal{D}| = d, \\ \frac{q^{d-|\mathcal{D}|-1}}{m_4} \left(1 + \frac{m_4 - 1}{q^{\min\{\min \mathcal{D} - 1, \varphi(dq)/\varphi(q)\}}}\right) & \text{if } |\mathcal{C}| = c, |\mathcal{D}| < d, \end{cases}$$

PROOF. We apply Lemma 4 to the algebraic function $x(t^{-1})$ replacing l_1, l_2, a, b, m_1, m_2 by $-l_4, -l_3, d, c, m_4, m_3$, respectively. $\square$

Lemma 6. *In the notation of [4] (Lemma 8) if $n \geq 5$ the number of distinct prime factors dividing the numerator or the denominator of t in the field $\overline{K}(t, y(t))$ is at most*

$$M_3 = \begin{cases} \frac{q^{n-4}}{2} \left(1 + \frac{1}{q^{\min\{\frac{n-3}{2}, \varphi((n-1)q)/\varphi(q)\}}} \right) + q^{n-3} & \text{if } n \equiv 1 \pmod{2}, m = 1, \\ \frac{q^{n-3}}{n-2} \left(1 + \frac{n-3}{q^{\varphi((n-2)q)/\varphi(q)}} \right) + q^{n-4} & \text{if } n \equiv 1 \pmod{2}, m = 2, \\ 2q^{n-3}, & \text{otherwise.} \end{cases}$$

PROOF. In the notation of [4] (Lemma 3) we have

$$f_m x^n - t^\alpha f_n x^m + t^\beta f_{n-m} = \prod_{i=1}^n (x - x_i(t)), \quad x^2 - tx + t = \prod_{i \in \mathcal{I}} (x - x_i(t)),$$

where f_n is a monic polynomial of degree $\lfloor \frac{n-1}{2} \rfloor$ with a non-zero constant term and

$$\alpha = \left\lfloor \frac{n}{2} \right\rfloor - \left\lfloor \frac{m}{2} \right\rfloor, \quad \beta = \left\lfloor \frac{n+m}{2} \right\rfloor - \left\lfloor \frac{m}{2} \right\rfloor.$$

We have to choose $a, b, c, d, \mathcal{A}, \mathcal{B}, \mathcal{C}, \mathcal{D}$ that

$$\{1, \dots, a+b\} \setminus \mathcal{A} \setminus (a+\mathcal{B}) = \{1, \dots, n\} \setminus \mathcal{I}, \quad c+d = n, \quad |\mathcal{C}| + |\mathcal{D}| = 2.$$

If $n \equiv m \equiv 1 \pmod{2}$ we take in Lemmas 4 and 5

$$\begin{aligned} a &= m, & l_1 &= \frac{m+1}{2}, & m_1 &= m, & \mathcal{A} &= \emptyset; \\ b &= n-m, & l_2 &= 1, & m_2 &= 2, & \mathcal{B} &= \left\{ \frac{n-m}{2}, n-m \right\}; \\ c &= n-m, & l_3 &= 1, & m_3 &= 1, & \mathcal{C} &= \{n-m\}; \\ d &= m, & l_4 &= 0, & m_4 &= 1, & \mathcal{D} &= \{m\}. \end{aligned}$$

If $n \equiv 1, m \equiv 0 \pmod{2}$ we take in Lemmas 4 and 5

$$\begin{aligned} a &= m, & l_1 &= 1, & m_1 &= 2, & \mathcal{A} &= \left\{ \frac{m}{2}, m \right\}; \\ b &= n-m, & l_2 &= \frac{n-m-1}{2}, & m_2 &= n-m, & \mathcal{B} &= \emptyset; \\ c &= n-m, & l_3 &= 1, & m_3 &= 1, & \mathcal{C} &= \{n-m\}; \\ d &= m, & l_4 &= 0, & m_4 &= 1, & \mathcal{D} &= \{m\}. \end{aligned} \quad \square$$

Lemma 7. *In the notation of [4] we have for $n \geq 5$, $n \geq 2m$, $(m, n) = 1$, $q \geq 2$*

$$g_{2*}(m, n, q) \begin{cases} \geq 1 & \text{if } \langle m, n, q \rangle = \langle 1, 5, 2 \rangle, \\ \geq 2 & \text{if } \langle m, n, q \rangle = \langle 2, 5, 2 \rangle, \\ \geq 3 & \text{if } \langle m, n, q \rangle = \langle 1, 5, 3 \rangle, \\ > \frac{5nq}{24} & \text{otherwise.} \end{cases}$$

PROOF. By Lemma 2(a) of [2], Lemma 20–22 of [4] and Lemma 6 we have

$$\begin{aligned} g_{2*}(m, n, q) \geq 1 + \frac{q^{n-4}}{2} \left(\frac{q-1}{2} \binom{n-2}{2} \right. \\ \left. + \left\lfloor \frac{m-1}{2} \right\rfloor \left(q - \frac{1}{n-m} \left(1 + \frac{n-m-1}{q^{\varphi((n-m)q)/\varphi(q)}} \right) \right) \right. \\ \left. + \left\lfloor \frac{n-m-1}{2} \right\rfloor \left(q - \frac{1}{m} \left(1 + \frac{m-1}{q^{\varphi(mq)/\varphi(q)}} \right) - M_3 q^{4-n} \right) \right). \end{aligned}$$

If $\langle m, n \rangle = \langle 1, 5 \rangle$ we obtain

$$g_{2*}(m, n, q) \geq \left\lfloor 1 + \frac{q}{2} \left(\frac{5}{2}(q-1) - \frac{1}{2} - \frac{1}{2q} - q \right) \right\rfloor = \left\lfloor \frac{3}{4}(q-1)^2 \right\rfloor,$$

thus $g_{2*}(m, n, q) > \frac{25q}{24}$ unless $q \leq 3$.

If $\langle m, n \rangle = \langle 2, 5 \rangle$ we obtain

$$\begin{aligned} g_{2*}(m, n, q) &\geq \left\lfloor 1 + \frac{q}{2} \left(\frac{3}{2}(q-1) + q - \frac{1}{2} - \frac{1}{2q} - \frac{q}{3} - \frac{2}{3q} - 1 \right) \right\rfloor \\ &= \left\lfloor \frac{1}{12}(q-1)(13q-5) \right\rfloor, \end{aligned}$$

thus $g_{2*}(m, n, q) > \frac{25q}{24}$ unless $q = 2$.

If $n \geq 6$ we have (cf. [4], p. 68)

$$g_{2*}(m, n, q) \geq 1 + \frac{q^{n-4}}{2}(3q-5) > \frac{5nq}{24}. \quad \square$$

PROOF OF THEOREM 4. *Necessity.* Let

$$Q(x; A, B) = \frac{x^{n_1} + Ax^{m_1} + B}{x^2 - Px + Q}. \quad (18)$$

If $\langle m_1, n_1 \rangle = \langle 1, 3 \rangle$, then

$$Q(x; A, B) = x + P$$

and condition (iv) follows from Capelli's theorem.

If $\langle m_1, n_1 \rangle = \langle 1, 4 \rangle$ then

$$Q(x; A, B) = x^2 + Px + (P^2 - Q)$$

and condition (v) follows from Capelli's lemma and Capelli's theorem. Therefore, let $n_1 \geq 5$. If $Q(x^{(m,n)}; A, B)$ is reducible over $K(\mathbf{y})$, then by Capelli's lemma either $Q(x; A, B)$ is reducible over $K(\mathbf{y})$, or $x^{(m,n)} - \xi$ is reducible over $K(\mathbf{y}, \xi)$, where ξ is a zero of $Q(x; A, B)$. Following the proof of Theorem 1 in [4] we find that either $g_2^*(k, m_1, n_1) = 0$ for a certain $k \leq \frac{n_1-2}{2}$ or $g_{2*}(m_1, n_1, q) = 0$ for a certain $q \mid (m, n)$, $q > 1$, respectively. The latter case is impossible by Lemma 7. In the former case by Lemma 2 above $\langle k, m_1, n_1 \rangle = \langle 1, 1, 5 \rangle$ and we have to consider the case $x^5 + Ax + B = (x^2 - Px + Q)(x + a)(x^2 + bx + c)$, where $a, b, c \in K(\mathbf{y})$. This gives the following system of equations:

$$\begin{aligned} a + b - P &= 0, & ab + c - Pa - Pb + Q &= 0, \\ ac - Pab - Pc + Qa + Qb &= 0 \end{aligned}$$

We cannot have $P = 0$, since this would imply $B = 0$. Taking $U_8 = a/P$ we obtain

$$\frac{P^2}{Q} = \frac{(a+b)^2(a+2b)}{2a^2b + 2ab^2 + b^3} = \frac{U_8 - 2}{U_8^3 - U_8^2 + U_8 - 1},$$

where $U_8 \in K(\mathbf{y}) \setminus \{1, \zeta_4, -\zeta_4\}$, which gives condition (vi).

Sufficiency. If (iv) is satisfied, $Q(x^{(m,n)}; A, B)$ is divisible either by

$$x^{m/l} - U_1^{m/l} \quad (P = U_1^l)$$

or by

$$x^{m/2} + 2U_2x^{m/4} + 2U_2^2 \quad (P = 4U_2^4).$$

If (v) is satisfied, $Q(x^{(m,n)}; A, B)$ is divisible either by $x^{m/l} - U_1^{m/l}$ ($P = U_1^l$) or by

$$x^{m/2} + \frac{P + U_3}{2},$$

or by

$$x^{2m/l} - 2U_4x^{m/l} + U_4^2 - U_5^2(4Q - 3P^2),$$

or by

$$\begin{aligned} x^m + 4U_6x^{3m/4} + 8U_6^2x^{m/2} + 8U_6(U_6^2 - U_7^2(4Q - 3P^2))x^{m/4} \\ + 4(U_6^2 - U_7^2(4Q - 3P^2))^2. \end{aligned}$$

If (vi) is satisfied, then

$$Q(x^{(m,n)}; A, B) = (x^{(m,n)} + P)(x^{2(m,n)} + (P - PU_8)x^{(m,n)} + P^2(U_8^2 - U_8 + 1) - Q).$$

□

Remark. The calculations performed in the case $\langle k_1, m_1, n_1 \rangle = \langle 1, 2, 5 \rangle$ are similar to those in [1], Proof of Theorem 3.1.

PROOF OF THEOREM 5. Necessity. Let $Q(x; A, B)$ be again given by (18). If $n_1 \leq 4$ the conditions (iv) and (v) with $K(\mathbf{y})$ replaced by L follow as in the proof of Theorem 4, or $g > \frac{5n_1}{24}$ and the condition (viii) holds with $\nu = n_1$, thus let $n_1 \geq 5$. If $Q(x^{(m,n)}; A, B)$ is reducible over L , then by Capelli's lemma either $Q(x; A, B)$ is reducible over L , or $x^{(m,n)} - \xi$ is reducible over $L(\xi)$, where ξ is a zero of $Q(x; A, B)$. Following the proof of Theorem 2 in [4] we find that either $g_2^*(k, m_1, n_1) \leq g$ for a certain $k \leq \frac{n_1-2}{2}$, or $g_{2*}(m_1, n_1, q) \leq g$ for a certain $q \mid (m, n)$, $q > 1$, respectively. In the former case, by Lemma 2 either, $\langle k, m_1, n_1 \rangle = \langle 1, 1, 5 \rangle, \langle 1, 2, 5 \rangle$ or $\langle 1, 1, 6 \rangle, \langle 1, 5, 3 \rangle, \langle 2, 5, 2 \rangle$ or $g > \frac{5n_1q}{24}$. For $g = 1$ we have $\langle k, m_1, n_1 \rangle = \langle 1, 1, 5 \rangle, \langle 1, 2, 5 \rangle, \langle 1, 1, 6 \rangle$ or $\langle m_1, n_1, q \rangle = \langle 1, 5, 2 \rangle$. We consider these cases successively. The case $\langle k, m_1, n_1 \rangle = \langle 1, 1, 5 \rangle$ leads to (vi) with $K(\mathbf{y})$ replaced by L , as in the proof of Theorem 2. The case $\langle k, m_1, n_1 \rangle = \langle 1, 2, 5 \rangle$ leads to the equality

$$x^5 + Ax^2 + B = (x^2 - Px + Q)(x + a)(x^2 + bx + c), \quad a, b, c \in L.$$

This gives the following system of equations:

$$a + b - P = 0, \quad ab + c - Pa - Pb + Q = 0, \quad -Pac + Qab + Qc = 0$$

and on eliminating P and Q

$$-(a + b)ac + ab(a^2 + ab + b^2 - c) + c(a^2 + ab + b^2 - c) = 0$$

$ab = 0$ implies $B = 0$, hence $ab \neq 0$ and or putting $b = \beta a$, $c = \gamma a^2$ it follows

$$\gamma^2 - (\beta^2 - \beta)\gamma - (\beta^3 + \beta^2 + \beta) = 0,$$

$$(2\gamma - (\beta^2 - \beta))^2 = (\beta^2 - \beta)^2 + 4(\beta^3 + \beta^2 + \beta) = \beta^4 + 2\beta^3 + 5\beta^2 + 4\beta.$$

Taking $4\beta^{-1} = v$, $8\gamma\beta^{-2} - 4 + 4\beta^{-1} = w$, $\frac{a\beta}{4} = u$ we obtain $w^2 = v^3 + 5v^2 + 8v + 16$, where $v, w \in L$ and $P = u(v + 4)$, $Q = u^2(v^2 + 6v + 8 - 2w)$.

Consider now $\langle k, m, n \rangle = \langle 1, 1, 6 \rangle$. The equality

$$x^6 + Ax + B = (x^2 - Px + Q)(x + a)(x^3 + bx^2 + cx + d),$$

leads to the system of equations

$$\begin{aligned} a + b - P &= 0, & ab + c - Pa - Pb + Q &= 0, \\ ac + d - Pab - Pc + Qa + Qb &= 0, & ad - Pac - Pd + Qab + Qc &= 0. \end{aligned}$$

Eliminating P, Q and d and taking $b = \beta a$, $c = \gamma a^2$ we obtain

$$\gamma^2 + \gamma(\beta^2 + 2\beta) - (\beta^4 + 2\beta^3 + 2\beta^2 + 2\beta) = 0.$$

It follows that

$$\begin{aligned} (2\gamma + \beta^2 + 2\beta)^2 &= (\beta^2 + 2\beta)^2 + 4(\beta^4 + 2\beta^3 + 2\beta^2 + 2\beta) \\ &= 5\beta^4 + 12\beta^3 + 12\beta^2 + 8\beta. \end{aligned}$$

Putting $2\beta^{-1} + 1 = v$, $2\gamma\beta^{-2} + 1 + 2\beta^{-1} = w$, $\frac{a\beta}{2} = u$ we obtain $w^2 = v^3 + 3v + 1$, where $v, w \in L$ and $P = u(v + 1)$, $Q = u^2(v^2 + 2v + 3 - 2w)$. Consider finally $\langle m_1, n_1, q \rangle = \langle 1, 5, 2 \rangle$. By Lemma 29 of [2] we have

$$\frac{x^5 + Ax + B}{x^2 - Px + Q} = xf(x)^2 - g(x)^2, \quad \text{where } f, g \in L[x]$$

and taking $f(x) = x + a$, $g(x) = bx + c$ we obtain

$$x^5 + Ax + B = (x^2 - Px + Q)(x^3 + (2a - b^2)x^2 + (a^2 - 2bc)x - c^2),$$

which leads to the system of equations

$$\begin{aligned} 2a - b^2 - P &= 0, & a^2 - 2bc - P(2a - b^2) + Q &= 0, \\ -c^2 - P(a^2 - 2bc) + Q(2a - b^2) &= 0. \end{aligned}$$

Eliminating P and Q and taking $a = \alpha b^2$, $c = \gamma b^3$ we obtain

$$\gamma^2 - 2\gamma(4\alpha - 2) - (4\alpha^3 - 10\alpha^2 + 6\alpha - 1) = 0.$$

It follows that

$$(\gamma - 4\alpha + 2)^2 = (4\alpha - 2)^2 + 4\alpha^3 - 10\alpha^2 + 6\alpha - 1 = 4\alpha^3 + 6\alpha^2 - 10\alpha + 3.$$

Putting $4\alpha + 2 = v$, $4\gamma - 16\alpha + 8 = w$, $\frac{b}{2} = u$ we obtain $w^2 = v^3 - 52v + 144$, $P = (2v - 8)u^2$, $Q = (3v^2 + 4v - 68 + 8w)u^4$.

Sufficiency. Proof of sufficiency in the cases (iv), (v) and (vi) is similar to that of Theorem 4. If there exists an integer l such that $\langle n/l, m/l \rangle = \langle \nu, \mu \rangle \in S_3$ and $P = P_{\nu, \mu}(v, w)u^{(\nu, \mu)}$, $Q = Q_{\nu, \mu}(v, w)u^{2(\nu, \mu)}$, where $\langle v, w \rangle \in E_{\nu, \mu}^2(L)$, $u \in L$, we shall consider successively the three cases.

If $\langle \nu, \mu \rangle = \langle 5, 2 \rangle$, then

$$\frac{x^n + Ax^m + B}{x^{2l} - Px^l + Q} = (x^l + uv)(x^{2l} + 4ux^l + 2u^2(w - v + 4)).$$

If $\langle \nu, \mu \rangle = \langle 6, 1 \rangle$, then

$$\begin{aligned} \frac{x^n + Ax^m + B}{x^{2l} - Px^l + Q} &= (x^l + u(v - 1)) (x^{3l} + 2ux^{2l} + 2u^2(w - v)x^l \\ &\quad + u^3((2v + 6)w - v^3 - v^2 - 9v - 5)). \end{aligned}$$

If $\langle \nu, \mu \rangle = \langle 10, 2 \rangle$, then

$$\begin{aligned} \frac{x^n + Ax^m + B}{x^{4l} - Px^{2l} + Q} &= (x^{3l} + 2ax^{2l} + u^2(v - 2)x^l + 2u^3(w + 4v - 16)) \\ &\quad \times (x^{3l} - 2ax^{2l} + u^2(v - 2)x^l - 2u^3(w + 4v - 16)). \end{aligned}$$

For $q > 1$ the sufficiency of the given condition is obvious. $\square$

Remark. The calculations performed for the cases $\langle k, m_1, n_1 \rangle = \langle 1, 2, 5 \rangle$ and $\langle 1, 1, 6 \rangle$ and $\langle m_1, n_1, q \rangle = \langle 1, 5, 2 \rangle$ are similar to those in the proof of Theorem 3.2, Theorem 4.1, and Theorem 6.1 of [1].

PROOF OF COROLLARY. The corollary follows from Theorem 2 of [2], Theorem 2 and Theorem 5 above. $\square$

PROOF OF THEOREM 6. In view of Theorem 5 the proof does not differ essentially from the proof of Theorem 3 in [3]. The finiteness of the set $F_{\nu, \mu}(K)$ is a consequence of the Faltings theorem. $\square$

References

- [1] A. BREMNER and M. ULAS, On the type of reducibility of trinomials, *Acta Arith.* (to appear).
- [2] A. SCHINZEL, On reducible trinomials, *Dissert. Math.* **329** (1993), and *Selecta* **1**, 466–548.
- [3] A. SCHINZEL, On reducible trinomials, II, *Publ. Math. Debrecen* **56** (2000), 575–608, and *Selecta* **1**, 580–604.
- [4] A. SCHINZEL, On reducible trinomials, III, *Periodica Math. Hungarica* **43** (2001), 43–69, and *Selecta* **1**, 605–631.

Corrigenda to the paper [2] (mistakes corrected in *Selecta*, vol. 1 are not included)

- p. 8 Table 2 $A_{8,1}$ (first): for $3v^2 - 12v - 10$ read $3v^2 - 10$
 Table 2 $A_{9,1}$: for $v^3 + 18v - 36$ read $v^3 - 18v + 36$

(I owe these corrections to A. Bremner).

- p. 9 line -6 for $\langle 7, 2 \rangle$ read $\langle 7, 2 \rangle, \langle 7, 3 \rangle$
 line -6 insert $E_{7,3}(Q) = \{\langle -33, 0 \rangle, \langle 3, 108 \rangle, \langle 3, -108 \rangle, \langle 39, 216 \rangle, \langle 39, -216 \rangle\}$
 p. 49 line 13 for u^3 read $u^3(v - 39)$
 p. 50 for $(v - 1)x + (w - 3v + 5)$
 read $u^2(v - 1)x + u^3(w - 3v + 5)$

(I owe these corrections to A. Jasinski).

- p. 64 line 17 insert $E_{7,3}(Q) = \{\langle -33, 0 \rangle, \langle 3, 108 \rangle, \langle 3, -108 \rangle, \langle 39, 216 \rangle, \langle 39, -216 \rangle\}$
 line -16 leave out $E_{7,3}$
 line -17 leave out $\langle 3, 108 \rangle$
 line -13 insert: All rational points on the curve $E_{7,3}$ are the indicated torsion points (see [1], Theorem 5.2 (3)).

ANDRZEJ SCHINZEL
 INSTITUTE OF MATHEMATICS
 POLISH ACADEMY OF SCIENCES
 NIADECKICH 8
 00-956 WARSAW
 POLAND

E-mail: schinzel@impan.pl

(Received November 23, 2010; revised August 30, 2011)