The least admissible value of the parameter in Hilbert’s Irreducibility Theorem

by

Andrzej Schinzel (Warszawa) and Umberto Zannier (Venezia)

Dedicated to Professor Wolfgang M. Schmidt
on the occasion of his 60th birthday

The simplest case of Hilbert’s Irreducibility Theorem asserts that if $F(t, x)$ is irreducible over $\mathbb{Q}$, then there exists $t^* \in \mathbb{Q}$ such that $F(t^*, x)$ is irreducible over $\mathbb{Q}$. Many different proofs have been given for this theorem, namely Hilbert’s (1892) [H], Mertens’s (1911) [Me], Skolem’s (1921) [Sk], Dörge’s (1927) [Do], Siegel’s (1929) [Si], Eichler’s (1939) [Ei], Inaba’s (1943) [In], Fried’s (1974) [Fr], Roquette’s (1975) [Ro], Cohen’s (1981) [Co], Sprindžuk’s (1981) [Spr], Débes’s (1986) [De1], (1993) [De2].

Only the last of the quoted papers explicitly mentions the problem of estimating the size of a $t^*$ with the above property in terms of the degree and height of $F$. By the height of $F$, to be abbreviated $H(F)$, we mean the maximum absolute value of the coefficients of a constant multiple of $F$ that has coprime integer coefficients. Débes gives actually an estimate valid for several polynomials $F_i$. His result reads (see Cor. 3.7 of [De2]):

Let $F_1, \ldots, F_h$ be irreducible polynomials in $\mathbb{Q}[t, x]$ such that $\deg F_i \leq D$ and $H(F_i) \leq H$.\(^{(1)}\) Then there exists a rational number $t^* = u/v$ such that each $F_i(t^*, x)$ is irreducible over $\mathbb{Q}$ and

$$
\max(|u|, |v|) \leq \exp(10^{10} D^{100h} D^2 \log D (\log^2 H + 1)).
$$

Débes also gives a corresponding result for algebraic number fields. We observe that Cohen’s result, formulated for algebraic number fields, is partially explicit and gives, in the case of the rational field, the following bound:

Under the same assumptions as before, for $H \geq e^e$ one may find a $t^* \in \mathbb{Z}$ with the above property such that

\(^{(1)}\) Débes in fact formulates his result in terms of the logarithmic height.
\[ |t^*| \leq h^2 \log(ch) H^c, \]

where \( c \) depends only on \( D \).

Actually, assuming the Riemann Hypothesis for zeta functions of number fields, Cohen obtained an estimate implying the sharp bound

\[ |t^*| \leq \max \{ ch^2 \log(ch), \log^4 H \}. \]

This includes a result by Fogels [Fo] concerning the special case \( h = 1, F(t, x) = f_1(x) + tf_2(x) \). Yasumoto [Ya] asked whether for \( h = 1 \) there exists a bound \( t^* \) independent of \( H \).

The aim of the present paper is to prove the following theorem, which improves on both (1) and (2), as far as the dependence on \( D \) and \( H \) is concerned.

**Theorem.** Let \( F_1, \ldots, F_h \in \mathbb{Z}[t, x] \) be irreducible over \( \mathbb{Q} \). There exists a positive integer \( t^* \) such that \( F_i(t^*, x) \) are irreducible for all \( i \leq h \) and

\[ |t^*| \leq \max \{ \exp(2(6m^{5/6})), \exp(36^6), h^9 \exp(450(\log H)^{5/6} + 11250m^5 + 45(m + 1)^2n + 45n(\log H)^2/5) \}, \]

where \( m = \max \{ \deg F_i \}, n = \max \{ \deg F_i \}, H = \max \{ 20, H(F_i) \} \).

**Auxiliary lemmas.** Our proof will make use of a sharp estimate by Bombieri and Pila [BP] of the number of integral points on algebraic plane curves. A direct application of their Theorem 5 would lead, however, to a bound weaker than the stated above. Nevertheless it is possible to modify their proof to produce a result which is more suitable for our purposes. This will be done in the course of the proof of our first lemma.

**Lemma 1.** Let \( \Phi \in \mathbb{Q}[t, y] \) be a polynomial irreducible over \( \mathbb{Q} \), of total degree \( D \). Then, for every positive integer \( \delta < D \) and for every \( N \geq 1 \), the number of integer points \( (t^*, y^*) \) such that \( \Phi(t^*, y^*) = 0 \) and \( \max \{|t^*|, |y^*|\} \leq N \) is bounded by

\[ (3D\Delta)^{\Delta+4} N^{8/(3(\delta+3))}, \]

where \( \Delta = (\delta + 1)(\delta + 2)/2 \).

**Proof.** Consider first the case when \( \Phi \) is reducible over \( \mathbb{C} \). Then \( \Phi(t^*, y^*) = 0 \) implies that \( \Psi(t^*, y^*) = 0 \) for some factor \( \Psi \) of \( \Phi \), irreducible over \( \mathbb{C} \) and with the coefficient of the leading term (in the anti-lexicographic order) equal to 1, hence also \( \Psi'(t^*, y^*) = 0 \), where \( \Psi' \) is conjugate to \( \Psi \) over \( \mathbb{Q} \), and so is another factor of \( \Phi \). Since \( \text{Res}_y(\Psi, \Psi')^2 \mid \text{disc}_y \Phi \), it follows that the number of integers \( t^* \) such that for some integer \( y^* \), \( \Psi(t^*, y^*) = \Psi'(t^*, y^*) = 0 \), does not exceed \( \frac{1}{2} \deg(\text{disc}_y \Phi) \leq D(D - 1) \). Since the same estimate applies to integers \( y^* \), the total number of integer points is \( \leq D^2(D - 1)^2 < (3D\Delta)^{\Delta+4} \).

Assume therefore that \( \Phi \) is absolutely irreducible. Let \( G(N) = G(D, N) \) be the maximum number of integer points on the graph of a \( C^\infty \) function
Given $A \geq 1$, by appealing to Lemma 6 of [BP], we can divide the domain $I$ of $g$ into at most $2D^2(\Delta - 1)^2 \leq 2D^2 \Delta^2$ subintervals $I_\nu$ such that, for each $I_\nu$ and each $l = 1, \ldots, \Delta - 1$, either (i) or (ii) holds:

(i) $|g^{(l)}(t)| \leq !A^{l/(\Delta-1)}N^{1-l}$ for all $t \in I_\nu$;
(ii) $|g^{(l)}(t)| > !A^{l/(\Delta-1)}N^{1-l}$ for all $t \in I_\nu$.

After translating the graph of $g(t)$ on each $I_\nu$ by an integer, we can assume, since $|g'(t)| \leq 1$, that $|g(t)| \leq N$ for all $t \in I_\nu$. Now, for each $I_\nu$, either (i) or (ii) holds:

(i) $|g^{(l)}(t)| \leq !A^{l/(\Delta-1)}N^{1-l}$ for all $t \in I_\nu$ and all $l = 0, \ldots, \Delta - 1$;
(ii) $|g^{(l)}(t)| \leq !A^{l/(\Delta-1)}N^{1-l}$ for all $t \in I_\nu$ and all $l < k$, and $|g^{(k)}(t)| \geq k!A^{k/(\Delta-1)}N^{1-k}$ for all $t \in I_\nu$.

In the case (i) we have

$$\|g\|_{\Delta-1} := \max_{0 \leq l \leq \Delta-1} \max_{t \in I_\nu} |g^{(l)}(t)| N^{1-l} \leq A.$$

In the case (ii) the hypotheses of Lemma 7 of [BP] hold with $A^{k/(\Delta-1)}$ in place of $A$, and hence

$$|I_\nu| \leq 2A^{-1/(\Delta-1)}N.$$

For the $I_\nu$ of the first type we apply the Main Lemma of [BP], with $d$ replaced by $\delta$, $D$ replaced by $\Delta$, $f$ replaced by $g$. We infer that integral points on $y = g(t), t \in I_\nu$, lie on the union of at most $4(A^{1/2}N)^{8/(3(\delta+3))}$ real algebraic curves of degree $\leq \delta$. Since $\delta < D$ these curves cannot contain the appropriate translation of $\Gamma(t, y) = 0$, thus we infer from Bézout’s theorem that each of them intersects the translation in question in at most $\delta D$ points.

We thus obtain the following recurrence relation for $G(N)$:

$$G(N) \leq K_1N^\alpha + K_2G(\lambda N),$$

where

$$K_1 = 8D^3\delta \Delta^2 A^{4/(3(\delta+3))}, \quad K_2 = 2D^2 \Delta^2, \quad \alpha = \frac{8}{3(\delta + 3)}, \quad \lambda = 2A^{-1/(\Delta-1)}.$$
and thus
\[ A = \left( \frac{2}{3} \right)^{D - 1} > 1. \]

Finally, we choose \( \nu \) so that \( \lambda/N \leq \lambda' < 1/N \). Then \( G(\lambda'N) \leq 1 \) and
\[ G(N) \leq 2K_1N^\alpha + 2^{-\nu}\lambda^{-\alpha}N^\alpha \leq 2(K_1 + K_2)N^\alpha. \]

Now,
\[
K_1 + K_2 = 8D^3\delta \Delta^2 A^{4/(3(\delta + 3))} + 2D^2 \Delta^2
\]
\[
= 8D^3\delta \Delta^2 2^{\theta(\Delta - 1)/(3(\delta + 3))} (4D^2 \Delta^2)^{(\Delta - 1)/2} + 2D^2 \Delta^2
\]
\[
< 10D^3\delta \Delta^2 (8D^2 \Delta^2)^{(\Delta - 1)/2},
\]
which gives
\[ G(N) < 20D^3\delta \Delta^2 (8D^2 \Delta^2)^{(\Delta - 1)/2}N^\alpha. \]

Our original curve \( \mathcal{C} : \Phi(t, y) = 0 \) has at most \( \frac{1}{2} D(D - 1) \) singular points, and at most \( 2D(D - 1) \) points of slope \( \pm 1 \). Hence \( \mathcal{C} \cap [0, N]^2 \) is made up of at most \( 3D^2 \) graphs of \( C^\infty \) functions with slope bounded by 1 with respect to one of the axes. The number of integral points is therefore at most
\[ 3D^2G(N) < 60D^5\delta \Delta^2 (8D^2 \Delta^2)^{(\Delta - 1)/2}N^\alpha < \frac{1}{2} (3D\Delta)^{\Delta + 4}N^\alpha. \]

Replacing \( N \) with \( 2N \) we obtain the lemma. \( \blacksquare \)

Let \( F(t, x) \in \mathbb{Z}[t, x] \), write \( F(t, x) = a_0(t) \prod_{i=1}^n(x - x_i) \), where \( x_i \) are elements of \( \overline{\mathbb{Q}}(t) \), and let \( D(t) \) be the discriminant of \( F \) with respect to \( x \). For a nonempty subset \( \omega \) of \( \{1, \ldots, n\} \) and for every positive integer \( j \leq \#\omega \), let \( P_{\omega, j}(t, y) \) be the minimal polynomial of \( a_0(t)\tau_j(x_i : i \in \omega) \) over \( \mathbb{Q}(t) \), where \( \tau_j \) is the \( j \)th fundamental symmetric function. We remark that, in virtue of an old theorem of Kronecker (see [Sch], Theorem 10, p. 48), \( a_0(t)\tau_j(x_i : i \in \omega) \) is in any case integral over \( \mathbb{Z}[t] \), whence \( P_{\omega, j} \) is a polynomial in \( \mathbb{Z}[t, y] \), monic in \( y \).

**Lemma 2.** For all \( t^* \in \mathbb{Z} \), if \( a_0(t^*)D(t^*) \neq 0 \) and \( F(t^*, x) \) is reducible over \( \mathbb{Q} \), then for some \( \omega \subset \{1, \ldots, n\} \) of cardinality \( k \leq n/2 \) all the polynomials \( P_{\omega, j}(t^*, y) \), \( j \leq k \), have a zero \( y_j \in \mathbb{Z} \).

**Proof.** Let \( K \) be the splitting field of \( F(t, x) \) over \( \mathbb{Q}(t) \), and let \( \Delta \) be the discriminant of \( K \) (over \( \mathbb{Q}(t) \)). If \( D(t^*) \neq 0 \), then \( t - t^* \) is not ramified in \( K \), hence \( \Delta(t^*) \neq 0 \). By a well known result (see [Ha], p. 464) there exists a generator \( \theta \) of \( K \) integral over \( \mathbb{Q}(t) \) and such that \( \text{disc}_x T(t^*) \neq 0 \), where \( T(t, x) \) is the minimal polynomial of \( \theta \) over \( \mathbb{Q}(t) \). We have accordingly
\[ x_i = \frac{L_i(t, \theta)}{M(t)} \quad (1 \leq i \leq n), \]
where $M \in \mathbb{Q}[t]$, $L_i \in \mathbb{Q}[t,u]$ and $M(t^*) \neq 0$ provided $a_0(t^*) \neq 0$. It follows that in the ring $\mathbb{Q}[t,u,x]$ we have the congruences

\begin{equation}
(3) \quad a_0(t)M(t)^n F(t, x) \equiv a_0(t) \prod_{i=1}^{n} (M(t)x - L_i(t, u)) \pmod{T(t, u)}
\end{equation}

and

\begin{equation}
(4) \quad M(t)^{j \deg_P} P_{\omega,j}(t, a_0(t)\tau_j(L_i/M : i \in \omega)) \equiv 0 \pmod{T(t, u)}
\end{equation}

for every nonempty $\omega \subset \{1, \ldots, n\}$ and every $j \leq \#\omega$.

Assume now that $a_0(t^*)D(t^*) \neq 0$ and $F(t^*, x)$ is reducible over $\mathbb{Q}$. Without loss of generality we may suppose that

\[ F(t^*, x) = a_0(t^*) \prod_{i=1}^{n} (x - x_i^*) \]

and that

\begin{equation}
(5) \quad a_0(t^*) \prod_{i=1}^{k} (x - x_i^*) \in \mathbb{Z}[x]
\end{equation}

where $1 \leq k \leq n/2$.

Choose $u^* \in \mathbb{C}$ such that $T(t^*, u^*) = 0$. By (3),

\[ a_0(t^*) \prod_{i=1}^{n} (x - x_i^*) = a_0(t^*) \prod_{i=1}^{n} \left( x - \frac{L_i(t^*, u^*)}{M(t^*)} \right) \]

hence there exists a subset $\omega$ of $\{1, \ldots, n\}$ of cardinality $k$ such that

\[ \{x_1^*, \ldots, x_k^*\} = \left\{ \frac{L_i(t^*, u^*)}{M(t^*)} : i \in \omega \right\} \]

By (4), for every $j \leq k$,

\[ P_{\omega,j}(t^*, a_0(t^*)\tau_j(x_1^*, \ldots, x_k^*)) = 0 \]

and since $y_j := a_0(t^*)\tau_j(x_1^*, \ldots, x_k^*) \in \mathbb{Z}$ by (5), the assertion follows. $\blacksquare$

Let $F$ have degree $m$ in $t$ and $n$ in $x$. We have

**Lemma 3.** The polynomials $P_{\omega,j}(t,y)$ defined before the statement of Lemma 2 have, for $k \leq n/2$, the property that, if $|t^*| \geq 1$, $a_0(t^*)D(t^*) \neq 0$ and $P_{\omega,j}(t^*, y^*) = 0$, then

\begin{equation}
(6) \quad |y^*| \leq 2^k \sqrt{n+1}(m+1)H|t^*|^m,
\end{equation}

where $H$ is the height of $F$. Moreover, $\deg(P_{\omega,j}) \leq m \deg_y(P_{\omega,j}) \leq m \binom{n}{k}$. 
Proof. We retain the notation of the proof of Lemma 2. First observe that the polynomial
\[ \prod_{\omega = k} (y - a_0(t)\tau_j(x_i : i \in \omega)), \]
the product being extended over all subsets \( \omega \) of \( \{1, \ldots, n\} \) having cardinality \( k \), lies clearly in \( \mathbb{Q}[t, y] \), and has degree \( \binom{n}{k} \) in \( y \). Hence, since \( P_{\omega,j} \) divides this polynomial, we have \( \deg_y P_{\omega,j} \leq \binom{n}{k} \).

For the same reason we may write
\[ P_{\omega,j}(t, y) = \prod_{I \in \Omega} \left( y - a_0(t)\tau_j\left( \frac{L_i(t, \theta)}{M(t)} : i \in I \right) \right) \]
the product being extended over a certain family \( \Omega \) of subsets \( I \) of \( \{1, \ldots, n\} \) with \( \#I = k \). Let
\[ Q_{\omega,j}(t, u, y) = \prod_{I \in \Omega} \left( y - a_0(t)\tau_j\left( \frac{L_i(t, u)}{M(t)} : i \in I \right) \right). \]
Then, as in the proof of Lemma 2, we have the congruence
\[ M(t)^j \deg P(Q_{\omega,j}(t, u, y) - P_{\omega,j}(t, y)) \equiv 0 \pmod{T(t, u)} \]
whence, setting \( t = t^*, u = u^* \), where \( T(t^*, u^*) = 0 \), we get
\[ P_{\omega,j}(t^*, y) = Q_{\omega,j}(t^*, u^*, y). \]
Hence all the zeros of \( P_{\omega,j}(t^*, y) \) are of the form \( a_0(t^*)\tau_j\left( \frac{L_i(t^*, u^*)}{M(t^*)} : i \in I \right) \), namely of the form \( a_0(t^*)\tau_j^* \), where \( \tau_j^* \) is the \( j \)th symmetric function of a certain subset of cardinality \( k \) of the set \( \{x_1^*, \ldots, x_n^*\} \) of all zeros of \( F(t^*, x) \).

By a classical theorem of Landau [La], for each \( t^* \in \mathbb{C} \),
\[ M := |a_0(t^*)| \prod_{i=1}^{n} \max\{1, |x_i^*|\} \leq \sqrt{\sum_{i=0}^{n} |a_i(t^*)|^2}, \]
where \( a_i(t) \) are the coefficients of \( F(t, x) \) viewed as polynomial in \( x \).

For \(|t^*| \geq 1\) we have
\[ |a_i(t^*)| \leq (m + 1)H|t^*|^m, \]
hence, by the above observations,
\[ |y^*| \leq \binom{k}{j} \sqrt{n + 1}(m + 1)H|t^*|^m \leq 2^k \sqrt{n + 1}(m + 1)Ht^m \]
and the first part of the lemma follows.

In order to prove the second part, write
\[ P_{\omega,j}(t, y) = y^p + \sum_{i=1}^{p} P_i(t)y^{p-i}. \]
For every fixed \( t^* \in \mathbb{C} \), \( P_i(t^*) \) is, up to a sign, the \( i \)th fundamental symmetric function in the zeros of \( P_{\omega,j}(t^*, y) \). Hence, if \( |t^*| \geq 1 \), by (6) we have
\[
|P_i(t^*)| \leq \left( \frac{p}{i} \right) 2^{ki(n+1)i/2}(m+1)^i H^i |t^*|^{mi} = O(|t^*|^{mi}),
\]
which implies that \( \deg(P_i) \leq mi \), so
\[
\deg(P_{\omega,j}) = \max_{0 \leq i \leq p} \{ p - i + \deg(P_i) \} \leq mp.
\]

This completes the proof. ■

**Lemma 4.** Let \( F(t, x) \in \mathbb{Z}[t, x] \) be a polynomial irreducible over \( \mathbb{Q} \), of degree \( m \) in \( t \) and \( n \geq 2 \) in \( x \), and let \( H \geq \max\{20, H(F)\} \). If \( T \geq \max\{\exp(2(6m)^6), \exp(36^6)\} \), then the number of positive integers \( t^* \leq T \) such that \( F(t^*, x) \) is reducible over \( \mathbb{Q} \) does not exceed
\[
T^{8/9} \exp(50 \log H)^{5/6} + 1250m^4 \log(m+1) + 5(m+1)^2n + 5n(\log H)^{2/5}.
\]

**Proof.** Retaining the notation used in Lemma 2, we let \( S(T) \) be the number of positive integers \( t^* \leq T \) such that \( a_0(t^*)D(t^*) \neq 0 \) and \( F(t^*, x) \) is reducible over \( \mathbb{Q} \).

Let \( \omega \) be a nonempty subset of \( \{1, \ldots, n\} \), of cardinality \( k \leq n/2 \). We contend that at least one of the polynomials \( P_{\omega,j}(t, y) \), \( j \leq k \), has degree \( \geq 2 \) in \( y \). If not then, by definition of the \( P_{\omega,j} \)'s, all the symmetric functions \( \tau_j(x_i : i \in \omega) \) would lie in \( \mathbb{Q}(t) \), whence \( F(t, x) \) would have a factor in \( \mathbb{Q}(t)[x] \) of positive degree \( k < n \), contrary to the assumptions. Pick for each \( \omega \) one such polynomial and denote it by \( P_{\omega}(t, y) \). Then \( P_{\omega} \) is a polynomial with rational integral coefficients, irreducible over \( \mathbb{Q} \), monic and of degree \( \geq 2 \) in \( y \). Moreover, if \( t^* \) is such that \( a_0(t^*)D(t^*) \neq 0 \) and \( F(t^*, x) \) is reducible over \( \mathbb{Q} \), then, by Lemma 2, some polynomial \( P_{\omega}(t^*, y) \) has an integral zero. So
\[
(7) \quad S(T) \leq \sum_{|\omega| \leq n/2} S_{\omega}(T),
\]
where \( S_{\omega}(T) \) is the number of positive integers \( t^* \leq T \) such that \( P_{\omega}(t^*, y) \) has an integral zero and \( a_0(t^*)D(t^*) \neq 0 \).

Letting \( d_{\omega} = \deg_y P_{\omega}, D_{\omega} = \deg P_{\omega} \), we have, by Lemma 3,
\[
(8) \quad 2 \leq d_{\omega} \leq \left( \frac{n}{k} \right), \quad D_{\omega} \leq md_{\omega}.
\]

To estimate \( S_{\omega}(T) \) we shall use Lemma 1 and distinguish three cases, putting, for simplicity of notation, \( L_1 = \log H \), \( L_2 = \log\log H \).

**Case 1:** \( d_{\omega} \geq 3 \) and \( D_{\omega} \geq \lceil \max\{3m, (L_1/L_2)^{1/5}\} \rceil + 1 \). In this case, if \( P_{\omega}(t^*, y^*) = 0 \), where \( |t^*| \leq T \), then, by (6), \( \max\{|t^*|, |y^*|\} \leq 2^{n/2}\sqrt{n+1} \times (m+1)HT^m \leq 2^n (m+1)HT^m \), so we may apply Lemma 1 with
\[
N = 2^n (m+1)HT^m, \quad \delta = \lceil \max\{3m, (L_1/L_2)^{1/5}\} \rceil
\]
and obtain
\[
S_\omega(T) < (2^n(m+1)T^n)^{1/n} \frac{8}{3} (L_1^{4/5})(L_2^{1/5})(3D_\omega \Delta)^{4+4} \\
\leq T^{8/9} \exp \left( \frac{8}{3}(L_1)^{4/5}(L_2)^{1/5} + \frac{8n \log 2}{3(3m+3)} \right) \\
+ \frac{8 \log(m+1)}{9(m+1)} + (\Delta + 4) \log(3D_\omega \Delta).
\]

To estimate the expression
\[
E = \frac{8 \log(m+1)}{9(m+1)} + (\Delta + 4) \log(3D_\omega \Delta) \leq \frac{8}{9} + (\Delta + 4) \log(3D_\omega \Delta)
\]
we distinguish two cases, according as $3m \geq (L_1/L_2)^{2/5}$ or not. In the first case a calculation shows that $E \leq 26(m+1)^2 \log(m+1) + 4(m+1)^2n$. In the other case we use the crude bound $\Delta + 5 \leq 2(L_1/L_2)^2/5$ and obtain
\[
E \leq L_1^{2/5}L_2^{3/5} + 4n(L_1/L_2)^{2/5}.
\]

Adding the bounds obtained we finally have
\[
S_\omega(T) < T^{8/9} \exp(4L_1^{4/5}L_2^{1/5} + 5n(L_1/L_2)^{2/5}) \\
\times \exp(26(m+1)^2 \log(m+1) + 4(m+1)^2n).
\]

**Case 2:** $3 \leq d_\omega < D_\omega < [\max\{3m, (L_1/L_2)^{1/5}\}] + 1$. In this case we take
\[
E = [\max\{3m, (L_1/L_2)^{1/5}\}] + 2
\]
and apply Lemma 1 to the polynomial $P_\omega(t, t^E + y)$. Now, for every zero $(t^*, y^*)$ with $|t^*| \leq T$ we have, again by (6), $|y^*| \leq T^E + 2^n(m+1)HT^m < (m+1)^2HT^E$, so we may take $N = (m+1)^2HT^E$ and $\delta = d_\omega E - 1$ (note that the polynomial $P_\omega(t, t^E + y)$ is of exact degree $d_\omega E$).

We readily see that $\Delta + 4 \leq E^4/2$. Distinguishing again whether $3m > (L_1/L_2)^{2/5}$ or not, and adding the bounds obtained for $\log((3D_\omega \Delta)^{4+4})$ in these cases, we obtain
\[
S_\omega(T) < T^{8/9} \exp \left( \frac{25(L_1)^{4/5}(L_2)^{1/5} + 1250m^4 \log(m+1)}{9(m+1)} + \frac{8n \log 2}{9(m+1)} \right).
\]

**Case 3:** $d_\omega = 2$. In this case, by Lemma 3, $D_\omega \leq 2m$. We take $E = [\max\{3m, \frac{1}{2}L_1^{1/6}\}]$ and apply Theorem 5 of [BP] to the polynomial $P_\omega(t, t^E + y)$, assumed irreducible over $\mathbb{C}$ (if it is reducible over $\mathbb{C}$ the opening argument in the proof of Lemma 1 applies). As in Case 2 we may take $N = (m+1)^2HT^E > T^E + (m+1)^2HT^m$ (note that the degree of $P_\omega(t, t^E + y)$ is $2E$).

Observe that the condition $N > \exp(2^6E^6)$ (an assumption of the theorem in question) is equivalent to
\[(m + 1)2^n HT^E > \exp(\max\{(6m)^6, \log H\})\]

and is satisfied provided \(T \geq \exp(2(6m)^5)\), as we are assuming.

The mentioned theorem gives

\[S_\omega(T) < N^{1/(2E)} \exp(12\sqrt{2E \log N \log \log N}).\]

Now \(2E \leq (\log N)^{1/6}\), and \(\log \log N \leq (\log N)^{1/6}\), since \(\log N \geq \log T > 36^6\) by assumption. Hence

\[S_\omega(T) < \exp\left(\frac{\log N}{2E} \left(1 + 12(2E)^{3/2} \sqrt{\log \log N}\right)\right)\]
\[\leq \exp\left(\frac{\log N}{2E} \left(1 + 12\left(\frac{1}{\log N}\right)^{1/6}\right)\right)\]
\[\leq \exp\left(\frac{2 \log N}{3E}\right) \leq T^{2/3} \exp\left(2L_1^{5/6} + \frac{2n \log 2}{9m}\right)\]

Observe now that since \(H > 20\) we have

\[L_1^{4/5} L_2^{1/5} < 2L_1^{5/6}\]

Using this inequality in the first two cases, comparing the three estimates and summing over \(\omega\), an operation which at most multiplies the bound by \(2^n\), we obtain

\[S(T) \leq T^{8/9} \exp(50L_1^{5/6} + 250m^4 \log(m + 1) + 4(m + 1)^2 n + 5nL_1^{2/5}).\]

We have still to take into account the solutions of \(a_0(t^*)D(t^*) = 0\), but these are at most \(2m(n + 1) < \exp((m + 1)^2 n)\) in number. This concludes the proof.

**Proof of Theorem.** Let \(m, n, H\) be as in the statement of the Theorem, and let \(T\) satisfy the lower bound in the statement of Lemma 4. Then the total number \(R\) of positive integers \(t^* \leq T\) such that at least one of the polynomials \(F_i(t^*, x)\) is reducible over \(\mathbb{Q}\) satisfies

\[R \leq hT^{8/9} \exp(50(\log H)^{5/6} + 250m^4 \log(m + 1) + 5(m + 1)^2 n + 5n(\log H)^{2/5}).\]

To find a suitable value of \(t^* \leq T\) it thus suffices that this quantity is less than \(T\), which holds if

\[T > h^9 \exp(450(\log H)^{5/6} + 2250m^5 + 45(m + 1)^2 n + 45n(\log H)^{2/5}).\]

Combining this with the lower bound necessary for an application of Lemma 4, we obtain the Theorem.

**Remark.** It is obviously possible by changing the splitting into cases to obtain a corresponding theorem, with different numerical values for the coefficients appearing in the final estimate.
References


INSTITUTE OF MATHEMATICS
POLISH ACADEMY OF SCIENCES
S. CROCE, 191
ŚNIADĘCKICH 8, P.O. BOX 137
00-950 WARSZAWA, POLAND
E-mail: SCHINZEL@PLEARN.BITNET

Received on 15.9.1994