ACTA ARITHMETICA
XCVIII.1 (2001)

On the greatest common divisor of two univariate polynomials, II

by

A. SCHINZEL (Warszawa)

To Andrzej Rotkiewicz on his 70th birthday

The first paper of this series [4] has concerned the supremum $A(r,s,K)$ of the number of non-zero coefficients of (f,g), where f,g run through all univariate polynomials over a field K with exactly r and s non-zero coefficients, respectively. The only case where $A(r,s,K)$ has remained to be evaluated is $r=s=3$, $p=\operatorname{char} K=0$. This case is studied in the present paper. Let us denote by ζ_q a primitive complex root of unity of order q, set

$$P_{n,m}(z)=(1-z^m)^{m/(n,m)}(z^m-z^n)^{(n-m)/(n,m)}(z^n-1)^{-n/(n,m)}$$

and for a trinomial

$$T(x)=x^n+ax^m+b\in\mathbb{C}[x],\qquad \text{where } n>m>0,\ ab\neq 0,$$

put

$$\operatorname{inv} T=a^{-n/(n,m)}b^{(n-m)/(n,m)}.$$

We shall prove the following results:

THEOREM 1. *Let $T_i=x^{n_i}+a_ix^{m_i}+b_i\in\mathbb{C}[x]$, $a_ib_i\neq 0$, $n_i>m_i>0$, and $d_i=(n_i,m_i)$ $(i=1,2)$. If $(d_1,d_2)=1$, then*

$$\deg(T_1,T_2) \tag{1}$$
$$\le\begin{cases} n_2/d_2 & \text{if } \operatorname{inv}T_1\neq P_{n_1,m_1}(\zeta_{d_2}^r) \text{ for all } r,\\ n_2/d_2+\min\{2,d_1\} & \text{if } n_1/d_1\neq 4 \text{ or } d_2\not\equiv 0 \bmod 10,\\ n_2/d_2+\min\{3,n_2/d_2\} & \text{always.}\end{cases}$$

THEOREM 2. *For every quadruple $\langle n_1,m_1,n_2,m_2\rangle\in\mathbb{N}^4$, where $n_1>m_1$, $n_2>m_2$, $\langle n_1,m_1\rangle\neq\langle n_2,m_2\rangle$ and $(n_1,m_1,n_2,m_2)=1$ there exists an effectively computable finite subset S of $\overline{\mathbb{Q}}^4$ with the following property. If*

2000 *Mathematics Subject Classification*: 12D05, 12E10.

$T_i = x^{n_i} + a_i x^{m_i} + b_i \in \mathbb{C}[x]$, $a_i b_i \neq 0$ $(i = 1, 2)$, *and* $\deg(T_1, T_2) > 2$, *then*

$$(2) \qquad T_i = u^{n_i} T_i^*\left(\frac{x}{u}\right), \qquad \text{where } u \in \mathbb{C}^*,\ T_i^* = x^{n_i} + a_i^* x^{m_i} + b_i^*$$

and $\langle a_1^*, b_1^*, a_2^*, b_2^* \rangle \in S$.

Corollary 1. *If* $\operatorname{inv} T_i \notin \overline{\mathbb{Q}}$ *for at least one* $i \leq 2$, *or*

$$T_1(0)^{-\deg T_2} T_2(0)^{\deg T_1} \notin \overline{\mathbb{Q}}$$

then (T_1, T_2) *has at most three non-zero coefficients.*

Corollary 2. *We have*

$$\sup_{K \subset \mathbb{C}} A(3, 3, K) = A(3, 3, \overline{\mathbb{Q}}) = \sup_{[K:\mathbb{Q}] < \infty} A(3, 3, K).$$

Theorem 3. *For every finite extension* K *of* $\mathbb{Q}$ *and every pair* $\langle n, m \rangle \in \mathbb{N}^2$, *where* $n > m$, *there exists a finite set* $E_{n,m}(K)$ *such that if* $T_i = x^{n_i} + a_i x^{m_i} + b_i \in K[x]$,

$$(3) \qquad \operatorname{inv} T_i \notin E_{n_i, m_i}(K) \quad (i = 1, 2)$$

and $(n_1, m_1, n_2, m_2) = 1$ *then either* $T_1 = T_2$, *or* $\deg(T_1, T_2) \leq 9$.

Corollary 3. *If* (3) *holds, then* (T_1, T_2) *has at most* 10 *non-zero coefficients.*

At the end of the paper we give three examples of some interest.

R. Dvornicich has kindly looked through the paper and corrected several mistakes. The proofs of Theorems 1 and 3 use a recent result of his [2] on the so-called cyclotomic numbers, which we formulate below as

Lemma 1. *Let* z_1, z_2 *be two complex roots of unity and let* Q *be the least common multiple of their orders. If* m, n *are integers such that* $(m, n, Q) = 1$ *and*

$$(4) \qquad |z_1^m - 1|^m |z_1^{n-m} - 1|^{n-m} |z_1^n - 1|^{-n} = |z_2^m - 1|^m |z_2^{n-m} - 1|^{n-m} |z_2^n - 1|^{-n},$$

where none of the six absolute values is 0, *then either* $z_1 = z_2^{\pm 1}$, *or* $Q = 10$, $\{m, n - m, -n\} = \{x, 3x, -4x\}$ *with* $(x, 10) = 1$ *and* z_1, z_2 *are two primitive tenth roots of unity.*

Proof. See [2], Theorem 1.

Remark 1. Lemma 1 can be extended to fields of arbitrary characteristic as follows. Let K be a field of characteristic p, $p = 0$ or a prime, let z_i $(i = 1, 2)$ be roots of unity in $\overline{K}$, $z_i^Q = 1$ and let m, n be positive integers such that $m < n$, $(m, n, Q) = 1$ and

$$1 \neq z_i^m \neq z_i^n \neq 1, \qquad P_{n,m}(z_1) = P_{n,m}(z_2).$$

If either $p = 0$ or $p > 2^{(2n/(n,m)+1)\varphi(Q)}$, then either $z_2 = z_1 = z_1^{\pm 1}$, or $n/(n,m) = 4$ and z_1, z_2 are primitive tenth roots of unity.

LEMMA 2. *If* $(n,m,q) = 1$ *and*

$$1 \neq \zeta_q^m \neq \zeta_q^n \neq 1, \qquad q \neq 10,$$

then $P_{n,m}(\zeta_q)$ *is an algebraic number of degree* $\frac{1}{2}\varphi(q)$.

Proof. We have $P_{n,m}(\zeta_q^{-1}) = P_{n,m}(\zeta_q)$. On the other hand, if $q > 2$, $0 < r < s < q/2$, $(r,s,q) = 1$ we have by Lemma 1,

$$|P_{n,m}(\zeta_q^r)| \neq |P_{n,m}(\zeta_q^s)|,$$

hence $P_{n,m}(\zeta_q)$ has $\frac{1}{2}\varphi(q)$ distinct conjugates.

LEMMA 3. *Let* n, m, q *be positive integers with* $(n,m,q) = 1$, $n > m$ *and* $T = x^n + ax^m + b \in \mathbb{C}[x]$, $ab \neq 0$. *Set*

$$C(T,q) = \{c^{(m,n)} : c \in \mathbb{C},\ \deg(T, x^q - c) \geq 2\}.$$

We have

$$\operatorname{card} C(T,q) \leq 1 \tag{5}$$

unless $n/(n,m) = 4$ *and* $q \equiv 0 \bmod 10$, *in which case*

$$\operatorname{card} C(T,q) \leq 2. \tag{6}$$

Moreover, *if* $C(T,q) \neq \emptyset$, *then* T *is separable and*

$$\operatorname{inv} T = P_{n,m}(\zeta_q^r) \quad \textit{for an } r \textit{ satisfying } 1 \neq \zeta_q^{rm} \neq \zeta_q^{rn} \neq 1. \tag{7}$$

Proof. By Theorem 1 of [4] we have $\deg(T, x^q - c) \leq 2$. Assume that $\deg(T, x^q - c) = 2$. Since the binomial $x^q - c$ is separable we have

$$(T, x^q - c) = (x - \xi_1)(x - \xi_2),$$

where $\xi_i^q = c$ $(i = 1,2)$, $\xi_2 = \xi_1\zeta_q^r$, $\zeta_q^r \neq 1$.

By the formulae (13) and (14) of [4] we have

$$a^q = c^{n-m}\left(\frac{\zeta_q^{rn} - 1}{1 - \zeta_q^{rm}}\right)^q, \qquad b^q = c^n\left(\frac{\zeta_q^{rm} - \zeta_q^{rn}}{1 - \zeta_q^{rm}}\right)^q, \tag{8}$$

where $1 \neq \zeta_q^{rm} \neq \zeta_q^{rn} \neq 1$ and

$$\operatorname{inv} T = P_{n,m}(\zeta_q^r),$$

which proves (7). Also, if for another value c' we have

$$(T, x^q - c') = (x - \xi_1')(x - \xi_2')$$

where $\xi_i'^q = c'$ $(i = 1,2)$, $\xi_2' = \xi_1'\zeta_q^{r'}$, it follows that

$$\operatorname{inv} T = P_{n,m}(\zeta_q^{r'}), \quad \text{hence} \quad P_{n,m}(\zeta_q^r) = P_{n,m}(\zeta_q^{r'}).$$

Applying Lemma 1 with $z_1 = \zeta_q^r$, $z_2 = \zeta_q^{r'}$ we infer that either $r' = \pm r$ or $n_1/d_1 = 4$ and $q \equiv 0 \bmod 10$, $r' \equiv \pm 3r \bmod q$. In the former case, by (8),

$$c'^{n-m} = c^{n-m}, \qquad c'^{n} = c^{n},$$

hence $c'^{(n,m)} = c^{(n,m)}$, which proves (5). In the latter case for any value c'' with $\deg(T, x^q - c'') \geq 2$ we have $c''^{(n,m)} = c^{(n,m)}$ or $c'^{(n,m)}$, which proves (6).

It remains to prove that if $c(T, q) \neq \emptyset$, then T is separable. Now, by formula (11) of [4],

$$\operatorname{disc}_x T = (-1)^{n(n-1)/2} a^n b^{m-1} (n^{n'} \operatorname{inv} T + (-1)^{n'-1} (n-m)^{n'-m'} m^{m'})^{(n,m)},$$

where $n' = n/(n,m)$, $m' = m/(n,m)$.

Thus, if T has double zeros we have

$$\operatorname{inv} T = (-1)^{n'} m'^{m'} (n' - m')^{n'-m'} n'^{-n'}.$$

Hence, by (7),

$$(9)\qquad (-1)^{n'} m'^{m'} (n' - m')^{n'-m'} n'^{-n'} = (1 - \zeta_q^{rm})^{m'} (\zeta_q^{rm} - \zeta_q^{rn})^{n'-m'} (\zeta_q^{rn} - 1)^{-n'}.$$

Now, since $(n', m'(n' - m')) = 1$ it follows that in the ring of integers of $\mathbb{Q}(\zeta_q)$ we have

$$n'^{n'} \mid (\zeta_q^{rn} - 1)^{n'}, \qquad n' \mid \zeta_q^{rn} - 1.$$

On taking norms from $\mathbb{Q}(\zeta_q^{rn})$ to $\mathbb{Q}$ we infer that $n' = 2$, $\zeta_q^{rn} = -1$, hence $m' = 1$, $\zeta_q^{rm} = \pm\zeta_4$ and (9) gives $1/4 = 1/2$. The contradiction obtained shows our contention.

Proof of Theorem 1. Let

$$T_2(x^{1/d_2}) = \prod_{c \in \mathbb{C}} (x - c)^{e(c)}, \qquad \sum_{c \in \mathbb{C}} e(c) = n_2/d_2.$$

We have

$$(10)\qquad \deg(T_1, T_2) \leq \sum_{c \in \mathbb{C}} \deg(T_1, (x^{d_2} - c)^{e(c)}) \leq \sum_{c \in \mathbb{C}} e(c) \deg(T_1, x^{d_2} - c).$$

If $\deg(T_1, x^{d_2} - c) \leq 1$ for all $c \in \mathbb{C}$ with $e(c) \geq 1$ the inequalities (1) follow.

If for at least one c, say c_1, we have $e(c_1) \geq 1$ and $\deg(T_1, x^{d_2} - c_1) \geq 2$ then, by Lemma 3, T_1 is separable and $\operatorname{inv} T_1 = P_{n_1,m_1}(\zeta_{d_2}^r)$ for an r satisfying

$$1 \neq \zeta_{d_2}^{rm_1} \neq \zeta_{d_2}^{rn_1} \neq 1.$$

This shows the first inequality of (1). Moreover, by (10),

$$\begin{aligned}(11)\qquad \deg(T_1,T_2) &\le \sum_{c\in\mathbb{C}} \min\{e(c),1\}\deg(T_1,x^{d_2}-c)\\ &\le \sum_{c\in\mathbb{C}} e(c) + \sum_{e(c)\ge 1} (\deg(T_1,x^{d_2}-c)-1)\\ &\le \frac{n_2}{d_2} + \sum_{\substack{e(c)\ge 1\\ \deg(T_1,x^{d_2}-c)=2}} 1.\end{aligned}$$

If $n_1/d_1 \ne 4$ or $d_2 \not\equiv 0 \bmod 10$, then by Lemma 3, $\deg(T_1, x^{d_2}-c) = 2$ implies $c^{d_1} = c_1^{d_1}$, hence by Theorem 1 of [4],

$$\sum_{\substack{e(c)\ge 1\\ \deg(T_1,x^{d_2}-c_1)=2}} 1 \le \deg(T_2(x^{1/d_2}), x^{d_1}-c_1^{d_1}) \le \min\{2,d_1\},$$

which together with (11) proves the second inequality of (1) and *a fortiori*, the third.

If $n_1/d_1 = 4$ and $d_2 \equiv 0 \bmod 10$, then by Lemma 3 there exists a c_2, possibly equal to c_1, such that $\deg(T_1, x^d - c) = 2$ implies $c^{d_1} = c_i^{d_i}$ for an $i \le 2$. If $c_2^{d_1} = c_1^{d_1}$ we are in the previous case, otherwise

$$(12)\qquad \sum_{\substack{e(c)\ge 1\\ \deg(T_1,x^{d_2}-c)=2}} 1 \le \sum_{i=1}^{2} \deg(T_2(x^{1/d_2}), x^{d_1}-c_i^{d_1}).$$

However, since $d_2 \equiv 0 \bmod 10$ we have $d_1 \not\equiv 0 \bmod 10$, hence, by Lemma 3, $C(T_2(x^{1/d_2}), d_1) \le 1$ and the right hand side of (12) does not exceed 3. Since it also does not exceed $\deg T_2(x^{1/d_2}) = n_2/d_2$ the third of the inequalities (1) follows.

LEMMA 4. *Let $n > m > 0$, $d = (n,m)$, $F = (1-t^m)x^n + (t^n-1)x^m + t^m - t^n$. All zeros of F in $\mathbb{C}((t))$ are given by the Puiseux expansions*

$$\begin{aligned}&\zeta_d^\delta,\ \zeta_d^\delta t: \quad 0\le\delta<d;\\ &\zeta_m^\mu t + \frac{\zeta_m^{\mu n}-1}{m}\zeta_m^\mu t^{n-m+1} + \ldots : \quad 0\le\mu<m,\ \mu\not\equiv 0 \bmod \frac{m}{d};\\ &\zeta_{n-m}^\nu + \frac{\zeta_{n-m}^{\nu n}-1}{n-m}\zeta_{n-m}^\nu t^m + \ldots : \quad 0\le\nu<n-m,\ \nu\not\equiv 0 \bmod \frac{n-m}{d}.\end{aligned}$$

Proof. One applies the usual procedure (Newton polygons) for finding Puiseux expansions.

LEMMA 5. *Let $n_i > m_i > 0$, $d_i = (n_i,m_i)$, and $F_i = (1-t^{m_i})x^{n_i} + (t^{n_i}-1)x^{m_i} + t^{m_i} - t^{n_i}$ $(i = 1,2)$. If $(d_1,d_2) = 1$ then either $F_1 = F_2$, or*

$$(F_1,F_2) = (t-1)(x-1)(x-t).$$

Proof. The content $C(F_i)$ of F_i viewed as a polynomial in x is $t^{d_i}-1$, hence $(C(F_1), C(F_2)) = t-1$. On the other hand, by Lemma 4, F_1 and F_2 have two common zeros in $\mathbb{C}((t))$, namely 1 and t, each with multiplicity 1; if there are any other common zeros we have either

$$\zeta_{m_1}^{\mu_1} t + \frac{\zeta_{m_1}^{\mu_1 n_1}-1}{m_1}\zeta_{m_1}^{\mu_1} t^{n_1-m_1+1} = \zeta_{m_2}^{\mu_2} t + \frac{\zeta_{m_2}^{\mu_2 n_2}-1}{m_2}\zeta_{m_2}^{\mu_2} t^{n_2-m_2+1}, \tag{13}$$

where $\mu_i \not\equiv 0 \bmod \frac{m_i}{d_i}$ $(i=1,2)$, or

$$\zeta_{n_1-m_1}^{\nu_1} + \frac{\zeta_{n_1-m_1}^{\nu_1 n_1}-1}{n_1-m_1}\zeta_{n_1-m_1}^{\nu_1} t^{m_1} = \zeta_{n_2-m_2}^{\nu_2} + \frac{\zeta_{n_2-m_2}^{\nu_2 n_2}-1}{n_2-m_2}\zeta_{n_2-m_2}^{\nu_2} t^{m_2}, \tag{14}$$

where $\nu_i \not\equiv 0 \bmod \frac{n_i-m_i}{d_i}$ $(i=1,2)$.

If (13) holds, we have

$$\begin{gathered} \zeta_{m_1}^{\mu_1} = \zeta_{m_2}^{\mu_2}, \qquad n_1-m_1+1 = n_2-m_2+1, \\ \frac{\zeta_{m_1}^{\mu_1 n_1}-1}{m_1} = \frac{\zeta_{m_2}^{\mu_2 n_2}-1}{m_2}. \end{gathered} \tag{15}$$

Dividing the last equality by its complex conjugate we obtain

$$-\zeta_{m_1}^{\mu_1 n_1} = -\zeta_{m_2}^{\mu_2 n_2} \neq -1,$$

hence $m_1 = m_2$, which together with (15) gives $F_1 = F_2$.

If (14) holds, we have

$$\begin{gathered} \zeta_{n_1-m_1}^{\nu_1} = \zeta_{n_2-m_2}^{\nu_2}, \qquad m_1 = m_2, \\ \frac{\zeta_{n_1-m_1}^{\nu_1 n_1}-1}{n_1-m_1} = \frac{\zeta_{n_2-m_2}^{\nu_2 n_2}-1}{n_2-m_2}. \end{gathered} \tag{16}$$

Dividing the last equality by its complex conjugate we obtain

$$-\zeta_{n_1-m_1}^{\nu_1 n_1} = -\zeta_{n_2-m_2}^{\nu_2 n_2} \neq -1,$$

hence $n_1-m_1 = n_2-m_2$, which together with (16) gives $F_1 = F_2$.

Proof of Theorem 2. Let $n_i > m_i > 0$, $(n_i, m_i) = d_i$ $(i=1,2)$, $(d_1,d_2) = 1$ and $\langle n_1, m_1\rangle \neq \langle n_2, m_2\rangle$. In the notation of Lemma 5 and by virtue of that lemma the polynomials $F_i/(t-1)(x-1)(x-t)$ $(i=1,2)$ are coprime, hence their resultant R with respect to x is non-zero. We set

$$\begin{aligned} S = {}& \left\{\left\langle \frac{-n_1}{m_1}, \frac{n_1-m_1}{m_1}, \frac{-n_2}{m_2}, \frac{n_2-m_2}{m_2}\right\rangle\right\} \\ & \cup \left\{\left\langle \frac{\zeta_{d_2}^{r_2 n_1}-1}{1-\zeta_{d_2}^{r_2 m_1}}, \frac{\zeta_{d_2}^{r_2 m_1}-\zeta_{d_2}^{r_2 n_1}}{1-\zeta_{d_2}^{r_2 m_1}}, \frac{\zeta_{d_1}^{r_1 n_2}-1}{1-\zeta_{d_1}^{r_1 m_2}}, \frac{\zeta_{d_1}^{r_1 m_2}-\zeta_{d_1}^{r_1 n_2}}{1-\zeta_{d_1}^{r_1 m_2}}\right\rangle : \right. \\ & \qquad\qquad\qquad\qquad \left. r_2 m_1 \not\equiv 0 \bmod d_2,\ r_1 m_2 \not\equiv 0 \bmod d_1 \right\} \end{aligned}$$

$$\cup \left\{ \left\langle \frac{t^{n_1}-1}{1-t^{m_1}}, \frac{t^{m_1}-t^{n_1}}{1-t^{m_1}}, \frac{t^{n_2}-1}{1-t^{m_2}}, \frac{t^{m_2}-t^{n_2}}{1-t^{m_2}} \right\rangle : R(t)=0,\ t^{m_1} \neq 1 \neq t^{m_2} \right\}.$$

We proceed to show that the set S has the property asserted in the theorem. Since $R \in \mathbb{Q}[t]$ we have $S \subset \overline{\mathbb{Q}}^4$. Assume that $\deg(T_1, T_2) \geq 3$. If (T_1, T_2) has a double zero ξ_0 we set

$$T_i^*(x) = \xi_0^{-n_i} T_i(\xi_0 x) \qquad (i = 1, 2)$$

and from the equations $T_i^*(1) = 0 = \frac{dT_i^*}{dx}(1)$ $(i = 1, 2)$ we find that

$$a_i^* = -\frac{n_i}{m_i}, \qquad b_i^* = \frac{n_i - m_i}{m_i} \qquad (i = 1, 2),$$

hence $\langle a_1^*, b_1^*, a_2^*, b_2^* \rangle \in S$ and (2) holds with $u = \xi_0$.

If (T_1, T_2) has three distinct zeros ξ_0, ξ_1, ξ_2 we set

$$T_i^*(x) = \xi_0^{-n_i} T_i(\xi_0 x) \qquad (i = 1, 2).$$

Changing, if necessary, the role of T_1 and T_2 we have one of the three cases:

(i) $(\xi_1/\xi_0)^{d_1} = 1$ and $(\xi_2/\xi_0)^{d_2} = 1$,
(ii) $(\xi_1/\xi_0)^{d_1} = 1$ and $(\xi_2/\xi_0)^{d_2} \neq 1$,
(iii) $(\xi_1/\xi_0)^{d_1} \neq 1$ and $(\xi_1/\xi_0)^{d_2} \neq 1$.

In case (i) we have $\xi_j/\xi_0 = \zeta_{d_j}^{r_j}$ $(j = 1, 2)$ and the equations $T_i^*(\xi_j/\xi_0) = 0$ $(i = 1, 2)$ give

$$a_i^* = \frac{\zeta_{d_{3-i}}^{r_{3-i}n_i} - 1}{1 - \zeta_{d_{3-i}}^{r_{3-i}m_i}}, \qquad b_i^* = \frac{\zeta_{d_{3-i}}^{r_{3-i}m_i} - \zeta_{d_{3-i}}^{r_{3-i}n_i}}{1 - \zeta_{d_{3-i}}^{r_{3-i}m_i}},$$
$$r_{3-i} m_i \not\equiv 0 \bmod d_{3-i} \qquad (i = 1, 2).$$

Hence $\langle a_1^*, b_1^*, a_2^*, b_2^* \rangle \in S$ and (2) holds with $u = \xi_0$. In case (ii) we have $(\xi_2/\xi_0)^{d_1} \neq 1$, since otherwise T_2 would have three common zeros with $x^{d_1} - \xi_0^{d_1}$, contrary to Theorem 1 of [4].

Hence $(\xi_2/\xi_0)^{d_i} \neq 1$ $(i = 1, 2)$ and the equations $T_i^*(\xi_2/\xi_0) = 0$ $(i = 1, 2)$ give

$$(\xi_2/\xi_0)^{m_1} \neq 1 \neq (\xi_2/\xi_0)^{m_2}$$

and

$$a_i^* = \frac{(\xi_2/\xi_0)^{n_i} - 1}{1 - (\xi_2/\xi_0)^{m_i}}, \qquad b_i^* = \frac{(\xi_2/\xi_0)^{m_i} - (\xi_2/\xi_0)^{n_i}}{1 - (\xi_2/\xi_0)^{m_i}}.$$

The polynomials $T_i^*/(x-1)(x-\xi_2/\xi_0)$ $(i = 1, 2)$ have a common zero ξ_1/ξ_0, hence $R(\xi_2/\xi_0) = 0$. It follows that $\langle a_1^*, b_1^*, a_2^*, b_2^* \rangle \in S$ and (2) holds with $u = \xi_0$.

In case (iii) we have $(\xi_1/\xi_0)^{d_i} \neq 1$ $(i = 1, 2)$ and we reach the desired conclusion replacing in the above argument ξ_2 by ξ_1.

Proof of Corollary 1. Since f and $f(x^d)$ have for every $f \in \mathbb{C}[x]$ and every $d \in \mathbb{N}$ the same number of non-zero coefficients we may assume that $(n_1, m_1, n_2, m_2) = 1$. If $T_1 = T_2$ then $(T_1, T_2) = T_1$ has three non-zero coefficients. If $T_1 \neq T_2$, but $\langle n_1, m_1 \rangle = \langle n_2, m_2 \rangle$, then by Theorem 2 of [4],

$$(T_1, T_2) = ((a_1 - a_2)x^{m_1} + b_1 - b_2, (a_1 - a_2)x^{n_1} + a_1 b_2 - a_2 b_1)$$

has at most two non-zero coefficients. If $\langle n_1, m_1 \rangle \neq \langle n_2, m_2 \rangle$ then by Theorem 2 either $\deg(T_1, T_2) \leq 2$, or (2) holds. However in the latter case

$$\operatorname{inv} T_i = \operatorname{inv} T_i^* \in \overline{\mathbb{Q}} \quad (i = 1, 2)$$

and

$$T_1(0)^{-\deg T_2} T_2(0)^{\deg T_1} = T_1^*(0)^{-\deg T_2} T_2^*(0)^{\deg T_1} \in \overline{\mathbb{Q}}.$$

Proof of Corollary 2. The second equality is clear. In order to prove the first, note that $A(3, 3, \overline{\mathbb{Q}}) \geq 3$. On the other hand, if (T_1, T_2) has more than three non-zero coefficients, then by Corollary 1,

$$\operatorname{inv} T_i \in \overline{\mathbb{Q}} \quad (i = 1, 2),$$

hence

$$T_i = u_i^{\deg T_i} T_i^{**}\left(\frac{x}{u_i}\right), \quad \text{where } u_i \in \mathbb{C}^*,\ T_i^{**} \in \overline{\mathbb{Q}}[x].$$

Moreover, also by Corollary 1,

$$\left(\frac{u_2}{u_1}\right)^{\deg T_1 \deg T_2} T_1^{**}(0)^{-\deg T_2} T_2^{**}(0)^{\deg T_1} \in \overline{\mathbb{Q}},$$

hence $v = u_2/u_1 \in \overline{\mathbb{Q}}$ and (T_1, T_2) has the same number of non-zero coefficients as $(T_1^{**}, T_2^{**}(x/v))$, where both terms belong to $\overline{\mathbb{Q}}[x]$.

LEMMA 6. *Let n, m be positive integers, $n > m$ and $a, b \in K^*$, where K is a finite extension of $\mathbb{Q}$. If F is a monic factor of $x^{n/(n,m)} + ax^{m/(n,m)} + b$ in $K[x]$ of maximal possible degree $d \leq 2$ and $n/(n,m) > \max\{6, 9 - 3d\}$, then*

$$\frac{x^n + ax^m + b}{F(x^{(n,m)})}$$

is reducible over K if and only if there exists a positive integer $l \mid (n,m)$ such that

$$a = u^{(n,m)/l} a_0, \quad b = u^{n/l} b_0, \quad F = u^d F_0\left(\frac{x}{u}\right),$$

where $u \in K^*$, $\langle a_0, b_0, F_0 \rangle \in F^d_{n/l, m/l}(K)$ and $F^d_{n/l, m/l}(K)$ is a certain finite set, possibly empty.

Proof. See [3], Theorem 3.

LEMMA 7. *Let $a, b \in K^*$, $n > m > 0$, $d = (n, m)$. Let $f(x)$ be a factor of $x^{n/d} + ax^{m/d} + b$ of degree at most 2. If $n > 2d$, then (n, m) is the greatest* *common divisor of the exponents of powers of x occurring with non-zero coefficients in $(x^n + ax^m + b)/f(x^{(n,m)}) =: Q(x)$.*

Proof. We may assume that f is monic and $d = 1$. If $f(x) = 1$ the assertion is obvious. If $f(x) = x - c$, then $Q(x)$ contains terms x^{n-1} and cx^{n-2}, unless $m = n-1$ and $a = -c$. But in the latter case $x - c \mid b$, which is impossible. If $f(x) = x^2 - px - q$, we first observe that $p \neq 0$. Otherwise, we should have $q^{n/2} + aq^{m/2} + b = 0$ and also $(-1)^n q^{n/2} + a(-1)^m q^{m/2} + b = 0$, which, since at least one of the numbers n, m is odd, gives $ab = 0$. Now $(x^n + ax^m + b)/(x^2 - px - q)$ contains the terms x^{n-2} and px^{n-3}, unless $m = n-1$ and $a = -p$. It also contains the terms $-b/q$ and $(b/q^2)px$, unless $m = 1$, $a = (b/q)p$. However $m = n-1$ and $m = 1$ give $n = 2$, contrary to the assumption.

LEMMA 8. *If $n > m > 0$, $n > 3$, $abc \neq 0$, then $(x^n + ax^m + b)(x - c)$ has six non-zero coefficients, unless either $m = n - 1$ or $m = 1$, when there are at least four non-zero coefficients. Only in the former case does x^{n-1} occur with a non-zero coefficient.*

Proof. We have

$$(x^n + ax^m + b)(x - c) = x^{n+1} - cx^n + ax^{m+1} - ax^m + bx - cb.$$

The cancellation can occur only between the second and the third term (if $m = n - 1$), or between the fourth and the fifth term (if $m = 1$).

LEMMA 9. *If $n > m > 0$, $n > 6$, $abpq \neq 0$, then $(x^n + ax^m + b)(x^2 - px + q)$ has nine non-zero coefficients, unless $m \geq n-2$ or $m \leq 2$, when there are at most eight. If $m = n-1$ there are at least five non-zero coefficients, including that of x^{n-1}; if $m = n - 2$ there are at least seven non-zero coefficients, including that of x^{n-2}. If $m \leq 2$ the coefficients of x^{n-1} and x^{n-2} are zero.*

Proof. We have

$$\begin{aligned}&(x^n + ax^m + b)(x^2 - px + q)\\&\qquad = x^{n+2} - px^{n+1} + qx^n + ax^{m+2} - apx^{m+1} + aqx^m + bx^2 - bpx + bq.\end{aligned}$$

The cancellation can occur only if $m \geq n-2$ or $m \leq 2$ and all the assertions are easily checked.

LEMMA 10. *Let $d_i = (n_i, m_i)$ $(i = 1, 2)$ and let $f_i(x)$ be a monic factor of degree ≤ 2 of $x^{n_i/d_i} + a_i x^{m_i/d_i} + b_i$. If $n_i/d_i > 6$ and*

$$\frac{x^{n_1} + a_1 x^{m_1} + b_1}{f_1(x^{d_1})} = \frac{x^{n_2} + a_2 x^{m_2} + b_2}{f_2(x^{d_2})}, \tag{17}$$

then

$$x^{n_1} + a_1 x^{m_1} + b_1 = x^{n_2} + a_2 x^{m_2} + b_2. \tag{18}$$

Proof. By Lemma 7, $d_1 = d_2$, hence we may assume without loss of generality that $d_1 = d_2 = 1$. Then the equality (17) gives

$$(x^{n_1} + a_1x^{m_1} + b_1)f_2(x) = (x^{n_2} + a_2x^{m_2} + b_2)f_1(x) \tag{19}$$

and we may assume without loss of generality that $\deg f_1 \ge \deg f_2$. Moreover, since (19) is equivalent to

$$(x^{n_1} + a_1b_1^{-1}x^{n_1-m_1} + b_1^{-1})\frac{x^{\deg f_2}f_2(x^{-1})}{f_2(0)} = (x^{n_2} + a_2b_2^{-1}x^{n_2-m_2} + b_2^{-1})\frac{x^{\deg f_1}f_1(x^{-1})}{f_1(0)},$$

we may assume that

$$2m_2 \ge n_2. \tag{20}$$

If $\deg f_2 = 0$, then the left hand side of (19) has only three non-zero coefficients, thus by Lemmas 8 and 9 applied to the right hand side $\deg f_1 = 0$ and (18) follows.

If $\deg f_2 = 1 < 2 = \deg f_1$, then the left hand side of (19) has at most six non-zero coefficients, which by Lemma 9 and condition (20) gives $m_2 = n_2 - 1$. Since $n_2 > 6$ taking the residues mod x^4 of both sides of (19) we obtain

$$(a_1x^{m_1} + b_1)f_2(x) \equiv b_2f_1(x) \bmod x^4, \tag{21}$$

hence $m_1 = 1$ and subtracting (21) from (19) gives

$$x^{n_1}f_2(x) = (x^{n_2} + a_2x^{n_2-1})f_1(x),$$

a contradiction mod f_1.

If $\deg f_2 = 1 = \deg f_1$, then $n_1 = n_2$. If $m_2 \ne n_2 - 1$, then by Lemma 8 and (20) the right hand side of (19) has six non-zero coefficients, thus also on the left hand side no terms coalesce and we have $b_1f_2 = b_2f_1$, hence $f_2 = f_1$ and (18) follows. If $m_2 = n_2 - 1$, then on the right hand side of (19) we have five or four non-zero coefficients, including that of x^{n_2-1}, hence by Lemma 8, $m_1 = n_1 - 1$. Taking the residues of both sides of (19) mod x^3 we find $b_1f_2 = b_2f_1$, hence $f_2 = f_1$ and (18) follows. If $\deg f_1 = \deg f_2 = 2$, then again $n_1 = n_2$. If $m_2 < n_2 - 2$, then on the right hand side of (19) we have nine non-zero coefficients, hence also on the left hand side no two terms coalesce and taking residues mod x^3 we obtain $b_1f_2 = b_2f_1$, hence $f_2 = f_1$ and (18) follows. If $m_2 \ge n_2 - 2$, then by Lemma 9 the number of non-zero coefficients on the right hand side of (19) is at most eight and x^{m_2} occurs with a non-zero coefficient, hence also on the left hand side we have at most eight non-zero coefficients and either x^{n_1-1} or x^{n_1-2} occurs with a non-zero coefficient. Again by Lemma 9, $m_1 \ge n_1 - 2$. Taking the residues of both sides of (19) mod x^3 we find $b_1f_2 = b_2f_1$, hence $f_2 = f_1$ and (18) follows.

Proof of Theorem 3. Put

$$F_{n,m}(K) = K \cap \{P_{n,m}(\zeta_q^r) : 0 \le r < q,\, 1 \ne \zeta_q^{rm} \ne \zeta_q^{rn} \ne 1\}.$$

The set $F_{n,m}(K)$ is finite since by Lemma 2 the condition $P_{n,m}(\zeta_q^r) \in K$ implies

$$\text{either} \quad \frac{q}{(q,r)} = 10 \quad \text{or} \quad \frac{1}{2}\varphi\left(\frac{q}{(q,r)}\right) \le [K : \mathbb{Q}]$$

and this leaves only finitely many possibilities for ζ_q^r. We set

$$E_{n,m}(K) = F_{n,m}(K) \cup \bigcup_{d\le 2} \bigcup_{l\mid(n,m)} \bigcup_{\langle a_0,b_0,F_0\rangle \in F^d_{n/l,m/l}(K)} \{a_0^{-n/(n,m)} b_0^{(n-m)/(n,m)}\},$$

where $F^d_{\nu,\mu}(K)$ are as in Lemma 6.

Now, let $d_i = (n_i, m_i)$ and let f_i be a monic polynomial over K of maximal possible degree $\delta_i \le 2$ dividing $T_i(x^{1/d_i})$ $(i = 1, 2)$. We may assume without loss of generality that $n_2/d_2 \le n_1/d_1$.

If $n_2/d_2 \le 9$, then, since $\operatorname{inv} T_2 \notin F_{n_2,m_2}(K)$, by Theorem 1 we have

$$\deg(T_1, T_2) \le n_2/d_2 \le 9. \tag{22}$$

If $n_2/d_2 > 9$, then by Lemma 6 either $T_i/f_i(x^{d_i})$ is irreducible over K or there exists an integer $l \mid d_i$, an element u of K^* and $\langle a_0, b_0, F_0\rangle \in F^{\delta_i}_{n_i/l,m_i/l}(K)$ such that

$$T_i(x) = x^{n_i} + u^{(n_i-m_i)/l} a_0 x^{m_i} + u^{n_i/l} b_0, \qquad f_i = u^{\delta_i} F_0\left(\frac{x}{u}\right).$$

These conditions give

$$\operatorname{inv} T_i = a_0^{-n_i/d_i} b_0^{(n_i-m_i)/d_i} \in E_{n_i,m_i}(K),$$

contrary to the assumption. Therefore $T_i/f_i(x^{d_i})$ is irreducible over K for $i = 1, 2$ and we have

$$\text{either} \quad T_1/f_1(x^{d_1}) = T_2/f_2(x^{d_2}) \quad \text{or} \quad (T_1/f_1(x^{d_1}), T_2/f_2(x^{d_2})) = 1.$$

In the former case we have $T_1 = T_2$ by Lemma 10; in the latter case

$$(T_1, T_2) = \frac{(T_1, f_2(x^{d_2}))(T_2, f_1(x^{d_1}))}{(f_1(x^{d_1}), f_2(x^{d_2}))}\,. \tag{23}$$

However, by Lemma 3 if $\deg f_{3-i} = 1$, or if $\deg f_{3-i} = 2$ and $f'_{3-i}(0) = 0$ and by Theorem 1 otherwise, we have

$$\deg(T_i, f_{3-i}(x^{d_{3-i}})) \le \deg f_{3-i} \le 2,$$

which by (23) gives

$$\deg(T_1, T_2) \le 2 + 2 = 4. \tag{24}$$

The alternative (22) or (24) gives the theorem.

We shall now give the promised examples.

Example 1. Let $n_i > m_i > 0$, $d_i = (n_i, m_i)$, $0 \not\equiv m_i \not\equiv n_i \not\equiv 0 \bmod d_{3-i}$ for $i = 1, 2$, $(d_1, d_2) = 1$, and

$$T_i(x) = x^{n_i} + \frac{\zeta_{d_{3-i}}^{r_{3-i}n_i} - 1}{1 - \zeta_{d_{3-i}}^{r_{3-i}m_i}} x^{m_i} + \frac{\zeta_{d_{3-i}}^{r_{3-i}m_i} - \zeta_{d_{3-i}}^{r_{3-i}n_i}}{1 - \zeta_{d_{3-i}}^{r_{3-i}m_i}} \qquad (i = 1, 2),$$

where r_{3-i} is chosen so that

$$1 \neq \zeta_{d_{3-i}}^{r_{3-i}m_i} \neq \zeta_{d_{3-i}}^{r_{3-i}n_i} \neq 1 \qquad (i = 1, 2).$$

Here (T_1, T_2) has the following distinct zeros: 1, $\zeta_{d_1}^{r_1}$, $\zeta_{d_2}^{r_2}$, $\zeta_{d_1}^{r_1}\zeta_{d_2}^{r_2}$, hence

$$\deg(T_1, T_2) \geq 4.$$

If $n_2/d_2 = 2$ this shows that the second and the third inequality of (1) are exact in infinitely many essentially different cases and the condition for the first inequality is not superfluous.

Example 2. Let $T_1 = x^4 - 5x + 5$ and $T_2 = x^{20} + 5^4x^{10} + 5^5$. Here $(T_1, T_2) = T_1$, hence

$$\deg(T_1, T_2) = 4 > n_2/d_2 + \min\{2, d_1\}.$$

This shows that the condition for the second inequality of (1) is not superfluous.

Example 3 (due to S. Chaładus [1]). Let $T_1 = x^7 + 9x^2 + 27$ and $T_2 = x^{15} - 27x^6 + 729$. Here

$$(T_1, T_2) = x^5 + 3x^4 + 6x^3 + 9x^2 + 9x + 9.$$

Since $\operatorname{inv} T_1 = 3$, $d_2 = 3$, and $P_{n_1,m_1}(\zeta_3^{\pm 1}) = 1$, in this case the first inequality of (1) is exact. Moreover (T_1, T_2) has six non-zero coefficients, which is the present record.

References

[1] S. Chaładus, Letter to the author of July 7, 1994.

[2] R. Dvornicich, *On an equation in cyclotomic numbers*, this issue, 71–94.

[3] A. Schinzel, *On reducible trinomials, III*, Period. Math. Hungar. 43 (2001), 43–69.

[4] —, *On the greatest common divisor of two univariate polynomials, I*, in: A Tribute to Alan Baker, to appear.

Institute of Mathematics
Polish Academy of Sciences
P.O. Box 137
00-950 Warszawa, Poland
E-mail: schinzel@impan.gov.pl

Received on 25.9.2000 (3882)