ACTA ARITHMETICA
LXXVIII.3 (1997)

Polynomials that divide many trinomials

by

HANS PETER SCHLICKEWEI (Ulm) and CARLO VIOLA (Pisa)

1. Introduction. Let

$$p(X) = a_k X^k + a_{k-1} X^{k-1} + \ldots + a_0 \tag{1.1}$$

be a polynomial of degree $k > 0$ with rational coefficients. We call a polynomial

$$T(X) = X^m + aX^n + b \tag{1.2}$$

with complex coefficients a, b and with $m > n > 0$ a *trinomial*. In 1965 Posner and Rumsey [2] made the following conjecture:

Suppose that $p(X)$ divides infinitely many trinomials. Then there exist a non-zero polynomial $Q(X)$ of degree ≤ 2 and a natural number r such that $p(X)$ divides $Q(X^r)$.

In a recent paper [1], this conjecture was shown to be true by Győry and Schinzel. They proved that it suffices to assume that p divides at least

$$(4sd)^{s^6 2^{180d} + 8sl} \tag{1.3}$$

trinomials with rational coefficients. Here d is the degree of the splitting field L of p over $\mathbb{Q}$. s is the cardinality of the set of places of L consisting of all infinite places and all places induced by the prime ideal factors of the non-zero roots of p. Moreover, l is the number of distinct roots of p.

It is the purpose of this paper to improve on this result. In fact, we will give an estimate that avoids the parameter s completely and involves only the degree k of the polynomial p. We have

THEOREM. *Let $p(X)$ be a polynomial of degree $k > 0$ with rational coefficients which divides more than*

$$2^{44000} k^{1000} \tag{1.4}$$

trinomials $T(X)$ as in (1.2) *with complex coefficients. Then there exist a non-zero polynomial $Q(X)$ of degree ≤ 2 with rational coefficients and a natural number r such that $p(X)$ divides $Q(X^r)$.*

We remark that L. Hajdu also improved (1.3) and extended it to the number field case, but his bound depends on s too.

Our proof depends upon a recent result of Schlickewei and Schmidt [3] on polynomial-exponential equations. We conjecture that the bound (1.4) may be replaced by an absolute bound which does not involve the degree of p at all. However, at present this seems to be out of reach.

In a subsequent paper we will deal with the generalization when the trinomials are replaced by k-nomials, i.e. the problem stated at the end of the Introduction in [1]. In that wider setting, we will treat also quantitative versions of Theorems 2A and 2B of [1].

2. A reduction. The following simple lemma will be useful.

LEMMA 2.1. *Suppose that the trinomial* $T(X) = X^m + aX^n + b$ *has a zero* α *of multiplicity* ≥ 3. *Then* $\alpha = 0$ (*and consequently* $b = 0$).

Proof. We have

$$T'(X) = mX^{m-1} + naX^{n-1} = X^{n-1}(mX^{m-n} + na).$$

Thus if $\alpha \neq 0$ is a zero of multiplicity ≥ 3 of T, α is a zero of multiplicity ≥ 2 of $T^* = mX^{m-n} + na$. But $T^{*\prime} = m(m-n)X^{m-n-1}$. So such an $\alpha \neq 0$ does not exist.

Let $\alpha_1, \ldots, \alpha_l$ be the distinct zeros of p. We partition the set $\{\alpha_1, \ldots, \alpha_l\}$ into disjoint classes as follows: two zeros α_i and α_j belong to the same class if there exists a root of unity ζ such that $\alpha_i = \zeta\alpha_j$.

It is clear that if $p(0) = 0$ then $\{0\}$ makes up one class.

PROPOSITION 2.2. *Let the hypotheses be the same as in the Theorem. Suppose moreover that* $p(0) \neq 0$. *Then*, *if* p *has a double zero* α, *the set of zeros of* p *lies in a single class. If* p *does not have a double zero*, *then its set of zeros splits into at most two distinct classes.*

We proceed to deduce the Theorem from Proposition 2.2. First suppose that $p(0) = 0$. Then any trinomial $T(X)$ which is divisible by $p(X)$ will be of the shape

$$T(X) = X^m + aX^n = X^n(X^{m-n} + a).$$

We may conclude that any zero $\alpha \neq 0$ of p is simple and satisfies the equation

$$\alpha^{m-n} + a = 0. \tag{2.1}$$

Let L be the splitting field of p over $\mathbb{Q}$ and write G for its Galois group. As p has rational coefficients, any $\sigma \in G$ permutes the non-zero roots of p. Thus (2.1) implies that $\sigma(a) = a$ for any $\sigma \in G$. We may conclude that $a \in \mathbb{Q}$.

Write $r = \mathrm{lcm}(n, m-n)$ and $t = r/(m-n)$. We put $Q(X) = X(X + a^t)$. Then obviously $p(X) \mid Q(X^r)$ and $Q(X) \in \mathbb{Q}[X]$, as asserted in the

Theorem. Thus we may suppose that $p(0) \neq 0$. If p has a double zero, then by Proposition 2.2 there exist an $a \in \mathbb{C}$ and a natural number r such that

$$\alpha_i^r = a \quad \text{for } i = 1, \ldots, l. \tag{2.2}$$

With the same argument as above we get $a \in \mathbb{Q}$. In view of Lemma 2.1 we may conclude that with r from (2.2) and with $Q(X) = (X-a)^2$ the assertion of the Theorem is true.

Next suppose that p has only simple zeros. By Proposition 2.2 we may find complex numbers a and b and a natural number r such that any root of $p(X)$ satisfies one of the equations

$$x^r = a \quad \text{or} \quad x^r = b. \tag{2.3}$$

Again consider the Galois group G of the splitting field L of p over $\mathbb{Q}$. If all the roots of p satisfy a single one of the equations in (2.3), say the first one, we may argue as above and infer that with r from (2.3) and $Q(X) = X - a$ the assertion of the Theorem is true. Otherwise, again since G permutes the roots of p, in view of (2.3) we obtain two alternatives: either $\sigma(a) = a$ and $\sigma(b) = b$ for each $\sigma \in G$, or we may conclude that a and b are permuted under G.

In the first case a and b are rational numbers. We may take r from (2.3) and $Q(X) = (X-a)(X-b)$ to get the Theorem. In the second case a and b are conjugates over $\mathbb{Q}$ and have degree 2. Therefore $Q(X) = (X-a)(X-b) \in \mathbb{Q}[X]$ and the Theorem follows with r from (2.3).

The remainder of the paper deals with a proof of Proposition 2.2.

3. Polynomial-exponential equations. We consider equations of the type

$$\sum_{l=1}^{q} P_l(\mathbf{x})\boldsymbol{\alpha}_l^{\mathbf{x}} = 0 \tag{3.1}$$

in variables $\mathbf{x} = (x_1, \ldots, x_N) \in \mathbb{Z}^N$, where the P_l are polynomials with coefficients in a number field K and where

$$\boldsymbol{\alpha}_l^{\mathbf{x}} = \alpha_{l1}^{x_1} \ldots \alpha_{lN}^{x_N}$$

with given $\alpha_{lj} \in K^*$ ($1 \leq l \leq q$, $1 \leq j \leq N$). Let $\mathcal{P}$ be a partition of the set $\Lambda = \{1, \ldots, q\}$. The sets $\lambda \subset \Lambda$ occurring in the partition $\mathcal{P}$ will be considered elements of $\mathcal{P}$: $\lambda \in \mathcal{P}$. Given $\mathcal{P}$, we may consider the system of equations

$$\sum_{l \in \lambda} P_l(\mathbf{x})\boldsymbol{\alpha}_l^{\mathbf{x}} = 0 \quad (\lambda \in \mathcal{P}), \tag{3.1$\mathcal{P}$}$$

which is a refinement of (3.1). Write $\mathfrak{S}(\mathcal{P})$ for the set of solutions $\mathbf{x}$ of (3.1$\mathcal{P}$) which are not solutions of (3.1$\mathcal{Q}$) if $\mathcal{Q}$ is a proper refinement of $\mathcal{P}$.

Given $\mathcal{P}$, set $l \overset{\mathcal{P}}{\sim} m$ if l and m lie in the same subset λ of $\mathcal{P}$. Let $G(\mathcal{P})$ be the subgroup of $\mathbb{Z}^N$ consisting of $\mathbf{z}$ satisfying

$$\boldsymbol{\alpha}_l^{\mathbf{z}} = \boldsymbol{\alpha}_m^{\mathbf{z}} \quad \text{for any } l, m \text{ with } l \overset{\mathcal{P}}{\sim} m.$$

Write

$$A_0 = \sum_{l \in \Lambda} \binom{N + \delta_l}{N},$$

where δ_l is the total degree of the polynomial P_l. Set

$$A = \max\{N, A_0\}.$$

The following proposition will be crucial in the proof of our Theorem.

Proposition 3.1. *Suppose* $G(\mathcal{P}) = \{\mathbf{0}\}$. *Then*

$$|\mathfrak{S}(\mathcal{P})| < 2^{60A^3} d^{6A^2}. \tag{3.2}$$

This is Theorem 1 of Schlickewei and Schmidt [3].

4. Application to our problem. We are considering trinomials

$$T(X) = X^m + aX^n + b.$$

The hypothesis in Proposition 2.2 says $b \neq 0$. If $a = 0$, then the assertion of Proposition 2.2 is trivial. Thus in the sequel we may suppose that $ab \neq 0$. Also, given two trinomials

$$T_1(X) = X^{m_1} + a_1 X^{n_1} + b_1, \quad T_2(X) = X^{m_2} + a_2 X^{n_2} + b_2,$$

we may suppose without loss of generality that $(m_1, n_1) \neq (m_2, n_2)$, as otherwise $p(X)$ divides $(a_1 - a_2)X^{n_1} + b_1 - b_2$. And thus the assertion of Proposition 2.2 would follow at once.

Let α be a zero of $p(X)$. Define

$$\widetilde{p}(X) = a_k \alpha^k X^k + a_{k-1}\alpha^{k-1} X^{k-1} + \ldots + a_1 \alpha X + a_0.$$

Then $\widetilde{p}(X/\alpha) = p(X)$. Thus, if $\alpha_1, \ldots, \alpha_k$ are the zeros of p, then $\alpha_1/\alpha, \ldots, \alpha_k/\alpha$ are the zeros of $\widetilde{p}$. Clearly, in general $\widetilde{p}$ does not have rational coefficients. However, given a trinomial T and defining $\widetilde{T}$ in analogy with $\widetilde{p}$, we see that if p divides T then $\widetilde{p}$ divides $\widetilde{T}$. We remark that our transformation preserves the classes of zeros introduced in Section 2. So it will suffice to prove Proposition 2.2 for $\widetilde{p}$, which has the advantage that $\widetilde{p}(1) = 0$.

Let α and β be any other zeros of $\widetilde{p}$. If $\widetilde{p}$ divides a trinomial $\widetilde{T} = X^m + AX^n + B$, we get

$$\begin{aligned} 1 + A + B &= 0, \\ \alpha^m + A\alpha^n + B &= 0, \\ \beta^m + A\beta^n + B &= 0. \end{aligned}$$

We may conclude that

$$\begin{vmatrix} 1 & 1 & 1 \\ \alpha^m & \alpha^n & 1 \\ \beta^m & \beta^n & 1 \end{vmatrix} = \alpha^n + \beta^m + \alpha^m\beta^n - \alpha^n\beta^m - \alpha^m - \beta^n = 0. \tag{4.1}$$

The hypothesis of our Theorem together with the reduction from the beginning of this section imply that (4.1) has at least

$$2^{44000}k^{1000} \tag{4.2}$$

solutions $(m,n) \in \mathbb{Z}^2$. On the other hand, equation (4.1) is a special instance of the type of equations discussed in Section 3, in fact with six summands, i.e. in the notation of Section 3 with $q = 6$. The elements α, β may be written as $\alpha_2/\alpha_1, \alpha_3/\alpha_1$, where $\alpha_1, \alpha_2, \alpha_3$ are the three zeros of p. As p has degree k, α and β generate a number field K of degree $\le k^3$.

In our case we have $N = 2$ and $\delta_1 = \ldots = \delta_6 = 0$. Thus we get $A = 6$. Therefore, by Proposition 3.1 for any partition $\mathcal{P}$ of $\{1, \ldots, 6\}$ with $G(\mathcal{P}) = \{(0,0)\}$ the equation (4.1$\mathcal{P}$) has not more than $2^{60\times 6^3}(k^3)^{6\times 6^2}$ solutions $(m,n) \in \mathbb{Z}^2$. Since the total number of partitions of $\{1, \ldots, 6\}$ does not exceed 6^6, we may conclude that the total set of partitions $\mathcal{P}$ with $G(\mathcal{P}) = \{(0,0)\}$ produces less than

$$2^{18+60\times 6^3}k^{3\times 6^3} < 2^{13000}k^{650} \tag{4.3}$$

solutions $(m,n) \in \mathbb{Z}^2$.

Comparing (4.2) and (4.3) we may infer that there exists a partition $\mathcal{P}$ of the set $\{1, \ldots, 6\}$ with $G(\mathcal{P}) \ne \{(0,0)\}$. We are going to prove that this implies that at least one of α, β, α/β is a root of unity. It will follow that the three roots $1, \alpha, \beta$ of $\widetilde{p}$ are contained in at most two different classes and this will imply the assertion of Proposition 2.1 if p has only simple zeros.

By a slight abuse of notation we will write $\{\alpha^x, \beta^y, \alpha^y\beta^x, \alpha^x\beta^y, \alpha^y, \beta^x\}$ instead of $\{1, \ldots, 6\}$. We proceed to study the possible partitions:

(a) $\{\alpha^x, \beta^y\}, \quad \{\alpha^y\beta^x, \alpha^x\beta^y, \alpha^y, \beta^x\}.$

Then $G(\mathcal{P})$ among others has the defining relations

$$\alpha^y\beta^x = \alpha^y, \qquad \alpha^y\beta^x = \beta^x,$$

whence $\beta^x = 1$ and $\alpha^y = 1$. Thus either $x = y = 0$, i.e. $G(\mathcal{P}) = \{(0,0)\}$, or one of α, β is a root of unity.

(b) $\{\alpha^x, \beta^y\}, \quad \{\alpha^y\beta^x, \alpha^x\beta^y\}, \quad \{\alpha^y, \beta^x\}.$

We get

$$\alpha^{y-x} = \beta^{y-x}, \qquad \alpha^x = \beta^y.$$

Thus either $y-x=0$ or α/β is a root of unity. If $y=x$ then either $x=y=0$ or again α/β is a root of unity.

(c) $$\{\alpha^x,\beta^y\},\quad \{\alpha^y\beta^x,\alpha^y\},\quad \{\alpha^x\beta^y,\beta^x\}.$$

We get

$$\alpha^y\beta^x=\alpha^y,\qquad \alpha^x\beta^y=\beta^x.$$

Thus either $x=0$ or β is a root of unity. If $x=0$, then either $y=0$ or again β has to be a root of unity. We may conclude that either $G(\mathcal{P})=\{(0,0)\}$ or one of $\alpha,\beta,\alpha/\beta$ is a root of unity.

(d) $$\{\alpha^x,\beta^y\},\quad \{\alpha^y\beta^x,\beta^x\},\quad \{\alpha^x\beta^y,\alpha^y\}.$$

This is symmetric to (c).

(e) $$\{\alpha^x,\alpha^y\beta^x\},\qquad \{\beta^y,\alpha^x\beta^y,\alpha^y,\beta^x\}.$$

We get

$$\beta^y=\alpha^y,\qquad \beta^y=\beta^x$$

and conclude $x=y=0$ or one of $\beta,\alpha/\beta$ is a root of unity.

(f) $$\{\alpha^x,\alpha^y\beta^x\},\quad \{\beta^y,\alpha^x\beta^y\},\quad \{\alpha^y,\beta^x\}.$$

We get

$$\alpha^x=\alpha^y\beta^x,\qquad \beta^y=\alpha^x\beta^y$$

which implies $x=0$ or α is a root of unity. If $x=0$ then either $y=0$ or again α is a root of unity.

All the partitions containing a subset with two elements are symmetric to the cases treated above or may be treated in a similarly easy way. So we now study partitions with subsets of three elements:

(g) $$\{\alpha^x,\beta^y,\alpha^y\beta^x\},\quad \{\alpha^x\beta^y,\alpha^y,\beta^x\}.$$

We get $\alpha^x=\beta^y$, $\alpha^y=\beta^x$. Hence $\alpha^{x+y}=\beta^{x+y}$. Thus either $x+y=0$ or α/β is a root of unity. If $x+y=0$, we use $\beta^y=\alpha^y\beta^x$ and $\alpha^x\beta^y=\alpha^y$. Together with the previous relations we obtain $\beta^y=\alpha^{2y}$, $\beta^{2y}=\alpha^y$, whence $\beta^{3y}=\alpha^{3y}$. Thus either $y=0$ (and therefore also $x=0$), or α/β is a root of unity.

(h) $$\{\alpha^x,\beta^y,\alpha^x\beta^y\},\quad \{\alpha^y\beta^x,\alpha^y,\beta^x\}.$$

Then $\alpha^x=\beta^y$, $\alpha^x=\alpha^x\beta^y$. Thus either $y=0$ or β is a root of unity. If $y=0$ then either $x=0$ or α is a root of unity.

(i) $$\{\alpha^x,\alpha^y\beta^x,\alpha^x\beta^y\},\quad \{\beta^y,\alpha^y,\beta^x\}.$$

We get $\beta^y=\alpha^y$, $\beta^y=\beta^x$. Either $y=0$ or α/β is a root of unity. If $y=0$ then either $x=0$ or β is a root of unity.

All other cases are symmetric to the ones treated above or at least equally easy. Altogether we have shown that if there exists a partition $\mathcal{P}$

with $G(\mathcal{P}) \neq \{(0,0)\}$ then at least one of $\alpha, \beta, \alpha/\beta$ is a root of unity. So Proposition 2.2 follows if p has only simple roots.

We next assume that p has a double root α. We may choose our transformation $p \mapsto \widetilde{p}$ such that 1 is a double root of $\widetilde{p}$. Let β be any other root of $\widetilde{p}$. Then given a trinomial $\widetilde{T} = X^m + AX^n + B$ we get $\widetilde{T}(1) = \widetilde{T}'(1) = \widetilde{T}(\beta) = 0$. Thus

$$\begin{vmatrix} 1 & 1 & 1 \\ m & n & 0 \\ \beta^m & \beta^n & 1 \end{vmatrix} = (n-m) + m\beta^n - n\beta^m = 0. \tag{4.4}$$

This is an equation of the type considered in Section 3. Here $N = 2$, $\delta_1 = \delta_2 = \delta_3 = 1$, $A = 9$, and as β is the quotient of two roots α_i, α_j of p, it has degree $\leq k^2$. With our reductions we see that we are only interested in solutions $(m,n) \in \mathbb{Z}^2$ such that no subsum in (4.4) vanishes. Thus for $\mathcal{P} = \{1,2,3\}$ Proposition 3.1 says that (4.4) has less than

$$2^{60\times 9^3}(k^2)^{6\times 9^2} < 2^{44000}k^{1000}$$

solutions $(m,n) \in \mathbb{Z}^2$, provided that $G(\mathcal{P}) = \{(0,0)\}$. On the other hand, the hypothesis of the Theorem guarantees that we have at least $2^{44000}k^{1000}$ solutions $(m,n) \in \mathbb{Z}^2$. We may infer that $G(\mathcal{P}) \neq \{(0,0)\}$. In our case the defining relations for $G(\mathcal{P})$ are

$$\beta^x = \beta^y = 1.$$

As $G(\mathcal{P}) \neq \{(0,0)\}$, this implies at once that β is a root of unity. Therefore the two zeros 1 and β of $\widetilde{p}$ lie in the same class. This proves Proposition 2.2 if p has a double root.

References

[1] K. Győry and A. Schinzel, *On a conjecture of Posner and Rumsey*, J. Number Theory 47 (1994), 63–78.

[2] E. C. Posner and H. Rumsey, Jr., *Polynomials that divide infinitely many trinomials*, Michigan Math. J. 12 (1965), 339–348.

[3] H. P. Schlickewei and W. M. Schmidt, *On polynomial-exponential equations, II*, to appear.

Abteilung Mathematik II
Universität Ulm
Helmholtzstrasse 18
89081 Ulm, Germany
E-mail: hps@mathematik.uni-ulm.de

Dipartimento di Matematica
Università di Pisa
Via Buonarroti 2
56127 Pisa, Italy
E-mail: viola@dm.unipi.it

Received on 1.4.1996 (2954)