ON A PROBLEM OF GYŐRY AND SCHINZEL CONCERNING POLYNOMIALS

L. Hajdu[1]

1. Introduction

In 1965, Posner and Rumsey [2] considered polynomials that divide infinitely many trinomials. They made an attempt to determine all such polynomials but they could only partially solve this problem. Further, they made a conjecture on polynomials which divide infinitely many k-nomials. To formulate their conjecture we need to introduce the concept of standard k-nomials. We remark that this concept in the form below is due to Győry and Schinzel [1].

A polynomial $P(x)$ with coefficients in a field of characteristic 0 which is of the form

$$P(x) = x^{m_1} + \sum_{i=2}^{k-1} c_i x^{m_i} + c_k \text{ with } m_1 > \ldots > m_{k-1} > 0,$$

is called a standard k-nomial.

Posner and Rumsey [2] conjectured that if a polynomial with rational coefficients divides infinitely many standard k-nomials over $\mathbb{Q}$, then it divides a non-zero polynomial of degree less than k in x^r for some integer $r \geq 1$.

For $k = 2$ the conjecture is clearly true. In their joint paper [1] Győry and Schinzel proved the conjecture (in a stronger sense) for $k = 3$, and disproved it for every $k \geq 4$. For $k = 3$ they proved that if a polynomial $P(x)$ with rational coefficients divides more than a certain (explicitely given) number of trinomials over $\mathbb{Q}$, then $P(x)$ divides a linear or quadratic polynomial in x^r for some integer $r \geq 1$. Very recently their explicit constant has been improved by H.P. Schlikewei and C. Viola (private communication). For $k = 3$, the above conjecture has been proved in [1] in a qualitative form for polynomials over any field of characteristic 0 as well.

Győry and Schinzel [1] disproved the conjecture for $k \geq 4$ by means of counterexamples. They showed that for every $k \geq 2$ there exists a polynomial $P \in \mathbb{Q}[x]$ that divides infinitely many standard quadrinomials over $\mathbb{Q}$, but does not divide any non-zero polynomial of degree less than k in x^r for any integer $r \geq 1$. The quadrinomials constructed have the constant term zero. For polynomials with the constant term non-zero the relevant problem is harder. In [1] the authors proved that for $k \geq 2$ there is a $P \in \mathbb{Q}[x]$ that divides infinitely many standard quintinomials over $\mathbb{Q}$ with the constant term non-zero, but does not divide any non-zero polynomial of degree less than k in x^r over $\mathbb{Q}$ for any integer $r \geq 1$. In these results

[1]Research supported in part by Grants 014245 and T 016 975 from the Hungarian National Foundation for Scientific Research and by the Universitas Foundation of Kereskedelmi Bank RT.

the polynomials $P(x)$ are all trinomials. This fact led the authors in [1] to propose the following problem.

Let K be a field of characteristic 0. Is it true that a polynomial $P \in K[x]$ with $P(0) \neq 0$ divides infinitely many standard k-nomials with the constant term non-zero if and only if either P divides a non-zero polynomial of degree less than k in x^r for any integer $r \geq 1$, or P divides a standard $\left[\frac{k+1}{2}\right]$-nomial?

The purpose of this paper is to considerably extend the set of counterexample polynomials and to give a negative answer to this problem in case $k \geq 6$. Further, we propose a new problem, in which the remaining cases of $k = 4$ and 5 are also included.

Theorem. *Let K be a field of characteristic 0. For every positive number C and for every integer $k \geq 6$ there exists a standard $(k-2)$-nomial $P(x) \in K[x]$ with $P(0) \neq 0$ and deg $P > C$, which divides over K infinitely many standard k-nomials with the constant term non-zero, but $P(x)$ divides over K neither any non-zero polynomial of degree less than deg P in x^r for any integer $r \geq 1$, nor any standard $(k-3)$-nomial.*

Remark 1. For $k \geq 6$, our Theorem gives a negative answer to the problem of Győry and Schinzel, since in this case we have

$$\left[\frac{k+1}{2}\right] \leq k-3 \ .$$

Remark 2. Following the method of the proof, one can see that the polynomials $P(x)$ in our Theorem can be effectively determined.

Remark 3. We obtain as a trivial consequence of the Theorem that for every integer $n \geq 4$ there exists a standard n-nomial $q(x)$ not dividing any standard r-nomial with $r < n$. (For $n \leq 3$ the statement is obvious.)

For the values $k = 4$ and 5 the problem of Győry and Schinzel remains open. We guess that the real difficulties lie in the case when the polynomial P, which divides infinitely many standard k-nomials, has more than $k-2$ non-zero coefficients. We propose the following.

Problem. Let K be a field of characteristic 0, and $k \geq 4$ be an integer. Is it true that if the polynomial $P(x) \in K[x]$ with non-zero constant term divides infinitely many standard k-nomials with the constant term non-zero then either P divides a non-zero polynomial of degree less than k in x^r for some integer $r \geq 1$, or P divides a standard l-nomial $q(x)$ such that $l \leq k-2$ and $q(x)$ divides infinitely many standard k-nomials?

For $k = 2$ and $k = 3$ the assertion formulated in the problem is true.

2. Proof

To prove our theorem we need some lemmas.

Lemma 1. *Every polynomial of the form*

$$P(x) = x^n + a_{r-4}x^{r-4} + a_{r-5}x^{r-5} + \ldots + a_1 x + a_0 \ , a_i \in \mathbb{Q}, \ i = 0, \ldots, r-4$$

with $a_0 \neq 0$, $r \geq 4$, $n \geq r-3$ divides infinitely many standard r-nomials over $\mathbb{Q}$ with non-zero constant term.

Proof. The statement is obvious, since for every non-zero $a \in \mathbb{Q}$ the polynomial $(x+a)P(x)$ is clearly a standard r-nomial with non-zero constant term.

Lemma 2. *Let*

$$P(x) = x^p + a_{p-1}x^{p-1} + a_{p-2}x^{p-2} + \ldots + a_1x + a_0 \ , a_i \in \mathbb{Q}, i = 0, \ldots, p-1 \ ,$$

where p is a prime. If P is irreducible over $\mathbb{Q}$ and has two roots in $\mathbb{C}$ with different absolute values, then P does not divide any non-zero polynomial of degree less than deg P in x^r over $\mathbb{Q}$ for any integer $r \geq 1$.

Proof. This is a simple consequnce of the *proof* of Theorems 3A and 3B in [1]. However, for convenience of the reader we repeat here the main steps of the proof.

Suppose that the polynomial P satisfies the conditions of Lemma 2, and for some polynomial $s(x)$ in $\mathbb{Q}[x]$ with $t = \deg s < \deg P$ and for some integer $r \geq 1$, $P(x)$ divides $s(x^r)$ over $\mathbb{Q}$. Since $P(x)$ is irreducible, we may assume that $s(x)$ is also irreducible over $\mathbb{Q}$. Denote by $\alpha_1, \ldots, \alpha_p$ the roots of $P(x)$ and by $\beta_1, \ldots, \beta_t$ the roots of $s(x)$ in $\mathbb{C}$. Hence $(x - \alpha_1)$ divides $(x^r - \beta_j)$ for some j $(1 \leq j \leq t)$ over the field of algebraic numbers. Thus we have

$$\alpha_1^r = \beta_j \ , \tag{1}$$

whence $\beta_j \in \mathbb{Q}(\alpha_1)$. But the field $\mathbb{Q}(\alpha_1)$ is of degree p over $\mathbb{Q}$, where p is a prime. This implies that β_j is either a rational number, or is of degree p. However, the latter case cannot hold, because β_j, as a root of $s(x)$, is of degree less than p. This implies that $\beta_j \in \mathbb{Q}$ and $t = 1$. Consequently, from (1) it follows that

$$\alpha_i^r = \alpha_1^r \text{ for } i = 1, \ldots, p \ .$$

But this is a contradiction, because $P(x)$ has two roots with different absolute values, and Lemma 2 follows.

The following lemma can be regarded as a generalization of a modified version of Lemma 2 in [2].

Lemma 3. *Let l be a natural number. Suppose that a polynomial $P(x)$ has rational coefficients with $P(0) \neq 0$, and $\vartheta_1, \ldots, \vartheta_l$ are roots of $P(x)$ in $\mathbb{C}$ with the property*

$$\frac{|\ \vartheta_{i+1}\ |}{|\ \vartheta_i\ |} < \frac{1}{l!} \text{ for } i = 1, \ldots, l-1 \ .$$

Then $P(x)$ does not divide any standard l-nomial over $\mathbb{Q}$.

Proof. Suppose, to the contrary, that $P(x)$ divides a standard l-nomial

$$x^{n_1} + a_{n_2}x^{n_2} + \ldots + a_{n_{l-1}}x^{n_{l-1}} + a_{n_l} \ , a_{n_i} \in \mathbb{Q}, i = 2, \ldots, l \ , \ a_{n_l} \neq 0$$

over $\mathbb{Q}$. In this case the determinant

$$D = \begin{vmatrix} \vartheta_1^{n_1} & \vartheta_1^{n_2} & \ldots & \vartheta_1^{n_{l-1}} & 1 \\ \vartheta_2^{n_1} & \vartheta_2^{n_2} & \ldots & \vartheta_2^{n_{l-1}} & 1 \\ \ldots & \ldots & \ldots & \ldots & \ldots \\ \vartheta_l^{n_1} & \vartheta_l^{n_2} & \ldots & \vartheta_l^{n_{l-1}} & 1 \end{vmatrix}$$

must vanish. Expanding D we get a sum consisting of $l!$ summands of the form

$$\pm\vartheta_{i_1}^{n_1}\vartheta_{i_2}^{n_2}\ldots\vartheta_{i_{l-1}}^{n_{l-1}} \ ,$$

where

$$i_j \neq i_k \text{ if } j \neq k \ , \text{ and } \{i_1, \ldots, i_{l-1}\} \subset \{1, \ldots, l\} \ . \tag{2}$$

We will prove that every summand can be written in the form

$$\pm \vartheta_1^{n_1} \vartheta_2^{n_2} \ldots \vartheta_{l-1}^{n_{l-1}} \prod_{\substack{i,j=1 \\ i<j}}^{l} \left(\frac{\vartheta_j}{\vartheta_i} \right)^{k_{ij}} \ , \tag{3}$$

where the exponents k_{ij} are nonnegative integers. We note that in the case when $k_{ij} = 0$ for $1 \leq i < j \leq l$, we obtain just the summand

$$\vartheta_1^{n_1} \vartheta_2^{n_2} \ldots \vartheta_{l-1}^{n_{l-1}} \ . \tag{4}$$

It suffices to deal with the case when in (2)

$$\{i_1, \ldots, i_{l-1}\} = \{1, \ldots, l-1\} \ ,$$

because the summand

$$\pm \vartheta_{i_1}^{n_1} \ldots \vartheta_{i_{j-1}}^{n_{j-1}} \vartheta_l^{n_j} \vartheta_{i_{j+1}}^{n_{j+1}} \ldots \vartheta_{i_{l-1}}^{n_{l-1}}$$

can be written as

$$\pm \vartheta_{i_1}^{n_1} \ldots \vartheta_{i_{j-1}}^{n_{j-1}} \vartheta_{i_j}^{n_j} \vartheta_{i_{j+1}}^{n_{j+1}} \ldots \vartheta_{i_{l-1}}^{n_{l-1}} \left(\frac{\vartheta_l}{\vartheta_{i_j}} \right)^{n_j} \ ,$$

and $n_j > 0$. Observe that if a summand

$$\pm \vartheta_{i_1}^{n_1} \vartheta_{i_2}^{n_2} \ldots \vartheta_{i_{l-1}}^{n_{l-1}} \ , \tag{5}$$

where $(i_1, \ldots, i_{l-1})$ is a permutation of $(1, \ldots, l-1)$ with $i_j > i_k$ and $n_j < n_k$, can be written in the form (3), then the summand S, obtained from (5) by exchanging the exponents of ϑ_{i_j} and ϑ_{i_k}, can also be written in the form (3). Indeed, for this summand S we have

$$S = \pm \vartheta_{n_1}^{i_1} \vartheta_{i_2}^{n_2} \ldots \vartheta_{i_{l-1}}^{n_{l-1}} \left(\frac{\vartheta_{i_j}}{\vartheta_{i_k}} \right)^{n_k - n_j} \ ,$$

and as the summand (5) can be written in the form (3), by $n_k - n_j > 0$ the same holds for the summand S. However, every summand can be obtained (up to sign) from the summand (4) with such changes of the exponents of the roots. Namely, let T be an arbitrary summand having the form

$$T = \pm \vartheta_1^{n_{i_1}} \vartheta_2^{n_{i_2}} \ldots \vartheta_{l-1}^{n_{i_{l-1}}} \ ,$$

where $(i_1, \ldots, i_{l-1})$ is a permutation of $(1, \ldots, l-1)$. We give a sequence of summands, with the property that every summand of the sequence is clearly obtained from the previous one by the above type changes of the exponents of two roots. We

start with the summand (4). By changing the exponents of adjacent roots only, from (4) we can get the summand

$$\vartheta_1^{n_{i_1}}\vartheta_2^{n_1}\vartheta_3^{n_2}\dots\vartheta_{i_1-1}^{n_{i_1-2}}\vartheta_{i_1}^{n_{i_1-1}}\vartheta_{i_1+1}^{n_{i_1+1}}\dots\vartheta_{l-1}^{n_{l-1}} ,$$

where the exponent of ϑ_1 is the same as in the summand T. Moreover, for $2 \le i < j \le l-1$ the exponent of ϑ_i is less than the exponent of ϑ_j. (The summand (4) also has this property, for $1 \le i < j \le l-1$.) Now we continue with the exponent n_{i_2} of ϑ_2 in T. By changing again the exponents of adjacent roots only, we can get the summand

$$\vartheta_1^{n_{i_1}}\vartheta_2^{n_{i_2}}\vartheta_3^{n_1}\dots\vartheta_{i_1-1}^{n_{i_1-3}}\vartheta_{i_1}^{n_{i_1-2}}\vartheta_{i_1+1}^{n_{i_1}}\dots\vartheta_{i_2-1}^{n_{i_2-2}}\vartheta_{i_2}^{n_{i_2-1}}\vartheta_{i_2+1}^{n_{i_2+1}}\dots\vartheta_{l-1}^{n_{l-1}} ,$$

where the exponents of ϑ_1 and ϑ_2 are the same as in the summand T. Moreover, for $3 \le i < j \le l-1$ the exponent of ϑ_i is less than the exponent of ϑ_j. (Here we assumed that $i_1 < i_2$, but the opposite case is similar.) Now we continue with n_{i_3}, and so on. Obviously, the last element of the sequence is the arbitrarily chosen summand T (up to sign), thus every summand can be transformed into the form (3). Now we can cancel out (4) from each summand of the expansion of the determinant D to obtain

$$D = \vartheta_1^{n_1}\vartheta_2^{n_2}\dots\vartheta_{l-1}^{n_{l-1}}(S_1 + S_2 + \dots + S_{l!}) ,$$

where for $t = 1, \dots, l!$ S_t is of the form

$$\pm\prod_{\substack{i,j=1\\ i<j}}^{l}\left(\frac{\vartheta_j}{\vartheta_i}\right)^{k_{ij}} .$$

Here the exponents k_{ij} are nonnegative integers, which are not all zero, except say S_1, for which $S_1 = 1$ holds. However, by the assumption made on the quotienst $\frac{|\vartheta_{i+1}|}{|\vartheta_i|}$, $i = 1, \dots, l-1$, we have $|\ S_1 + \dots + S_{l!}\ | > \frac{1}{l!}$. Hence $D \neq 0$, which is a contradiction, and Lemma 3 follows.

Lemma 4. *Let l and t be integers with $l \ge 2$ and $t \ge 3$. Let $\varepsilon_0 \in [0,2]$, $\varepsilon_i \in [0,1]$, $i = 1, \dots, l$ be rational numbers. Then for every natural number n with*

$$n > N = \frac{(2l^2 + l + 1)\log t}{\log(t^l + 1) - \log t^l}$$

and for every integer r with $0 \le r \le l$ the polynomial

$$P(x) = x^n - \sum_{j=0}^{l} t^{jn}\frac{\prod\limits_{\substack{i=0\\ i\neq j}}^{l}(x - t^i)}{\prod\limits_{\substack{i=0\\ i\neq j}}^{l}(t^j - t^i)} + \varepsilon_l x^l + \dots + \varepsilon_1 x + \varepsilon_0$$

has a (real) root in the open interval $(t^r - 1, t^r + 1)$, and $P(0) \neq 0$.

Proof. Let $l,\ t,\ \varepsilon_i$ be fixed for $i = 0, \ldots, l$. First we prove that if $n > N_1 = 4l^2 + 4l + 2$ then for $0 \leq r < l$

$$P(t^r - 1)P(t^r + 1) < 0 \tag{6}$$

holds. To do this, we show that in this case the sign of $P(t^r \pm 1)$ is 'ruled' by the term

$$m(x) = t^{ln} \frac{\prod_{i=0}^{l-1}(x - t^i)}{\prod_{i=0}^{l-1}(t^l - t^i)} \ ,$$

that is

$$sgn(P(t^r \pm 1)) = sgn(m(t^r \pm 1)) \ . \tag{7}$$

For the absolute value of $m(t^r \pm 1)$ we have

$$\mid m(t^r \pm 1) \mid > t^{ln - l^2} \ .$$

On the other hand, by a simple computation we get

$$\mid P(t^r \pm 1) - m(t^r \pm 1) \mid < t^{ln - \frac{n}{2} + l^2 + 2l + 1} \ ,$$

which proves (7). Since $m(t^r + 1)m(t^r - 1) < 0$ is trivial, for these values of r (6) is proved.

Now we turn to the case $r = l$. Clearly we have

$$P(t^l + 1) > (t^l + 1)^n - (l + 1)t^{ln + l^2} \ ,$$

but the right hand side of this inequality is positive if $n > N_2 = \frac{(l^2 + l)\log t}{\log(t^l + 1) - \log t^l}$. Further, we have

$$P(t^l - 1) < t^{l^2 + l + 1}(t^l - 1)^n - t^{ln - l^2} \ ,$$

with negative right hand side if $n > N_3 = \frac{(2l^2 + l + 1)\log t}{\log t^l - \log(t^l - 1)}$. This proves that if $n > \max\{N_1, N_2, N_3\}$, then the polynomial $P(x)$ has the desired properties ($P(0) \neq 0$ follows from (6) with $r = 0$). However, $N > \max\{N_1, N_2, N_3\}$, and Lemma 4 follows.

Lemma 5. *Let K be a field of characteristic 0, let $P(x) = a_d x^d + \ldots + a_1 x + a_0$ be a polynomial with rational coefficients and let n be an integer. If $P(x)$ does not divide any standard n-nomial with rational coefficients over $\mathbb{Q}$, then $P(x)$ does not divide over K any standard n-nomial with coefficients in K. Moreover, if s is an integer with the property that $P(x)$ does not divide any non-zero polynomial of degree less then s in x^r for any integer $r \geq 1$ with rational coefficients over $\mathbb{Q}$, then $P(x)$ does not divide over K any non-zero polynomial of degree less then s in x^r for any integer $r \geq 1$ with coefficients in K.*

Proof. We only prove here the first part of the statement, the second part can be proved in a similar way.

We can suppose that $d \geq n$, otherwise Lemma 5 is trivial. In the rest of the proof of Lemma 5, by a nontrivial coefficient of a polynomial we will mean a coefficient of

a nonconstant term of this polynomial. Suppose that for some fixed integer n the polynomial $P(x)$ does not divide any standard n-nomial over $\mathbb{Q}$. This means that for any integer m and for any non-zero polynomial $T(x) \in \mathbb{Q}[x]$ of degree at most m, the polynomial $P(x)T(x)$ has at least n non-zero nontrivial coefficients. This property can be formulated in the following way. (Without loss of generality we may suppose that $m \geq d$.) Consider the $m+1$ coefficients of the polynomial $T(x)$ as variables. The fact that P does not divide any standard n-nomial over $\mathbb{Q}$ means that among the nontrivial coefficients of $P(x)T(x)$ there are at most $m+d-n$ which are 0. In other words, fixing any $m+d-n$ nontrivial coefficients of $P(x)T(x)$, and choosing them as 0, the homogeneous linear system of equations (the variables are the coefficients of T) is not solvable over $\mathbb{Q}$. But this implies that this system of equations is not solvable over K, and (the first part of) Lemma 5 follows.

Now we are in a position to prove our Theorem.

Proof of the Theorem. By Lemma 5 we can suppose that $K = \mathbb{Q}$. Let k be an integer with $k \geq 6$ and let $L = k - 4$. Let t be an integer with

$$t > 2(L+1)! + 1 \ . \tag{9}$$

Let n be a prime with

$$n > \max\left\{C, \frac{(2L^2+L+1)\log t}{\log\left(t^L+1\right) - \log t^L}\right\} \ ,$$

where C is an arbitrary positive number. Denote by $Q(x)$ the polynomial

$$x^n - \sum_{j=0}^{L} t^{jn} \frac{\prod\limits_{\substack{i=0 \\ i\neq j}}^{L} (x - t^i)}{\prod\limits_{\substack{i=0 \\ i\neq j}}^{L} (t^j - t^i)} \ .$$

From Eisenstein's theorem it follows that there exist rational numbers $\varepsilon_0, \varepsilon_1, \ldots, \varepsilon_L$ with $\varepsilon_0 \in [0,2]$, $\varepsilon_i \in [0,1]$, $i = 1, \ldots, L$ such that the polynomial $P(x) = Q(x) + \varepsilon_L x^L + \ldots + \varepsilon_1 x + \varepsilon_0$ is irreducible over $\mathbb{Q}$. Indeed, the rational numbers ε_i, $i = 0, \ldots, L$ can be chosen in such a way that the above defined polynomial $P(x)$ will have integer coefficients, and that the coefficients of $P(x)$, except its leading coefficient, will be even, but its constant term will not be divisible by four. Now it follows from Eisenstein's theorem that the polynomial $P(x)$ so obtained is irreducible over $\mathbb{Q}$. (At this point we would like to remark that the coefficients of the polynomial Q in fact are integers. This assertion could be proved easily, however it is not needed in the proof of our Theorem, and we omit the details.) By Lemma 4 for every integer r with $0 \leq r \leq L$, $P(x)$ has a root ϑ_r in the interval $(t^r - 1, t^r + 1)$, and condition (9) implies that for the quotients of these roots we have

$$\frac{|\ \vartheta_{r+1}\ |}{|\ \vartheta_r\ |} < \frac{1}{(L+1)!} \ , r = 0, \ldots, L-1 \ .$$

Hence, by Lemma 3 $P(x)$ does not divide any $(k-3)$-nomial over $\mathbb{Q}$. Further, Lemma 2 implies that $P(x)$ does not divide any polynomial of degree less than n in x^r for any integer $r \geq 1$. On the other hand, by Lemma 3 $P(x)$ is clearly a standard $(k-2)$-nomial with non-zero constant term, and from Lemma 1 it follows that $P(x)$ divides infinitely many standard k-nomials with non-zero constant term over $\mathbb{Q}$. The proof of the Theorem is now complete.

Acknowledgements

I would like to thank Professor K. Győry for his generous and continuous help and for his many suggestions, and Professor A. Schinzel for his important and useful advice.

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.

Department of Mathematics and Informatics, Kossuth Lajos University, 4010 Debrecen, Pf. 12, Hungary

E-mail address: hajdul@math.klte.hu