ACTA ARITHMETICA
LXVII.3 (1994)

On the irreducibility of neighbouring polynomials

by

K. Győry (Debrecen)

To Professor W. M. Schmidt on his 60th birthday

1. Introduction. Denote by $|P|$ the length of a polynomial $P \in \mathbb{Z}[x]$, i.e. the sum of the absolute values of the coefficients of P. The purpose of this paper is to investigate the irreducibility of non-constant neighbouring polynomials over $\mathbb{Q}$. Here we say that two polynomials with integer coefficients are *neighbouring* if their difference is of relatively small length and small degree. By means of Eisenstein's irreducibility theorem it is easy to show that for given $P \in \mathbb{Z}[x]$ of degree m, there is an irreducible polynomial $Q \in \mathbb{Z}[x]$ with degree m such that $|P - Q| \le m + 2$. The following problem was proposed by P. Turán in 1962 (cf. [12]):

Does there exist an absolute constant c_1 such that for every $P \in \mathbb{Z}[x]$ of degree m, there is a polynomial $Q \in \mathbb{Z}[x]$ irreducible over $\mathbb{Q}$ and satisfying $\deg(Q) \le m$ and $|P - Q| \le c_1$?

This seems to be a very difficult problem. It becomes simpler if one removes the condition $\deg(Q) \le m$. It was proved by A. Schinzel [13] that for every $P \in \mathbb{Z}[x]$ of degree m there are infinitely many irreducible $Q \in \mathbb{Z}[x]$ such that

$$|P - Q| \le \begin{cases} 2 & \text{if } P(0) \ne 0, \\ 3 & \text{always.} \end{cases}$$

Further, one of them, say Q_0, satisfies

$$\deg(Q_0) \le \exp\{(5m + 7)(|P|^2 + 3)\}.$$

This nice result gives a partial answer to Turán's problem. The complete answer would require $\deg(Q_0) \le m$.

In what follows, $c_i(\cdot)$ $(i = 2, 3, \ldots)$ will denote constants which depend only on the parameters occurring in parentheses.

Research supported in part by Grant 1641 from the Hungarian National Foundation for Scientific Research and by the Mathematical Sciences Research Institute of Berkeley.

The next problem is concerned with the irreducibility of neighbouring polynomials of a special form. There exist several irreducibility theorems (for references see e.g. [7], [9] and [1]) for polynomials of the form $P(x) + b \in \mathbb{Z}[x]$, where P has more than $\deg(P)/2$ distinct integer zeros and $b \in \mathbb{Z}$ has relatively small absolute value. It follows from Hilbert's irreducibility theorem (see e.g. [14]) that for any given $P \in \mathbb{Z}[x]$, there are infinitely many $b \in \mathbb{Z}$ for which $P(x) + b$ is irreducible over $\mathbb{Q}$. For these polynomials, M. Szegedy proposed in 1984 the following problem:

Does there exist a constant $c_2 = c_2(m)$ such that for any $P \in \mathbb{Z}[x]$ of degree m, $P(x) + b$ is irreducible over $\mathbb{Q}$ for some $b \in \mathbb{Z}$ with $|b| \le c_2$?

For $m = 2$, such a bound $c_2(2)$ does exist and an appropriate choice is $c_2(2) = 2$. This follows from the fact that four square numbers cannot form an arithmetic progression. For $m > 2$, the problem is much more difficult. Denote by $\omega(a)$ the number of distinct prime factors of a non-zero integer a.

THEOREM 1. *Let $P \in \mathbb{Z}[x]$ be a polynomial of degree m with leading coefficient a_0. There exist an effectively computable number $c_3 = c_3(m, \omega(a_0))$ and a $b \in \mathbb{Z}$ with $|b| \le c_3$ for which $P(x) + b$ is irreducible over $\mathbb{Q}$.*

If P is monic, i.e. if $a_0 = 1$ then $\omega(a_0) = 0$. Thus, for monic polynomials P, Theorem 1 gives an affirmative answer to the problem of Szegedy.

We shall prove Theorem 1 with the explicit value

$$c_3 = \exp\exp\{(\omega + 1)^6 2^{19(m+1)!}\} \tag{1}$$

where $\omega = \omega(a_0)$. The proof depends on our explicit upper bound for the number of solutions of decomposable form equations (cf. [4] and Theorem 6 of the present paper). This bound has recently been improved by J. H. Evertse (private communication). Using this improvement, the above value of c_3 can be replaced by

$$c_3 = \exp\{(\omega + 1)\log(\omega + 2)(2^{17}m)^{m^3}\}. \tag{2}$$

The example $x^m + bx^k$ shows that Theorem 1 cannot be extended to polynomials of the form $P(x) + bx^k$ where $k \ge 1$.

When I obtained Theorem 1 I did not know about Szegedy's problem. I am grateful to Professor Schinzel for calling my attention to this problem and for his helpful remarks.

Several people, including I. Schur, A. and R. Brauer, G. Pólya, I. Seres and the author (for references see [2], [3] and [9]) investigated the reducibility of polynomials of the form $Q(P(x))$ over $\mathbb{Q}$, where $Q \in \mathbb{Z}[x]$ is a fixed irreducible monic polynomial and the $P \in \mathbb{Z}[x]$ are monic polynomials with a given splitting field. As a generalization of the situation considered in Theorem 1, we deal now with the case when $P \in \mathbb{Z}[x]$ is an arbitrary but fixed non-constant polynomial of degree m with leading coefficient a_0, and

the $Q \in \mathbb{Z}[x]$ are irreducible monic polynomials with a given splitting field, say K, over $\mathbb{Q}$. Let n denote the degree, and D_K the discriminant of K over $\mathbb{Q}$.

THEOREM 2. *Let P and K be as above. There exist an effectively computable number $c_4 = c_4(m, \omega(a_0), n, |D_K|)$ and an irreducible monic polynomial $Q \in \mathbb{Z}[x]$ with splitting field K and height $\leq c_4$ such that $Q(P(x))$ is irreducible over $\mathbb{Q}$.*

By the *height* of Q we mean the maximum absolute value of the coefficients of Q.

In the particular case $K = \mathbb{Q}$ the polynomials $Q(x)$ under consideration are of the form $x + b$, hence Theorem 1 is a special case of Theorem 2.

It is easy to verify that the constant c_4 must depend on $|D_K|$.

Let $\{p_1, \ldots, p_t\}$ be a finite (possibly empty) set of primes, and T the set of non-zero integers not divisible by primes different from $p_1, \ldots, p_t$. Further, let $P \in \mathbb{Z}[x]$ be a non-constant polynomial of degree m with leading coefficient a_0 and constant term a_m. Let k be an integer with $0 \leq k \leq m$, and put

$$a = \begin{cases} a_0 & \text{if } k = 0, \\ a_0 a_m & \text{if } 0 < k < m, \\ a_m & \text{if } k = m. \end{cases}$$

Assume that P has distinct zeros and that $a_m \neq 0$ if $k > 0$. Denote by $\omega_T(a)$ the number of distinct prime factors of a different from $p_1, \ldots, p_t$.

THEOREM 3. *Let P, T and k be as above. The number of reducible polynomials of the form $P(x) + bx^k$ with $b \in T$ is bounded above by an effectively computable number $c_5 = c_5(m, t + \omega_T(a) + 1)$.*

For $k > 0$, it is necessary to assume that $a_m \neq 0$. The assumption that P has distinct zeros is also necessary as is shown by the following example. If $P(x) = Q(x)^2$ for some $Q \in \mathbb{Z}[x]$, then $P(x) - b^2$ is reducible over $\mathbb{Q}$ for every $b \in T$.

For explicit values of c_5, we refer to Remark 2 in Section 3.

Denote by $|a|_T$ the T-free part of a non-zero rational integer a, i.e. the greatest positive divisor of a which is relatively prime to $p_1, \ldots, p_t$. Put $|0|_T = 0$. Let $|P|_T$ denote the sum of the T-free parts of the coefficients of $P \in \mathbb{Z}[x]$. For $t = 0$, we have $|a|_T = |a|$ and $|P|_T = |P|$.

We consider now an analogue of Turán's problem for $t > 0$. In contrast with the case $t = 0$, for $t > 0$ there are infinitely many $Q \in \mathbb{Z}[x]$ with $\deg(Q) \leq \deg(P)$ and $|P - Q|_T \leq 1$. Further, if P satisfies the assumptions of Theorem 3 then, by Theorem 3, almost all of these Q are irreducible over $\mathbb{Q}$. The following more precise result is an immediate consequence of Theorem 3.

THEOREM 4. *Let $t > 0$ and let $P(x) = a_0x^m + \ldots + a_m \in \mathbb{Z}[x]$ with $a_0a_m \neq 0$ and with distinct zeros. There are at most $(m+2) \times c_5(m, t+\omega_T(a_0a_m)+1)$ reducible polynomials $Q \in \mathbb{Z}[x]$ with $\deg(Q) \leq m$ and $|P-Q|_T \leq 1$.*

Here c_5 denotes the same constant as in Theorem 3.

In Theorem 4 it is also necessary to assume that the zeros of P are distinct. Further, the upper bound 1 for $|P-Q|_T$ cannot be replaced by 2. Indeed, for $P(x) = x^m - 1$ and $Q(x) = x^m - bx$ we get $|P-Q|_T = 2$ for all $b \in T$.

Theorems 1 to 3 will be proved in Section 3. We shall deduce Theorem 1 from Theorem 3. Further, we shall prove Theorems 3 and 2 by means of a more general irreducibility result (cf. Theorem 7 in Section 3), established over number fields.

Theorem 7 will be deduced from a general finiteness result (cf. Theorem 5 in Section 2) on resultant equations. Over number fields, Theorem 5 gives a quantitative version of Theorem 2 of [5]. Our Theorem 5 is a consequence of Theorem 6 which is concerned with decomposable form equations. Over number fields, it is a quantitative version of Theorem 3 of [5]. Theorem 6 follows from some results of the author [4] and [5] on decomposable form equations. We note that the proofs in [4] depend, among other things, on Schlickewei's p-adic quantitative version (cf. [16]) of Schmidt's Subspace Theorem [17]. It is interesting to observe that, in our Theorems 1 and 2, the use of an ineffective method leads to effective results.

2. Bound for the numbers of solutions of resultant equations. Let K be an algebraic number field with ring of integers O_K, and let M_K denote the set of places (equivalence classes of multiplicative valuations) of K. In every place v of M_K we choose a fixed valuation $|\cdot|_v$. Let S be a finite subset of M_K with cardinality s which contains all infinite places. Then

$$O_S = \{\alpha \in K : |\alpha|_v \leq 1 \text{ for all } v \in M_K \setminus S\}$$

is called the *ring of S-integers* and the units of O_S are called *S-units*. They form a multiplicative group which is denoted by O_S^*.

Let $P \in O_S[x]$ be a polynomial of degree $m \geq 2$ without multiple zeros and with splitting field G over K. Denote by D the degree of the normal closure of G over $\mathbb{Q}$. Consider the solutions of the *resultant equation*

$$\text{Res}(P, Q) \in O_S^* \quad \text{in } Q \in O_S[x]. \tag{3}$$

If Q is a solution of (3) then so is λQ for every $\lambda \in O_S^*$. Such solutions of (3) are called *proportional*. Equations of this type were studied by several authors; for references we refer to [5]. In [5], a general finiteness theorem has

been established for (3) in the more general situation when O_S is replaced by an arbitrary finitely generated integral domain over $\mathbb{Z}$. The next theorem is a quantitative version of this result in the case considered above.

THEOREM 5. *Let n be a positive integer with $2n < m$. Then up to a proportional factor from O_S^*, the number of solutions $Q(x)$ of (3) with degree n is at most $c_6 = c_6(n, D, s)$, where c_6 can be given explicitly. Further, in case of solutions $Q(x)$ with leading coefficients in O_S^*, the assumption $2n < m$ can be replaced by $2n \le m$.*

We prove Theorem 5 with the value

$$c_6 = (5sD)^{2^{37nD}s^6}. \tag{4}$$

It is easy to show that $D \le (dm)!$, where d denotes the degree of K over $\mathbb{Q}$. We note that Evertse's recent result mentioned in Section 1 enables one to prove Theorem 5 with

$$c_6 = (2^{34}m^2)^{n^3 s}. \tag{5}$$

In Theorem 5, it is necessary to assume that P has distinct zeros. Indeed, for $P(x) = x^m$, equation (3) takes the form

$$\mathrm{Res}(x^m, Q) = Q(0)^m \in O_S^*,$$

hence, if $s > 1$, it has infinitely many pairwise non-proportional solutions Q with $\deg(Q) = n$. Further, in the general case, $2n < m$ cannot be replaced by $2n \le m$ (see [5]).

Let $F(x_0, x_1, \ldots, x_n)$ $(n \ge 1)$ be a decomposable form of degree m with coefficients in O_S, i.e. a homogeneous polynomial which factorizes into linear factors over a finite extension G of K. Two solutions $\boldsymbol{x}$, $\boldsymbol{x}'$ of the *decomposable form equation*

$$F(x_0, x_1, \ldots, x_n) \in O_S^* \quad \text{in } \boldsymbol{x} = (x_0, \ldots, x_n) \in O_S^{n+1} \tag{6}$$

are called *proportional* if $\boldsymbol{x}' = \varepsilon\boldsymbol{x}$ for some $\varepsilon \in O_S^*$. Let D have the same meaning as in Theorem 5. Theorem 5 will be deduced from the following

THEOREM 6. *Suppose that there is an integer k with $n \le k - 1$ and $m > 2(k-1)$ such that any k linear factors in the factorization of F have rank $n + 1$. Then equation (6) has at most $c_6 = c_6(n, D, s)$ pairwise non-proportional solutions, where c_6 denotes the same bound as in Theorem 5.*

A more general but qualitative version was proved in [5] over an arbitrary finitely generated integral domain over $\mathbb{Z}$. Our Theorem 6 is an immediate consequence of Theorem 3 of [5] and of Corollary 2 of [4] concerning decomposable form equations. We note that the proof of Corollary 2 in [4] involves, among other things, an estimate of Schlickewei [15] for the number of solutions of S-unit equations. On combining the above-mentioned result

of Evertse with the proof of Theorem 3 of [5], Theorem 6 can be proved with the bound c_6 specified in (5).

Finally, we remark that a further application of Theorem 6 will be published in our paper [6].

P r o o f o f T h e o r e m 5. We shall follow the proof of Theorem 1 of [5]. Let $P \in O_S[x]$ be a polynomial of degree $m \geq 2$ without multiple zeros and with splitting field G over K. Further, let n be a positive integer with $2n \leq m$. We can write

$$P(x) = a_0(x - \alpha_1) \dots (x - \alpha_m),$$

where $a_0 \in O_S$ and $\alpha_1, \dots, \alpha_m$ are distinct elements of G.

First assume that $2n < m$. Consider an arbitrary polynomial

$$Q(x) = x_0 x^n + x_1 x^{n-1} + \dots + x_n$$

with degree n and coefficients in O_S which satisfies (3). Then (3) can be written in the form (6) where

$$F(x_0, x_1, \dots, x_n) = a_0^n \prod_{i=1}^{m} (x_0 \alpha_i^n + x_1 \alpha_i^{n-1} + \dots + x_n)$$

is a decomposable form of degree m with coefficients in O_S. This form F satisfies the conditions of our Theorem 6 with $k = n+1$. Hence the assertion of Theorem 5 follows from Theorem 6.

Next suppose that $2n = m$, and consider only those solutions $Q(x) = x_0 x^n + x_1 x^{n-1} + \dots + x_n$ of (3) in $O_S[x]$ for which $x_0 \in O_S^*$. Then we can write (3) in the form (6) with

$$F^*(x_0, \dots, x_n) = x_0 F(x_0, \dots, x_n)$$

instead of F, and the assertion follows again from Theorem 6. ∎

3. Applications to irreducible polynomials. In this section, we prove our irreducibility theorems. In the proofs, our Theorem 5 will be the main tool.

We keep the notation of Section 2. For $\alpha \in K \setminus \{0\}$, there are only finitely many $v \in M_K \setminus S$ for which $|\alpha|_v \neq 1$. In the sequel the number of these v will be denoted by $\omega_S(\alpha)$. If in particular $\alpha \in O_S^*$, then $\omega_S(\alpha) = 0$.

Let $P, Q \in O_S[x]$ be relatively prime polynomials over K such that P has distinct zeros and that $m = \deg(P) > \deg(Q)$. Let a_0 denote the leading coefficient of P, and put $\omega_S = \omega_S(a_0 \operatorname{Res}(P, Q))$. Further, denote by D the degree of the normal closure over $\mathbb{Q}$ of the splitting field of P over K.

The next theorem will be deduced from Theorem 5.

THEOREM 7. *The number of $\varepsilon \in O_S^*$ for which $P(x)+\varepsilon Q(x)$ is reducible over K is at most $c_7 = c_7(m, D, s+\omega_S)$, where c_7 can be given explicitly.*

We shall prove Theorem 7 with the value

$$c_7 = (5(s+\omega_S)D)^{2^{19mD(s+\omega_S)^6}}. \tag{7}$$

We note that using Theorem 5 with the value c_6 occurring in (5), we may take here

$$c_7 = m(2^{17}m)^{m^3(s+\omega_S)/4}. \tag{8}$$

It is easy to see that Theorem 7 does not remain valid in general if P and Q are not relatively prime or if the zeros of P are not distinct.

We remark that using Theorem 2 of [5] instead of our Theorem 5, a qualitative version of Theorem 7 can be proved in a more general form, over an arbitrary finitely generated and integrally closed integral domain over $\mathbb{Z}$.

Finally, we mention a reducibility result of K. Langmann [8] on polynomials of the form considered above. Let P and Q be as in Theorem 7, and suppose that Q also has distinct zeros. In [8] it is proved that if

$$(2+s)n \le \deg(P) + \deg(Q)$$

then there are only finitely many $\varepsilon \in \mathbb{Z}$ with at most s prime divisors such that $P(x)+\varepsilon Q(x)$ has a polynomial divisor of degree $\le n$ in $K[x]$.

Proof of Theorem 7. Suppose that P, Q satisfy the assumptions of Theorem 7. Let n be a positive integer with $n \le m/2$, and consider those $\varepsilon \in O_S^*$ for which

$$F_\varepsilon(x) := P(x) + \varepsilon Q(x)$$

has a polynomial divisor of degree n over K. Then for each of these ε, $F_\varepsilon(x)$ can be factorized over K in the form

$$F_\varepsilon(x) = Q_1(x)Q_2(x), \tag{9}$$

where Q_1 is a polynomial of degree n. Denote by S' the set of places of K which consists of the elements of S and those $v \in M_K \setminus S$ for which $|a_0 \operatorname{Res}(P,Q)|_v \ne 1$. Then S' is finite and $O_{S'}$, the ring of S'-integers in K, is integrally closed in K. Further, by the choice of S' the leading coefficient of F_ε is an S'-unit. Hence we may assume that Q_1 and Q_2 have their coefficients in $O_{S'}$. This implies that the leading coefficient of Q_1 is an S'-unit.

Using some well-known properties of resultants (see e.g. [19]), from (9) we get

$$\operatorname{Res}(F_\varepsilon, P) = \operatorname{Res}(Q_1, P)\operatorname{Res}(Q_2, P) \tag{10}$$

where both $\mathrm{Res}(Q_1, P)$ and $\mathrm{Res}(Q_2, P)$ are elements of $O_{S'}$. On the other hand, we have

$$\mathrm{Res}(F_\varepsilon, P) = a_0^{m-n} \mathrm{Res}(\varepsilon Q, P) = a_0^{m-n} \varepsilon^m \mathrm{Res}(Q, P). \tag{11}$$

But a_0, ε and $\mathrm{Res}(P, Q)$ are elements of $O_{S'}^*$, the group of S'-units. Thus (10) and (11) give

$$\mathrm{Res}(P, Q_1) \in O_{S'}^*. \tag{12}$$

If, for some $\varepsilon' \in O_S^*$ with $\varepsilon' \neq \varepsilon$, $F_{\varepsilon'}(x) := P(x) + \varepsilon' Q(x)$ has a polynomial divisor, say Q_1', over K with degree n, then Q_1' cannot be of the form λQ_1 with $\lambda \in O_{S'}^*$. Indeed, for $Q_1'(x) = \lambda Q_1(x)$, $\lambda \in O_{S'}^*$, we would deduce from (9) that $Q_1(x)$ divides $(\varepsilon - \varepsilon')P(x)$ over K, contrary to the assumption that P and Q are relatively prime over K. Thus, to derive an upper bound for the number of ε under consideration, it is enough to give an upper bound for the number of pairwise non-proportional solutions $Q_1(x)$ of degree n of equation (12). However, it follows from Theorem 5 that the latter number is at most $c_6(n, D, s + \omega_S)$ where c_6 denotes the same bound as in Theorem 5. Consequently, the total number of $\varepsilon \in O_S^*$ for which $F_\varepsilon(x)$ is reducible over K is at most

$$(m/2) c_6(m/2, D, s + \omega_S).$$

This completes the proof of Theorem 7. ∎

Remark 1. It is clear from the above proof that using Theorem 5 with c_6 specified in (4), the expression given in (7) is an appropriate choice for c_7 in Theorem 7. Similarly, by applying Theorem 5 with c_6 specified in (5) we may take for c_7 the expression in (8).

Proof of Theorem 3. To prove Theorem 3, we apply Theorem 7 with $K = \mathbb{Q}$, $Q(x) = x^k$. Let S denote the set of places of $\mathbb{Q}$ consisting of the ordinary absolute value and of the finite places determined by $p_1, \ldots, p_t$. Then S is of cardinality $t + 1$. Denote by D the degree of the splitting field of P over $\mathbb{Q}$, and by ω_T the number of distinct prime factors of a different from $p_1, \ldots, p_t$. Then $\omega_S(a) = \omega_T$.

First assume that $0 < k < m$. Then $\mathrm{Res}(P, x^k) = a_m^k$. It follows from Theorem 7 that the number of reducible polynomials of the form $P(x) + bx^k$ with $b \in T$ is at most $c_7(m, D, (t+1) + \omega_T)$ with the c_7 occurring in Theorem 7. Since $D \leq m!$, $c_7(m, m!, (t+1) + \omega_T)$ is an appropriate choice for $c_5(m, t + \omega_T(a) + 1)$.

Next assume that $k = 0$. Then, by definition, $a = a_0$ and $\mathrm{Res}(P, 1) = 1$. Thus Theorem 3 follows from Theorem 7 in the same way as above.

Finally, assume that $k = m$. Then we can apply Theorem 7 to the polynomials $x^m P(1/x) + b$ instead of $P(x) + bx^k$, and the assertion follows. ∎

R e m a r k 2. On using the explicit values of c_7 given in (7) or (8), the above proof provides immediately explicit values for c_5.

P r o o f o f T h e o r e m 1. Let $P \in \mathbb{Z}[x]$ be a polynomial of degree m with leading coefficient a_0. First we show that there exists a $b_0 \in \mathbb{Z}$ with $0 < b_0 \le m$ such that $P(x)+b_0$ has no multiple zeros. Indeed, if $P(x)+b_0$ has a multiple zero then $P(\alpha)+b_0 = 0$ for some zero α of $P'(x)$. But $P'(x)$ has at most $m-1$ zeros. Hence for at least one of the numbers $b_0 = 1, 2, \ldots, m$, $P(x)+b_0$ has no multiple zeros.

In what follows, we fix a $b_0 \in \mathbb{Z}$ with $0 < b_0 \le m$ such that $P_0(x) := P(x)+b_0$ has no multiple zeros. We shall deduce Theorem 1 from Theorem 3 with $k = 0$. Let ω denote the number of distinct prime factors of a_0, and let $t = \omega + 1$. Denote by p_i the ith prime number, and by T the set of non-zero integers not divisible by primes different from $p_1, \ldots, p_t$. Clearly $\omega_T(a_0) \le \omega$. Set

$$c_8 = c_5(m, t+\omega+1) = c_5(m, 2(\omega+1))$$

and

$$C = [4\log(t+1)c_8^{1/t}] + 1,$$

where c_5 denotes the number occurring in Theorem 3.

Consider in T the numbers of the form

$$b_1 = p_1^{a_1} \ldots p_t^{a_t}$$

where a_i runs through the numbers $0, 1, \ldots, [C/\log p_i]$, $i = 1, \ldots, t$. The number of these b_1's is

$$\prod_{i=1}^{t} ([C/\log p_i] + 1).$$

We have (cf. [11])

$$\sum_{i=1}^{t} \log p_i < p_t \log 4 < 4t\log(t+1).$$

Thus we infer that

$$\log p_1 \ldots \log p_t < \left(\frac{\log p_1 + \ldots + \log p_t}{t}\right)^t < (4\log(t+1))^t.$$

Hence, for the number of b_1's under consideration we get the following lower estimates:

$$\prod_{i=1}^{t} ([C/\log p_i] + 1) > \frac{C^t}{\log p_1 \ldots \log p_t} > \left(\frac{C}{4\log(t+1)}\right)^t > c_8.$$

By Theorem 3, for at least one of the numbers b_1 under consideration, $P_0(x) + b_1$ is irreducible over $\mathbb{Q}$. Considering this b_1 in the form $p_1^{a_1} \ldots p_t^{a_t}$,

we infer that

$$\log b_1 = \sum_{i=1}^{t} a_i \log p_i \le \sum_{i=1}^{t} [C/\log p_i] \log p_i \le tC$$
$$= t([4\log(t+1)c_8^{1/t}] + 1).$$

Now the assertion follows with

$$c_3 = m + \exp\{5(\omega+1)\log(\omega+2)c_8^{1/(\omega+1)}\}. \quad (13)$$ ∎

Remark 3. Using Remark 2 and (13), it is easy to derive the explicit values of c_3 given in (1) and (2).

To prove Theorem 2, we need the following.

Lemma (Capelli). *Let $P, Q \in \mathbb{Z}[x]$ be non-constant polynomials, and suppose that Q is monic and irreducible over $\mathbb{Q}$. Further, let β be one of the zeros of Q. Then $Q(P(x))$ is irreducible over $\mathbb{Q}$ if and only if $P(x) - \beta$ is irreducible over $\mathbb{Q}(\beta)$.*

Proof. See [20] or [10]. We remark that Capelli proved this theorem in a less general form (cf. [20]).

Proof of Theorem 2. Let $P \in \mathbb{Z}[x]$ be a polynomial of degree $m \ge 1$ with leading coefficient a_0, and let $K/\mathbb{Q}$ be a finite normal extension. As was shown in the proof of Theorem 1, there is an integer b_0 with $1 \le b_0 \le m$ such that $P_0(x) := P(x) + b_0$ has distinct zeros. Denote by O_K the ring of integers of K, and by n and D_K the degree and discriminant of K, respectively. By the above lemma, it suffices to prove that there are an effectively computable $c_9 = c_9(m, \omega(a_0), n, |D_K|)$ and a primitive integral element β in K with height at most c_9 such that the polynomial $P_0(x) - \beta$ is irreducible over K.

There is a primitive integral element α in K with $\overline{|\alpha|} \le |D_K|^{1/2}$ (see e.g. [18]), where $\overline{|\alpha|}$ denotes the maximum absolute value of the conjugates of α. This implies that

$$|N_{K/\mathbb{Q}}(\alpha)| \le |D_K|^{n/2}.$$

Denote by S the subset of M_K (the set of places of K) which consists of all infinite places and of the finite places determined by the prime ideals in O_K with norms not exceeding $(2|D_K|^{1/2})^n$. The cardinality of S is at most $n((2|D_K|^{1/2})^n + 1)$. The numbers $2^a\alpha$ are S-units in K for all non-negative rational integers a. We now apply Theorem 7 over $\mathbb{Q}$ with $Q(x) \equiv 1$ and we use the fact that here D, the degree of the splitting field of P, is at most $m!$ and $\omega_S(a_0 \operatorname{Res}(P, 1)) \le \omega(a_0)$. By Theorem 7, there exists an effectively computable number $c_{10} = c_{10}(m, \omega(a_0), n, |D_K|)$ such that the number of non-negative integers a for which $P_0(x) - 2^a\alpha$

is reducible over K is at most c_{10}. Consequently, there is a non-negative integer a with $a \leq c_{10}$ such that $P_0(x) - 2^a\alpha$ is irreducible over K. Put $\beta = 2^a\alpha$. Then β is a primitive integral element in K and has height at most $c_{11} = c_{11}(m, \omega(a_0), n, |D_K|)$, where c_{11} is effectively computable. This completes the proof of Theorem 2. ∎

References

[1] R. K. Guy (ed.), *Reviews in Number Theory, 1973–83*, Vol. I, Ch. C, Amer. Math. Soc., Providence, R.I., 1984.

[2] K. Győry, *On the irreducibility of a class of polynomials, III*, J. Number Theory 15 (1982), 164–181.

[3] —, *On the irreducibility of a class of polynomials, IV*, Acta Arith. 62 (1992), 399–405.

[4] —, *On the numbers of solutions of systems of decomposable form equations*, Publ. Math. Debrecen 42 (1993), 65–101.

[5] —, *Some applications of decomposable form equations*, Colloq. Math. 65 (1993), 267–275.

[6] —, *On a problem of A. M. Odlyzko on algebraic units of bounded degree*, Acta Math. Hungar., to appear.

[7] K. Győry and J. Rimán, *On irreducibility criteria of Schur type*, Mat. Lapok 24 (1973), 225–253 (in Hungarian).

[8] K. Langmann, *Der Hilbertsche Irreduzibilitätssatz und Primzahlfragen*, J. Reine Angew. Math. 413 (1991), 213–219.

[9] W. J. LeVeque (ed.), *Reviews in Number Theory, 1940–72*, Vol. I, Ch. C, Amer. Math. Soc., Providence, R.I., 1974.

[10] L. Rédei, *Algebra*, Akadémiai Kiadó, Budapest, 1967.

[11] J. B. Rosser and L. Schoenfeld, *Approximate formulas for some functions of prime numbers*, Illinois J. Math. 6 (1962), 64–94.

[12] A. Schinzel, *Reducibility of polynomials and covering systems of congruences*, Acta Arith. 13 (1967), 91–101.

[13] —, *Reducibility of lacunary polynomials II*, ibid. 16 (1970), 371–392.

[14] —, *Selected Topics on Polynomials*, University of Michigan, Ann Arbor, 1982.

[15] H. P. Schlickewei, *S-unit equations over number fields*, Invent. Math. 102 (1990), 95–107.

[16] —, *The quantitative Subspace Theorem for number fields*, Compositio Math. 82 (1992), 245–273.

[17] W. M. Schmidt, *Simultaneous approximation to algebraic numbers by elements of a number field*, Monatsh. Math. 79 (1975), 55–66.

[18] T. N. Shorey and R. Tijdeman, *Exponential Diophantine Equations*, Cambridge University Press, 1986.

[19] R. G. Swan, *Factorization of polynomials over finite fields*, Pacific J. Math. 12 (1962), 1099–1106.

[20] N. Tschebotaröw und H. Schwerdtfeger, *Grundzüge der Galois'schen Theorie*, Noordhoff, Groningen/Djakarta, 1950.

MATHEMATICAL INSTITUTE
KOSSUTH LAJOS UNIVERSITY
H-4010 DEBRECEN, HUNGARY

Received on 24.4.1994 (2607)