ACTA ARITHMETICA
113.2 (2004)

Upper bounds for the number of factors for a class of polynomials with rational coefficients

by

Nicolae Ciprian Bonciocat (Bucureşti)

1. Introduction. Some results related to Hilbert's irreducibility theorem have been provided in [1]–[4]. In [1] it is shown that for any relatively prime polynomials $f(X), g(X) \in \mathbb{Q}[X]$ with $\deg f < \deg g$, the polynomial $f(X)+pg(X)$ is irreducible over $\mathbb{Q}$ for all but finitely many prime numbers p. In [2] this result has been improved by providing an explicit lower bound b depending on f and g, such that for all primes $p > b$, the polynomial $f(X) + pg(X)$ is irreducible over $\mathbb{Q}$.

Let now $f, g \in \mathbb{Q}[X]$ be relatively prime polynomials with $\deg f \le \deg g$.

In the present paper we adapt the method in [2] in order to provide explicit upper bounds for the number of factors over $\mathbb{Q}$ of the polynomials $n_1 f(X)+n_2 g(X)$, where n_1 and n_2 are nonzero integers with absolute value of n_2/n_1 greater than an explicit lower bound b. Here and henceforth, by the number of factors of a polynomial f we shall understand the number of irreducible factors of f counted with multiplicities.

We treat separately the cases $\deg f < \deg g$ and $\deg f = \deg g$.

In the first case we prove that for any nonzero integers n_1 and n_2 with absolute value of n_2/n_1 greater than an explicit lower bound b depending on f and g, the number of factors over $\mathbb{Q}$ of the polynomial $n_1 f(X) + n_2 g(X)$ cannot exceed the total number of prime factors of n_2 counting multiplicities. We actually prove a slightly more general version of this result, in which the lower bound b and the upper bound for the number of factors depend on a suitable divisor of n_2. As a corollary we find an improved form of the irreducibility criterion given in [2, Th. 1]. Sharper bounds are then obtained for polynomials with integral coefficients. We finally consider the case when the polynomial $n_1 f(X) + n_2 g(X)$ has no rational roots.

2000 *Mathematics Subject Classification*: Primary 11C08.

This work was partially supported by the CERES Program of the Romanian Ministry of Education, Youth and Research, contract no. 39/2002 and by the EURROMMAT program ICA1-CT-2000-70022 of the European Commission.

Similar results are provided in the case $\deg f = \deg g$.

For any polynomial $f \in \mathbb{Q}[X]$ of degree k, we write $f(X)$ uniquely in the reduced form

$$f(X) = \frac{a_0 + a_1 X + \ldots + a_k X^k}{q},$$

where $q, a_0, \ldots, a_k \in \mathbb{Z}$, $a_k \neq 0$, $q \geq 1$, q as small as possible. Then for this reduced form we set

$$H(f) = \max\{|a_0|, |a_1|, \ldots, |a_k|, q\}, \qquad M(f) = \max\{|a_0|, |a_1|, \ldots, |a_k|\}.$$

For any integer n with $|n| > 1$, we denote by $\Omega(n)$ the total number of prime factors of n counting multiplicities.

In the case $\deg f < \deg g$ we prove the following results:

THEOREM 1. *Let $f(X)$, $g(X) \in \mathbb{Q}[X]$ be relatively prime polynomials with $k = \deg f < \deg g = m$. Then for any nonzero integers n_1, n_2 and any positive divisor d of n_2 such that*

$$\left|\frac{n_2}{n_1}\right| > \left(2 + \frac{1}{2^{k+1} d^m}\right)^{k+1} d^m H(f)^m H(g)^{m+1},$$

the polynomial $n_1 f(X) + n_2 g(X)$ has at most $\Omega(n_2/d)$ factors over $\mathbb{Q}$.

COROLLARY 1. *For any relatively prime polynomials $f(X), g(X) \in \mathbb{Q}[X]$ with $k = \deg f < \deg g = m$, and any prime p satisfying*

$$p > \left(2 + \frac{1}{2^{k+1}}\right)^{k+1} H(f)^m H(g)^{m+1},$$

the polynomial $f(X) + pg(X)$ is irreducible over $\mathbb{Q}$.

COROLLARY 2 (of the proof of Theorem 1). *Let $f(X), g(X) \in \mathbb{Z}[X]$ be relatively prime polynomials with $k = \deg f < \deg g = m$. Then for any nonzero integers n_1, n_2 and any positive divisor d of n_2 such that*

$$\left|\frac{n_2}{n_1}\right| > \left(2 + \frac{1}{2^{k+1} d^m H(g)^{m+1}}\right)^{k+1} d^m H(f) H(g)^m,$$

the polynomial $n_1 f(X) + n_2 g(X)$ has at most $\Omega(n_2/d)$ nonconstant factors over $\mathbb{Z}$.

We also prove a result similar to Theorem 1 in the case when the polynomial $n_1 f(X) + n_2 g(X)$ has no rational roots:

THEOREM 2. *Let $f(X), g(X) \in \mathbb{Q}[X]$ be relatively prime polynomials with $k = \deg f < \deg g = m$. Then for any nonzero integers n_1, n_2 and any positive divisor d of n_2 such that*

$$\left|\frac{n_2}{n_1}\right| > \left(2 + \frac{1}{2^{k+1} d^{m/2}}\right)^{k+1} d^{m/2} H(f)^{m/2} H(g)^{1+\max(m/2,k)},$$

if the polynomial $n_1 f(X)+n_2 g(X)$ *has no rational roots, then it has at most* $\Omega(n_2/d)$ *factors over* $\mathbb{Q}$.

Corollary 3 (of the proof of Theorem 2). *Let* $f(X)$, $g(X) \in \mathbb{Z}[X]$ *be relatively prime polynomials with* $k = \deg f < \deg g = m$. *Then for any nonzero integers* n_1, n_2 *and any positive divisor* d *of* n_2 *such that*

$$\left|\frac{n_2}{n_1}\right| > \left(2 + \frac{1}{2^{k+1} d^{m/2} H(g)^{1+\max(m/2,k)}}\right)^{k+1} d^{m/2} H(f) H(g)^{\max(m/2,k)},$$

if the polynomial $n_1 f(X)+n_2 g(X)$ *has no rational roots, then it has at most* $\Omega(n_2/d)$ *nonconstant factors over* $\mathbb{Z}$.

In the case $\deg f = \deg g$ we prove the following results:

Theorem 3. *Let*

$$f(X) = \frac{a_0 + a_1 X + \ldots + a_m X^m}{q_1}, \qquad g(X) = \frac{b_0 + b_1 X + \ldots + b_m X^m}{q_2}$$

be relatively prime polynomials in $\mathbb{Q}[X]$ *of degree* m, *written in reduced form. Let also* n_1, n_2 *be nonzero integers,* $h = (n_1 a_m q_2 + n_2 b_m q_1)/\gcd(q_1, q_2)$ *and* d *a positive divisor of* h. *If*

$$\left|\frac{n_2}{n_1}\right| > d^m H(f) H(g) \left(1 + H(f)H(g) + \frac{1}{2^m d^m}\right)^{m+1},$$

then the polynomial $n_1 f(X) + n_2 g(X)$ *has at most* $\Omega(h/d)$ *factors over* $\mathbb{Q}$.

Corollary 4. *Let* $f(X)$ *and* $g(X)$ *be as in Theorem* 3. *If* n_1 *and* n_2 *are nonzero integers such that* $|(n_1 a_m q_2 + n_2 b_m q_1)/\gcd(q_1, q_2)|$ *is a prime and*

$$\left|\frac{n_2}{n_1}\right| > H(f) H(g) \left(1 + H(f)H(g) + \frac{1}{2^m}\right)^{m+1},$$

then the polynomial $n_1 f(X) + n_2 g(X)$ *is irreducible over* $\mathbb{Q}$.

Corollary 5 (of the proof of Theorem 3). *Let* $f(X)$, $g(X) \in \mathbb{Z}[X]$ *be relatively prime polynomials of degree* m, *with leading coefficients* a_m *and* b_m *respectively. Let* n_1 *and* n_2 *be nonzero integers,* $h = n_1 a_m + n_2 b_m$ *and* d *a positive divisor of* h. *If*

$$\left|\frac{n_2}{n_1}\right| > d^m H(f) \left(1 + H(g) + \frac{1}{d^m [1 + H(g)]^m}\right)^{m+1},$$

then $n_1 f(X) + n_2 g(X)$ *has at most* $\Omega(h/d)$ *nonconstant factors over* $\mathbb{Z}$.

In particular, we have

Corollary 6. *Let* $f(X), g(X) \in \mathbb{Z}[X]$ *be relatively prime polynomials of degree* m, *with leading coefficients* a_m *and* b_m *respectively. If* n_1 *and* n_2

are nonzero integers such that $|n_1a_m + n_2b_m|$ *is a prime number and*

$$\left|\frac{n_2}{n_1}\right| > H(f)\left(1 + H(g) + \frac{1}{[1+H(g)]^m}\right)^{m+1},$$

then the polynomial $n_1f(X) + n_2g(X)$ *is irreducible over* $\mathbb{Z}$.

The proofs of these results are presented in Sections 2 and 3 below.

2. The case $\deg f < \deg g$

2.1. *Proof of Theorem 1.* Let

$$f(X) = \frac{a_0 + a_1X + \ldots + a_kX^k}{q_1} \quad \text{and} \quad g(X) = \frac{b_0 + b_1X + \ldots + b_mX^m}{q_2}$$

be two relatively prime polynomials in $\mathbb{Q}[X]$ written in reduced form, with $k = \deg f < \deg g = m$, and let also n_1, n_2 and d be as in the statement of the theorem. Our assumption on n_1, n_2 and d shows that $|n_2| > d$, so $\Omega(n_2/d)$ makes sense. We may obviously assume $\Omega(n_2/d) < m$.

We write $g(X)$ in the following form:

$$g(X) = \frac{b_0 + b_1X + \ldots + b_mX^m}{q_2} = \frac{\overline{b}\overline{g}(X)}{q_2},$$

where $\overline{b} \in \mathbb{Z}$ and $\overline{g}(X) \in \mathbb{Z}[X]$, $\overline{g}(X)$ primitive. Then we write

$$n_1f(X) + n_2g(X) = \frac{a}{q}F(X),$$

with $\gcd(a, q) = 1$ and $F(X) \in \mathbb{Z}[X]$, $F(X)$ primitive. Assume now that $n_1f(X)+n_2g(X)$ has more than $\Omega(n_2/d)$ factors. Then by Gauss's Lemma, $F(X)$ decomposes as $F(X) = F_1(X)\ldots F_s(X)$ with $\Omega(n_2/d) < s \le m$ and $F_1(X), \ldots, F_s(X) \in \mathbb{Z}[X]$, $F_1, \ldots, F_s$ primitive with $\deg F_1, \ldots, \deg F_s \ge 1$. Let $t_1, \ldots, t_s \in \mathbb{Z}$ be the leading coefficients of $F_1, \ldots, F_s$, respectively. Then one finds

$$t_1 \ldots t_s = \frac{n_2qb_m}{aq_2}.$$

If $q/q_2 = \beta/\gamma$ with $\gcd(\beta, \gamma) = 1$, then β divides q_1, since q divides q_1q_2. Therefore we have $a\gamma t_1 \ldots t_s = n_2\beta b_m$, and since $\Omega(n_2/d) < s$, at least one of the t_i's, say t_1, divides $d\beta b_m$. So we have

$$|t_1| \le dq_1|b_m|. \tag{1}$$

Now we are going to estimate the resultant $R(\overline{g}, F_1)$. Since $\overline{g}$ and F_1 are relatively prime, $R(\overline{g}, F_1)$ must be a nonzero integer, so in particular

$$|R(\overline{g}, F_1)| \ge 1. \tag{2}$$

If we decompose F_1, say $F_1(X) = t_1(X-\theta_1)\dots(X-\theta_r)$, then

$$|R(\overline{g}, F_1)| = |t_1|^m \prod_{1\le j\le r} |\overline{g}(\theta_j)|. \tag{3}$$

Since each root θ_j of F_1 is also a root of $F(X)$, we have

$$g(\theta_j) = -\frac{n_1 f(\theta_j)}{n_2} \tag{4}$$

and moreover, since f and g are relatively prime, $f(\theta_j) \neq 0$ and $g(\theta_j) \neq 0$ for any $j \in \{1,\dots,r\}$. The definition of $\overline{g}$ shows that

$$|\overline{g}(\theta_j)| \le q_2 |g(\theta_j)|. \tag{5}$$

Using now (3)–(5) we obtain

$$|R(\overline{g}, F_1)| \le |t_1|^m \frac{q_2^r |n_1|^r}{|n_2|^r} \prod_{1\le j\le r} |f(\theta_j)|. \tag{6}$$

We now proceed to find an upper bound for $|f(\theta_j)|$. The equality $n_1 f(\theta_j) + n_2 g(\theta_j) = 0$ implies

$$\left(\frac{n_1a_0}{q_1}+\frac{n_2b_0}{q_2}\right)+\dots+\left(\frac{n_1a_k}{q_1}+\frac{n_2b_k}{q_2}\right)\theta_j^k+\frac{n_2b_{k+1}}{q_2}\,\theta_j^{k+1}+\dots+\frac{n_2b_m}{q_2}\,\theta_j^m=0,$$

from which we deduce that

$$\begin{aligned}\frac{|n_2b_m|}{q_2}\,|\theta_j|^m &\le \left(\frac{|n_1a_0|}{q_1}+\frac{|n_2b_0|}{q_2}\right)+\dots+\left(\frac{|n_1a_k|}{q_1}+\frac{|n_2b_k|}{q_2}\right)|\theta_j|^k\\ &\quad+\frac{|n_2b_{k+1}|}{q_2}\,|\theta_j|^{k+1}+\dots+\frac{|n_2b_{m-1}|}{q_2}\,|\theta_j|^{m-1}\\ &\le \left(\frac{|n_1|M(f)}{q_1}+\frac{|n_2|M(g)}{q_2}\right)(1+|\theta_j|+\dots+|\theta_j|^{m-1}).\end{aligned}$$

Therefore, either $|\theta_j| \le 1$, or if not, then

$$\frac{|n_2b_m|}{q_2}\,|\theta_j|^m < \left(\frac{|n_1|M(f)}{q_1}+\frac{|n_2|M(g)}{q_2}\right)\frac{|\theta_j|^m}{|\theta_j|-1},$$

so in both cases we have

$$|\theta_j| < 1 + \frac{1}{|b_m|}\left(\frac{|n_1|q_2}{|n_2|q_1}\,M(f)+M(g)\right). \tag{7}$$

Now, since obviously

$$|f(\theta_j)| \le \frac{M(f)}{q_1}\,(1+|\theta_j|+\dots+|\theta_j|^k),$$

inequality (7) yields

$$|f(\theta_j)| < \frac{M(f)}{q_1}\cdot\frac{\left[1+\frac{1}{|b_m|}\left(\frac{|n_1|q_2}{|n_2|q_1}M(f)+M(g)\right)\right]^{k+1}-1}{\frac{1}{|b_m|}\left(\frac{|n_1|q_2}{|n_2|q_1}M(f)+M(g)\right)}. \tag{8}$$

Instead of (8) it will be more convenient to consider

$$(9)\qquad |f(\theta_j)| < \frac{|b_m|M(f)}{q_1}\cdot\frac{\left[1+\frac{1}{|b_m|}\left(\frac{|n_1|q_2}{|n_2|q_1}M(f)+M(g)\right)\right]^{k+1}}{\frac{|n_1|q_2}{|n_2|q_1}M(f)+M(g)}.$$

Using now (6) and (9), we obtain

$$|R(\overline{g},F_1)| < |t_1|^m\left[\frac{|n_1|q_2}{|n_2|q_1}M(f)\,\frac{|b_m|\left[1+\frac{1}{|b_m|}\left(\frac{|n_1|q_2}{|n_2|q_1}M(f)+M(g)\right)\right]^{k+1}}{\frac{|n_1|q_2}{|n_2|q_1}M(f)+M(g)}\right]^r.$$

Since $r\geq 1$, all we need to prove is that our assumption on n_1, n_2 and d forces

$$|t_1|^m\cdot\frac{|b_m|\left[1+\frac{1}{|b_m|}\left(\frac{|n_1|q_2}{|n_2|q_1}M(f)+M(g)\right)\right]^{k+1}}{1+\frac{|n_2|q_1M(g)}{|n_1|q_2M(f)}} < 1.$$

In view of (1), it is sufficient to prove that

$$d^mq_1^m|b_m|^{m+1}\left[1+\frac{1}{|b_m|}\left(\frac{|n_1|q_2}{|n_2|q_1}M(f)+M(g)\right)\right]^{k+1} < 1+\frac{|n_2|q_1M(g)}{|n_1|q_2M(f)},$$

which is equivalent to

$$(10)\qquad d^mq_1^m|b_m|^{m-k}\left(|b_m|+M(g)+\frac{|n_1|q_2}{|n_2|q_1}M(f)\right)^{k+1} < 1+\frac{|n_2|q_1M(g)}{|n_1|q_2M(f)}.$$

Now since $|b_m|\leq M(g)$, it suffices to prove that

$$d^mq_1^mM(g)^{m+1}\left(2+\frac{|n_1|q_2M(f)}{|n_2|q_1M(g)}\right)^{k+1} < \frac{|n_2|q_1M(g)}{|n_1|q_2M(f)},$$

or equivalently,

$$(11)\qquad \left|\frac{n_2}{n_1}\right| > d^mq_1^{m-1}q_2M(f)M(g)^m\left(2+\frac{q_2M(f)}{\left|\frac{n_2}{n_1}\right|q_1M(g)}\right)^{k+1}.$$

We search for a suitable δ such that if $|n_2/n_1| > \delta\cdot d^mq_1^{m-1}q_2M(f)M(g)^m$, then $|n_2/n_1|$ also satisfies (11). So it is sufficient to find a δ satisfying

$$\delta > \left(2+\frac{1}{\delta\cdot d^mq_1^mM(g)^{m+1}}\right)^{k+1}.$$

Denote $d^mq_1^mM(g)^{m+1}$ by w. A suitable candidate for δ is $\left(2+\frac{1}{2^{k+1}w}\right)^{k+1}$, since

$$\left(2+\frac{1}{2^{k+1}w}\right)^{k+1} > \left(2+\frac{1}{\left(2+\frac{1}{2^{k+1}w}\right)^{k+1}w}\right)^{k+1}.$$

This proves that for

$$(12)\qquad \left|\frac{n_2}{n_1}\right| > \left(2+\frac{1}{2^{k+1}d^m q_1^m M(g)^{m+1}}\right)^{k+1} d^m q_1^{m-1} q_2 M(f) M(g)^m$$

we have $|R(\overline{g},F_1)|<1$, which contradicts (2). The desired conclusion follows now by noting that $q_1^{m-1}M(f)\le H(f)^m$ and $q_2M(g)^m\le H(g)^{m+1}$. This completes the proof of the theorem. ∎

REMARKS. 1. The inequality (12) leads to an improved version of Theorem 1. If $|b_m|<M(g)$ it might be useful to directly test inequality (10). Further improvements can be done, for instance, by considering the upper bound for $|f(\theta_j)|$ given by (8), instead of (9), but they lead to more complicated assumptions on n_1, n_2 and d.

2. In [2, Th. 1], the following result has been provided:

THEOREM. *For any relatively prime polynomials $f(X),g(X)\in\mathbb{Q}[X]$ with $\deg f<\deg g=m$, and any prime $p>2m^mH(f)^{m+1}H(g)^{3m}$, the polynomial $f(X)+pg(X)$ is irreducible over $\mathbb{Q}$.*

For $m>1$, Corollary 1 provides a sharper bound, since

$$\left(2+\frac{1}{2^m}\right)^m H(f)^m H(g)^{m+1} < 2m^m H(f)^{m+1} H(g)^{3m}.$$

3. Corollary 2 follows immediately by (12).

A result similar to Corollary 2 is the following:

PROPOSITION 1. *Let $f(X)=a_0+a_1X+\ldots+a_kX^k$ and $g(X)=b_0+b_1X+\ldots+b_mX^m\in\mathbb{Z}[X]$ be two relatively prime polynomials with $k=\deg f<\deg g=m$. If n_1,n_2 are nonzero integers and d is a positive divisor of n_2b_m such that*

$$\left|\frac{n_2}{n_1}\right| > \left(2+\frac{1}{2^{k+1}d^m H(g)^{k+1}}\right)^{k+1} d^m H(f)H(g)^k,$$

then $n_1f(X)+n_2g(X)$ has at most $\Omega(n_2b_m/d)$ nonconstant factors over $\mathbb{Z}$.

Sketch of the proof. The proof goes as that of Theorem 1, except that $q_1=q_2=1$ and instead of (1) we find $|t_1|\le d$. Indeed, since we have $at_1\ldots t_s=n_2b_m$ with $\Omega(n_2b_m/d)<s\le m$, at least one of the t_i's divides d. Thus, instead of (10) we have to prove that

$$\frac{d^m}{|b_m|^k}\left(|b_m|+H(g)+\frac{|n_1|}{|n_2|}H(f)\right)^{k+1} < 1+\frac{|n_2|H(g)}{|n_1|H(f)}.$$

Since $|b_m|\le H(g)$ it is sufficient to prove that

$$(13)\qquad \left|\frac{n_2}{n_1}\right| > d^m H(f)H(g)^k\left(2+\frac{H(f)}{\left|\frac{n_2}{n_1}\right|H(g)}\right)^{k+1}.$$

Computations as in Theorem 1 show that inequality (13) is satisfied if $|n_2/n_1| > \delta \cdot d^m H(f)H(g)^k$ with $\delta = (2 + 2^{-k-1}d^{-m}H(g)^{-k-1})^{k+1}$. ∎

2.2. *Proof of Theorem 2.* In this case we may obviously assume $m \geq 2$, and since the degree r of the polynomial F_1 is at least 2, it is sufficient instead of (10) to prove that

$$d^m q_1^m |b_m|^{m-2k}\left(|b_m| + M(g) + \frac{|n_1|q_2}{|n_2|q_1}M(f)\right)^{2(k+1)} < \left(1 + \frac{|n_2|q_1 M(g)}{|n_1|q_2 M(f)}\right)^2,$$

or even more, that

$$d^{m/2} q_1^{m/2} |b_m|^{m/2-k}\left(|b_m| + M(g) + \frac{|n_1|q_2}{|n_2|q_1}M(f)\right)^{k+1} < \frac{|n_2|q_1 M(g)}{|n_1|q_2 M(f)}.$$

Now, since $|b_m| \leq M(g)$ it suffices to prove that

$$\left|\frac{n_2}{n_1}\right| > d^{m/2} q_1^{m/2-1} q_2 M(f) M(g)^{m/2}\left(2 + \frac{q_2 M(f)}{\left|\frac{n_2}{n_1}\right| q_1 M(g)}\right)^{k+1},$$

if $m/2 \geq k$, and

$$\left|\frac{n_2}{n_1}\right| > d^{m/2} q_1^{m/2-1} q_2 M(f) M(g)^{k}\left(2 + \frac{q_2 M(f)}{\left|\frac{n_2}{n_1}\right| q_1 M(g)}\right)^{k+1},$$

if $m/2 < k$. So in both cases it is sufficient to prove that

$$\left|\frac{n_2}{n_1}\right| > d^{m/2} q_1^{m/2-1} q_2 M(f) M(g)^{\max(m/2,k)}\left(2 + \frac{q_2 M(f)}{\left|\frac{n_2}{n_1}\right| q_1 M(g)}\right)^{k+1}.$$

Let $w = 2^{k+1} d^{m/2} q_1^{m/2} M(g)^{1+\max(m/2,k)}$. It is straightforward to verify that the last inequality holds for

$$\left|\frac{n_2}{n_1}\right| > \left(2 + \frac{1}{w}\right)^{k+1} d^{m/2} q_1^{m/2-1} q_2 M(f) M(g)^{\max(m/2,k)}, \tag{14}$$

which completes the proof. ∎

Corollary 3 follows immediately from (14).

3. The case $\deg f = \deg g$

3.1. *Proof of Theorem 3.* We use slightly different arguments than those used in the proof of Theorem 1. First of all, in order to see that $\Omega(h/d)$ makes sense, we have to prove that

$$|h| > d. \tag{15}$$

The definition of h shows that

$$|h| \geq |n_2| - |n_1|q_2 M(f) > 0. \tag{16}$$

Indeed, if $n_1 a_m$ and $n_2 b_m$ have the same sign, we find $|h| \geq |n_2| + 1$. Our assumption that

$$\left|\frac{n_2}{n_1}\right| > d^m H(f)H(g)\left(1 + H(f)H(g) + \frac{1}{2^m d^m}\right)^{m+1} \tag{17}$$

implies $|n_2| > |n_1| q_2 M(f)$, so we obviously have $|n_2 b_m| q_1 > |n_1 a_m| q_2$. Thus, if $n_1 a_m$ and $n_2 b_m$ have opposite signs, we find

$$|h| = \frac{|n_2 b_m| q_1 - |n_1 a_m| q_2}{\gcd(q_1, q_2)} \geq |n_2| - |n_1| q_2 M(f) > 0.$$

Dividing now by d in (16) and using again (17), we find

$$\frac{|h|}{d} > |n_1| \cdot d^{m-1} H(f)H(g)\left[\left(1 + H(f)H(g) + \frac{1}{2^m d^m}\right)^{m+1} - 1\right] > 1,$$

which proves (15).

Now we may obviously assume $\Omega(h/d) < m$. We write again $g(X)$ in the form

$$g(X) = \frac{b_0 + b_1 X + \ldots + b_m X^m}{q_2} = \frac{\overline{b}\,\overline{g}(X)}{q_2},$$

where $\overline{b} \in \mathbb{Z}$ and $\overline{g}(X) \in \mathbb{Z}[X]$, $\overline{g}(X)$ primitive. Then we write

$$n_1 f(X) + n_2 g(X) = \frac{a}{q} F(X)$$

with $\gcd(a, q) = 1$ and $F(X) \in \mathbb{Z}[X]$, $F(X)$ primitive.

Assume now that $n_1 f(X) + n_2 g(X)$ has more than $\Omega(h/d)$ factors. Then by the Gauss Lemma, $F(X)$ will decompose as $F(X) = F_1(X) \ldots F_s(X)$ with $\Omega(h/d) < s \leq m$ and $F_1(X), \ldots, F_s(X) \in \mathbb{Z}[X]$, $F_1, \ldots, F_s$ primitive with $\deg F_1, \ldots, \deg F_s \geq 1$. Let $t_1, \ldots, t_s \in \mathbb{Z}$ be the leading coefficients of $F_1, \ldots, F_s$, respectively. Let also $\overline{q}_1 = q_1/\gcd(q_1, q_2)$, $\overline{q}_2 = q_2/\gcd(q_1, q_2)$ and denote $n_1 a_i \overline{q}_2 + n_2 b_i \overline{q}_1$ by h_i for all $i \in \{0, \ldots, m-1\}$. Since

$$\frac{h_0 + h_1 X + \ldots + h_{m-1} X^{m-1} + h X^m}{\operatorname{lcm}(q_1, q_2)} = \frac{a}{q} F_1(X) \ldots F_s(X),$$

we see that a divides h and q divides $\operatorname{lcm}(q_1, q_2)$. On the other hand, by comparing the leading coefficients we find

$$h = t_1 \ldots t_s a \cdot \frac{\operatorname{lcm}(q_1, q_2)}{q}. \tag{18}$$

Now, since $(\operatorname{lcm}(q_1, q_2))/q$ is an integer and $\Omega(h/d) < s$, (18) shows that at least one of the t_i's, say t_1, divides d. So we have

$$|t_1| \leq d. \tag{19}$$

Again we proceed to estimate the resultant $R(\overline{g}, F_1)$. As in Theorem 1, since $\overline{g}$ and F_1 are relatively prime, we must have $|R(\overline{g}, F_1)| \geq 1$. If F_1 decomposes as $F_1(X) = t_1(X-\theta_1)\dots(X-\theta_r)$, we have

$$|R(\overline{g}, F_1)| = |t_1|^m \prod_{1\le j\le r} |\overline{g}(\theta_j)|.$$

Using (19) together with $|\overline{g}(\theta_j)| \le q_2|g(\theta_j)|$ and $g(\theta_j) = -n_1 f(\theta_j)/n_2$, we find

$$|R(\overline{g}, F_1)| \le d^m \frac{q_2^r |n_1|^r}{|n_2|^r} \prod_{1\le j\le r} |f(\theta_j)|. \tag{20}$$

We now proceed to find the upper bound for $|f(\theta_j)|$. The equality $n_1 f(\theta_j) + n_2 g(\theta_j) = 0$ implies

$$\left(\frac{n_1 a_0}{q_1} + \frac{n_2 b_0}{q_2}\right) + \dots + \left(\frac{n_1 a_{m-1}}{q_1} + \frac{n_2 b_{m-1}}{q_2}\right)\theta_j^{m-1} + \frac{h}{\mathrm{lcm}(q_1,q_2)}\,\theta_j^m = 0.$$

Since (16) allows us to divide by $|h|$, we further have

$$|\theta_j|^m \le \frac{\mathrm{lcm}(q_1,q_2)}{|h|}\left(\frac{|n_1|M(f)}{q_1} + \frac{|n_2|M(g)}{q_2}\right)(1 + |\theta_j| + \dots + |\theta_j|^{m-1}).$$

Therefore, either $|\theta_j| \le 1$, or if not, then

$$|\theta_j|^m < \frac{q_1 q_2}{|h|}\left(\frac{|n_1|M(f)}{q_1} + \frac{|n_2|M(g)}{q_2}\right)\frac{|\theta_j|^m}{|\theta_j| - 1}.$$

So in both cases we have

$$|\theta_j| < 1 + \frac{q_1 q_2}{|h|}\left(\frac{|n_1|M(f)}{q_1} + \frac{|n_2|M(g)}{q_2}\right),$$

and since obviously

$$|f(\theta_j)| \le \frac{M(f)}{q_1}\,(1 + |\theta_j| + \dots + |\theta_j|^m),$$

we obtain the following upper bound for $|f(\theta_j)|$:

$$|f(\theta_j)| < \frac{M(f)}{q_1} \cdot \frac{\left[1 + \frac{q_1q_2}{|h|}\left(\frac{|n_1|M(f)}{q_1} + \frac{|n_2|M(g)}{q_2}\right)\right]^{m+1} - 1}{\frac{q_1q_2}{|h|}\left(\frac{|n_1|M(f)}{q_1} + \frac{|n_2|M(g)}{q_2}\right)}.$$

It is more convenient to use

$$|f(\theta_j)| < |h|M(f)\,\frac{\left[1 + \frac{q_1q_2}{|h|}\left(\frac{|n_1|M(f)}{q_1} + \frac{|n_2|M(g)}{q_2}\right)\right]^{m+1}}{q_1[|n_1|q_2M(f) + |n_2|q_1M(g)]},$$

which further gives

$$|f(\theta_j)| < M(f)\left[1 + \frac{q_1q_2}{|h|}\left(\frac{|n_1|M(f)}{q_1} + \frac{|n_2|M(g)}{q_2}\right)\right]^{m+1},$$

since $|h| \le |n_1|q_2M(f) + |n_2|q_1M(g)$ and $q_1 \ge 1$. Therefore by (16) we find

$$|f(\theta_j)| < M(f)\left(1 + \frac{|n_1|q_2M(f) + |n_2|q_1M(g)}{|n_2| - |n_1|q_2M(f)}\right)^{m+1},$$

that is,

$$|f(\theta_j)| < |n_2|^{m+1} M(f) \left(\frac{1+q_1M(g)}{|n_2| - |n_1|q_2M(f)} \right)^{m+1}. \tag{21}$$

Together with (20), (21) yields

$$|R(\overline{g},F_1)| < d^m \left[q_2|n_1| \cdot |n_2|^m M(f) \left(\frac{1+q_1M(g)}{|n_2| - |n_1|q_2M(f)} \right)^{m+1} \right]^r. \tag{22}$$

Let us denote $d^m q_2 |n_1| M(f)[1+q_1M(g)]^{m+1}$ by α. We shall prove that

$$[|n_2| - |n_1|q_2M(f)]^{m+1} > \alpha |n_2|^m, \tag{23}$$

which by (22) will contradict the fact that $|R(\overline{g},F_1)| \geq 1$.

We search for a suitable $\delta > 1$ such that $|n_2| - |n_1|q_2M(f) > |n_2|/\delta$, which is equivalent to

$$|n_2| > |n_1|q_2M(f)\,\frac{\delta}{\delta - 1}. \tag{24}$$

For such a δ we then require

$$\left(\frac{|n_2|}{\delta} \right)^{m+1} > \alpha |n_2|^m,$$

or equivalently

$$|n_2| > \alpha\delta^{m+1}. \tag{25}$$

So if we find a $\delta > 1$ such that $\alpha\delta^{m+1} > |n_1|q_2M(f)\delta/(\delta-1)$, then any n_2 satisfying (25) will also satisfy (23). Such a δ should verify

$$(\delta - 1)\delta^m > \frac{1}{d^m[1+q_1M(g)]^{m+1}}.$$

Denote $d^m[1+q_1M(g)]^{m+1}$ by w. One candidate for δ is $1+1/w$, since obviously

$$\frac{1}{w}\left(1 + \frac{1}{w}\right)^m > \frac{1}{w}.$$

So we have proved that for

$$|n_2| > |n_1| d^m q_2 M(f) \left(1 + q_1M(g) + \frac{1}{d^m[1+q_1M(g)]^m} \right)^{m+1} \tag{26}$$

we have $|R(\overline{g},F_1)| < 1$, a contradiction. The proof finishes by noting that $q_2M(f) \leq H(f)H(g)$ and $q_1M(g) \leq H(f)H(g)$. ∎

Remarks. 1. Since the sharper bound given by (26) still implies (15) and (16), one can use (26) to rephrase Theorem 2 in terms of q_1, q_2, $M(f)$ and $M(g)$ instead of $H(f)$ and $H(g)$.

2. Corollary 5 follows immediately from (26).

3. As in the preceding section, we may also consider the case when the polynomial $n_1f(X)+n_2g(X)$ has no rational roots. In that case, we see from

(22) that the same conclusion as in Theorem 3 holds, provided that (26) is replaced by

$$\left|\frac{n_2}{n_1}\right| > d^{m/2} q_2 M(f)\left(1 + q_1 M(g) + \frac{1}{d^{m/2}[1 + q_1 M(g)]^m}\right)^{m+1}.$$

3.2. *Proof of Corollary 6.* In this case all that remains is to show that our assumptions force $n_1 f(X) + n_2 g(X)$ to be primitive.

Let $\lambda = H(f)(1 + H(g) + [1 + H(g)]^{-m})^{m+1}$. Since $|n_1 a_m + n_2 b_m| = p$, we have either $n_2 = (p - n_1 a_m)/b_m$, or $n_2 = -(p + n_1 a_m)/b_m$.

In the first case we must have $p > n_1 a_m$, otherwise our assumption that $|n_2| > \lambda |n_1|$ would imply $p < n_1 a_m - \lambda |n_1 b_m| < 0$, a contradiction. Thus $|n_2| > \lambda |n_1|$ becomes $(p - n_1 a_m)/|b_m| > \lambda |n_1|$, which further gives

$$p > |n_1| \cdot [\lambda - H(f)]. \tag{27}$$

Assume now that p divides $n_1 a_i + \frac{p - n_1 a_m}{b_m} b_i$ for all $i \in \{0, \ldots, m-1\}$, that is, p divides $n_1(a_i b_m - a_m b_i)$ for all $i \in \{0, \ldots, m-1\}$. Since

$$|n_1(a_i b_m - a_m b_i)| \leq 2|n_1| H(f) H(g) < |n_1| \cdot [\lambda - H(f)],$$

the inequality (27) forces $a_i b_m = a_m b_i$ for all $i \in \{0, \ldots, m-1\}$, that is, $b_m f(X) = a_m g(X)$, a contradiction.

Similarly, in the second case we must have $p > -n_1 a_m$, which also implies (27). Assuming now that p divides $n_1 a_i - \frac{p + n_1 a_m}{b_m} b_i$ for all $i \in \{0, \ldots, m-1\}$, we will get the same contradiction, which completes the proof. ∎

One may improve Corollary 6 as follows. Let $f(X) = a_0 + \ldots + a_m X^m$ and $g(X) = b_0 + \ldots + b_m X^m \in \mathbb{Z}[X]$ be two relatively prime polynomials of degree m. Assume n_1 and n_2 are nonzero integers such that $n_1 a_m + n_2 b_m$ is a prime number p and let $h(X) = n_1 f(X) + n_2 g(X)$. For any integer j such that $n_1 a_m + j b_m \neq 0$, the polynomials $n_1 f(X) + j g(X)$ and $g(X)$ are relatively prime of degree m, with leading coefficients $n_1 a_m + j b_m$ and b_m respectively. We obviously have $n_1 a_m + j b_m + (n_2 - j) b_m = p$ and

$$h(X) = n_1 f(X) + j g(X) + (n_2 - j) g(X).$$

Let $K(g) = (1 + H(g) + [1 + H(g)]^{-m})^{m+1}$. Then by Corollary 6, $h(X)$ is irreducible over $\mathbb{Z}$ if $|n_2 - j| > H(n_1 f + j g) K(g)$, or equivalently

$$|p - n_1 a_m - j b_m| > H(n_1 f + j g) \cdot |b_m| \cdot K(g).$$

If $p \leq n_1 a_m + j b_m$, we find $p < n_1 a_m + j b_m - H(n_1 f + j g) \cdot |b_m| \cdot K(g) < 0$, a contradiction. Therefore we conclude that $h(X)$ is irreducible over $\mathbb{Z}$ for primes p satisfying

$$p > \min_{j \neq -n_1 a_m / b_m} \{n_1 a_m + j b_m + H(n_1 f + j g) \cdot |b_m| \cdot K(g)\}.$$

Similarly, if $n_1a_m + n_2b_m = -p$, then $h(X)$ is irreducible over $\mathbb{Z}$ for

$$p > \min_{j \neq -n_1a_m/b_m} \{-n_1a_m - jb_m + H(n_1f + jg) \cdot |b_m| \cdot K(g)\}.$$

Acknowledgements. The author is grateful to Marian Vâjâitu, Mihai Cipu, Alexandru Zaharescu for useful discussions, and to an anonymous referee for valuable suggestions.

References

[1] M. Cavachi, *On a special case of Hilbert's irreducibility theorem*, J. Number Theory 82 (2000), 96–99.

[2] M. Cavachi, M. Vâjâitu and A. Zaharescu, *A class of irreducible polynomials*, J. Ramanujan Math. Soc. 17 (2002), 161–172.

[3] M. Fried, *On Hilbert's irreducibility theorem*, J. Number Theory 6 (1974), 211–231.

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

Institute of Mathematics
of the Romanian Academy
P.O. Box 1-764
RO-70700 Bucureşti, Romania
E-mail: Nicolae.Bonciocat@imar.ro

Received on 16.4.2003
and in revised form on 29.12.2003 (4509)