JOURNAL OF NUMBER THEORY 30, 156–166 (1988)

# An Inequality about Irreducible Factors of Integer Polynomials

MAURICE MIGNOTTE

*Université Louis Pasteur, Mathématique, 67084 Strasbourg, France*

*Communicated by M. Waldschmidt*

Received July 31, 1987; revised January 18, 1988

We give a new upper bound for the height of an irreducible factor of an integer polynomial. This paper also contains several bounds for the case of polynomials with complex coefficients. © 1988 Academic Press, Inc.

## 1. INTRODUCTION

**1.** In the sequel we need the following definitions which describe the "size" of a polynomial with complex coefficients.

Let

$$F = \sum_{i=0}^{n} a_i X^i, \qquad a_n \neq 0,$$

be a polynomial with complex coefficients; we use the following classical notations:

$$H(F) = \max_{0 \leqslant i \leqslant n} |a_i|, \qquad \text{the height of } F,$$

$$\|F\|_2 = \left( \sum_{i=0}^{n} |a_i|^2 \right)^{1/2}, \qquad \text{the norm of } F,$$

$$\|F\|_1 = \sum_{i=0}^{n} |a_i|, \qquad \text{the length of } F,$$

$$|F| = \max\{|F(z)|;\ |z| = 1\}.$$

A very imortant notion was introduced by K. Mahler: the measure of $F$, which is defined by

$$M(F) = |a_n| \prod_{j=1}^{n} \max\{1, |z_j|\},$$



0022-314X/88 $3.00

where $z_1, ..., z_n$ are the complex roots of $F$. Notice that $M$ is multiplicative:

$$M(PQ) = M(P) \cdot M(Q).$$

All these sizes, except the measure, have the same order of magnitude up to a factor bounded by the degree. We have

$$H(F) \leqslant \|F\|_2 \leqslant |F| \leqslant \|F\|_1 \leqslant (n+1)\, H(F);$$

all these relations are trivial except perhaps $\|F\|_2 \leqslant |F|$, which is a consequence of Parseval's formula.

**2.** We consider the relations between the measure and the size of a polynomial—for example, its length. We are mostly interested in the case of polynomials over the integers, and especially in the case of irreducible polynomials.

If $P$ is a polynomial over the complex numbers, the relations between the coefficients of $P$ and its roots lead at once to the inequality

$$\|P\|_1 \leqslant 2^d M(P), \qquad \text{where} \quad d = \deg(P). \tag{1}$$

In some sense, this relation is the best possible even if $P$ has integer coefficients: the equality holds for $P = (X+1)^d$.

But what happens when $P$ is irreducible?

Consider now the polynomial

$$E(X) = a(X+1)^d + 2,$$

where $a$ is a positive odd integer. This polynomial is irreducible over the integers (since $aY^d + 2$ is irreducible over Z). It satisfies $\|E\|_1 = a2^d + 2$. We want to bound its measure.

First, we choose $a = 1$, We use one step of Graeffe's method. Consider the polynomial

$$E_1(X) = E(\sqrt{X})\, E(-\sqrt{X}),$$

which is equal to

$$E_1(X) = (1-X)^d + 2 \sum_{k, 0 \leqslant 2k \leqslant d} \binom{d}{2k} X^k + 4.$$

The roots of $E_1$ are the squares of the roots of $E$, and

$$\|E_1\|_1 \leqslant 2^{d+1} + 4.$$

If we apply Landau's inequality (i.e., $M(F) \leqslant \|F\|_2$; see (3) below) to $E_1$, we get

$$M(E) = M(E_1)^{1/2} \leqslant (2^{d+1} + 4)^{1/2}.$$

Thus we see that, in the case of irreducible monic polynomials over the integers, the constant 2 in inequality (1) cannot be replaced by $\sqrt{2} - \varepsilon$, for any fixed $\varepsilon > 0$.

Taking now $a = b^{d^2}$, where $b$ is a large odd integer, all the roots of $E$ are close to 1 and its measure is at most $2a$. This shows that, for irreducible polynomials over $Z$, the constant 2 in inequality (1) cannot be replaced by $2 - \varepsilon$, for any fixed $\varepsilon > 0$.

It is easy to verify that $M(E) \geqslant C^d$ for some absolute constant $C > 1$. This example shows that (1) cannot be much improved when $M(P)$ is big, even if $P$ is irreducible.

But what happens if $P$ is irreducible and its measure not too big?

The following theorem, which is a simple instance of the main result of this paper (Theorem 5), shows that (1) is not the best possible in that case.

THEOREM 1. *Let $P$ be an irreducible integer polynomial, then*

$$\|P\|_2 \leqslant e^{\sqrt{d}}(d + 2\sqrt{d} + 2)^{1+\sqrt{d}} M(P)^{1+\sqrt{d}}, \qquad \textit{where} \quad d = \deg P.$$

**3.** Estimates like (1) have applications to the following question: given an integer polynomial $F$, find a number $B$ such that the coefficients of any irreducible factor $P$ of $F$ have absolute values bounded above by $B$. This problem is important in modern algorithms for the factorization of polynomials: for the Berlekamp–Zassenhaus algorithm (see Knuth,* Vol 2), in the famous Lenstra–Lenstra–Lovasz algorithm, called also the $L^3$-algorithm, $B$ plays an important role (see [LLL]), and also for factoring polynomials with algebraic coefficients. The case of irreducible factors is the only one used in these algorithms and our result decreases their cost in an obvious way.

Suppose that $F$ is an integer polynomial and that $P$ is some integer polynomial which divides $F$. Then the following inequality is well known:

$$\|P\|_1 \leqslant 2^d \|F\|_2, \qquad \text{where} \quad d = \deg(P). \tag{2}$$

The proof of (2) is the following. Use (1) and the bound

$$M(P) \leqslant M(F),$$

* The Art of Computer Programming, Vol. 2, Addison Wesley, Reading, Mass., 1969.

which comes from the two following facts:

(i) the roots of $P$ are roots of $F$,

(ii) the leading coefficient of $P$ divides the leading coefficient of $F$.

This proves that

$$\|P\|_1 \leqslant 2^d M(F). \tag{2'}$$

Then the conclusion follows from Landau's inequality

$$M(F) \leqslant \|F\|_2. \tag{3}$$

Of course (2') is generally sharper than (2).

As I was told by A. Schinzel, inequality (3) goes back to Landau [L]; it has been rediscovered several times (Specht [S], Vicente Gonçalves [V], Mignotte [M1]; these two last papers contain a slight refinement of (2); the last one seems to be the first where this result is applied to bound the coefficients of the factors of a polynomial). See also [O].

We give here a brief proof of (3), since some ideas of this proof will be used later to obtain Theorem 3. Recall that a Blaschke factor relative to a complex number $\alpha$ is

$$B(z;\alpha) = \frac{\bar{\alpha}z - 1}{z - \alpha}.$$

Let $z_1, \ldots, z_k$ be the roots of $F$ which lie outside of the unit circle and let

$$B(z) = \prod_{i=1}^{k} B(z; z_i)$$

be the product of the Blaschke factors relative to these roots. Put $F^*(z) = F(z)\, B(z)$.

For $|z| = 1$ we have the relation

$$|F^*(z)| = |F(z)|,$$

which comes from the well-known (and easily proved) fact that a Blaschke factor has modulus one when the variable is on the unit circle.

By Parseval's formula and the previous relation, we get

$$\|F\|_2^2 = \frac{1}{2\pi}\int_0^{2\pi} |F(e^{i\theta})|^2\, d\theta = \frac{1}{2\pi}\int_0^{2\pi} |F^*(e^{i\theta})|^2\, d\theta.$$

Then (3) follows by an application of Parseval's formula to the polynomial $F^*$ and the fact that its leading coefficient is nothing but $M(F)$.

**4.** The fact that (2)—and a fortiori (2')—is almost the best possible for general integer polynomials has been (at least implicitely) proved in

exists an integer polynomial $F$, divisible by $P$, of height equal to 1 with $\deg(F) \ll d^2 \log d$.

This shows that the constant 2 in inequality (2) cannot be replaced by $2-\varepsilon$, for any fixed $\varepsilon > 0$.

Applying Theorem 1 we get

THEOREM 1'. *Let $F$ be a nonzero integer polynomial and $P$ an irreducible factor of $F$. Then*

$$\|P\|_2 \leqslant e^{\sqrt{d}}(d+2\sqrt{d}+2)^{1+\sqrt{d}} M(F)^{1+\sqrt{d}}, \qquad \text{where} \quad d = \deg P.$$

This result is better than (2)—or even (2')—for $M(F) \leqslant e^{\sqrt{d}/2}$, when $d$ is large enough. We remark that Theorem 1' implies Theorem 1: take $F = P$.

**5.** In practice, to apply Theorem 1' (or estimate (2')) we can use Landau's inequality, $M(F) \leqslant \|F\|_2$, or compute directly some upper bound for $M(F)$. This second way leads to sharper estimates and is studied in [CMP]. The simplest method being some variant of Graeffe's method. (In a few words: if $F_m$ is the polynomial whose roots are the $2^m$ powers of the roots of $F$, then we have the inequality

$$\log M(F) \leqslant 2^{-m} \cdot \log \|F_m\|_2$$

which is generally rather sharp for $m \geqslant 4$. This method was used above to study $E$.)

## 2. General Inequalities about Factors of Polynomials

We give here a list of bounds for the sizes of the factors of a polynomial with complex coefficients. The last two are new, others are more or less classical.

In this section (but only in this section), we use the following notations: $P$ and $Q$ are nonconstant polynomials with complex coefficients. We put

$$p = \deg(P) \qquad \text{and} \qquad q = \deg(Q).$$

**1.** Classical inequalities. The multiplicativity of the measure and inequality (2') lead to

$$\|P\|_1 M(Q) \leqslant 2^p M(PQ). \tag{4}$$

A variant, proved in the same way, is

$$\|P\|_1 \, \|Q\|_1 \leqslant 2^{p+q} M(PQ). \tag{5}$$

[M2]. The example consists of $P(X)=(X+1)^d$ and of some integer polynomial $F$ of height one (see Sect. 5, corollary to Theorem 4'): there

**2.** Güting's inequality. Güting [G], Lemma H, proved the following result:

$$\|P\|_1 M(Q) \leqslant \frac{(p+q)!}{p!}\|PQ\|_1, \qquad \text{if} \quad q \leqslant 3. \tag{6}$$

**3.** Durand's inequality. If $a$ is any real number then A. Durand [D1] proved the inequality,

$$|P| \leqslant ((p+1)/(1+|a|))\,|P(X)\cdot(X-a)|,$$

which implies

$$|P|\,\|Q\|_1 \leqslant \frac{(p+q)!}{p!}\,|PQ|. \tag{7}$$

**4.** An application of real analysis. In [DR], Donaldson and Rahman obtained the following inequality.

LEMMA 1. *Let $P$ be a complex polynomial of degree $d$ and $\beta$ any complex number. Then*

$$\|P\|_2 \leqslant \left(1+|\beta|^2-2|\beta|\cos\left(\frac{\pi}{d+2}\right)\right)^{-1/2}\|P(X)(X-\beta)\|_2.$$

*Proof.* Their proof consists of translating this problem into the search of the maximum of a real function in several variables. Applying differential calculus, they compute explicitly the solution for the maximum, so their inequality is sharp. A shorter proof, using Lagrange's interpolation, was given by Durand (see [D2, Vol. 2, Sect. 5, C. 8]).

Considering the cases $|\beta| \leqslant 1$ and $|\beta| > 1$, we get the following corollary.

COROLLARY. *Let $P$ and $\beta$ as in Lemma 1. Then*

$$\|P\|_2 \cdot \max\{1, |\beta|\} \leqslant \left(\sin\left(\frac{\pi}{d+2}\right)\right)^{-1} \cdot \|P(X)(X-\beta)\|_2.$$

An obvious induction gives

THEOREM 2. *Let $P$ and $Q$ be polynomials with complex coefficients, with respective degrees $p$ and $q$. Then*

$$\|P\|_2 \cdot M(Q) \leqslant \prod_{k=p}^{p+q-1} \frac{1}{\sin(\pi/(k+2))} \cdot \|PQ\|_2, \tag{8}$$

*which is the best possible when $q=1$ (but not for $q>1$).*

**5.** Use of complex analysis.

THEOREM 3. *Let $P$ and $Q$ be polynomials with complex coefficients of respective degrees $p$ and $q$. Then*

$$|P|\, M(Q) \leqslant \frac{(p+q)^{p+q}}{p^p q^q}\, |PQ|. \tag{9}$$

*Proof.* Let $z_1, \ldots, z_k$ be the roots of $Q$ which lie outside of the unit circle and let $B$ be the product of the Blaschke factors relative to these roots. Put

$$Q^*(z) = Q(z)\, B(z), \qquad F = PQ, \qquad F^* = PQ^*.$$

By the maximum modulus principle, for $\rho > 1$ we have

$$|P| \leqslant \max\{|P(z)|;\ |z| = \rho\},$$

so that

$$|P| \leqslant \frac{\max\{|F^*(z)|;\ |z| = \rho\}}{\min\{|Q^*(z)|;\ |z| = \rho\}}.$$

To bound the numerator we apply again the maximum modulus principle (to the polynomial reciprocal to $F^*$) to get

$$\max\{|F^*(z)|;\ |z| = \rho\} \leqslant |F^*|\, \rho^{p+q},$$

and the equality

$$|F^*| = |F| \qquad \text{(implied by } |B(z)| = 1 \text{ if } |z| = 1).$$

For the denominator, we notice that the leading coefficient of $Q^*$ is equal to $M(Q)$ and that any point of the circle $|z| = \rho$ is at a distance at least $\rho - 1$ from any root of $Q^*$ (indeed all the roots of $Q^*$ lie in the unit disk), so that

$$\min\{|Q^*(z)|;\ |z| = \rho\} \geqslant M(Q)(\rho - 1)^q.$$

The theorem follows from the choice $\rho = (p+q)/p$.

*Remark.* Suppose that the product $PQ$ and the degree of $P$ are known and that we want to estimate $|P|$ (for example). In the general case, all the previous inequalities cannot be completely compared. Roughly speaking, one can say that

- (4) is the best when $q$ is not too small, say for $q \geqslant p/\log p$;
- (6) or (7) are better than (4) for $q \leqslant p/\log p$, but in this range (8) is better than (6) and (7),
- (9) gives better results than (8) for $q \geqslant 10$.

## 3. Construction of Some Multiple of $P$ with Low Height

THEOREM 4. *Let $P$ be a polynomial with integer coefficients, irreducible, of degree $d \geqslant 2$. Let $N$ be an integer, $N \geqslant d$. Then there exists a nonzero polynomial $G$ with integer coefficients, divisible by $P$, of degree at most $N$ which satisfies*

$$H(G) \leqslant ((N+2)^{d/2} M^N)^{1/(N+1-d)},$$

*where $M$ is the measure of $P$.*

*Proof.* This is a direct application of the sharpening of Siegel's lemma obtained by Bombieri and Vaaler [BV1].

*Remark.* A similar result was proved in [M2], where we get the slightly weaker bound

$$H(G) \leqslant (2(N+1)^d M^N)^{1/(N+1-d)}.$$

But the proof is much easier than that of Theorem 4: it uses only the pigeon-hole principle.

## 4. A Relation between the Height and the Measure of an Irreducible Integer Polynomial

Let $P$ be an irreducible integer polynomial of degree $d$. Let $N$ be an integer $> d$ and consider the polynomial $G$ constructed in Theorem 4. Using some estimates of Sect. 2, we get the following result.

THEOREM 5. *Let $P$ be an irreducible integer polynomial of degree $d$ and measure at most $M$. Then, for any integer $N \geqslant d$, we have*

$$|P| \leqslant C_N \cdot ((N+2)^{d/2} M^N)^{1/(N+1-d)},$$

*where*

$$C_N = \min\left\{(N+1)2^n, (N+1)\prod_{k=d}^{N-1}\left(\sin\left(\frac{\pi}{k+2}\right)\right)^{-1}, \frac{N^N(N+1)}{d^d(N-d)^{N-d}}\right\}.$$

Taking some suitable values of $N$ we get the following corollaries.

COROLLARY 1. *Let $P$ be an irreducible integer polynomial of degree $d$ and measure at most $M$. Then*

$$\|P\|_2 \leqslant e^{\sqrt{d}}(d+2\sqrt{d}+2)^{1+\sqrt{d}} M^{1+\sqrt{d}}.$$

*Proof.* We choose $N = d + [\sqrt{d}]$ and $C_N \leqslant N^N(N+1)\, d^{-d}\, (N-d)^{-N+d}$. The details of computation are not difficult. We them.

We wrote down Corollary 1 because of its relative simplicity. The following result is sharper than Corollary 1 in the range $M \geqslant e^{\sqrt{d}/2}$ and sharper than (1) for

$$M \leqslant \exp\left(\frac{d}{5\log(2d)}\right).$$

COROLLARY 2. *Let $P$ be an irreducible integer polynomial of degree $d$ and measure at most $M$. Then*

$$\|P\|_2 \leqslant (2d+1)M \exp\{2\sqrt{d(2+\log\sqrt{d})\log((2d+1)^{1/2}M)}\}.$$

*Proof.* For $M \leqslant e^2$, Corollary 2 is implied by Corollary 1. Whereas in the range

$$M \geqslant e^d/\sqrt{d}$$

it is implied by (1). Moreover, (1) implies Corollary 2 for $d \leqslant 4$. Thus we suppose that

$$e^2 \leqslant M \leqslant e^d/\sqrt{d} \qquad \text{and} \qquad d \geqslant 5.$$

In Theorem 5, put $N = d + x$. Then we get

$$|P| \leqslant (d+x+1)\, M e^x (1+d/x)^x\, ((d+x+2)^{1/2}\, M)^{d/(x+1)}.$$

Choose now

$$x = \left[\sqrt{\frac{d\log((2d+1)^{1/2}M)}{2+\log(\sqrt{d})}}\right].$$

Then

$$[\sqrt{d}] \leqslant x < d,$$

and the conclusion follows easily.

## 5. COMMENTS

**1.** Theorem 2 can be generalized in the following way. In [M2], we proved

THEOREM 4′. *Let $P$ be a nonzero polynomial with integer coefficients, of degree $d \geqslant 2$, whose decomposition over $Z[X]$ is of the form*

$$P = aP_1^{r_1} \cdots P_k^{r_k},$$

*the $P_j$ being pairwise distinct irreducible polynomials. Let $N$ and $T$ be positive integers, $N > dT$. Then there exists a nonzero polynomial $Q$, with integer coefficients, divisible by $P$, of degree at most $N$ which satisfies*

$$H(Q) \leqslant \{2^{\Omega}(N+1)^{d^*(T+1)/2}\, M(P)^N\}^{1/(N+1-dT)}$$

*where*

$$d_j = \deg P_j, \qquad 1 \leqslant j \leqslant k, \qquad \Omega = r_1 + \cdots + r_k, \qquad d^* = r_1^2 d_1 + \cdots + r_k^2 d_k.$$

This theorem can be used in an obvious way to generalize Theorem 5. It also implies that there exists an integer polynomial $F$ of degree $\ll d^2 \log d$, with height one, and divisible by the polynomial $P(X) = (X+1)^d$.

Moreover, Theorem 4′ has been sharpened and generalized to polynomials with algebraic coefficients by Bombieri and Vaaler; see [BV2]. Thus, Theorem 5 can also be generalized to polynomials with algebraic coefficients.

**2.** It is difficult to guess whether Theorem 4 is sharp or not. The following example shows that it is not sharp when the measure is equal to 1. Consider the cyclotomic polynomial $\Phi_n$. Then it is known (see [EV]) that

$$\log(|\Phi_n|) \leqslant n^{c/\log\log n},$$

for some positive constant $c$, and that this result is essentially best possible. But our theorem gives only

$$\log(|\Phi_n|) \leqslant n^{1/2+\varepsilon}.$$

## ACKNOWLEDGMENTS

I am very grateful to E. Belaga, Ph. Glesser, M. Langevin, and M. Waldschmidt whose interesting remarks helped me to improve a first version of this paper.

## REFERENCES

[BV1] E. BOMBIERI AND J. D. VAALER, On Siegel's lemma, *Invent. Math.* **73** (1983), 539–560.

[BV2] E. BOMBIERI AND J. D. VAALER, Polynomials with low height and prescribed vanishing, *in* "Proc. Conf. of Number Theory, Stillwater, Oklahoma, July 1984."

[CMP] L. CERLIENCO, M. MIGNOTTE, F. PIRAS, Computing the measure of a polynomial, *J. Symbolic. Comput.* **4**, No. 1 (1987), 21–34.

[D1] A. DURAND, A propos d'une théorème de S. Berstein sur la dérivée d'un polynôme, *C. R. Acad. Sci. Paris Sér. I Math.* **290** (1980), 523–525.

[D2] A. DURAND, Quelques aspects de la théorie analytique des polynômes, notes. Université de Limoges, 1984.

[DR] J. D. DONALDSON AND Q. I. RAHMAN, Inequalities for polynomials with a prescribed zero, *Pacific J. Math.* **41** (1983), 375–378.

[EV] P. ERDÖS AND R. C. VAUGHAN, Bounds for the $r$th coefficients of cyclotomic polynomials, *J. London Math. Soc. (2)* **8** (1974), 393–400.

[G] R. GÜTING, Polynomials with multiple zeroes, *Mathematika* **14** (1967), 181–196.

[L] E. LANDAU, Sur quelques théorèmes de M. Petrovic relatifs aux zéros des fonctions analytiques, *Bull. Soc. Math. France* **33** (1905), 251–261.

[LLL] A. K. LENSTRA, H. W. LENSTRA, JR., AND L. LOVÀSZ, Factoring polynomials with rational integer coefficients, *Math. Ann.* **261** (1982), 515–531.

[M1] M. MIGNOTTE, An inequality about factors of polynomials, *Math. Comp.* **28** (1974), 1153–1157.

[M2] M. MIGNOTTE, Sur la répartition des racines des polynômes, *in* "Journées de Théorie des Nombres, Caen, Septembre 1980."

[O] A. M. OSTROWSKI, On an inequality of J. Vicente Gonçalves, *Univ. Lisboa Revista Fac. Ci A. Ci Mat.* (1960), 115–119.

[S] W. SPECHT, Abschätzungen der Wurzeln algebraischer Gleichungen, *Math. Z.* **52** (1949), 310–321.

[V] J. VICENTE GONÇALVES, L'inégalité de W. Specht, *Univ. Lisboa Revista Fac. Ci A. Ci Mat.* **1** (1950), 167–171.