ACTA ARITHMETICA
155.4 (2012)

Exceptional units and cyclic resultants

by

C. L. Stewart (Waterloo)

Dedicated to Professor A. Schinzel on the occasion of his 75th birthday

1. Introduction. Let α be a non-zero algebraic integer of degree d over $\mathbb{Q}$. Put $K = \mathbb{Q}(\alpha)$ and let $\mathcal{O}_K$ denote the ring of algebraic integers of K. Let $E(\alpha)$ be the number of positive integers n for which $\alpha^n - 1$ is a unit in $\mathcal{O}_K$. If $\alpha - 1$ is not a unit define $E_0(\alpha)$ to be 0 and otherwise define $E_0(\alpha)$ to be the largest integer n such that $\alpha^j - 1$ is a unit for $1 \leq j \leq n$. Next put $\zeta_n = e^{2\pi i/n}$ for each positive integer n and denote by $\Phi_n(x)$ the nth cyclotomic polynomial in x, so

$$\Phi_n(x) = \prod_{\substack{j=1\\(j,n)=1}}^{n} (x - \zeta_n^j). \tag{1}$$

Then

$$x^n - 1 = \prod_{m|n} \Phi_m(x). \tag{2}$$

We define $U(\alpha)$ to be the number of positive integers n for which $\Phi_n(\alpha)$ is a unit.

We proved in [16], following an approach introduced by Schinzel [14] in his study of primitive divisors of expressions of the form $A^n - B^n$ with A and B algebraic integers, that $\Phi_n(\alpha)$ is not a unit for n larger than $e^{452}d^{67}$ provided that α is not a root of unity. In 1995 Silverman [15] proved that there is an effectively computable positive number c such that if α is an algebraic unit of degree $d \geq 2$ that is not a root of unity then

$$U(\alpha) \leq cd^{1+0.7/\log\log d}. \tag{3}$$

2010 *Mathematics Subject Classification*: Primary 11R27; Secondary 11J68.
Key words and phrases: units, resultants, Groebner basis.

DOI: 10.4064/aa155-4-5

Note that

$$E_0(\alpha) \le E(\alpha) \le U(\alpha), \tag{4}$$

and by (2) and [16], $\alpha^n - 1$ is not a unit for n larger than $e^{452}d^{67}$. A construction of Mossinghoff, Pinner and Vaaler [12] shows that there are α, not roots of unity, of arbitrarily large degree for which

$$E_0(\alpha) \ge \pi\sqrt{\frac{d}{3}} + O(\log d). \tag{5}$$

In this article we shall strengthen the upper bound for integers n for which $\Phi_n(\alpha)$ is a unit and the upper bound for $E_0(\alpha)$ given from (3) and (4). For any β in $\mathbb{Q}(\alpha)$ we denote the norm of β from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}$ by $N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\beta$.

THEOREM 1. *Let ε be a positive real number. There is a positive number $c = c(\varepsilon)$, which is effectively computable in terms of ε, such that if α is a non-zero algebraic integer of degree d over the rationals which is not a root of unity and n is a positive integer for which*

$$|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\Phi_n(\alpha)| \le n^d \tag{6}$$

then

$$n < cd^{3+(\log 2+\varepsilon)/\log\log(d+2)}.$$

We now turn our attention to the number of integers n for which (6) holds. We shall modify Silverman's proof of (3) in order to establish the following result.

THEOREM 2. *Let k be a positive integer. There is a positive number $c_0 = c_0(k)$, which is effectively computable in terms of k, such that if α is a non-zero algebraic integer of degree d over the rationals which is not a root of unity then the number of positive integers n with at most k distinct prime factors for which*

$$|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\Phi_n(\alpha)| \le n^d \tag{7}$$

is at most

$$c_0 d(\log(d+1))^3(\log\log(d+2))^{k-4}.$$

If $\alpha^n - 1$ is a unit then so is $\Phi_n(\alpha)$ and as a consequence $|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\Phi_n(\alpha)| = 1$. We may then deduce from the proof of Theorem 2 our next result.

COROLLARY 1. *There is an effectively computable positive number c_1 such that if α is a non-zero algebraic integer of degree d over the rationals then*

$$E_0(\alpha) \le c_1 d(\log(d+1))^4/(\log\log(d+2))^3.$$

By definition $\alpha^j - 1$ is a unit for $1 \le j \le E_0(\alpha)$ and if α is a unit then, for $1 \le j < k \le E_0(\alpha)$,

$$(\alpha^k - 1) - (\alpha^j - 1) = \alpha^j(\alpha^{k-j} - 1),$$

which is a unit of $\mathcal{O}_K$. Therefore if α is a unit then

$$E_0(\alpha) + 2 \le L(K), \tag{8}$$

where $L(K)$ denotes the Lenstra constant of K. Recall that

$$L(K) = \sup\{m \mid \text{there exist } w_1, \dots, w_m \text{ in } \mathcal{O}_K \text{ such that } w_i - w_j \text{ is a unit for } 1 \le i < j \le m\}.$$

Thus we may take $w_1, \dots, w_m$ to be $0, 1, \alpha, \alpha^2, \dots, \alpha^{E_0(\alpha)}$ respectively and (8) follows. Lenstra [11] has shown that if $L(K)$ is large enough with respect to the discriminant of K and an associated packing constant then $\mathcal{O}_K$ is Euclidean with respect to the norm map.

2. Cyclic and cyclotomic resultants. For any pair of polynomials f and g from $\mathbb{C}[x]$, let $\mathrm{Res}(f, g)$ denote the resultant of f and g. For a non-constant polynomial f and for each positive integer n define the nth *cyclic resultant* of f, denoted $R_n(f)$, by

$$R_n(f) = \mathrm{Res}(f, x^n - 1).$$

If f factors as $f(x) = a_d(x - \alpha_1) \cdots (x - \alpha_d)$ over $\mathbb{C}$ then

$$R_n(f) = a_d^n \prod_{i=1}^{d} (\alpha_i^n - 1). \tag{9}$$

The arithmetic character of the numbers $R_n(f)$ for $f \in \mathbb{Z}[x]$ has been investigated by Pierce [13] and Lehmer [10] (see also [9]). Further, Fried [5] studied the question of whether the sequence $(R_1(f), R_2(f), \dots)$ characterizes f. He proved, in the case when f is reciprocal with real coefficients, a_d is positive and f has no roots which are roots of unity, that the sequence determines f. Hillar [7], and later Bézivin [2, 3], studied the general case and characterized polynomials f and g in $\mathbb{C}[x]$ which generate the same sequence of non-zero cyclic resultants. Hillar and Levine [8] proved that a generic monic polynomial f is determined by its first 2^{d+1} cyclic resultants and conjectured that the first $d + 1$ cyclic resultants suffice to determine f. Lehmer [10], in the case where f has integer coefficients, proved that the sequence $(R_1(f), R_2(f), \dots)$ satisfies a linear recurrence of order at most 2^d.

As a consequence of the proof of Theorem 2 we deduce the following.

COROLLARY 2. *There exists an effectively computable positive number c_2 such that if f is a non-constant monic polynomial with integer coefficients of degree d, different from x^d, with $f(1) \neq 0$ and*

$$|R_1(f)| = \cdots = |R_k(f)| \tag{10}$$

then

$$k < c_2 d(\log(d + 1))^4 / (\log\log(d + 2))^3. \tag{11}$$

Let f be a non-constant polynomial with coefficients in $\mathbb{C}$. For each positive integer n define the nth *cyclotomic resultant* of f, denoted $C_n(f)$, by

$$C_n(f) = \mathrm{Res}(f, \Phi_n(x)).$$

If f factors as $f(x) = a_d(x-\alpha_1)\cdots(x-\alpha_d)$ over $\mathbb{C}$ then

$$C_n(f) = a_d^{\varphi(n)} \prod_{i=1}^{d} \Phi_n(\alpha_i), \tag{12}$$

where $\varphi(n)$ denotes Euler's φ-function. Thus, by (2),

$$R_n(f) = \prod_{m\mid n} C_m(f). \tag{13}$$

It follows, therefore, that if (10) holds and $f(1)\neq 0$, or equivalently $C_1(f)\neq 0$, then

$$|C_2(f)| = |C_3(f)| = \cdots = |C_k(f)| = 1. \tag{14}$$

Of course if (14) holds then (10) follows from (13) and we deduce (11) once again.

3. Preliminary lemmas. Let α be an algebraic number of degree d over the rationals and let

$$f(x) = a_d x^d + \cdots + a_1 x + a_0$$

be the minimal polynomial of α over the rationals. Suppose that f factors over $\mathbb{C}$ as

$$f(x) = a_d \prod_{i=1}^{d} (x - \alpha_i).$$

The *Mahler measure*, $M(\alpha)$ of α, is defined by

$$M(\alpha) = |a_d| \prod_{i=1}^{d} \max(1, |\alpha_i|).$$

LEMMA 1. *Let α be a non-zero algebraic integer of degree d and let ε be a positive real number. There is a positive number $d_0 = d_0(\varepsilon)$, which is effectively computable in terms of ε, such that if d exceeds d_0 and*

$$M(\alpha) \le 1 + (1-\varepsilon)\left(\frac{\log\log d}{\log d}\right)^3,$$

then α is a root of unity.

Proof. This is Theorem 1 of Dobrowolski [4]. ∎

The Mahler measure is a height function and we may state our next result in terms of it. Let α_1 and α_2 be algebraic numbers different from 0 and 1 and let $\log\alpha_1$, $\log\alpha_2$ denote the principal values of the logarithms of α_1 and α_2 respectively. Let b_1 and b_2 be integers, not both zero, of absolute value at most B with $B \geq 3$. Put

$$\Lambda = b_1 \log\alpha_1 + b_2 \log\alpha_2 \quad \text{and} \quad d = [\mathbb{Q}(\alpha_1, \alpha_2) : \mathbb{Q}].$$

LEMMA 2. *There exists an effectively computable positive number c such that if $\Lambda \neq 0$ then*

$$|\Lambda| > \exp(-cd^2 \log(d+1)\log(2M(\alpha_1))\log(2M(\alpha_2))\log B).$$

Proof. This follows from the main theorem of Baker and Wüstholz [1]. ∎

We shall use Lemma 2 in the proof of our next result.

LEMMA 3. *Let α be a non-zero algebraic integer of degree d over the rationals which is not a root of unity. Let n be a positive integer. There exists an effectively computable positive number c such that*

$$(15) \qquad \log 2 + n\log(\max(|\alpha|, 1) \geq \log|\alpha^n - 1| \\ \geq n\log(\max(|\alpha|, 1)) - cd^2\log(d+1)\log(2M(\alpha))\log 3n.$$

Proof. Note that

$$\log|\alpha^n - 1| = n\log|\alpha| + \log|\alpha^{-n} - 1|,$$

and so the left hand inequality of (15) follows directly. For any complex number z, either $1/2 < |e^z - 1|$ or

$$\tfrac{1}{2}|z - ik\pi| \leq |e^z - 1|$$

for some integer k. Put $z = n\log(\alpha)$ where the logarithm takes its principal value and put

$$\Lambda = n\log(\alpha) - ik\pi$$

where k is chosen to minimize $|\Lambda|$. Observe that k is at most $2n$, $\log(-1) = i\pi$ and that

$$\Lambda = n\log(\alpha) - k\log(-1)$$

is non-zero since α is not a root of unity. Thus, by Lemma 2,

$$|\Lambda| > \exp(-cd^2\log(d+1)\log 3n \log(2M(\alpha))),$$

and (15) now follows. ∎

4. Proof of Theorem 1. Let ε be a positive real number and let $c_1, c_2, \ldots$ be positive numbers which are effectively computable in terms of ε. Let $\alpha = \alpha_1, \ldots, \alpha_d$ be the conjugates of α over $\mathbb{Q}$. The inequality

$$\mathrm{Res}(f(x), \Phi_n(x)) = \prod_{m|n} \mathrm{Res}(f(x), x^n - 1)^{\mu(n/m)}$$

implies

$$\log|N_{\mathbb{Q}(\alpha)/\mathbb{Q}}\Phi_n(\alpha)| = \sum_{i=1}^{d}\sum_{m|n}\mu\left(\frac{n}{m}\right)\log|\alpha_i^m - 1|,$$

and by Lemma 3 this is bounded below by

$$\varphi(n)\log M(\alpha) - q(n)c_1 d^3\log(d+1)\log(2M(\alpha))\log 3n,$$

where $q(n) = 2^{\omega(n)}$ denotes the number of squarefree divisors of n. If n is a positive integer for which (6) holds then

$$d\log n + q(n)c_1 d^3\log(d+1)\log(2M(\alpha))\log 3n > \varphi(n)\log M(\alpha).$$

But, by Lemma 1, $\log M(\alpha) > c_2/(\log(d+1))^3$ say, so

$$\log(2M(\alpha)) < c_3\log(M(\alpha))(\log(d+1))^3.$$

It then follows that

$$q(n)c_4 d^3(\log(d+1))^4\log(M(\alpha))\log 3n > \varphi(n)\log M(\alpha),$$

hence

$$\varphi(n)/(q(n)\log 3n) < c_4 d^3(\log(d+1))^4. \tag{16}$$

By Theorem 328 of [6],

$$\varphi(n) > c_5 n/\log\log 3n,$$

and by the prime number theorem, for $n > c_6$,

$$q(n) < 2^{(1+\varepsilon)\log n/\log\log n}.$$

Thus, by (16),

$$n < c_7 d^{3+(\log 2+\varepsilon)/\log\log(d+2)}$$

as required.

5. Further preliminaries. We shall require an estimate for the nth cyclotomic polynomial on the unit disc in terms of its roots due to Silverman [15].

LEMMA 4. *If α is a complex number of absolute value at most* 1 *which is not a root of unity and n is a positive integer then*

$$|\Phi_n(\alpha)| \ge (118n)^{-(3/2)q(n)}\min_{\substack{1\le j\le n\\ (j,n)=1}}|\alpha - \zeta_n^j|.$$

Proof. This is Proposition 3.3 of [15] provided that one notes that the proof of that proposition remains valid if we replace $\sigma_0(m)$, the number of divisors of m, by $q(m)$, the number of squarefree divisors of m. ∎

LEMMA 5. *Let α be a non-zero algebraic integer of degree d over the rationals which is not a root of unity and let k be a positive integer. There* *is a positive number $c(k)$, which is effectively computable in terms of k, such that there are at most d integers n for which* (7) *holds with n larger than*

$$c(k)d(\log(d+1))^4/(\log\log(d+2))^3$$

and composed of at most k distinct prime factors.

Proof. Let $c_1, c_2, \ldots$ denote positive numbers which are effectively computable in terms of k. Suppose that n is at least 2. Let $\alpha = \alpha_1, \ldots, \alpha_d$ be the conjugates of α and define $\beta_1, \ldots, \beta_d$ by

$$\beta_i = \begin{cases} \alpha_i & \text{if } |\alpha_i| \le 1, \\ \alpha_i^{-1} & \text{if } |\alpha_i| > 1. \end{cases}$$

Then

$$|N_{\mathbb{Q}(\alpha)/\mathbb{Q}} \Phi_n(\alpha)| = M(\alpha)^{\varphi(n)} \prod_{i=1}^{d} |\Phi_n(\beta_i)|. \tag{17}$$

By Lemma 4,

$$\prod_{i=1}^{d} |\Phi_n(\beta_i)| \ge n^{-c_1 d} \Big(\min_{1 \le i \le d} \min_{\substack{1 \le j \le n \\ (j,n)=1}} |\beta_i - \zeta_n^j| \Big)^d. \tag{18}$$

Thus, by (7), (17) and (18),

$$\min_{1 \le i \le d} \min_{\substack{1 \le j \le n \\ (j,n)=1}} |\beta_i - \zeta_n^j| \le n^{c_2} M(\alpha)^{-\varphi(n)/d}. \tag{19}$$

But since n has at most k distinct prime factors, we find that $\varphi(n) > c_3 n$, and so, by Lemma 1,

$$M(\alpha)^{-\varphi(n)/d} < e^{-c_4 n d^{-1} (\frac{\log\log(d+2)}{\log(d+1)})^3}. \tag{20}$$

Thus, by (19) and (20),

$$\min_{1 \le i \le d} \min_{\substack{1 \le j \le n \\ (j,n)=1}} |\beta_i - \zeta_n^j| < e^{c_2 \log n - c_5 n d^{-1} (\frac{\log\log(d+2)}{\log(d+1)})^3}. \tag{21}$$

Therefore for

$$n > c_6 d(\log(d+1))^4/(\log\log(d+2))^3 \tag{22}$$

we find that

$$\min_{1 \le i \le d} \min_{\substack{1 \le j \le n \\ (j,n)=1}} |\beta_i - \zeta_n^j| < (d+1)^{-c_7}. \tag{23}$$

Suppose now that there are $d+1$ integers n satisfying (7) and (22) with at most k distinct prime factors. Then two of the integers, n_1 and n_2 say, take the minimum over i in (23) at the same integer i_0. In particular there are integers j_1 and j_2 with $1 \le j_1 \le n_1$, $(j_1, n_1) = 1$ and $1 \le j_2 \le n_2$, $(j_2, n_2) = 1$ such that

$$|\beta_{i_0} - \zeta_{n_1}^{j_1}| < (d+1)^{-c_7} \quad \text{and} \quad |\beta_{i_0} - \zeta_{n_2}^{j_2}| < (d+1)^{-c_7}.$$

Therefore

$$(24) \qquad |\zeta_{n_1}^{j_1} - \zeta_{n_2}^{j_2}| \le |\beta_{i_0} - \zeta_{n_1}^{j_1}| + |\beta_{i_0} - \zeta_{n_2}^{j_2}| < 2(d+1)^{-c_7}.$$

On the other hand

$$|\zeta_{n_1}^{j_1} - \zeta_{n_2}^{j_2}| = |e^{2\pi i(j_1 n_2 - j_2 n_1)/n_1 n_2} - 1|,$$

and since $j_1 n_2 - j_2 n_1$ is non-zero,

$$(25) \qquad |\zeta_{n}^{j_1} - \zeta_{n_2}^{j_2}| \ge |e^{2\pi i/n_1 n_2} - 1| \ge 1/n_1 n_2.$$

Now, by (24) and (25),

$$2n_1 n_2 > (d+1)^{c_7},$$

and if we suppose that $n_1 < n_2$ we see that

$$(26) \qquad n_2 > ((d+1)^{c_7}/2)^{1/2}.$$

On the other hand, by Theorem 1 with $\varepsilon = 1/4$,

$$n_2 < c_8(d+1)^4$$

and this is incompatible with (26) provided c_7 is sufficiently large. Note that we can ensure that c_7 is as large as required by choosing c_6 appropriately. The result now follows. ■

6. Proof of Theorem 2. By Lemma 5 there are at most d integers n, composed of at most k prime factors, for which (7) holds with n larger than $c(k)d\log(d+1)^4/(\log\log(d+2))^3$. Our result now follows from estimates for the number of integers up to a given bound having at most k prime factors, see Theorem 437 of [6].

7. Proof of Corollary 1. Let $c_1, c_2, \ldots$ denote positive effectively computable numbers.

On taking $k = 1$ in Lemma 5 we see that provided that α is a non-zero algebraic integer of degree d which is not a root of unity, there are at most d terms $\Phi_p(\alpha)$ which are units for p a prime greater than $c(1)d(\log(d+1))^4/(\log\log(d+2))^3$. Thus there is, by the prime number theorem, a prime p_1 with

$$p_1 < c_2 d(\log(d+1))^4/(\log\log(d+2))^3$$

for which $\Phi_{p_1}(\alpha)$ is not a unit, hence for which $\alpha^{p_1} - 1$ is not a unit. Furthermore, if α is a root of unity of degree d then $\alpha^n - 1$ is zero for some positive integer n with

$$n < c_3 d \log\log(d+2)$$

since for any positive integer m,

$$\varphi(m) > c_4 m / \log\log(m+2).$$

The result now follows.

8. Proof of Corollary 2. As we remarked in §2, if (10) holds and $f(1) \neq 0$ then (14) holds. Since f is different from x^d there is a non-zero root α of f. Let f_1 be the irreducible polynomial of α over $\mathbb{Q}$. Then

$$1 = |C_2(f_1)| = |C_3(f_1)| = \cdots = |C_k(f_1)|.$$

Our result follows from Lemma 5 as in the proof of Corollary 1.

9. Computations for small degrees. Let

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0 \tag{27}$$

with $a_0, a_1, \ldots, a_{d-1}$ integers. For d small we shall determine the polynomials f, different from x^d, with

$$1 = |R_1(f)| = \cdots = |R_k(f)| \tag{28}$$

and k as large as possible. By (13) this is equivalent to finding f so that

$$1 = |C_1(f)| = \cdots = |C_k(f)| \tag{29}$$

with k as large as possible. Observe that if α is a non-zero algebraic integer of degree d then $E_0(\alpha) \leq k$.

In addition to (12) we have

$$C_n(f) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} f(\zeta_n^j),$$

or equivalently

$$C_n(f) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} (\zeta_n^{jd} + a_{d-1}\zeta^{j(d-1)} + \cdots + a_0).$$

Let ε_n be from $\{1, -1\}$ and put

$$g_{n,\varepsilon_n}[y_0, \ldots, y_{d-1}] = \Big(\prod_{\substack{j=1 \\ (j,n)=1}}^{n} (\zeta_n^{jd} + y_{d-1}\zeta^{j(d-1)} + \cdots + y_0) \Big) - \varepsilon_n.$$

Note that g_{n,ε_n} is a polynomial with integer coefficients.

Let $V_n(\varepsilon_n)$ be the affine variety over $\mathbb{C}$ defined by

$$V_n(\varepsilon_n) = \{(t_0, \ldots, t_{d-1}) \in \mathbb{C}^d \mid g_{n,\varepsilon_n}(t_0, \ldots, t_{d-1}) = 0\}.$$

There is a monic polynomial f with integer coefficients satisfying (29) and different from x^d provided that for some sequence $(\varepsilon_1, \ldots, \varepsilon_k)$ with ε_i in

$\{1,-1\}$ for $i = 1,\dots,k$ there is an integer point $(a_0,\dots,a_{d-1})$, different from $(0,0,\dots,0)$, on the variety

$$V_1(\varepsilon_1)\cap\dots\cap V_k(\varepsilon_k). \tag{30}$$

We have used Groebner basis techniques to study varieties of the form (30) for small degrees d. In particular, we call on the program `Basis` in the Groebner package in the symbolic computation system `Maple`. By taking k to be d and considering each possible sequence $(\varepsilon_1,\dots,\varepsilon_d)$ in turn we are able to find all polynomials f of degree d satisfying (28) and (29) for $k = d$ and $d = 1,\dots,6$. On calling on `Basis` in reverse lexicographic order we find, as the first term in the Groebner basis, a polynomial in t_0 which we then test for integer roots. Once t_0 is determined we then proceed to $t_1,\dots,t_{d-1}$. In this manner we have found that the largest integer k for which (28) holds is d for $d = 1,\dots,6$ and that for $d = 7$ we have $k = 6$. We give below the complete list of polynomials of degree d, different from x^d, for which (28) holds with $k = d$ and $d = 1,\dots,6$:

d	$f(x)$	d	$f(x)$
1	$x-2$	4	x^4+x^3-1
			x^4-x-1
2	x^2+x-1	5	$x^5+x^4+x^3-x-1$
	x^2-x-1		$x^5+x^4-x^2-x-1$
	x^2-2		
3	x^3+x^2-1	6	x^6+x^4-1
	x^3-x-1		x^6-x^2-1

For none of these polynomials does (28) hold with $k = d+1$.

For $d = 7$ there are no monic polynomials with integer coefficients, different from x^7, for which (28) holds with $k = 7$. Note that $x(x^6+x^4-1)$ and $x(x^6-x^2-1)$ are monic polynomials of degree 7 with integer coefficients, different from x^7, for which (28) holds with $k = 6$. However there are no polynomials f of degree 7 as in (27) with $|a_0| = 1$ for which (28) holds with $k = 6$. By contrast there are exactly two polynomials f as in (27) of degree 8 with $|a_0| = 1$ for which (28) holds with $k = 7$, and they are

$$x^8+x^7+x^6+x^5-x^2-x-1 \quad \text{and} \quad x^8+x^7+x^6-x^3-x^2-x-1.$$

The computations for the results in this paragraph required 38.7 CPU days and they were done on the cluster Gamay at the University of Waterloo and supported by a CFI/OIT grant. I would like to thank Kevin G. Hare for providing access to this cluster and for helping me to adapt my computer program to this setting.

For any positive integer d let us define $e(d)$ by

$$e(d) = \max\{E_0(\alpha) \mid \alpha \text{ an algebraic integer of degree } d\}.$$

Our results show that

$$e(d) = d \quad \text{for } d = 1, \ldots, 6$$

and that

$$e(7) < 7 \quad \text{and} \quad e(8) \geq 7.$$

We suspect that $e(d) < d$ for $d \geq 7$.

Acknowledgments. This research was supported in part by the Canada Research Chairs Program and by Grant A3528 from the Natural Sciences and Engineering Research Council of Canada.

References

[1] A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. Reine Angew. Math. 442 (1993), 19–62.
[2] J.-P. Bézivin, *Sur les résultants cycliques*, Proc. Japan Acad. Ser. A Math. Sci. 83 (2007), 157–160.
[3] J.-P. Bézivin, *Résultants cycliques et polynômes cyclotomiques*, Acta Arith. 131 (2008), 171–181.
[4] E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. 34 (1979), 391–401.
[5] D. Fried, *Cyclic resultants of reciprocal polynomials*, in: Holomorphic Dynamics (Mexico, 1986), Lecture Notes in Math. 1345, Springer, 1988, 124–128.
[6] G. H. Hardy and E. M. Wright, *An Introduction to the Theory of Numbers*, 5th ed., Oxford Univ. Press, 1979.
[7] C. J. Hillar, *Cyclic resultants*, J. Symbolic Comput. 39 (2005), 653–669; Erratum, ibid. 40 (2005), 1126–1127.
[8] C. J. Hillar and L. Levine, *Polynomial recurrences and cyclic resultants*, Proc. Amer. Math. Soc. 135 (2007), 1607–1618.
[9] J. C. Lagarias and A. M. Odlyzko, *Divisibility properties of some cyclotomic sequences*, Amer. Math. Monthly 87 (1980), 561–564.
[10] D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. 34 (1933), 461–479.
[11] H. W. Lenstra, Jr., *Euclidean number fields of large degree*, Invent. Math. 38 (1977), 237–254.
[12] M. J. Mossinghoff, C. G. Pinner and J. D. Vaaler, *Perturbing polynomials with all their roots on the unit circle*, Math. Comp. 67 (1998), 1707–1726.
[13] T. A. Pierce, *The numerical factors of the arithmetic forms* $\prod_{i=1}^{n}(1 \pm \alpha_i^m)$, Ann. of Math. 18 (1916), 53–64.
[14] A. Schinzel, *Primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields*, J. Reine Angew. Math. 268/269 (1974), 27–33.
[15] J. H. Silverman, *Exceptional units and numbers of small Mahler measure*, Experiment. Math. 4 (1995), 69–83.

[16] C. L. Stewart, *Primitive divisors of Lucas and Lehmer numbers*, in: Transcendence Theory: Advances and Applications, A. Baker and D. W. Masser (eds.), Academic Press, 1977, 79–92.

C. L. Stewart
Department of Pure Mathematics
University of Waterloo
Waterloo, Ontario, Canada
E-mail: cstewart@uwaterloo.ca

Received on 9.11.2011
and in revised form on 22.2.2012 (6885)