Exceptional units and cyclic resultants, II

C.L. Stewart

ABSTRACT. Let α be a non-zero algebraic integer and put $K = \mathbb{Q}(\alpha)$. In this article we give estimates for the largest integer n such that $\alpha^j - 1$ is a unit in the ring of algebraic integers of K for $1 \le j \le n$ and for related quantities.

1. Introduction

Let α be a non-zero algebraic integer and put $K = \mathbb{Q}(\alpha)$. Let d be the degree of K over $\mathbb{Q}$ and let $\mathcal{O}_K$ denote the ring of algebraic integers of K. For each positive integer n put $\zeta_n = e^{2\pi i/n}$ and denote the n-th cyclotomic polynomial in x by $\Phi_n(x)$, so

$$\Phi_n(x) = \prod_{\substack{j=1 \\ (j,n)=1}}^{n} (x - \zeta_n^j). \tag{1.1}$$

Let $E(\alpha)$ be the number of positive integers n for which $\alpha^n - 1$ is a unit and let $U(\alpha)$ be the number of positive integers n for which $\Phi_n(\alpha)$ is a unit. Note that $E(\alpha)$ and $U(\alpha)$ may be infinite if α is a root of unity. If $\alpha - 1$ is not a unit put $E_0(\alpha) = 0$ and otherwise define $E_0(\alpha)$ to be the largest integer n such that $\alpha^j - 1$ is a unit for $1 \le j \le n$. Since

$$x^n - 1 = \prod_{m|n} \Phi_m(x), \tag{1.2}$$

we see that

$$E_0(\alpha) \le E(\alpha) \le U(\alpha). \tag{1.3}$$

In 1995 Silverman, (see Theorem 4.1 of [**10**]), investigated the function $U(\alpha)$ in connection with his study of numbers having small Mahler measure. He proved that for each positive real number ε there is an effectively computable positive number $c = c(\varepsilon)$ such that if α is an algebraic unit of degree $d \ge 2$ that is not a root of unity then

$$U(\alpha) < cd^{1+(\log 2+\varepsilon)/\log\log d}. \tag{1.4}$$

2010 *Mathematics Subject Classification.* Primary 11R27; Secondary 11J68.

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.

In 1998 Mossinghoff, Pinner and Vaaler [**8**], sharpening an earlier result of Boyd [**10**], remarked that there are α, not roots of unity, of arbitrarily large degree d for which

$$E_0(\alpha) > \pi\sqrt{\frac{d}{3}} + 0(\log d). \tag{1.5}$$

In [**13**] we showed that 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

$$E_0(\alpha) \le c_1 d(\log(d+1))^4/(\log\log(d+2))^3. \tag{1.6}$$

For any β in $\mathbb{Q}(\alpha)$ we denote the norm of β from $\mathbb{Q}(\alpha)$ to $\mathbb{Q}$ by $N\beta$. Estimates (1.4) and (1.6) were deduced from estimates for integers n for which $N\Phi_n(\alpha)$ is small in absolute value. For instance in [**13**], sharpening earlier work in [**12**], we proved that for each positive real number ε 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

$$|N\Phi_n(\alpha)| \le n^d$$

then

$$n < cd^{3+(\log 2+\varepsilon)/\log\log(d+2)}. \tag{1.7}$$

Of course if $\Phi_n(\alpha)$ is a unit then $|N\Phi_n(\alpha)| = 1$ and so the right hand side of (1.7) gives an upper bound for those integers n for which $\Phi_n(\alpha)$ is a unit and so, by (1.2), for which $\alpha^n - 1$ is a unit.

If α is a unit for which $\alpha - 1$ is also a unit then α is known as an exceptional unit. Further, if α is a unit then the difference of any two elements of $\{0, 1, \alpha, \ldots, \alpha^{E_0(\alpha)}\}$ is a unit. Put

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

Then

$$E_0(\alpha) + 2 \le L(K).$$

$L(K)$ is known as the Lenstra constant of K and in [**7**] Lenstra showed that if $L(K)$ is large relative to the discriminant then $\mathcal{O}_K$ is Euclidean with respect to the norm map.

Let $f(x)$ be a non-constant polynomial with integer coefficients and degree d and suppose that f factors over $\mathbb{C}$ as

$$f(x) = a_d(x-\alpha_1)\cdots(x-\alpha_d). \tag{1.8}$$

The n-th cyclic resultant of f, denoted by $R_n(f)$, is the resultant of f and $x^n - 1$. Thus

$$R_n(f) = a_d^n \prod_{i=1}^{d} (\alpha_i^n - 1). \tag{1.9}$$

In 1933 Lehmer [**5**] showed that the sequence of integers $(R_1(f), R_2(f), \ldots)$ satisfies a linear recurrence relation of order at most 2^d. In addition he studied, following earlier work of Pierce [**9**], the divisibility properties of the terms of the sequence. This led him to search for polynomials for which the sequence grows slowly with the idea that this would give an efficient way to find large prime numbers. The growth of the terms $|R_n(f)|$ is roughly $M(f)^n$ where $M(f)$ denotes the Mahler measure of f. Recall that if $f(x) = a_d x^d + \cdots + a_1 x + a_0$ is a polynomial with integer coefficients and f factors over $\mathbb{C}$ as in (1.8) then

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

Further for any algebraic number α we define $M(\alpha)$ to be $M(f)$ where f is the minimal polynomial of α over the integers. In [**5**] Lehmer posed the fundamental question of whether for each positive number ε there is a polynomial f with integer coefficients such that $1 < M(f) < 1 + \varepsilon$. Lehmer's question remains open although Smyth [**11**] proved that if we restrict to non-reciprocal polynomials the answer is no. In the general situation the best known result is due to Dobrowolski [**3**].

Let f be as in (1.8). For each positive integer n define the n-th cyclotomic resultant of f, denoted $C_n(f)$, to be the resultant of f and $\Phi_n(x)$. Then

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

where $\varphi(n)$ denotes Euler's function. By (1.2),

$$R_n(f) = \prod_{m|n} C_m(f). \tag{1.10}$$

$|C_n(f)|$ is roughly $M(f)^{\varphi(n)}$ and we shall make this claim more precise.

Our first result is of a similar nature to (1.7).

Theorem 1.1. *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*

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

then

$$M(\alpha)^{(1-\varepsilon)\varphi(n)} < |N\Phi_n(\alpha)| < M(\alpha)^{(1+\varepsilon)\varphi(n)}. \tag{1.11}$$

Our second result may be viewed as a counterpart to Silverman's estimate (1.4) and our proof follows closely his proof of Theorem 0.1 of [**10**].

Theorem 1.2. *Let ε be a positive real number. There is a positive number $c_1 = c_1(\varepsilon)$, 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 then the number of positive integers n for which*

$$|N\Phi_n(\alpha)| < M(\alpha)^{(1-\varepsilon)\varphi(n)} \tag{1.12}$$

is at most

$$c_1 d^{1+(\log 2+\varepsilon)/\log\log(d+2)}.$$

Our next result shows that estimate (1.6) is close to best possible. Let γ denote Euler's constant, so

$$\gamma = 1 - \int_1^\infty \frac{t-[t]}{t^2} dt.$$

Note that $e^\gamma = 1.7810\ldots$.

Theorem 1.3. *For each positive real number ε, there exist roots of unity α of arbitrarily large degree d for which*

$$E_0(\alpha) > (e^\gamma - \varepsilon) d \log\log d / \log d. \tag{1.13}$$

The lower bound (1.13) may be contrasted with that of (1.5) where roots of unity α are excluded from consideration.

Finally we shall discuss computations related to the function $E_0(\alpha)$ in the last section of this paper.

2. Preliminary lemmas

We shall first record Dobrowolski's Theorem [**3**].

Lemma 2.1. *There is an effectively computable positive real number c such that if α is a non-zero algebraic integer of degree d and*

$$M(\alpha) \le 1 + c\left(\frac{\log\log(d+2)}{\log(d+1)}\right)^3,$$

then α is a root of unity.

We shall also need the following result which is a consequence of the main theorem of Baker and Wüstholz [**2**].

Lemma 2.2. *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*

$$\begin{aligned} \log 2 + n\log(\max(|\alpha|,1)) &\ge \log|\alpha^n - 1| \\ &\ge n\log(\max(|\alpha|,1)) - cd^2\log(d+1)\log(2M(\alpha))\log 3n. \end{aligned}$$

Proof. This is Lemma 3 of [**13**]. □

For any positive integer n let $q(n)$ denote the number of squarefree divisors of n.

Lemma 2.3. *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 may be deduced from the proof of Proposition 3.3 of [**10**], due to Silverman. □

3. Proof of Theorem 1.1

Let ε be a positive real number and let $c_1, c_2, \dots$ be positive numbers which are effectively computable in terms of ε. Let $\alpha = \alpha_1, \dots, \alpha_d$ be the conjugates of α over $\mathbb{Q}$. It follows from (1.2) by Möbius inversion that

$$\log|N\Phi_n(\alpha)| = \sum_{i=1}^{d}\sum_{m|n}\mu\left(\frac{n}{m}\right)\log|\alpha_i^m - 1|.$$

Thus, by Lemma 2.2,

$$|\log|N\Phi_n(\alpha)| - \varphi(n)\log M(\alpha)| < c_1 q(n) d^3 \log(d+1)\log(2M(\alpha))\log 3n.$$

Suppose that (1.11) does not hold. We then have

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

By Lemma 2.1

$$\varepsilon\varphi(n) < c_2 q(n) d^3 (\log(d+1))^4 \log 3n.$$

For any positive integer n let $\omega(n)$ denote the number of distinct prime factors of n. Then

$$(\varphi(n)/2^{\omega(n)}\log 3n) < c_3 d^3 (\log(d+1))^4. \tag{3.1}$$

By Theorem 328 of [**4**],

$$\varphi(n) > c_4 n/\log\log 3n, \tag{3.2}$$

and by the prime number theorem $\omega(n)$ is at most $(1+o(1))\log n/\log\log n$. Therefore by (3.1) and (3.2)

$$n < c_5 d^{3+(\log 2+\varepsilon)/\log\log(d+2)}$$

whenever (1.11) does not hold, as required.

4. Proof of Theorem 1.2

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

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

Then

$$|N\Phi_n(\alpha)| = M(\alpha)^{\varphi(n)} \prod_{i=1}^{d} |\Phi_n(\beta_i)|. \tag{4.1}$$

By Lemma 2.3

$$\prod_{i=1}^{d} |\Phi_n(\beta_i)| \ge n^{-c_1 q(n) d} \left(\min_{1\le i\le d} \min_{\substack{1\le j\le n\\ (j,n)=1}} |\beta_i - \zeta_n^j| \right)^d. \tag{4.2}$$

Therefore by (1.12), (4.1), and (4.2),

$$\min_{1\le i\le d} \min_{\substack{1\le j\le n\\ (j,n)=1}} |\beta_i - \zeta_n^j| \le n^{c_1 q(n)} M(\alpha)^{-\varepsilon\varphi(n)/d}. \tag{4.3}$$

Observe that

$$c_1 q(n) \log n < c_2 \exp\left(\left(\log 2 + \frac{\varepsilon}{2}\right)\log n/\log\log n\right) \tag{4.4}$$

and, by Lemma 2.1,

$$\varepsilon\varphi(n)(\log(M(\alpha))/d > c_3 \frac{n}{\log\log n}\frac{1}{d}\left(\frac{\log\log(d+2)}{\log(d+1)}\right)^3. \tag{4.5}$$

The right hand side of inequality (4.5) is more than double the right hand side of inequality (4.4) provided that n exceeds

$$c_4 d \exp((\log 2+\varepsilon)\log(d+1)/\log\log(d+2)). \tag{4.6}$$

In this case

$$c_1 q(n)\log n - \varepsilon\varphi(n)(\log(M(\alpha))/d < -c_5\exp\left(\left(\log 2+\frac{\varepsilon}{2}\right)\frac{\log(d+1)}{\log\log(d+2)}\right)$$

and so, by (4.3),

$$\min_{1\le i\le d}\ \min_{\substack{1\le j\le d\\(j,d)=1}} |\beta_i-\zeta_n^j| < \exp(-c_5 d^{\log 2/\log\log(d+2)}). \tag{4.7}$$

Suppose that there are $d+1$ integers n satisfying (1.12) and (4.6). Two of the integers n_1 and n_2 say take the minimum over i in (4.7) at the same integer i_0. Therefore 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

$$|\beta_{i_0}-\zeta_{n_k}^{j_k}| < \exp(-c_5 d^{\log 2/\log\log(d+2)})\quad\text{for } k=1,2.$$

Thus

$$|\zeta_{n_1}^{j_1}-\zeta_{n_2}^{j_2}| < 2\exp(-c_5 d^{\log 2/\log\log(d+2)}). \tag{4.8}$$

On the other hand, since $(j_1,n_1)=1$ and $(j_2,n_2)=1$,

$$|\zeta_{n_1}^{j_1}-\zeta_{n_2}^{j_2}| = |e^{2\pi i(j_1n_2-j_2n_1)/n_1n_2}-1| \ge |e^{2\pi i/n_1n_2}-1| \ge \frac{1}{n_1n_2}. \tag{4.9}$$

Therefore, by (4.8) and (4.9),

$$2n_1n_2 > \exp(c_5 d^{\log 2/\log\log(d+2)}).$$

We may suppose that n_2 exceeds n_1 hence

$$n_2 > \frac{1}{\sqrt{2}}\exp\left(\frac{1}{2}c_5 d^{\log 2/\log\log(d+2)}\right). \tag{4.10}$$

On the other hand, since (1.12) holds, it follows from Theorem 1.1 that

$$n_2 < c_6 d^4 \tag{4.11}$$

and a comparison of (4.10) and (4.11) yields a contradiction for c_5 sufficiently large which we can ensure by taking c_4 sufficiently large in (4.6). Our result now follows since the number of positive integers n for which (1.12) holds is at most

$$d + c_4 d\exp((\log 2+\varepsilon)\log(d+1)/\log\log(d+2)),$$

as required.

5. Proof of Theorem 1.3

Let n be a positive integer and put

$$m = \text{l.c.m.}[1,\ldots,n],$$

where l.c.m. denotes the least common multiple. Let $\alpha=\zeta_m$ so that the degree of α is d with

$$d=\varphi(m).$$

Then, by Merten's Theorem (see Theorem 429 of [**4**]),

$$d = m\prod_{p\le n}\left(1-\frac{1}{p}\right) = (e^{-\gamma}+o(1))m/\log n.$$

Further it follows from the prime number theorem, in particular estimates for $\pi(x)$ and $\psi(x)$, that

$$m = e^{(1+o(1))n},$$

hence that

$$n = (1 + o(1)) \log m. \tag{5.1}$$

Therefore

$$d = (e^{-\gamma} + o(1))m/ \log\log m$$

hence

$$m = (e^{\gamma} + o(1))d \log\log d. \tag{5.2}$$

By (1.9) and (1.10), $E_0(\alpha) = E_0(\zeta_m)$ is the largest positive integer k for which $|C_j(\Phi_m)| = 1$ for $j = 1, \dots, k$. By Theorems 1 and 4 of Apostol [**1**], see also [**6**], we see that if r and s are positive integers with $r > s \geq 1$ then

$$C_r(\Phi_s) = 1$$

unless r/s is a power of a prime p in which case $C_r(\Phi_s) = p^{\varphi(s)}$. Thus $C_j(\Phi_m) = 1$ for $1 \leq j \leq (m/p^a) - 1$ where p^a is the largest prime power which divides m. Certainly p^a is at most n from the definition of m and thus

$$E_0(\alpha) \geq \frac{m}{n} - 1. \tag{5.3}$$

By (5.1) and (5.2)

$$\frac{m}{n} - 1 = (e^{\gamma} + o(1)) \frac{d \log\log d}{\log d}.$$

Our result now follows from (5.3).

6. Computations for small degrees

For any positive integer d we define $e(d)$ by

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

In [**13**] we established that $e(d) = d$ for $d = 1, \dots, 6$, that $e(7) < 7$ and $e(8) \geq 7$. In addition, we conjectured that $e(d) < d$ for $d \geq 7$. These results were proved using Groebner basis techniques in conjunction with the symbolic computation system `Maple`.

We shall extend our computations by restricting our attention to algebraic integers α whose minimal polynomial f has coefficients from $\{-1, 0, 1\}$. In particular

$$f(x) = x^d + a_{d-1}x^{d-1} + \cdots + a_0, \tag{6.1}$$

where a_0 is in $\{-1, 1\}$ and a_j is in $\{-1, 0, 1\}$ for $j = 1, \dots, d-1$. Further we have

$$1 = |R_1(f)| = \cdots = |R_k(f)|$$

or, by (1.10),

$$1 = |C_1(f)| = \cdots = |C_k(f)|, \tag{6.2}$$

and we seek to maximize k for each degree d. For fixed degree the set of f we must consider is finite and for each f we calculate $C_1(f), C_2(f), \dots$ until we find a term for which the cyclotomic resultant with f is different from 1 in absolute value. We performed our computations using `Maple`. For d up to 15 we used our personal computer. In order to treat the range up to 20 we made use of the cluster Gamay at the University of Waterloo. 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.

We remark that if f, as in (6.1), satisfies (6.2) then so does $\tilde{f}(x) = a_0 x^d f(1/x)$ and in the table below we list only one term of the pair $\{f, \tilde{f}\}$. In addition we have checked that the polynomials listed in Table 1 are irreducible over the rationals.

Table 1

Monic polynomials of degree d with coefficients from $\{-1, 0, 1\}$, constant coefficient from $\{-1, 1\}$ and for which k $(= k(d))$ is maximal in (6.2).

d	$k(d)$	Representative of $\{f, \tilde{f}\}$
2	2	$x^2 + x - 1$
3	3	$x^3 + x^2 - 1$
4	4	$x^4 + x^3 - 1$
5	5	$x^5 + x^4 + x^3 - x - 1$
6	6	$x^6 + x^4 - 1$
7	5	$x^7 + x^6 + x^5 + x^4 - x^2 - x - 1$
8	7	$x^8 + x^7 + x^6 + x^5 - x^2 - x - 1$
9	6	$x^9 + x^8 + x^7 + x^6 + x^5 - x^3 - x^2 - x - 1$ $x^9 + x^8 + x^7 + x^6 - x^3 - x^2 - 1$
10	8	$x^{10} + x^8 + x^6 - x^2 - 1$
11	7	$x^{11} + x^{10} + x^9 - x^7 - x^6 - x^5 - x^4 - x^3 + 1$
12	8	$x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 - x^4 - x^3 - x^2 - x - 1$
13	8	$x^{13} + x^{12} + x^{11} + x^{10} + x^9 + x^8 + x^7 - x^5 - x^4 - x^3 - x^2 - x - 1$
14	10	$x^{14} + x^{12} + x^{10} + x^8 - x^4 - x^2 - 1$
15	8	$x^{15} + x^{14} + x^{13} + x^{12} + x^{11} + x^{10} - x^7 - x^6 - x^5 - x^4 - x^3 - x^2 - 1$ $x^{15} + x^{13} + x^{11} - x^8 - x^7 - x^5 - x^3 + x^2 + 1$ $x^{15} + x^{13} + x^{11} - x^8 - x^7 - x^6 - x^5 - x^3 + 1$
16	11	$x^{16} + x^{14} - x^{10} - x^8 - x^6 + x^2 + 1$
17	9	$x^{17} + x^{16} + x^{15} + x^{14} + x^{13} - x^9 - x^8 - x^7 - x^6 - x^5 + 1$

d	$k(d)$	Representative of $\{f, \tilde{f}\}$
18	8	$x^{18}+x^{17}+x^{16}+x^{15}+x^{14}+x^{13}+x^{12}+x^{11}-x^{6}-x^{5}-x^{4}-x^{3}-x^{2}-x-1$
		$x^{18}+x^{16}+x^{15}+x^{14}+x^{12}+x^{11}-x^{6}-x^{4}-x^{3}-x^{2}-1$
		$x^{18}+x^{16}+x^{14}+x^{12}+x^{7}-x^{6}-x^{4}-x^{2}-1$
		$x^{18}-x^{16}+x^{14}-x^{12}+x^{9}-x^{6}+x^{4}-x^{2}+1$
19	8	$x^{19}+x^{18}+x^{17}+x^{16}+x^{15}-x^{13}-x^{12}-x^{11}-x^{10}+x^{8}+x^{7}+x^{6}+x^{5}-x^{3}-x^{2}-x-1$
		$x^{19}+x^{18}+x^{16}+x^{15}-x^{10}-x^{7}-x^{4}-x^{3}-1$
		$x^{19}+x^{18}+x^{16}+x^{15}-x^{13}-x^{11}-x^{10}-x^{9}+x^{5}+x-1$
		$x^{19}+x^{17}+x^{15}+x^{13}-x^{12}-x^{10}-x^{9}-x^{8}-x^{7}-x^{5}+x^{4}+x^{2}+1$
20	11	$x^{20}+x^{19}+x^{18}+x^{17}-x^{14}-x^{13}-x^{12}-x^{11}-x^{10}-x^{9}-x^{8}-x^{7}-x^{6}+x^{3}+x^{2}+x+1$

All of the polynomials in the table above are irreducible and so each one is the minimal polynomial of a unit. Only one of the polynomials corresponds to a root of unity and that is $x^{16}+x^{14}-x^{10}-x^{8}-x^{6}+x^{2}+1$ which is $\Phi_{60}(x)$. Apart from $\Phi_{60}(x)$ there is exactly one equivalence class of monic irreducible polynomials of degree 16 with coefficients from $\{-1,0,1\}$ for which (6.2) holds with $k=8$. A representative of the equivalence class is $f(x)=x^{16}+x^{14}+x^{12}+x^{10}-x^{4}-x^{2}-1$. In particular we have $f(\zeta_n)$ is a unit for $n=1,\ldots,8$ but $f(\zeta_9)$ is not a unit.

Note that $e(d)\geq k(d)$ where $k=k(d)$ is given in the above table.

References

1. T. M. Apostol, *Resultants of cyclotomic polynomials*, Proceedings of the A.M.S. **24** (1970), 457–462.
2. A. Baker and G. Wüstholz, *Logarithmic forms and group varieties*, J. reine angew. Math. **442** (1993), 19–62.
3. E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.
4. G. H. Hardy and E. M. Wright, *An introduction to the theory of numbers*, 5th edn., Oxford University Press, 1979.
5. D. H. Lehmer, *Factorization of certain cyclotomic functions*, Ann. of Math. **34** (1933), 461–479.
6. E. T. Lehmer, *A numerical function applied to cyclotomy*, Bull. Amer. Math. Soc. **36** (1930), 291–298.
7. H. W. Lenstra, Jr., *Euclidean number fields of large degree*, Inventiones Math. **38** (1977), 237–254.
8. 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.
9. T. A. Pierce, *The numerical factors of the arithmetic forms* $\prod_{i=1}^{n}(1\pm\alpha_i^m)$, Ann. of Math. **18** (1917), 53–64.
10. J. H. Silverman, *Exceptional units and numbers of small Mahler measure*, Experimental Math. **4** (1995), 69–83.
11. C. J. Smyth, *On the product of the conjugates outside the unit circle of an algebraic integer*, Bull. London Math. Soc. **3** (1971), 169–175.

12. C. L. Stewart, *Primitive divisors of Lucas and Lehmer numbers*, pp. 79–92 in Transcendence Theory: Advances and Applications (edited by A. Baker and D.W. Masser), Academic Press, London, 1977.
13. C. L. Stewart, *Exceptional units and cyclic resultants*, Acta Arithmetica, to appear.

Department of Pure Mathematics, University of Waterloo, Waterloo, Ontario, Canada N2L 3G1

E-mail address: cstewart@uwaterloo.ca