MATHEMATICS OF COMPUTATION
VOLUME 61, NUMBER 203
JULY 1993, PAGES 441–444

AN EXTENSION OF THE THEOREM ON PRIMITIVE DIVISORS IN ALGEBRAIC NUMBER FIELDS

A. SCHINZEL

In memory of D. H. Lehmer

ABSTRACT. The theorem about primitive divisors in algebraic number fields is generalized in the following manner. Let A, B be algebraic integers, $(A, B) = 1$, $AB \neq 0$, A/B not a root of unity, and ζ_k a primitive root of unity of order k. For all sufficiently large n, the number $A^n - \zeta_k B^n$ has a prime ideal factor that does not divide $A^m - \zeta_k^j B^m$ for arbitrary $m < n$ and $j < k$.

The analogue of Zsigmondy's theorem in algebraic number fields [3] asserts the following.

If A, B are algebraic integers, $(A, B) = 1$, $AB \neq 0$, and A/B of degree d is not a root of unity, there exists a constant $n_0(d)$ such that for $n > n_0(d)$, $A^n - B^n$ has a prime ideal factor that does not divide $A^m - B^m$ for $m < n$.

This theorem will be extended as follows:

Theorem. *Let K be an algebraic number field, A, B integers of K, $(A, B) = 1$, $AB \neq 0$, A/B of degree d not a root of unity, and ζ_k a primitive kth root of unity in K. For every $\varepsilon > 0$ there exists a constant $c(d, \varepsilon)$ such that if $n > c(d, \varepsilon)(1+\log k)^{1+\varepsilon}$, there exists a prime ideal of K that divides $A^n - \zeta_k B^n$, but does not divide $A^m - \zeta_k^j B^m$ for $m < n$ and arbitrary j.*

The above theorem implies the finiteness of the number of solutions of generalized cyclotomic equations considered by Browkin [1, p. 236].

The proof will follow closely the proof given in [3]. Let $\mathbb{Q}(A/B) = K_0$, $\frac{A}{B} = \frac{\alpha}{\beta}$, where $\alpha, \beta \in K_0$, α, β are integers, and $(\alpha, \beta) = \mathfrak{d}$. Let S and S_0 be the set of all isomorphic injections of $K_0(\zeta_k)$ and K_0, respectively, in the complex field, and set

$$w(\alpha/\beta) = \log \prod_{\sigma \in S_0} \max\{|\alpha^\sigma|, |\beta^\sigma|\} - \log N\mathfrak{d},$$

where N denotes the absolute norm in K_0. Here, $w(\alpha/\beta)$ is the logarithm of the Mahler measure of α/β and so it is independent of the choice of α, β in K_0.

Lemma 1. *If $|\alpha| = |\beta|$, but α/β is not a root of unity, then*

$$\log|\alpha^n - \zeta_k \beta^n| = n \log|\beta| + O(d + w(\alpha/\beta)) \log kn,$$

Received by the editor July 27, 1992.
1991 *Mathematics Subject Classification*. Primary 11R04.

where the constant in the O-symbol depends only on d and is effectively computable.

Lemma 2. *If $|\alpha| \neq |\beta|$, then*

$$\log|\alpha^n - \zeta_k \beta^n| = n \log \max\{|\alpha|, |\beta|\} + O(d^2 + dw(\alpha/\beta)),$$

where the constant in the O-symbol is absolute and effectively computable.

The next lemma is just quoted from [3], where it occurs as Lemma 4.

Lemma 3. *Let $\phi_n(x, y)$ be the nth cyclotomic polynomial in homogeneous form. If $\mathfrak{P}$ is a prime ideal of K, $n > 2(2^d - 1)$, $\mathfrak{P} | \phi_n(A, B)$, and $\mathfrak{P}$ is not a primitive divisor of $A^n - B^n$, then*

$$\operatorname{ord}_{\mathfrak{P}} \phi_n(A, B) \le \operatorname{ord}_{\mathfrak{P}} n.$$

Finally, we prove

Lemma 4. *Let*

$$\psi_n(x, y; \zeta_k) = \prod_{\substack{(j, n)=1 \\ j \equiv 1 \bmod k}} (x - \zeta_{kn}^j y).$$

We have

$$\psi_n(x, y; \zeta_k) = \prod_{\substack{m|n \\ (m, k)=1}} (x^{n/m} - \zeta_k^{\overline{m}} y^{n/m})^{\mu(m)}, \tag{1}$$

where $m\overline{m} \equiv 1 \bmod k$ and

$$\deg \psi_n = \varphi(n) \frac{(k, n)}{\varphi((k, n))}.$$

Proof. The right-hand side of (1) can be written as

$$\prod_{\substack{m|n \\ (m, k)=1}} \prod_{i=0}^{n/m-1} (x - \zeta_{n/m}^{i} \zeta_{kn/m}^{\overline{m}} y)^{\mu(m)}.$$

A factor $x - \zeta_{kn}^j y$ occurs in this product with the exponent

$$E = \sum_{\substack{m|n \\ (m, k)=1}} \mu(m) \sum_{\substack{i=0 \\ m(ki+\overline{m}) \equiv j \bmod kn}}^{n/m-1} 1.$$

Now,

$$\sum_{\substack{i=0 \\ m(ki+\overline{m}) \equiv j \bmod kn}}^{n/m-1} 1 = \begin{cases} \displaystyle\sum_{\substack{i=0 \\ ki+\overline{m} \equiv j/m \bmod kn/m}}^{n/m-1} 1 & \text{if } m|j, \\ 0 & \text{otherwise}, \end{cases}$$

and if $m|j$,

$$\sum_{\substack{i=0 \\ ki+\overline{m} \equiv j/m \bmod kn/m}}^{n/m-1} 1 = \begin{cases} 1 & \text{if } j \equiv 1 \bmod k, \\ 0 & \text{otherwise}. \end{cases}$$

Hence,

$$E = \begin{cases} \sum_{m|n, m|j} \mu(m) & \text{if } j \equiv 1 \bmod k, \\ 0 & \text{otherwise}, \end{cases}$$

and finally

$$E = \begin{cases} 1 & \text{if } (n, j) = 1, \ j \equiv 1 \bmod k, \\ 0 & \text{otherwise}, \end{cases}$$

which proves the first part of the lemma.

In order to prove the second part, we notice that there are exactly $\varphi(n)\frac{(k, n)}{\varphi((k, n))}$ positive integers $j \le kn$ such that $(n, j) = 1$, $j \equiv 1 \bmod k$. □

Lemma 5. *For every* $\varepsilon > 0$ *there exists* $c(d, \varepsilon)$ *such that, if*

$$n > c(d, \varepsilon)(1 + \log k)^{1+\varepsilon},$$

then we have

$$|N_{K/\mathbb{Q}} \psi_n(A, B; \zeta_k)| > (nk)^{[K:\mathbb{Q}]}. \tag{2}$$

Proof. By Lemma 4,

$$\psi_n(A, B; \zeta_k) = \left(\frac{B}{\beta}\right)^{\phi(n)(k, n)/\phi((k, n))} \psi_n(\alpha, \beta; \zeta_k),$$

and since $(\frac{B}{\beta}) = \mathfrak{d}^{-1}$, we have

$$(\psi_n(A, B; \zeta_k)) = \mathfrak{d}^{-\varphi(n)(k, n)/\varphi((k, n))} \psi_n(\alpha, \beta; \zeta_k),$$

$$\begin{aligned}
&\frac{1}{[K : K_0(\zeta_k)]} \log |N_{K/\mathbb{Q}} \psi_n(A, B; \zeta_k)| \\
&\quad = \log |N_{K_0(\zeta_k)/\mathbb{Q}} \psi_n(\alpha, \beta; \zeta_k)| - [K_0(\zeta_k) : K_0] \varphi(n) \frac{(k, n)}{\varphi((k, n))} \log N\mathfrak{d} \\
&\quad = \sum_{\sigma \in S} \sum_{\substack{m|n \\ (m, k)=1}} \mu(m) \log |(\alpha^\sigma)^{n/m} - \zeta_k^{\overline{m}} (\beta^\sigma)^{n/m}| \\
&\qquad - [K_0(\zeta_k) : K_0] \varphi(n) \frac{(k, n)}{\varphi((k, n))} \log N\mathfrak{d} \\
&\quad = \sum_{\sigma \in S} \sum_{\substack{m|n \\ (m, k)=1}} \mu(m) \left(\frac{n}{m} \log \max\{|\alpha^\sigma|, |\beta^\sigma|\} + O\left(d + w\left(\frac{\alpha}{\beta}\right)\right) \log kn \right) \\
&\qquad - [K_0(\zeta_k) : K_0] \varphi(n) \frac{(k, n)}{\varphi((k, n))} \log N\mathfrak{d} \\
&\quad = [K_0(\zeta_k) : K_0] \left(\varphi(n) \frac{(k, n)}{\varphi((k, n))} w\left(\frac{\alpha}{\beta}\right) + O\left(d + w\left(\frac{\alpha}{\beta}\right)\right) 2^{\nu(n)} \log kn \right),
\end{aligned}$$

where the constant in O depends only on d and is effectively computable. Now, by Dobrowolski's theorem [2], if α/β is an integer, then

$$\begin{aligned}
w\left(\frac{\alpha}{\beta}\right) &= \log \prod_{\sigma \in S_0} \max\left\{ \left|\frac{\alpha^\sigma}{\beta^\sigma}\right|, 1 \right\} \\
&\ge \log \left(1 + c_1 \left(\frac{\log \log ed}{\log d} \right)^3 \right) \ge c_2 \left(\frac{\log \log ed}{\log d} \right)^3,
\end{aligned}$$

where c_1 and c_2 are absolute constants.

If α/β is not an integer, then $(\beta) \neq \mathfrak{d}$ and

$$w\left(\frac{\alpha}{\beta}\right) \geq \log N\beta - \log N\mathfrak{d} \geq \log 2 .$$

Thus, in both cases,

$$w\left(\frac{\alpha}{\beta}\right) \geq c_2 \left(\frac{\log\log ed}{\log d}\right)^3 ,$$

provided $c_2 \leq \log 2$.

Since for every $\varepsilon > 0$

$$\frac{\varphi(n)}{2^{\nu(n)}} > c_3(\varepsilon) n^{1-\varepsilon} ,$$

it follows that for $n > c(d, \varepsilon)(1 + \log k)^{1+\varepsilon}$

$$\log |N_{K/\mathbb{Q}} \psi_n(A, B; \zeta_k)| > [K : \mathbb{Q}] \log nk ,$$

which proves the lemma. □

Proof of the theorem. By Lemma 5, for $n > c(d, \varepsilon)(\log k)^{1+\varepsilon}$ we have (2), and thus $\psi_n(A, B; \zeta_k)$ has a prime ideal factor $\mathfrak{P}$ in K such that

$$\operatorname{ord}_{\mathfrak{P}} \psi_n(A, B; \zeta_k) > \operatorname{ord}_{\mathfrak{P}} kn .$$

But $\mathfrak{P} | \psi_n(A, B; \zeta_k) | \phi_{kn}(A, B)$, hence by Lemma 3 we have that $\mathfrak{P}$ is a primitive prime divisor of $A^{kn} - B^{kn}$ and thus does not divide $A^m - \zeta_k^j B^m$ for $m < n$ and arbitrary j. On the other hand,

$$\mathfrak{P} | \psi_n(A, B; \zeta_k) | A^n - \zeta_k B^n ,$$

thus $\mathfrak{P}$ has the desired property. □

Bibliography

1. J. Browkin, *K-theory, cyclotomic equations, and Clausen's function*, Chapter 11, Math. Surveys Monographs (L. Lewin, ed.), vol. 37, Amer. Math. Soc., Providence, RI, 1991, pp. 233–273.
2. E. Dobrowolski, *On a question of Lehmer and the number of irreducible factors of a polynomial*, Acta Arith. **34** (1979), 391–401.
3. A. Schinzel, *Primitive divisors of the expression* $A^n - B^n$ *in algebraic number fields*, J. Reine Angew. Math. **268/269** (1974), 27–33.

Institute of Mathematics, Polish Academy of Sciences, P.O. Box 137, 00-950 Warsaw, Poland

E-mail address: schinzel@impan.impan.gov.pl