POLYNOMIALS WITH MANY FACTORS IN CYCLOTOMIC EXTENSIONS

Artūras DUBICKAS

Faculty of Mathematics and Informatics, Vilnius University, Naugarduko 24, 2600, Vilnius, Lithuania.

e-mail: arturas.dubickas@maf.vu.lt

Abstract. We prove that there is a polynomial with integer coefficients which has many cyclotomic factors in a field generated by the primitive \( L \)th root of unity. This shows that an upper bound obtained earlier by C.G. Pinner and J.D. Vaaler is very close to being sharp, the small difference being only in constants. In particular, the quotient between the constant involved and that in the upper bound is greater than \( 0.99 \) for every \( L \) divisible by 15.

Key words: irreducible factor, cyclotomic polynomial, cyclotomic extension.

Mathematics Subject Classification: 11R09, 11R18, 12D05.

1. Introduction

Let \( K \) be an algebraic number field, i.e. a finite extension of the field of rational numbers \( \mathbb{Q} \), and let \( f(x) \), where \( f(0) \neq 0 \), be a polynomial in \( K[x] \). The problem of estimating the number of irreducible factors of the polynomial \( f(x) \) in terms of its degree and height was first studied by A. Schinzel [8], [9] and E. Dobrowolski [1] in the case \( K = \mathbb{Q} \). Later, C.G. Pinner and J.D. Vaaler [5]–[7] obtained some upper bounds in the general case and showed that these are not far from being sharp.

More precisely, set \( ||f|| = \max_{|z| \leq 1} |f(z)| \) and \( r(f) = \deg f / \log ||f|| \). Assume that the \( n \)th cyclotomic polynomial

\[
\Phi_n(x) = \prod_{(j,n)=1} (x - \mu_j^n),
\]

where \( \mu_n = \exp\{2\pi \sqrt{-1}/n\} \) and the product is taken over every positive \( j \leq n \) relatively prime to \( n \), factors in \( K[x] \) as

\[
\Phi_n(x) = \prod_{s=1}^{\delta(K;n)} \Phi_{n,s}(x),
\]

where \( \Phi_{n,s} \) are all monic and irreducible in \( K[x] \). Write

\[
f(x) = \tilde{f}(x) \prod_{n=1}^{\infty} \prod_{s=1}^{\delta(K;n)} \Phi_{n,s}(x)^{e(n,s)},
\]
where \( \hat{f}(x) \) has no cyclotomic factors in \( K[x] \). Then the total number of cyclotomic factors of \( f \) in \( K \) counted with multiplicity is \( \Omega(K; f) = \sum_{n=1}^{\infty} \sum_{s=1}^{\delta(K;n)} e(n, s) \). Here, \( e(n, s) = 0 \) for all but finitely many pairs \( n, s \).

For arbitrary number field \( K \), it is shown in [5] that for every \( \varepsilon > 0 \) there is a \( r_0(K; \varepsilon) \) such that for every \( f(x) \in K[x] \) with \( r(f) > r_0(K; \varepsilon) \) we have

\[
\Omega(K; f) < (1 + \varepsilon) \deg f \sqrt{\frac{c(K) \log r(f)}{r(f)}},
\]

where

\[
c(K) = \prod_{p \mid J} \left(1 + \frac{1}{p(p-1)}\right) \sum_{l \mid J} \frac{\delta(K;l)^2 \phi(J/l)}{\phi(l) J}.\]

Here, \( J = J(K) \) is the minimal positive integer with the property that the maximal abelian subfield of \( K \) is contained in \( \mathbb{Q}(\mu_J) \), \( \mu_J = \exp\{2\pi\sqrt{-1}/J\} \), and \( \phi(l) \) is Euler’s function (\( J \) is finite, by the theorem of Kronecker–Weber). In particular, for \( K = \mathbb{Q}(\mu_L) \), \( \mu_L = \exp\{2\pi\sqrt{-1}/L\} \), the constant defined above was calculated in [5]. It is equal to

\[
c(\mathbb{Q}(\mu_L)) = \frac{\zeta(2) \zeta(3)L}{\zeta(6)} \prod_{p \mid L} \left(1 - \frac{1}{p^2}\right) \left(1 + \frac{1}{p(p-1)}\right)^{-1},
\]

where \( \zeta \) stands for the Riemann zeta-function. (Throughout, we will use the letter \( p \) to denote the prime numbers.)

In the case \( K = \mathbb{Q} \) it was shown in [5] that the constant

\[
\sqrt{c(\mathbb{Q})} = \sqrt{\frac{\zeta(2) \zeta(3)}{\zeta(6)}} = 1.39412 \ldots
\]

cannot be replaced by a constant smaller than \( 3\sqrt{3}/4 = 1.29903 \ldots \). Moreover, the author [4] showed that it cannot be replaced by a constant smaller than \( 3\sqrt{2}/\pi = 1.35047 \ldots \). Note that the quotient between this constant \( 3\sqrt{2}/\pi \) which was obtained for the polynomial \( f_N(x^2) \), where

\[
f_N(x) = \prod_{1 \leq u < v \leq N} (x^{v-u} - 1)^{J_u J_v},
\]

\( J_u = [N \sin(\pi u/N)] \), \( u = 1, \ldots, N \), and that in upper bound (1), \( \sqrt{\zeta(2) \zeta(3)}/\zeta(6) \), is equal to \( 2\pi/\sqrt{35\zeta(3)} > 0.968 \). (Here, \( [\ldots] \) stands for the integral part of a number.)

The polynomials defined in (3) were first introduced in [2]. They proved to be useful also in [3]. Now, we show that they have many factors in \( K = \mathbb{Q}(\mu_L) \).
Theorem. Let \( L \) be a positive integer, and let \( \varepsilon > 0 \). For every \( N \) sufficiently large, there is a polynomial, namely, \( g(x) = f_N(x^\ell) \) with \( \ell = 2L \) for \( L \) odd, \( \ell = L \) for \( L \) even, such that

\[
\Omega(\mathbb{Q}(\mu_L); g) > (1 - \varepsilon) \deg g \sqrt{\frac{\epsilon^*(\mathbb{Q}(\mu_L)) \log r(g)}{r(g)}}.
\]

Here,

\[
\sqrt{\frac{\epsilon^*(\mathbb{Q}(\mu_L))}{c(\mathbb{Q}(\mu_L))}} = 4\pi \sqrt{\frac{2\prod_p(1 + p^{-3})}{315\zeta(3)}},
\]

where \( c(\mathbb{Q}(\mu_L)) \) is given by (2).

Assume that \( L \) is divisible by many odd prime numbers, for instance, by every odd prime \( \leq p^* \). Then, for \( p^* \to \infty \), the constant (4) tends to \( 4\sqrt{5}/\pi^2 = 0.99274 \ldots \). Similarly, if \( L \) is divisible by 15, then \( \prod_p(1 + p^{-3}) \geq 147/125 \). Hence the constant (4) (which shows how close the example of the theorem to the upper bound (1)) is greater than or equal to

\[
\frac{4\pi}{25} \sqrt{\frac{14}{3\zeta(3)}} > 0.99.
\]

2. Preliminaries

We begin with the following simple lemmas.

Lemma 1. Let \( \varepsilon > 0 \), and let \( g(x) \) be as in the theorem with \( N \) being sufficiently large. Then

\[
\frac{(1 - \varepsilon)\ell N^5}{2\pi^2} < \deg g < \frac{(1 + \varepsilon)\ell N^5}{2\pi^2},
\]

and

\[
r(g) > \frac{(1 - \varepsilon)2\ell N^2}{\pi^2 \log N}.
\]

Proof. Since \( \deg g = \ell \sum_{1 \leq u < v \leq N} (v - u)[N \sin(\pi u/N)][N \sin(\pi v/N)] \), the inequalities (5) follow from changing the sum by the respective integral (see also [2] and [4]). Furthermore, \( \|g\| = \|f_N(x^\ell)\| = \|f_N\| \), so, by (14) in [4], \( \log \|g\| < (1 + \varepsilon/2)(N^3/4) \log N \) for \( N \) sufficiently large. Now, combining this with the left inequality in (5), where \( \varepsilon \) is replaced by \( \varepsilon/2 \), we will obtain (6).

Lemma 2. If \( L \) is a positive integer, then

\[
\sum_{t \mid L} \phi(t)\phi(L/t)t = L^2 \prod_{p \mid L} \left( 1 - \frac{1}{p^2} \right).
\]
Proof. The function \( \sum_{t \in \mathbb{L}} \phi(t) \phi(L/t)t \) is multiplicative, as so are \( \phi(t) \) and \( \phi(t)t \). Therefore it suffices to show that the sum is equal to \( p^{2k-2}(p^2 - 1) \) for \( L = p^k \), where \( p \) is a prime number and \( k \) is a positive integer. Since \( \phi(p^j) = p^j(p - 1) \) for \( j > 0 \), the sum on the left hand side is indeed equal to

\[
p^{k-1}(p - 1) + p^{2k-1}(p - 1) + \sum_{j=1}^{k-1} p^{k+j-2}(p - 1)^2 = p^{2k-2}(p^2 - 1),
\]

as claimed.

3. Proof of the theorem

Since \( \mathbb{Q}(\mu_L) = \mathbb{Q}(\mu_{L/2}) \) for \( L \equiv 2(\text{mod} \, 4) \), there is no loss of generality to assume that \( L \) is either odd, or it is divisible by 4. (Indeed, if \( L \equiv 2(\text{mod} \, 4) \), then \( L/2 \) is odd, so we can first replace \( L \) by \( L/2 \) and then, by induction, set \( \ell = 2(L/2) = L \), as claimed.) Let throughout \( \ell = 2L \) for \( L \) odd, and \( \ell = L \) for \( L \) divisible by 4. From (5) and (6) it is easily seen that

\[
\deg g \sqrt{\frac{\log r(g)}{r(g)}} < \frac{(1 + 2\varepsilon)\sqrt{t}N^4 \log N}{2\pi}.
\]

Using (3) let us write

\[
g(x) = f_N(x^\ell) = \prod_{1 \leq u < v \leq N} (x^{(v-u)\ell} - 1)^{J_u J_v} \prod_{m=1}^{(N-1)\ell} \Phi_m(x)^{e(m)},
\]

where

\[
e(m) = \sum_{1 \leq u < v \leq N} J_u J_v.
\]

Set \((a, b)\) for the greatest common divisor of \( a \) and \( b \). It was shown in [5] that \( \delta(\mathbb{Q}(\mu_L); m) = \phi((m, L)) \). Over the field \( \mathbb{Q}(\mu_L) \) we have that

\[
g(x) = \prod_{m=1}^{(N-1)\ell} \Phi_{m,s}(x)^{e(m,s)}
\]

with \( e(m, s) = e(m) \) for \( 1 \leq s \leq \phi((m, L)) \). It follows that

\[
\Omega(\mathbb{Q}(\mu_L); g) = \sum_{m=1}^{(N-1)\ell} \sum_{s=1}^{\phi((m, L))} e(m, s) = \sum_{1 \leq u < v \leq N} J_u J_v \sum_{m \mid (v-u)\ell} \phi((m, L)).
\]
Writing \((m, L) = t, m/t = h\) and \(w = v - u\) we deduce that

\[ \Omega(\mathbb{Q}(\mu_L); g) = \sum_{t|L} \frac{\phi(t)}{\pi^2} \sum_{1 \leq u \leq N-1} J_u \sum_{1 \leq w \leq N-u} J_{u+w} \sum_{h|w + t/L, (h, L/t) = 1} 1. \quad (8) \]

Assume first that \(L\) is even, so \(\ell = L\). Then, since \(J_u = \lfloor N \sin(\pi u/N) \rfloor\) and

\[ \sum_{1 \leq u \leq N-1} J_u \sum_{1 \leq w \leq N-u} J_{u+w} \sum_{h|w} 1 \sim \frac{2N^4}{h\pi^2}, \]

we deduce that

\[ \Omega(\mathbb{Q}(\mu_L); g) \sim \frac{2N^4}{\pi^2} \sum_{t|L} \frac{\phi(t)}{t} \sum_{h|w} \frac{1}{h}, \]

where the inner sum is taken over every positive integer \(h < N\) such that \((h, L/t) = 1\). By considering \(\phi(L/t)\) residue classes and by noting that the sum \(1/h\) over the fractions which belong to one residue class is \(\sim (t/L) \log N\), we see that

\[ \Omega(\mathbb{Q}(\mu_L); g) \sim \frac{2N^4 \log N}{L\pi^2} \sum_{t|L} \phi(t)\phi(L/t)t. \]

This combined with Lemma 2 implies that

\[ \Omega(\mathbb{Q}(\mu_L); g) > (1 - \epsilon)2L \prod_{p|L} \left(1 - \frac{1}{p^2}\right) N^4 \log N. \quad (9) \]

If, however, \(L\) is odd, then \(\ell = 2L\), and, by considering (in (8)) \(h\) odd and even, we will gain an extra \(1/2\), so that

\[ \Omega(\mathbb{Q}(\mu_L); g) \sim \frac{3N^4 \log N}{L\pi^2} \sum_{t|L} \phi(t)\phi(L/t)t. \]

Now, instead of (9) we will get

\[ \Omega(\mathbb{Q}(\mu_L); g) > (1 - \epsilon)3L \prod_{p|L} \left(1 - \frac{1}{p^2}\right) N^4 \log N. \quad (10) \]

Notice that the right hand side of (9) is equal to

\[ \frac{(1 - \epsilon)2\ell \prod_{p|\ell} \left(1 - \frac{1}{p^2}\right)}{\pi^2} N^4 \log N, \]

and so is that of (10). Consequently, in both cases,

\[ \Omega(\mathbb{Q}(\mu_L); g) > \frac{(1 - \epsilon)2\ell \prod_{p|\ell} \left(1 - \frac{1}{p^2}\right)}{\pi^2} N^4 \log N. \]
Using the lower bound for $N^4 \log N$ from (7) we see that $\Omega(\mathbb{Q}(\mu_L); g)$ is greater than

$$(1 - 4\varepsilon) \deg g \sqrt{\frac{c^*(\mathbb{Q}(\mu_L)) \log r(g)}{r(g)}},$$

where

$$\sqrt{c^*(\mathbb{Q}(\mu_L))} = \frac{4\sqrt{7} \prod_{p\mid \ell} (1 - p^{-2})}{\pi}. \quad (11)$$

(Of course, $1 - 4\varepsilon$ above can be replaced by $1 - \varepsilon$ at the expense of $\varepsilon$ in Lemma 1.)

Combining (2) and (11) we get

$$\frac{c^*(\mathbb{Q}(\mu_L))}{c(\mathbb{Q}(\mu_L))} = \frac{16\ell \zeta(6) \prod_{p\mid \ell} (1 - p^{-2})^2 \prod_{p\mid L} (1 + 1/p(p - 1))}{\pi^2 L \zeta(2) \zeta(3) \prod_{p\mid L} (1 - p^{-2})}.$$

If $L$ is even, then, by substituting $\ell = L$, $\zeta(2) = \pi^2/6$, $\zeta(6) = \pi^6/945$, it follows without difficulty that

$$\frac{c^*(\mathbb{Q}(\mu_L))}{c(\mathbb{Q}(\mu_L))} = \frac{32\pi^2 \prod_{p\mid L} (1 + p^{-3})}{315 \zeta(3)},$$

giving (4). If $L$ is odd, then $\ell = 2L$, so

$$\frac{c^*(\mathbb{Q}(\mu_L))}{c(\mathbb{Q}(\mu_L))} = \frac{36\pi^2 \prod_{p\mid L} (1 + p^{-3})}{315 \zeta(3)} = \frac{32\pi^2 \prod_{p\mid 2L} (1 + p^{-3})}{315 \zeta(3)},$$

once again giving (4).

This research was partially supported by a grant from Lithuanian State Science and Studies Foundation.

REFERENCES


**Daugianariai, turintys daug daugiklių ciklotominiuose plėtiniuose**

A. Dubickas

Įrodome, kad egzistuoja daugianaris su sveikaisiais koeficientais, turintis daug ciklotominių daugiklių racionaliųjų skaičių kūno plėtiniuose, generuotuose $L$—tojo laipsnio šaknimi iš vieneto. Tai parodo, kad anksčiau gautas C. J. Pinner ir J. D. Vaaler viršutinis įvertis yra beveik tikslus, o nedidelis skirtumas yra tik konstantose. Pavyzdžiui, kai $L$ dalijasi iš 15, tu konstantų santykis yra didesnis už 0,99.

*Rankraščis gautas*

2002 04 15