Journal de Théorie des Nombres de Bordeaux

anciennement Séminaire de Théorie des Nombres de Bordeaux

Tetsuya TANIGUCHI

Prime factors of class number of cyclotomic fields

Tome 20, n° 2 (2008), p. 525-530.

<http://jtnb.cedram.org/item?id=JTNB_2008__20_2_525_0>

© Université Bordeaux 1, 2008, tous droits réservés.

L'accès aux articles de la revue « Journal de Théorie des Nombres de Bordeaux » (http://jtnb.cedram.org/), implique l'accord avec les conditions générales d'utilisation (http://jtnb.cedram.org/legal/). Toute reproduction en tout ou partie cet article sous quelque forme que ce soit pour tout usage autre que l'utilisation à fin strictement personnelle du copiste est constitutive d'une infraction pénale. Toute copie ou impression de ce fichier doit contenir la présente mention de copyright.

cedram

Article mis en ligne dans le cadre du
Centre de diffusion des revues académiques de mathématiques
http://www.cedram.org/

Journal de Théorie des Nombres
de Bordeaux **20** (2008), 525-530

Prime factors of class number of cyclotomic fields

par Tetsuya TANIGUCHI

Résumé. Soit p un nombre premier impair, r une racine primitive modulo p et $r_i \equiv r^i \pmod{p}$ avec $1 \leq r_i \leq p-1$. En 2007, R. Queme a posé la question : le ℓ-rang (ℓ premier impair $\neq p$) du groupe des classes d'idéaux du p-ième corps cyclotomique est-il égal au degré du plus grand diviseur commun sur le corps fini $\mathbb{F}_\ell$ de $x^{(p-1)/2}+1$ et du polynôme de Kummer $f(x) = \sum_{i=0}^{p-2} r_{-i}x^i$. Dans cet article, nous donnons une réponse complète à cette question en produisant un contre-exemple.

Abstract. Let p be an odd prime, r be a primitive root modulo p and $r_i \equiv r^i \pmod{p}$ with $1 \leq r_i \leq p-1$. In 2007, R. Queme raised the question whether the ℓ-rank (ℓ an odd prime $\neq p$) of the ideal class group of the p-th cyclotomic field is equal to the degree of the greatest common divisor over the finite field $\mathbb{F}_\ell$ of $x^{(p-1)/2}+1$ and Kummer's polynomial $f(x) = \sum_{i=0}^{p-2} r_{-i}x^i$. In this paper, we shall give the complete answer for this question enumerating a counter-example.

1. Introduction

Let $\zeta_n = e^{2\pi i/n}$ $(n \geq 2)$ be a primitive n-th root of unity and $\mathbb{Q}(\zeta_n)$ be the cyclotomic field defined by ζ_n. Also, let h_n be the ideal class number of $\mathbb{Q}(\zeta_n)$. It is well-known that h_n can be written as $h_n = h_n^- h_n^+$, where h_n^- and h_n^+ are the so-called relative and real class numbers of $\mathbb{Q}(\zeta_n)$, respectively.

We put that p is an odd prime, $N = \frac{p-1}{2}$, r is a primitive root modulo p and r_i is the least positive residue of r^i $(i \in \mathbb{Z})$ modulo p, i.e., $r_i \equiv r^i$ $\pmod{p}$ with $1 \leq r_i \leq p-1$.

In 1850, Kummer [3] established the following formula for h_p^-:

$$h_p^- = \frac{1}{(2p)^{N-1}} \left| \prod_{j=1}^{N} F(\zeta_{p-1}^{2j-1}) \right|,$$

where

$$F(x) = r_0 + r_{-1}x + r_{-2}x^2 + \cdots + r_{-(p-2)}x^{p-2}.$$

Manuscrit reçu le 31 octobre 2007.

This formula was slightly modified by Lehmer [4] and it was shown that

$$h_p^- = \frac{1}{(2p)^{N-1}} \left| \prod_{j=1}^{N} G(\zeta_{p-1}^{2j-1}) \right|, \tag{1.1}$$

where G is the "monic" polynomial defined by

$$G(x) = x^{p-2} F\left(\frac{1}{x}\right) = r_{-(p-2)} + r_{-(p-3)}x + \cdots + r_{-1}x^{p-3} + r_0 x^{p-2},\ r_0 = 1. \tag{1.2}$$

In his papers , Queme investigated the structure of class group of $\mathbb{Q}(\zeta_p)$ and raised the following question.
Question (Queme, 2007): Let p be an odd prime and ℓ be an odd prime with $\ell \neq p$. Is the degree of the greatest common divisor over $\mathbb{F}_\ell$ (the finite field with ℓ elements) of $F(x)$ and $x^N + 1$ equal to the ℓ-rank of the ℓ-Sylow subgroup of relative class group $Cl^-_{\mathbb{Q}(\zeta_p)}$ of $\mathbb{Q}(\zeta_p)$?

In the present paper, we shall give an answer to the above Question. This will be done by inspecting the ℓ-part of the class group of $\mathbb{Q}(\zeta_p)$ with an argument about resultants of certain polynomials and by producing concretely counter-evidence using computer.

2. Some preliminaries on resultants

In this section, we deal with some basic properties of resultants as preliminaries, which will be needed later in order to discuss a prime-divisibility of h_p^- in the next section.

Let L be any field. For $f \in L[x]$, we write ∂f for the degree of f and $c(f)$ for the leading coefficient of f. Given two non-constant polynomials f and g in $L[x]$, we denote by $\mathrm{R}_L(f, g)$ the resultant of f and g, that is, using roots α_i and β_j in $\overline{L}$ (an algebraic closure of L) of f and g, respectively,

$$\mathrm{R}_L(f, g) = c(f)^{\partial g} c(g)^{\partial f} \prod_{i=1}^{\partial f} \prod_{j=1}^{\partial g} (\alpha_i - \beta_j).$$

Lemma 2.1 (cf. [5]). *Let L be any field and f, f_1, f_2, g, g_1, g_2 be non-constant polynomials in $L[x]$. Then we have*

(i) $\mathrm{R}_L(f_1 f_2, g) = \mathrm{R}_L(f_1, g)\ \mathrm{R}_L(f_2, g)$,
(ii) $\mathrm{R}_L(f, g_1 g_2) = \mathrm{R}_L(f, g_1)\ \mathrm{R}_L(f, g_2)$,
(iii) *if* $f = sg + t$ $(s,\ t \in L[x],\ \partial t < \partial g)$, *then*

$$\mathrm{R}_L(f, g) = \begin{cases} c(g)^{\partial f - \partial t}\, \mathrm{R}_L(t, g) & \text{if } \ \partial t > 0, \\ c(g)^{\partial f} t^{\partial g} & \text{if } \ \partial t = 0. \end{cases}$$

Let Φ_n $(n \geq 1)$ be the n-th cyclotomic polynomial, i.e.,

$$\Phi_n(x) = \prod_{\substack{k=1 \\ (k,n)=1}}^{n-1} \left(x - \zeta_n^k\right).$$

Concerning the resultant of cyclotomic polynomials, we can state

Lemma 2.2 (cf. [1]). *Let φ be the Euler totient function. Then we get*

(i) *if $n > 1$, then*
$$\mathrm{R}_{\mathbb{Q}}(\Phi_1, \Phi_n) = \begin{cases} u & \text{if } n = u^a \ (\exists u \text{ a prime}, a \geq 1), \\ 1 & \text{otherwise}, \end{cases}$$

(ii) *if $n > m > 1$ and $\gcd(m,n) = 1$, then $\mathrm{R}_{\mathbb{Q}}(\Phi_m, \Phi_n) = 1$,*

(iii) *if $n > m > 1$ and $\gcd(m,n) > 1$, then*
$$\mathrm{R}_{\mathbb{Q}}(\Phi_m, \Phi_n) = \begin{cases} u^{\varphi(m)} & \text{if } m \mid n \text{ and } \frac{n}{m} = u^a \ (\exists u \text{ a prime}, a \geq 1), \\ 1 & \text{otherwise.} \end{cases}$$

Lemma 2.3. *Define two polynomials S and T in $\mathbb{Q}[x]$ by*

$$S(x) = \frac{\prod_{d \mid N} \Phi_d(x)}{\Phi_1(x)} = \frac{x^N - 1}{x - 1}, \quad T(x) = \frac{\prod_{d \mid p-1} \Phi_d(x)}{\prod_{d \mid N} \Phi_d(x)} = x^N + 1. \tag{2.1}$$

Then it follows that $\mathrm{R}_{\mathbb{Q}}(S, T) = 2^{N-1}$.

Proof. Using Lemma 2.1, we know

$$\mathrm{R}_{\mathbb{Q}}(S, T) = \mathrm{R}_{\mathbb{Q}}\left(\prod_m{}' \Phi_m, \prod_n{}'' \Phi_n\right) = \prod_m{}' \prod_n{}'' \mathrm{R}_{\mathbb{Q}}(\Phi_m, \Phi_n),$$

where the products $\prod_m'$ and $\prod_n''$ are taken over all positive m and n such that $m \mid N$ for $m \geq 2$ and $n \mid p-1$ with $n \nmid N$, respectively. Hence, for each fixed m there exists only one single $n = 2^e m$ such that $\mathrm{R}_{\mathbb{Q}}(\Phi_m, \Phi_n) \neq 1$, where $e = \mathrm{ord}_2(p-1) - \mathrm{ord}_2 m$. Here note that if $\gcd(m,n) = 1$, then $\mathrm{R}_{\mathbb{Q}}(\Phi_m, \Phi_n) = 1$. Also, it is clear that if $m \mid n$ and $\frac{n}{m} = u^a$ ($\exists u$ a prime, $a \geq 1$), then $u = 2$.

Using Lemma 2.2 and Möbius' inversion formula, we can deduce

$$\mathrm{R}_{\mathbb{Q}}(S, T) = \prod_m{}' \prod_n{}'' 2^{\varphi(m)} = \prod_m{}' 2^{\varphi(m)} = 2^{\sum_m' \varphi(m)} = 2^{N-1},$$

where the sum $\sum_m'$ runs over all $m \geq 2$ such that $m \mid N$. □

3. Divisibility properties of h_p^-

In this section, we will discuss the ℓ-divisibility properties (ℓ a prime, $\ell \neq p$), and as a consequence, we are able to answer to the Question introduced in Section 1.

Let S, T be the polynomials as in (2.1) and put $G_0 = G/S$ for the polynomial G in (1.2). Here we comment that G_0 is a polynomial with integer coefficients. Indeed,

$$\begin{aligned}&(x-1)G_0\\ &\quad\equiv r_{-(p-2)} + r_{-(p-2)+(p-1)/2-1} - r_0 - r_{-(p-2)+(p-1)/2}\\ &\quad+ \sum_{i=1}^{(p-3)/2} \left(r_{-(p-2)+i-1} - r_{-(p-2)+i} + r_{-(p-3)/2+i-1} - r_{-(p-3)/2+i}\right) x^i\\ &\quad\equiv 0 \pmod{(x-1)S},\end{aligned}$$

hence $G_0 = G/S \in \mathbb{Z}[x]$. We shall state

Proposition 3.1. *We get*

(i) $(2p)^{N-1}h_p^- = |\mathrm{R}_{\mathbb{Q}}(G,T)|$,

(ii) $p^{N-1}h_p^- = |\mathrm{R}_{\mathbb{Q}}(G_0,T)|$.

Proof. Let $\alpha_i \in \mathbb{C}$, $i = 1, \dots, p-2$, be the roots of G. From (1.1), we obtain

$$h_p^- = \frac{1}{(2p)^{N-1}} \left| \prod_{j=1}^{N} \prod_{i=1}^{p-2} (\alpha_i - \zeta_{p-1}^{2j-1}) \right| = \frac{1}{(2p)^{N-1}} \left|\mathrm{R}_{\mathbb{Q}}(G,T)\right|,$$

as desired in (i). For (ii), we deduce from Lemmas 2.1 and 2.1 that, since $G = SG_0$,

$$(2p)^{N-1}h_p^- = |\mathrm{R}_{\mathbb{Q}}(G,T)| = |\mathrm{R}_{\mathbb{Q}}(S,T)\,\mathrm{R}_{\mathbb{Q}}(G_0,T)| = 2^{N-1}\left|\mathrm{R}_{\mathbb{Q}}(G_0,T)\right|.$$

This gives at once $p^{N-1}h_p^- = |\mathrm{R}_{\mathbb{Q}}(G_0,T)|$ and we are done. □

Here, we should remark that above (i) has been mentioned in Lehmer [4].

Proposition 3.2. *For a prime ℓ with $\ell \neq p$, we have*

$$\ell \mid h_p^- \Leftrightarrow \partial \gcd(G_0,T) \geq 1 \text{ in } \mathbb{F}_\ell. \tag{3.1}$$

Proof. From Proposition 3.1, we can see that

$$\ell \mid h_p^- \Leftrightarrow \ell \mid \mathrm{R}_{\mathbb{Q}}(G_0,T) \Leftrightarrow \mathrm{R}_{\mathbb{F}_\ell}(G_0,T) = 0,$$

which yields the proposition. □

We now quote the following one from [8, Lemma 16.15] for stating our main Proposition 3.4 given below.

Proposition 3.3. *Let ℓ be a prime and let L/K be an extension of number fields of degree prime to ℓ. Let A_L and A_K be the ℓ-parts of the class groups of L and K. Then, the natural map $A_K \to A_L$ is injective and*

$$A_L \simeq A_K \oplus (A_L/A_K).$$

The next proposition answers to the Question by Queme stated in Section 1.

Proposition 3.4. *There exists a pair (p, ℓ) of distinct primes p and ℓ such that*

$$\mathrm{rank}_\ell\, Cl^-_{\mathbb{Q}(\zeta_p)} > \partial \gcd(G, T) \text{ in } \mathbb{F}_\ell,$$

where $\mathrm{rank}_\ell\, Cl^-_{\mathbb{Q}(\zeta_p)}$ means the ℓ-rank of the ℓ-Sylow subgroup of $Cl^-_{\mathbb{Q}(\zeta_p)}$.

Proof. We will produce counter-evidence for the Question by finding a concrete pair (p, ℓ) of primes p and ℓ with $p \neq \ell$. In fact, choosing particularly $(p, \ell) = (3299, 3)$, we know that

$$Cl_{\mathbb{Q}(\sqrt{-p})} \simeq \mathbb{Z}/\ell^2\,\mathbb{Z} \times \mathbb{Z}/\ell\,\mathbb{Z}. \tag{3.2}$$

The degree of $\mathbb{Q}(\zeta_p)$ over $\mathbb{Q}(\sqrt{-p})$ is equal to $N = 1649 = 17 \times 97$, which is prime to ℓ. From Proposition 3.3, we obtain $A_{\mathbb{Q}(\zeta_p)} \supseteq \mathbb{Z}/\ell^2\,\mathbb{Z} \times \mathbb{Z}/\ell\,\mathbb{Z}$, and hence $\mathrm{rank}_\ell\, Cl_{\mathbb{Q}(\zeta_p)} \geq 2$. Further, since the class-group of $\mathbb{Q}(\sqrt{-p})$ is in the minus eigenspace with respect to complex conjugation acting on ideal classes and so is its isomorphic image in the class group of $\mathbb{Q}(\zeta_p)$, we may conclude that $\mathrm{rank}_\ell\, Cl^-_{\mathbb{Q}(\zeta_p)} \geq 2$.

On the one hand, we can know that, for the above pair (p, ℓ),

$$\gcd(G_0, T) = x + 1 \text{ over } \mathbb{F}_\ell, \tag{3.3}$$

and hereby $\gcd(G, T) = x + 1$ over $\mathbb{F}_\ell$. This implies the assertion immediately. ☐

Addendum. We verified the facts (3.2) and (3.3) by computer with aid of the softwares "GP/PARI CALCULATOR Version 2.3.3 (released)" and "Mathematica 6.0.1.0 for Linux x86 (32bit)", respectively. For details, consult with our on-line resources [7]. It should be noted that by several authors (see e.g. [2, 6]) the isomorphism (3.2) has been also confirmed by computer for the same pair (p, ℓ) as indicated above.

Acknowledgments. The author thanks professor T.Agoh for his generous help.

References

[1] Tom M. Apostol. Resultants of cyclotomic polynomials. *Proc. Amer. Math. Soc.*, 24:457–462, 1970.

[2] H. Kisilevsky. Olga Taussky-Todd's work in class field theory. *Pacific J. Math.*, (Special Issue):219–224, 1997.

[3] Eduard Ernst Kummer. Bestimmung der Anzahl nicht äquivalenter Classen für die aus λ ten Wurzeln der Einheit gebildeten complexen Zahlen und die idealen Factoren derselben. *J. Reine Angew. Math.*, 40:43–116, 1850.
[4] D. H. Lehmer. Prime factors of cyclotomic class numbers. *Math. Comp.*, 31:599–607, 1977.
[5] M. Pohst and H. Zassenhaus. *Algorithmic algebraic number theory*, volume 30 of *Encyclopedia of Mathematics and its Applications*. Cambridge Univ. Press, Cambridge, 1997.
[6] René Schoof. Minus class groups of the fields of the lth roots of unity. *Math. Comp.*, 67:1225–1245, 1998.
[7] Tetsuya Taniguchi. Program codes of "Prime factors of class number of cyclotomic fields". http://www.ma.noda.tus.ac.jp/g/tt/jtnb2008/.
[8] Lawrence C. Washington. *Introduction to cyclotomic fields*. Springer-Verlag, New York, 2nd ed., 1997.

Tetsuya TANIGUCHI
Department of Mathematics,
Tokyo University of Science,
Noda, Chiba 278-8510, Japan
E-mail: taniguti_tetuya@ma.noda.tus.ac.jp
URL: http://www.ma.noda.tus.ac.jp/g/tt/