RIMS Kôkyûroku Bessatsu
B12 (2009), 149–172

Prime divisors of the class number of the real p^rth cyclotomic field and characteristic polynomials attached to them

By

Youichi KOYAMA* and Ken-ichi YOSHINO**

Abstract

Let p be an odd prime and $r \geq 1$ an integer. We investigate to characterize the prime divisors of the class number of the real p^rth cyclotomic field $\mathbb{Q}(\zeta_{p^r})^+$. Let E be the group of units of $\mathbb{Q}(\zeta_{p^r})^+$, and C the subgroup generated by cyclotomic units of $\mathbb{Q}(\zeta_{p^r})^+$. Then the class number of $\mathbb{Q}(\zeta_{p^r})^+$ coincides with the order of the quotient group E/C. For a prime ℓ distinct from p, we show that there is an intimate connection between certain polynomials in $\mathbb{F}_\ell[x]$ which are divisors of $x^n - 1$, where $n = \phi(p^r)/2$, and the ℓ-part of E/C. As a consequence, the ℓ-rank of E/C is given by the degree of a particular one among such polynomials. Moreover we give a concrete algorithm by which we can compute such polynomial to obtain the ℓ-rank of E/C.

Introduction

Let p be an odd prime and $r \geq 1$ an integer. Let $\zeta = \zeta_{p^r} = \cos(2\pi/p^r) + i\sin(2\pi/p^r)$ be a primitive p^rth root of unity and $h_{p^r}^+$ the class number of $\mathbb{Q}(\zeta_{p^r})^+$. Let E be the group of units of $\mathbb{Q}(\zeta_{p^r})^+$, and C the subgroup generated by cyclotomic units of $\mathbb{Q}(\zeta_{p^r})^+$. Then it is well known that $h_{p^r}^+ = [E : C]$ (cf. [13]). It is difficult to determine $h_{p^r}^+$ itself. Indeed, the values of h_p^+ are not known for $p \geq 71$ (cf. [10]). Hence it is interesting to study which prime divisors appear in $h_{p^r}^+$. The class number parity of $h_{p^r}^+$ can be completely checked by easy calculation (see [1], [2], [14]). So it suffices to study odd prime divisors ℓ of $h_{p^r}^+$. In the case $\ell = p$, there is a famous conjecture of Kummer-Vandiver that p never divides $h_{p^r}^+$. The conjecture has been verified for all

Received March 26, 2008. Revised September 4, 2008.
2000 Mathematics Subject Classification(s): Primary 11R18, 11R29; Secondary 11R27
*Kanazawa Institute of Technology, Ogigaoka 7-1, Nonoichi-machi, Ishikawa 921-8501, Japan.
e-mail: `y.koyama@neptune.kanazawa-it.ac.jp`
**Kanazawa Medical University, Daigaku 1-1, Uchinada-machi, Ishikawa 920-0293, Japan.
e-mail: `yoshino@kanazawa-med.ac.jp`

$p < 12 \times 10^6$ (cf. [3]). Therefore, excluding this case, we may study odd prime divisors of $h_{p^r}^+$ distinct from p.

E. E. Kummer [8] investigated this problem firstly and gave a necessary condition for an odd prime distinct from p to divide h_p^+ (Satz VI). For a real abelian field K, H. W. Leopoldt [9] studied the divisibility condition of the class number h_K of K by an odd prime ℓ which does not appear in the degree of K. He showed that if ℓ is a prime divisor of h_K, then ℓ divides a generalized Bernoulli number. However the converse is not necessarily valid in general. Subsequently G. Cornell and M. Rosen [4] investigated the ℓ-rank of the ideal class group of $\mathbb{Q}(\zeta_f)^+$ for a composite conductor f. Their method does not give any information about the ℓ-rank of the ideal class group of $\mathbb{Q}(\zeta_{p^r})^+$. We have already given a necessary and sufficient condition for ℓ to divide h_p^+ in the previous paper [15]. The method used there depends on certain matrix computations, so that it is difficult to calculate the $\mathbb{F}_\ell$-rank of such a matrix if p becomes large. Hence the practical computation of divisibility of h_p^+ by ℓ turns out to be almost impossible.

In 2003, Schoof [12] investigated the quotient group E/C of $\mathbb{Q}(\zeta_p)^+$ and gave a method by which one can calculate all the simple Jordan-Hölder factors of it of order less than 8×10^5. In this way he obtained an "approximate" value $\widetilde{h_p^+}$ of h_p^+ in the sense that (a) $\widetilde{h_p^+}$ divides h_p^+, and (b) the quotient $h_p^+/\widetilde{h_p^+}$ is a possibly empty product of prime powers, each of which is greater than 8×10^5. Cohen-Lenstra heuristics suggests that $h_p^+ = \widetilde{h_p^+}$ for all $p < 10^4$, but it is very difficult to prove the coincidence at present.

In this paper, we treat only with the real p^r th cyclotomic field $\mathbb{Q}(\zeta_{p^r})^+$ and investigate which prime divisors appear in the class number $h_{p^r}^+$ of $\mathbb{Q}(\zeta_{p^r})^+$. Moreover we study the structure of the group E/C, which is deeply related to the ideal class group of $\mathbb{Q}(\zeta_{p^r})^+$. Our study is done independently of Schoof's work. Roughly speaking, our aim of this paper is as follows: (i) We introduce two polynomials $v_n(x)$ and $w_n(x) \in \mathbb{F}_\ell[x]$ associated with the group theoretical structure of E/C for a prime $\ell \neq p$. (ii) These polynomials $v_n(x)$ and $w_n(x)$ have a number theoretical meaning respectively and satisfy $w_n \,|\, v_n \,|\, x^n - 1$ in $\mathbb{F}_\ell[x]$. In particular, we show that the ℓ-rank of E/C is given by $\deg w_n - 1$ or by $\deg w_n$ according as $\ell > 2$ or $\ell = 2$. (iii) Although it is easy to obtaine v_n by definition, the calculation of w_n is difficult. We establish an effective method by which we determine w_n from v_n. (iv) By our method we calculate all the ℓ-rank$\,(E/C)$ of $\mathbb{Q}(\zeta_p)^+$ in the range $2 \leq \ell < 10^4$, $3 \leq p < 10^4$, and $\ell \neq p$ except one case $(\ell, p) = (131, 7411)$.

Acknowledgement. The authors would like to express their sincere thanks to the organizers of the conference, "Algebraic Number Theory and Related Topics", especially to Professor M. Asada. They thank deeply Professor T. Shimada for reading the first version of the manuscript and for giving many valuable comments. They also express

their sincere gratitude to the referee for many valuable comments and suggestions.

§ 1. Notations and Main result

Let $n = \varphi(p^r)/2$. Let g be a primitive root modulo p^r. For every $i \in \mathbb{Z}$, we put

$$e_i = \frac{\zeta^{g^{i+1}} - \zeta^{-g^{i+1}}}{\zeta^{g^i} - \zeta^{-g^i}},$$

which is a cyclotomic unit of $\mathbb{Q}(\zeta_{p^r})^+$. Then we have $e_{n+i} = e_i$ for each $i \in \mathbb{Z}$. Among $e_0, e_1, \ldots, e_{n-1}$ there exists one relation $e_0 e_1 \ldots e_{n-1} = -1$. Let $E_{p^r}^+$ be the group of units of $\mathbb{Q}(\zeta_{p^r})^+$ and $C_{p^r}^+$ its subgroup of cyclotomic units. $C_{p^r}^+$ is generated by $e_0, e_1, \ldots, e_{n-1}$, i.e., $C_{p^r}^+ = \langle e_0, e_1, \ldots, e_{n-1} \rangle$. It is well known that $h_{p^r}^+ = [E_{p^r}^+ : C_{p^r}^+]$ (cf. [13]). Hence, to search a prime divisor ℓ of $h_{p^r}^+$, we must find a cyclotomic unit ξ such that $\sqrt[\ell]{\xi} \in E_{p^r}^+ \setminus C_{p^r}^+$. Let g_i be the least positive residue of g^i modulo p^r for every $i \in \mathbb{Z}$, i.e., $g_i \equiv g^i \,(\mathrm{mod}\, p^r)$ and $0 < g_i < p^r$. Then $g_{i+2n} = g_i$ and $g_{i+n} = p^r - g_i$ for every $i \in \mathbb{Z}$. Let ℓ be an odd prime distinct from p. For any integers a and b such that $(a, p) = 1$, $R(a, b)$ denotes the least positive solution which satisfies $ax \equiv b \,(\mathrm{mod}\, p^r)$. For any integers a, b such that $a + b \equiv 1 \pmod 2$, let $[a, b]_{\mathrm{odd}}$ be the odd integer which equals either a or b.

For $k = 1, 2, \cdots, (\ell-1)/2$ and any integer j, we let

$$\varepsilon_j^{(k)} = \begin{cases} 1 \text{ if } [R(\ell, \ell-2k) - g_{2n-j}, R(\ell, \ell-2k) - g_{n-j}]_{\mathrm{odd}} > 0, \\ 0 \text{ otherwise.} \end{cases}$$

The number $\varepsilon_j^{(k)}$ is well defined, because $g_{n-j} + g_{2n-j} = p^r$ is odd. Let $c_j \in \mathbb{F}_\ell$ be defined by

$$c_j = \sum_{k=1}^{(\ell-1)/2} k^{-1}(\varepsilon_j^{(k)} - \varepsilon_{j+1}^{(k)}).$$

Since $\varepsilon_{j+n}^{(k)} = \varepsilon_j^{(k)}$ for any integer j and $k = 1, 2, \cdots, (\ell-1)/2$, we have $c_{j+n} = c_j$ and $\sum_{j=0}^{n-1} c_j = 0$. We define the polynomials u_n and v_n in $\mathbb{F}_\ell[x]$ by

$$u_n(x) = \sum_{j=0}^{n-1} c_j x^j \quad \text{and} \quad v_n(x) = \gcd(u_n(x), x^n - 1).$$

Then u_n and v_n have a trivial divisor $x-1$ because $\sum_{j=0}^{n-1} c_j = 0$. For any $m \mid n$, we define u_m and v_m in $\mathbb{F}_\ell[x]$ by $u_m(x) = \sum_{j=0}^{m-1}(\sum_{k=0}^{t-1} c_{j+km})x^j$ and $v_m(x) = \gcd(u_m(x), x^m - 1)$ respectively, where $t = n/m$. We notice that $\gcd(u_n, x^m - 1)$ divides u_m, but it does not necessarily coincide with u_m. From now on let $v_n(x)$ and $v_m(x)$ be monic polynomials. We denote by K_m the subfield of $\mathbb{Q}(\zeta_{p^r})^+$ of degree m and by h_{K_m} the class number of K_m. In particular $K_n = \mathbb{Q}(\zeta_{p^r})^+$ and $h_{K_n} = h_{p^r}^+$. Let E_{K_m} be the group of units in K_m and C_{K_m} the subgroup of cyclotomic units in K_m, that is, $C_{K_m} = C_{p^r}^+ \cap E_{K_m} = \langle \xi_0, \xi_1, \ldots, \xi_{m-1} \rangle$, where $\xi_i = N_{\mathbb{Q}(\zeta_{p^r})^+/K_m}(e_i)$ for each i.

Let $R = \mathbb{F}_\ell[x]/(x^m - 1)$ and let $\Phi : R \to \mathbb{F}_\ell^m$ be the natural isomorphism such that $\Phi(\sum_{i=0}^{m-1} a_i \bar{x}^i) = (a_0, a_1, \ldots, a_{m-1})$. Put $G = Gal(\mathbb{Q}(\zeta_{p^r})^+/\mathbb{Q})$. We define the group action of G on $\mathbb{F}_\ell^m$ by $(a_0, a_1, \ldots, a_{m-1})^\sigma = (a_{m-1}, a_0, \ldots, a_{m-2})$, where σ is the generator of G such that $\zeta^\sigma = \zeta^g$.

The content of this paper is as follows. In §2 we generalize a certain sum considered by Kummer [8] and obtain the value of the sum, which plays a role when we give a number theoretical meaning of the above polynomial v_n in §4. In §3 we illustrate a connection between the polynomial ring $\mathbb{F}_\ell[x]$ and the vector subspace $\operatorname{Ker} f(A)$ of $\mathbb{F}_\ell^m$, where A is the circular matrix of degree m such that

$$A = \begin{pmatrix} 0\,1\,0 \ldots 0\,0 \\ 0\,0\,1 \ldots 0\,0 \\ 0\,0\,0 \ldots 0\,0 \\ \ldots\ldots\ldots\ldots \\ 0\,0\,0 \ldots 0\,1 \\ 1\,0\,0 \ldots 0\,0 \end{pmatrix}.$$

We write it as $A = circ(0, 1, 0, \cdots, 0)$. For a polynomial $f(x) = a_0 + a_1 x + \cdots + a_{m-1}x^{m-1}$ in $\mathbb{F}_\ell[x]$, we obtain the circular matrix $f(A) = circ(a_0, a_1, a_2, \ldots, a_{m-1})$. We denote by $\operatorname{Ker} f(A)$ the kernel of the linear transformation $f(A)$ from $\mathbb{F}_\ell^m$ to itself. Let $\mathcal{L} \subseteq \mathbb{F}_\ell^m$ be a non-trivial $\mathbb{F}_\ell$-vector space closed under the action of G. Then there exists a unique monic polynomial $f \in \mathbb{F}_\ell[x]$ such that $\mathcal{L} = \operatorname{Ker} f(A)$ and $f(x) | x^m - 1$ (Theorem 3.8). Such a polynomial f is given by $f = (x^m - 1)/\gcd(\alpha^*, x^m - 1)$, where α is a generator of the principal ideal $\Phi^{-1}(\mathcal{L})$ of R with the least degree and $\alpha^*(x) = x^{m-1}\alpha(1/x)$. In §4 we show a number theoretical meaning of $v_n(x)$ which is important to obtain its divisor $w_n(x)$ defined below. As a consequence, if $v_n(x) = x - 1$, then $\ell \nmid h_{p^r}^+$. Moreover, for every divisor m of n, if $v_m(x) = x - 1$, then $\ell \nmid h_{K_m}$ (Theorem 4.3). This result improves Kummer's Satz VI in [8] a little. For a divisor m of n and $\boldsymbol{y} = (y_0, y_1, \ldots, y_{m-1}) \in \mathbb{F}_\ell^m$, we consider the cyclotomic unit $\xi(\boldsymbol{y}) = \xi_0^{y_0}\xi_1^{y_1} \ldots \xi_{m-1}^{y_{m-1}}$ in §5. Since the vector space $\{\boldsymbol{y} \in \mathbb{F}_\ell^m\,;\, \sqrt[\ell]{\xi(\boldsymbol{y})} \in E_{K_m}\}$ is closed under the action of G, it follows from Theorem 3.8 that among the divisors of $x^m - 1$, there exists a unique monic polynomial $w_m(x) \in \mathbb{F}_\ell[x]$ such that

$$\operatorname{Ker} w_m(A) = \{\boldsymbol{y} \in \mathbb{F}_\ell^m\,;\, \sqrt[\ell]{\xi(\boldsymbol{y})} \in E_{K_m}\}.$$

The polynomial $w_n(x)$ plays a significant role for our study. It satisfies $x-1 \mid w_m(x) \mid v_m(x)$

for every $m \mid n$. Then the ℓ-rank of $E^+_{p^r}/C^+_{p^r}$ is given by $\deg w_n - 1$. More generally, for the subfield K_m of $\mathbb{Q}(\zeta_{p^r})^+$, the ℓ-rank of E_{K_m}/C_{K_m} is given by $\deg w_m - 1$ (Theorem 5.4). In §6 we explain a concrete algorithm to compute $w_n(x)$ for an odd prime $\ell \neq p$. In §7 we show that the corresponding results in the previous sections hold true in the case $\ell = 2$. Our method is proved to be sufficiently effective. In §8 we put $r = 1$ and by our algorithm we make a table of all the non-trivial polynomials $w_n(x)$ for the pairs (ℓ, p) in the range $2 \leq \ell < 10^4$, $3 \leq p < 10^4$, and $\ell \neq p$ except the only one case $(\ell, p) = (131, 7411)$. In this exceptional case, we can obtain an "approximate" polynomial $\hat{w}_n(x) = (x-1)(x+31)$ of $w_n(x)$, but we can not determine whether $w_n(x) = (x-1)(x+31)$ or not. Finally we notice that our method yields nothing with respect to $\mathbb{Q}(\zeta_{2^r})^+$.

§ 2. Certain sum introduced by Kummer

Let $m > 1$ be an odd integer and a, b, c integers such that $(ac, m) = 1$. We do not exclude the case $(b, m) > 1$ in the following. Since $(a, m) = 1$, we obtain the least positive solution, say $R(a, b)$, of $ax \equiv b \pmod{m}$. Either $R(a,b) - R(a,c)$ or $R(a,b) - R(a,-c)$ is odd, because $R(a,c) + R(a,-c) = m$ by $(ac, m) = 1$. We let

$$\varepsilon(m; a, b, c) = \begin{cases} 1 \text{ if } [R(a,b) - R(a,c), R(a,b) - R(a,-c)]_{\text{odd}} > 0, \\ 0 \text{ otherwise.} \end{cases}$$

Here we denote by $S(m; a, b, c)$ the following sum which was first considered by Kummer [8] in the case $m = p$:

$$S(m; a, b, c) = \sum_{\zeta \neq 1} \frac{(\zeta^b - \zeta^{-b})(\zeta^c + \zeta^{-c})}{\zeta^a - \zeta^{-a}},$$

where ζ runs through all the mth roots of unity except 1. We can determine the value of $S(m; a, b, c)$ by means of $\varepsilon(m; a, b, c)$.

Proposition 2.1. *Let $m > 1$ be an odd integer and a, b, c integers such that $(abc, m) = 1$. Let m' be a proper divisor of m. Then*

$$S(m; a, bm', c) = 2m\varepsilon(m; a, bm', c) - 2R(a, bm').$$

Corollary 2.2. *Let $m > 1$ be an odd integer and a, b, c integers such that $(abc, m) = 1$. Then*

$$S(m; a, b, c) = 2m\varepsilon(m; a, b, c) - 2R(a, b).$$

Proposition 2.1 and Corollary 2.2 are proved by a same way. So, it suffices to prove Corollary 2.2. Then we may assume that $a = 1$, that is, we may prove that $S(m; 1, b, c) = 2m\varepsilon(m; 1, b, c) - 2R(1, b)$. We expand each term in $S(m; 1, b, c)$ as follows:

$$\frac{(\zeta^b - \zeta^{-b})(\zeta^c + \zeta^{-c})}{\zeta - \zeta^{-1}} = \sum_{k=1}^{b} \zeta^{b+c-2k+1} + \sum_{k=1}^{b} \zeta^{b-c-2k+1}.$$

We take out the exponents of ζ in the right side to obtain two arithmetic sequences $\{b+c-2k+1\}_{k=1}^{b}$ and $\{b-c-2k+1\}_{k=1}^{b}$. Multiplying each integer in the first sequence by -1, we obtain the second one. Since $S(m; 1, b, c) = S(m; 1, b', c')$ if $b \equiv b', c \equiv c' \pmod{m}$, we may consider that $0 < b, c < m$. So $R(1, b) = b$ and $R(1, -c) = m - c$. Therefore the first sequence lies between $-m + 1$ and $2m$ and the second between $-2m$ and m. We denote by T the set of the integers appearing in the first sequence. We divide our consideration into two cases.

First we consider the case where $b + c$ is odd. Then, since $b + c - m$ is even and $b - c$ is odd, we have $\varepsilon = 1$ or $\varepsilon = 0$ according as $b - c > 0$ or $b - c \leq 0$, where $\varepsilon = \varepsilon(m; 1, b, c)$. Here we observe that T consists on b successive even integers and that $b - c > 0$ if and only if $0 \in T$. Since

$$\sum_{\zeta \neq 1} \zeta^x = \begin{cases} -1 & \text{if } m \nmid x, \\ m - 1 & \text{if } m \mid x, \end{cases}$$

where ζ runs through all the mth roots of unity except 1, we prove $S(m; 1, b, c) = 2m\varepsilon(m; 1, b, c) - 2R(1, b)$ in this case. In the same way as above we can give the proof for the remainding case $b + c$ is even. This completes the proof of Corollary 2.2.

§ 3. Polynomial ring $\mathbb{F}_\ell[x]$ and the vector space $\mathrm{Ker} f(A)$

In this section we denote by A the circular matrix of degree m such that $A = circ(0, 1, 0, \cdots, 0)$. For a polynomial $f(x) = a_0 + a_1x + \cdots + a_{m-1}x^{m-1}$ in $\mathbb{F}_\ell[x]$, we obtain the circular matrix $f(A) = circ(a_0, a_1, a_2, \ldots, a_{m-1})$. We denote by $\mathrm{Ker}\, f(A)$ the kernel of the linear transformation $f(A)$ from $\mathbb{F}_\ell^m$ to itself, that is, $\mathrm{Ker}\, f(A) = \{\boldsymbol{x} \in \mathbb{F}_\ell^m; f(A)\boldsymbol{x}^t = \boldsymbol{0}\}$, where $\boldsymbol{x}^t$ is the transpose of $\boldsymbol{x} = (x_0, x_1, \ldots, x_{m-1})$ and $\boldsymbol{0}$ is the zero vector of size m. We notice that each element of $\mathrm{Ker}\, f(A)$ is corresponding to a cyclotomic unit of $\mathbb{Q}(\zeta_{p^r})^+$. Some of the results of this section are well known in the theory of error-correcting codes, so that we leave the proofs to the reader except Proposition 3.6 and Theorem 3.8.

Proposition 3.1. *Let f be a polynomial in $\mathbb{F}_\ell[x]$ of degree less than m. Then*

$$\dim_{\mathbb{F}_\ell} \mathrm{Ker}\, f(A) = \deg \gcd(f, x^m - 1).$$

Corollary 3.2. *Let m be a divisor of $n = \varphi(p^r)/2$. Then* $\operatorname{Ker} u_m(A) = \operatorname{Ker} v_m(A)$ *for every $m|n$, where u_m and v_m are the polynomials defined in §1.*

Remark 3.3. *Though we assume that ℓ is an odd prime distinct from p except in §7, all the results in this section are also true for $\ell = 2$. We use them for $\ell = 2$ in §7.*

Proposition 3.4. *Let f and g be polynomials in $\mathbb{F}_\ell[x]$ which divide $x^m - 1$. Then $f|g$ if and only if* $\operatorname{Ker} f(A) \subseteq \operatorname{Ker} g(A)$. *As a consequence, for the divisors f, g of $x^m - 1$ in $\mathbb{F}_\ell[x]$,* $\operatorname{Ker} f(A) = \operatorname{Ker} g(A)$ *if and only if $f = cg$ for some non-zero constant $c \in \mathbb{F}_\ell$.*

Now, putting $R = \mathbb{F}_\ell[x]/(x^m - 1)$, we define $\Phi : R \to \mathbb{F}_\ell^m$ by $\Phi(\sum_{i=0}^{m-1} a_i \bar{x}^i) = (a_0, a_1, \ldots, a_{m-1})$, where $\bar{x} = x \mod (x^m - 1)$ is a unit of R. Then Φ is obviously an isomorphism as a $\mathbb{F}_\ell$-vector space. We simply use x instead of $\bar{x}$. For $\boldsymbol{a} = (a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}_\ell^m$, the group action of G on $\mathbb{F}_\ell^m$ is defined by $\boldsymbol{a}^\sigma = (a_{m-1}, a_0, \ldots, a_{m-2})$, where $\zeta^\sigma = \zeta^g$. Since Φ is an isomorphism as a $\mathbb{F}_\ell$-vector space and R is a ring, we can naturally define the ring structure to $\mathbb{F}_\ell^m$. Hence Φ is a ring isomorphism. That is, for a polynomial $\beta = \sum_{i=0}^{m-1} b_i x^i \in R$, we obtain $\Phi(\beta(x))^{\sigma^i} = \Phi(x^i \beta(x)) = (0, \ldots, 0, 1, 0, \ldots, 0)\Phi(\beta(x))$ for every $i, 0 \le i \le m-1$, where 1 in the right side has the $i + 1$st position.

Let $\mathcal{L} \subseteq \mathbb{F}_\ell^m$ be a $\mathbb{F}_\ell$-vector space closed under the action of G. Then $\Phi^{-1}(\mathcal{L})$ is an ideal of R and so it is principal, i.e., $\Phi^{-1}(\mathcal{L}) = \alpha R$ with some $\alpha \in R$. For any $f = \sum_{i=0}^{m-1} a_i x^i \in \mathbb{F}_\ell[x]$, we put $f^*(x) = x^{m-1} f(1/x) = \sum_{i=0}^{m-1} a_i x^{m-1-i}$ and $f^\triangle(x) = x^{\deg f} f(1/x)$, where $f^\triangle$ is called the reciprocal polynomial of f. Since $f^* = f^\triangle \cdot x^{m-1-\deg f}$ and x is a unit, f^* and $f^\triangle$ have the same effect as an operator in the following.

Now we suppose that $\mathcal{L} = \operatorname{Ker} f(A)$ with $f \in \mathbb{F}_\ell[x]$. Then $\Phi^{-1}(\mathcal{L}) = \alpha R$ for some $\alpha \in R$. We consider a relation between f and α. We denote by τ the automorphism of $\mathbb{F}_\ell^m$ defined by $\boldsymbol{a}^\tau = (a_0, a_{m-1}, a_{m-2}, \ldots, a_1)$ for any $\boldsymbol{a} = (a_0, a_1, \ldots, a_{m-1})$. Obviously τ is an involution and satisfies the relation $\tau^{-1}\sigma\tau = \sigma^{-1}$ and $(\boldsymbol{ab})^\tau = \boldsymbol{a}^\tau \boldsymbol{b}^\tau$ for any $\boldsymbol{a}, \boldsymbol{b} \in \mathbb{F}_\ell^m$. Here, for any $\boldsymbol{a} = (a_0, a_1, \ldots, a_{m-1})$ and $\boldsymbol{b} = (b_0, b_1, \ldots, b_{m-1})$, we have $f(A)\boldsymbol{b} = (\boldsymbol{a}^\tau \boldsymbol{b})^t$ by definition of the product in $\mathbb{F}_\ell^m$, where $f(A) = circ(a_0, a_1, a_2, \ldots, a_{m-1})$. Therefore, $\boldsymbol{b} \in \operatorname{Ker} f(A)$ if and only if $\boldsymbol{a}^\tau \boldsymbol{b} = \boldsymbol{0}$.

Lemma 3.5. *Let $\mathcal{L} = \operatorname{Ker} f(A)$ for a polynomial f in $\mathbb{F}_\ell[x]$ with $\deg f < m$. Then we have*

$$\mathcal{L} = \{\boldsymbol{b} \in \mathbb{F}_\ell^m \,;\, \Phi^{-1}(\boldsymbol{b}) f^* \equiv 0 \pmod{x^m - 1}\}.$$

Now there exists an ideal I of $\mathbb{F}_\ell[x]$ such that $\Phi^{-1}(\mathcal{L}) = I/(x^m - 1)$. Then replacing α by $\gcd(\alpha, x^m - 1)$, we choose the generator α of I with the least degree among the non-zero polynomials in I. It is uniquely determined up to multiplication by non-zero element of $\mathbb{F}_\ell$. Here, putting $\gamma = (x^m - 1)/\gcd(f^*, x^m - 1)$, we have $\gamma f^* \equiv 0 \pmod{x^m - 1}$. By the definition $I = \{\beta \in \mathbb{F}_\ell[x] \,;\, \beta f^* \equiv 0 \pmod{x^m - 1}\}$. Thus we have $I = \gamma\mathbb{F}_\ell[x]$, which leads to $\alpha = \gamma$. This proves the following

Proposition 3.6. *Let f be a polynomial in $\mathbb{F}_\ell[x]$ with $\deg f < m$. Put $\mathcal{L} = \operatorname{Ker} f(A)$ and $\alpha = (x^m - 1)/\gcd(f^*, x^m - 1)$. Then we have $\Phi^{-1}(\mathcal{L}) = \alpha R$.*

Remark 3.7. $\operatorname{Ker} f(A)$ *is a $\mathbb{F}_\ell$-vector space generated by $\boldsymbol{b}, \boldsymbol{b}^\sigma, \cdots, \boldsymbol{b}^{\sigma^{m-1}}$, where α is given by Proposition* 3.6 *and $\boldsymbol{b} = \Phi(\alpha)$.*

Theorem 3.8. *Let $\mathcal{L} \subsetneq \mathbb{F}_\ell^m$ be a non-trivial $\mathbb{F}_\ell$-vector space closed under the action of G. Then, among the divisors of $x^m - 1$, there exists a unique monic polynomial $f \in \mathbb{F}_\ell[x]$ such that $\mathcal{L} = \operatorname{Ker} f(A)$. The polynomial f is given by $f = (x^m - 1)/\gcd(\alpha^*, x^m - 1)$, where $\Phi^{-1}(\mathcal{L}) = \alpha R$.*

Proof of Theorem 3.8 Let $\mathcal{N}$ be the diagonal part of $\mathbb{F}_\ell^m$. Put $\Phi^{-1}(\mathcal{L}) = \alpha R$ with some $\alpha \in \mathbb{F}_\ell[x]$. We may choose α as a monic polynomial with the possibly least degree. Obviously $\deg \alpha < m$. We define f by α as in Theorem 3.8.

If $\mathcal{L} = \mathcal{N}$ then the assertion is trivial. Hence we may assume that $\mathcal{L} \neq \mathcal{N}$. Let $\alpha = \sum_{i=0}^{m-1} b_i x^i \in \mathbb{F}_\ell[x]$ and $\boldsymbol{b} = \Phi(\alpha)$. Then $\mathcal{L} = \Phi(\alpha R)$ implies that $\mathcal{L}$ is generated by $\boldsymbol{b}, \boldsymbol{b}^\sigma, \cdots, \boldsymbol{b}^{\sigma^{m-1}}$ as a $\mathbb{F}_\ell$-vector space. From the assumption, it follows that $\boldsymbol{b} \notin \mathcal{N}$. First we show that $\mathcal{L} \subseteq \operatorname{Ker} f(A)$. By the assumption we have $\alpha^* f \equiv 0 \pmod{x^m - 1}$, which is equivalent to $\boldsymbol{b}\boldsymbol{a}^\tau = \boldsymbol{0}$, where $\boldsymbol{a} = \Phi(f)$. Hence $\boldsymbol{b} \in \operatorname{Ker} f(A)$ by the fact written just before Lemma 3.5. Therefore, since $\boldsymbol{b}^{\sigma^j} \in \operatorname{Ker} f(A)$ for each j, we have $\mathcal{L} \subseteq \operatorname{Ker} f(A)$. Similar argument shows the converse, so we have $\mathcal{L} = \operatorname{Ker} f(A)$. The uniqueness of f is followed from Proposition 3.4. This completes the proof of Theorem 3.8.

§ 4. The polynomial $v_n(x)$ and $E_U^{(\ell)}$

Let p be an odd prime and $r \geq 1$ an integer. Put $n = \varphi(p^r)/2$ and let $\ell \neq p$ be an odd prime. In this section we use the results on the sum $S(p^r; a, b, c)$ in §2 to show that all the results in [15] are generalized to the case p^r. For $k = 1, 2, \ldots, (\ell - 1)/2$ and for any integers i, j, we have $\varepsilon_{j-i}^{(k)} = \varepsilon(p^r; \ell g^j, (\ell - 2k)g^j, \ell g^i)$, where $\varepsilon_j^{(k)}$ is defined in §1. Let $c_j, u_n(x)$ and $v_n(x)$ be the same as in §1. By $E_U^{(\ell)}$ we denote the group of the primary cyclotomic units of $\mathbb{Q}(\zeta_{p^r})^+$, i.e.,

$$E_U^{(\ell)} = \{\eta \in C_{p^r}^+; \alpha^\ell \equiv \eta \pmod{\ell^2} \text{ for some integer } \alpha \in \mathbb{Q}(\zeta_{p^r})^+\}.$$

Theorem 4.1. *Let $\ell \neq p$ be an odd prime. Then*

$$E_U^{(\ell)} \subseteq \{e_0^{x_0} e_1^{x_1} \ldots e_{n-1}^{x_{n-1}} \in C_{p^r}^+; v_n(A)\boldsymbol{x}^t \equiv \boldsymbol{0} \pmod{\ell}\},$$

where A is the circular matrix of degree n. Therefore $E_U^{(\ell)}/(C_{p^r}^+)^\ell$ is isomorphic to a subgroup of $\operatorname{Ker} v_n(A)/\mathcal{N}$*, where $\mathcal{N}$ is the diagonal part of $\mathbb{F}_\ell^n$.*

Proof of Theorem 4.1(cf. Theorem 1 [15]) Put $\alpha = ((\zeta-\zeta^{-1})^\ell - (\zeta^\ell - \zeta^{-\ell}))/\ell \in \mathbb{Q}(\zeta_{p^r})$. Then we have $e_0^\ell = (\zeta-\zeta^{-1})^{(\sigma-1)\ell} = (\zeta^\ell-\zeta^{-\ell}+\ell\alpha)^{\sigma-1}$. Let β be the number in $\mathbb{Q}(\zeta_{p^r})^+$ defined by

$$\beta = -\frac{\alpha}{(\zeta-\zeta^{-1})^\ell} + \frac{(\zeta^\ell-\zeta^{-\ell})\alpha^\sigma}{(\zeta-\zeta^{-1})^\ell(\zeta^{\ell g}-\zeta^{-\ell g})}.$$

Then $\beta \in \mathbb{Q}(\zeta_{p^r})^+$ and

$$\beta \equiv -\frac{\alpha}{\zeta^\ell-\zeta^{-\ell}} + \frac{\alpha^\sigma}{\zeta^{\ell g}-\zeta^{-\ell g}} \pmod{\ell}.$$

This implies that $e_0^\ell \equiv e_0^{\sigma^s}(1+\ell\beta) \pmod{\ell^2}$, where s is an integer such that $1 \le s \le 2n$ and $g^s \equiv \ell \pmod{p^r}$. So, for a cyclotomic unit $\xi = e_0^{x_0}e_1^{x_1}\dots e_{n-1}^{x_{n-1}}$,

$$\xi^\ell \;\equiv\; \xi^{\sigma^s}\prod_{j=0}^{n-1}(1+\ell\beta^{\sigma^j})^{x_j} \;\equiv\; \xi^{\sigma^s}(1+\ell\sum_{j=0}^{n-1}x_j\beta^{\sigma^j}) \pmod{\ell^2}.$$

Noting that σ^s is the Frobenius automorphism of $\mathbb{Q}(\zeta_{p^r})$ at the prime ℓ, we can show that $E_U^{(\ell)} = \{\xi \in C_{p^r}^+; \xi^\ell \equiv \xi^{\sigma^s} \pmod{\ell^2}\}$. Therefore, we have $\xi \in E_U^{(\ell)}$ if and only if $\sum_{j=0}^{n-1} x_j\beta^{\sigma^j} \equiv 0 \pmod{\ell}$. The latter is equivalent to

$$\sum_{j=0}^{n-1}x_j\sum_{k=1}^{(\ell-1)/2}k^{-1}\frac{\zeta^{(\ell-2k)g^j}-\zeta^{-(\ell-2k)g^j}}{\zeta^{\ell g^j}-\zeta^{-\ell g^j}} \equiv \sum_{j=0}^{n-1}x_j\sum_{k=1}^{(\ell-1)/2}k^{-1}\frac{\zeta^{(\ell-2k)g^{j+1}}-\zeta^{-(\ell-2k)g^{j+1}}}{\zeta^{\ell g^{j+1}}-\zeta^{-\ell g^{j+1}}},$$

because $\alpha \equiv -\sum_{k=1}^{(\ell-1)/2}k^{-1}(\zeta^{\ell-2k}-\zeta^{-\ell+2k}) \pmod{\ell}$. Multiplying $\zeta^{\ell g^i}+\zeta^{-\ell g^i}$ in both sides of this congruence and summing them with respect to $\zeta \ne 1$, we get

$$\begin{aligned}&\sum_{j=0}^{n-1}x_j\sum_{k=1}^{(\ell-1)/2}k^{-1}S(p^r;\ell g^j,(\ell-2k)g^j,\ell g^i)\\ &\equiv \sum_{j=0}^{n-1}x_j\sum_{k=1}^{(\ell-1)/2}k^{-1}S(p^r;\ell g^{j+1},(\ell-2k)g^{j+1},\ell g^i) \pmod{\ell}.\end{aligned}$$

Here there are perhaps positive integers k such that $\ell-2k = bp^u$ for some positive integers u and b coprime to p. Hence it follows from Proposition 2.1 and Corollary 2.2 that

$$\sum_{j=0}^{n-1}x_j\sum_{k=1}^{(\ell-1)/2}k^{-1}(2p^r\varepsilon_{j-i}^{(k)}-2R(\ell,\ell-2k)) \equiv \sum_{j=0}^{n-1}x_j\sum_{k=1}^{(\ell-1)/2}k^{-1}(2p^r\varepsilon_{j+1-i}^{(k)}-2R(\ell,\ell-2k)).$$

Therefore, by $(\ell, 2p) = 1$, we have $\sum_{j=0}^{n-1} x_j c_{j-i} \equiv 0 \pmod{\ell}$ for every i. Thus, if $\xi = e_0^{x_0} e_1^{x_1} \dots e_{n-1}^{x_{n-1}} \in E_U^{(\ell)}$, then $u_n(A)(x_0, \dots, x_{n-1})^t \equiv \mathbf{0} \pmod{\ell}$. Therefore Corollary 3.2 shows that $E_U^{(\ell)}/(C_{p^r}^+)^\ell$ is isomorphic to a subgroup of $\operatorname{Ker} v_n(A)/\mathcal{N}$. This completes the proof of Theorem 4.1.

Remark 4.2. *Theorem* 4.1 *is valid for any subfield K_m of $\mathbb{Q}(\zeta_{p^r})^+$. In fact, putting $E_{U_{K_m}}^{(\ell)} = \{\eta \in C_{K_m}; \alpha^\ell \equiv \eta \pmod{\ell^2}$ for some integer $\alpha \in K_m\}$, we can similarly show that $E_{U_{K_m}}^{(\ell)}/(C_{K_m})^\ell$ is isomorphic to a subgroup of $\operatorname{Ker} v_m(A)/\mathcal{N}$ for a divisor m of n.*

Theorem 4.3. *Let p be an odd prime and $\ell \neq p$ an odd prime. If $v_n(x) = x - 1$, then $\ell \nmid h_{p^r}^+$. Moreover, for every $m|n$, if $v_m(x) = x - 1$, then $\ell \nmid h_{K_m}$.*

Proof of Theorem 4.3 If $\ell \,|\, h_{p^r}^+$, then $\ell \,|\, \#(E_U^{(\ell)}/(C_{p^r}^+)^\ell)$. This implies that $\operatorname{Ker} v_n(A)/\mathcal{N} \neq \{1\}$. Hence $v_n(x)$ is not trivial. The latter assertion is proved similarly by Remark 4.2. This completes the proof of Theorem 4.3.

Remark 4.4. *Theorem* 4.3 *is sufficiently effective to find the pair (ℓ, p) such that $\ell \nmid h_p^+$. In fact, we treat with the case $r = 1$ and calculate $v_n(x)$ for* 1227 *primes p in the range $5 \leq p < 10^4$ and for $\ell = 3, 11, 113$ and* 1009*. Then it turns out that the numbers of non-trivial $v_n(x)$ are $437, 216, 40$ and* 12 *for $\ell = 3, 11, 113$ and* 1009 *respectively.*

§ 5. The polynomial $w_n(x)$ for odd prime ℓ

Let $\xi_i = N_{\mathbb{Q}(\zeta_{p^r})^+/K_m}(e_i)$ for each i. For $\boldsymbol{y} = (y_0, y_1, \dots, y_{m-1}) \in \mathbb{F}_\ell^m$, we put $\xi(\boldsymbol{y}) = \xi_0^{y_0} \xi_1^{y_1} \dots \xi_{m-1}^{y_{m-1}}$. Since $\{\boldsymbol{y} \in \mathbb{F}_\ell^m; \sqrt[\ell]{\xi(\boldsymbol{y})} \in E_{K_m}\}$ is closed under the action of G, it follows from Theorem 3.8 that among the divisors of $x^m - 1$, there exists a unique monic polynomial $w_m(x) \in \mathbb{F}_\ell[x]$ such that

$$\operatorname{Ker} w_m(A) = \{\boldsymbol{y} \in \mathbb{F}_\ell^m; \sqrt[\ell]{\xi(\boldsymbol{y})} \in E_{K_m}\},$$

where $A = circ(0, 1, 0, \dots, 0)$. Then $w_m(x)$ satisfies $x - 1 \,|\, w_m(x) \,|\, v_m(x)$ for every $m \,|\, n$, because $\mathcal{N} \subseteq \operatorname{Ker} w_m(A) \subseteq \operatorname{Ker} r_m(A) \subseteq \operatorname{Ker} v_m(A)$, where $r_m(x)|x^m - 1$ is defined by $E_{U_{K_m}}/(C_{K_m})^\ell \simeq \operatorname{Ker} r_m(A)/\mathcal{N}$. When $w_m(x) = x - 1$, we call it trivial. We define μ_m by

$$\mu_m = \deg w_m - 1.$$

The polynomial $v_m(x)$ is dependent on the choice of the primitive root g modulo p^r, but $w_m(x)$ and μ_m are independent on the choice of g.

Proposition 5.1. *Let f be a divisor of $x^m - 1$. Put $\alpha = (x^m - 1)/f^\triangle(x)$ and $\boldsymbol{a} = \Phi(\alpha) \in \mathbb{F}_\ell^m$. Then f is a factor of w_m if and only if $\sqrt[\ell]{\xi(\boldsymbol{a})} \in E_{K_m}$.*

Proof of Proposition 5.1 By Proposition 4.4, $f|w_m$ if and only if $\operatorname{Ker} f(A) \subseteq \operatorname{Ker} w_m(A)$. On the other hand, as seen in the proof of Theorem 3.8, we have $\operatorname{Ker} f(A) = \Phi(\alpha R) = \{\sum_{j=0}^{m-1} b_j \boldsymbol{a}^{\sigma^j}\ ;\ b_j \in \mathbb{F}_\ell\}$. Therefore, noting that $\sqrt[\ell]{\xi(\boldsymbol{a})} \in E_{K_m}$ if and only if $\boldsymbol{a} \in \operatorname{Ker} w_m(A)$, we obtain the assertion of Proposition 5.1.

We notice that Proposition 5.1 is also valid in the case $\ell = 2$. The following proposition shows that $w_n(x)$ dominates all the $w_m(x)$ for the proper divisors $m \,|\, n$.

Proposition 5.2. *Let m, m' be divisors of n. Then if m divides m', we have $w_m(x) = \gcd(w_{m'}(x), x^m - 1)$. In particular, $w_m(x) = \gcd(w_n(x), x^m - 1)$ for every $m \,|\, n$.*

Corollary 5.3. *Let m_1 and m_2 be divisors of n and $m_3 = \gcd(m_1, m_2)$. Suppose that $w_{m_1}(x) = w_{m_2}(x) = w_n(x)$. Then we have $w_{m_3}(x) = w_n(x)$.*

Corollary 5.3 is an immediate consequence of Proposition 5.2.

Now, as stated in §1, the ℓ-rank of $E_{p^r}^+/C_{p^r}^+$ is determined by the following

Theorem 5.4. *Let p be a prime and ℓ an odd prime distinct from p. Then μ_n is equal to the ℓ-rank of $E_{p^r}^+/C_{p^r}^+$. More generally, for the subfield K_m of $\mathbb{Q}(\zeta_{p^r})^+$, μ_m is equal to the ℓ-rank of E_{K_m}/C_{K_m}.*

As a corollary we obtain a generalization of Theorem 5 in [15]. Put $\rho_m = \deg v_m - 1$ for each $m \,|\, n$.

Corollary 5.5. *$\ell \,|\, h_{p^r}^+$ if and only if $w_n(x)$ is non-trivial. In general, for the subfield K_m of $\mathbb{Q}(\zeta_{p^r})^+$, we have that $\ell | h_{K_m}$ if and only if $w_m(x)$ is not trivial. And if $\rho_m = \rho_n$, then $w_m(x) = w_n(x)$, so that $\mu_m = \mu_n$. Therefore $\ell | h_{p^r}^+$ if and only if $\ell | h_{K_m}$ for such $m \,|\, n$.*

Proof of Theorem 5.4 It suffices to prove the assertion only in case $m = n$, because the proof in the general case is similarly deduced. Suppose that $\ell | h_{p^r}^+$. For the simplicity, we put $E = E_{p^r}^+$ and $C = C_{p^r}^+$. We denote by $(E/C)_\ell$ the ℓ-elementary subgroup of E/C, i.e., $(E/C)_\ell = \{xC \in E/C\,;\, (xC)^\ell = 1\}$. Then we have a natural isomorphism $(E/C)_\ell \simeq E^\ell \cap C/C^\ell$.

Next we consider the homomorphism $\psi : \operatorname{Ker} w_n(A)/\mathcal{N} \longrightarrow E^\ell \cap C/C^\ell$ such that $\psi(\boldsymbol{y}\mathcal{N}) = \xi(\boldsymbol{y})C^\ell$ for any $\boldsymbol{y} \in \mathbb{F}_\ell^n$. This homomorphism is obviously well defined and surjective. On the other hand, since $e_0, e_1, \ldots, e_{n-2}$ is a basis of C, we can easily show that ψ is also injective. Thus ψ is an isomorphism. Therefore we have

$$\ell\text{-rank}\,(E/C)_\ell = \dim_{\mathbb{F}_\ell} \operatorname{Ker} w_n(A)/\mathcal{N} = \deg w_n - 1 = \mu_n$$

This completes the proof of Theorem 5.4.

Corollary 5.6. *Let m and m' be the divisors of $n = \varphi(p^r)/2$. Suppose that $w_m(x) \neq w_{m'}(x)$ for $m|m'$. Then ℓ divides the relative class number $h_{K_{m'}}/h_{K_m}$.*

The proofs of Corollaries 5.5 and 5.6 are almost obvious.

Remark 5.7. *The converse of Corollary* 5.6 *is not necessarily true. Indeed, let $p = 2089, r = 1, \ell = 3$ and $m' = 6, m = 2$. Then we obtain $w_2(x) = w_6(x) = w_{1044}(x) = (x-1)(x+1)$, and so $3\text{-rank}\,(E_{K_2}/C_{K_2}) = 3\text{-rank}\,(E_{K_6}/C_{K_6}) = 1$. On the other hand, putting $\boldsymbol{a} = (4,6,7,3,1,0) \in (\mathbb{Z}/9\mathbb{Z})^6$, we have $\sqrt[9]{\xi(\boldsymbol{a})} \in E_{K_6} \setminus C_{K_6}$ by an easy calculation, and so $3|h_{K_6}/h_{K_2}$. This shows that $3^2\text{-rank}\,(E_{K_6}/C_{K_6}) = 1$.*

Corollary 5.8. *Let $n_i = \varphi(p^{i+1})/2$ for $i \geq 0$. Then $w_{n_i}(x)|w_{n_{i+1}}(x)$ for every $i \geq 0$ and $w_{n_i}(x) = w_{n_s}(x)$ for every $i \geq s$ with some positive integer s.*

Corollary 5.8 is proved by Theorem 16.12 in [13].

§ 6. Algorithm to compute $w_n(x)$ for odd prime ℓ

In this section we explain our algorithm to compute the polynomial $w_n(x)$ for an odd prime $\ell \neq p$. Now we fix the least divisor m of n such that $\rho_m = \rho_n$, so $v_m(x) = v_n(x)$ and $w_m(x) = w_n(x)$ by Corollary 5.5. Here, if $\rho_m = 0$, then $\ell \nmid h_{p^r}^+$ by Theorem 4.3, i.e., $w_m(x) = w_n(x) = x - 1$. In the following it suffices to give an algorithm by which we can compute $w_m(x)$ in the case $\rho_m > 0$.

Our algorithm consists on two steps: The first step is necessary and useful to save the time of calculation when $v_m(x)$ has many divisors. So, if $v_m(x)$ has at most two distinct divisors including $x - 1$, we can skip the first step. On the other hand the second step is essential to determine $w_m(x)$.

The first step is to calculate an "approximate" polynomial, say $\hat{w}_m(x)$, of $w_m(x)$ satisfying

$$w_m(x) \,|\, \hat{w}_m(x) \,|\, v_m(x) \,|\, x^m - 1$$

Using Proposition 5.1 and the following Proposition 6.1, we can calculate $\hat{w}_m(x)$ from $v_m(x)$.

Proposition 6.1. *Let p be an odd prime and $\ell \neq p$ an odd prime. For a prime q such that $q \equiv 1 \pmod{p\ell}$, we let $\mathcal{Q}|q$ be a prime ideal of the first degree of $\mathbb{Q}(\zeta_{p^r})$. Let $b \in \mathbb{Z}$ satisfy $\zeta_{p^r} \equiv b \pmod{\mathcal{Q}}$ and $b^{p^r} \equiv 1$, $b \not\equiv 1 \pmod{q}$. For $\boldsymbol{a} = (a_0, a_1, \ldots, a_{m-1}) \in \mathbb{F}_\ell^m$, we write $\xi(\boldsymbol{a}) = f(\zeta_{p^r})$ by some polynomial $f \in \mathbb{Z}[x]$.*

If $f(\zeta_{p^r})$ is a ℓth power in K_m, then $f(b)$ is a ℓth power residue modulo q. Therefore if $\sqrt[\ell]{\xi(\boldsymbol{a})} \in E_{K_m}$, then $f(b)^{\frac{q-1}{\ell}} \equiv 1 \pmod{q}$ for any integer b such that $b^{p^r} \equiv 1$ and $b \not\equiv 1 \pmod{q}$.

Proposition 6.1 is proved by a short calculation. So we leave it to the readers.

Now we decompose $v_m(x)$ into irreducible factors as $v_m(x) = g_1^{r_1}(x)g_2^{r_2}(x)\cdots g_t^{r_t}(x)$ in $\mathbb{F}_\ell[x]$. Put $g(x) = g_i^{s_i}(x)\,(s_i \le r_i)$ and $\alpha(x) = (x^m - 1)/g^{\triangle}(x)$. Let $\Phi(\alpha) = \boldsymbol{a} \in \mathbb{F}_\ell^m$. For the first *seven* primes $q_1 < q_2 < \cdots < q_7$ satisfying $q_i \equiv 1 \pmod{p\ell}$, we make *seven* pairs (q_i, b_i) as in Proposition 6.1 and examine whether $f(b_i)^{\frac{q_i-1}{\ell}} \equiv 1 \pmod{q_i}$ is satisfied. If these congruent equations are all satisfied for the *seven* pairs (q_i, b_i), we regard $g_i^{s_i}(x)$ as a factor of $\hat{w}_m(x)$. Otherwise $g_i^{s_i}(x)$ is not a factor of $\hat{w}_m(x)$. In this way, collecting all the divisors of $\hat{w}_m(x)$, we define a "approximate" polynomial $\hat{w}_m(x)$ of $w_m(x)$. Here, as we temporarily choose *seven* primes q_i to define $\hat{w}_m(x)$, *seven* has not a particular meaning. Namely, $\hat{w}_m(x)$ only plays a auxiliary role to obtain an essential polynomial $w_m(x)$.

Remark 6.2. *In Proposition* 6.1, *we concretely calculate* $f(b)^{\frac{q-1}{\ell}}$ *as follows: Fix the least divisor* m *of* n *such that* $\rho_m = \rho_n$. *Then* $v_n(x) = v_m(x)$. *For a factor* $h(x)$ *of* $v_m(x)$, *put* $\alpha(x) = (x^m - 1)/h^{\triangle}(x) = \sum_{i=0}^{m-1} a_i x^i$ *and* $\boldsymbol{a} = \Phi(\alpha) = (a_0, a_1, \ldots, a_{m-1})$. *Here we have*

$$\xi(\boldsymbol{a}) \;=\; N_{\mathbb{Q}(\zeta_{p^r})^+/K_m}(e_0^{a_0} e_1^{a_1} \cdots e_{m-1}^{a_{m-1}}) \;=\; \prod_{k=0}^{n-1} \left(\frac{\zeta^{g_{k+1}} - \zeta^{-g_{k+1}}}{\zeta^{g_k} - \zeta^{-g_k}} \right)^{a_k},$$

where $a_{i+m} = a_i$ *for every* i. *In this equation we substitute* b *for* ζ *and obtain the following number* $z = f(b)$ *in* $\mathbb{F}_q$.

$$z = \prod_{k=0}^{n-1} \left(\frac{b^{g_{k+1}} - b^{-g_{k+1}}}{b^{g_k} - b^{-g_k}} \right)^{a_k} \bmod q.$$

If $z^{(q-1)/\ell} \not\equiv 1 \bmod q$, *then* $\sqrt[\ell]{\xi(\boldsymbol{a})} \notin E_{K_m}$. *This shows that* $h(x)$ *does not divide* $w_n(x)$, *so that* $h(x) \nmid \hat{w}_m(x)$. *If* $z^{(q-1)/\ell} \equiv 1 \bmod q$, *we choose another pair* (q', b') *and calculate the corresponding number* z' *for it. And we examine whether* $z'^{(q'-1)/\ell} \equiv 1 \bmod q'$ *and we repeat these calculations seven times to get a divisor of* $\hat{w}_m(x)$.

The second step: For each factor of $\hat{w}_m(x)$ obtained in the first step, we examine whether it is a factor of $w_m(x)$ by Proposition 5.1 and the following Proposition 6.3. When we skip the first step, we consider $\hat{w}_m(x) = v_m(x)$ and examine the same test.

Proposition 6.3. *Let* p *be an odd prime and* $\ell \ne p$ *an odd prime. Let* K_m *be the subfield of* $\mathbb{Q}(\zeta_{p^r})^+$ *of degree* m. *Let* ξ *be a unit of* K_m. *Suppose that* $\mathbb{Q}(\xi) = K_m$. *We denote by* $g(x)$ *the minimal polynomial of* ξ *over* $\mathbb{Q}$. *Then* $\sqrt[\ell]{\xi} \in K_m$ *if and only if* $g(x^\ell)$ *has a unique irreducible factor of degree* m *in* $\mathbb{Z}[x]$.

The proof of Proposition 6.3 is a routine one. So we omit it. Applying Proposition 6.3 to a cyclotomic unit ξ in K_m, we can decide whether $\sqrt[\ell]{\xi}$ is contained in K_m.

From now on, we treat only with the case $r = 1$. That is, we consider the class number h_p^+ of the field $\mathbb{Q}(\zeta_p)$. Put $f = (p-1)/m$. For the subfield K_m of $\mathbb{Q}(\zeta_p)$ of degree m, let $\eta_j^{(f)}$ be the Gaussian periods of f terms, that is, $\eta_j^{(f)} = \sum_{s=0}^{f-1} \zeta^{g^{j+sm}}$ $(0 \le j < m)$. Then a $\mathbb{Z}$-basis of the ring of integers of K_m is given by $\eta_0^{(f)}, \eta_1^{(f)}, \cdots, \eta_{m-1}^{(f)}$. So a cyclotomic unit ξ of K_m is represented as $\xi = \sum_{i=0}^{m-1} a_i \eta_i^{(f)}$, where $a_i \in \mathbb{Z}$. To get the minimal polynomial $g(x)$ of ξ over $\mathbb{Q}$, we use the Gauss formula

$$\eta_i^{(f)} \eta_j^{(f)} = \sum_{s \bmod f} \eta^{[g^i + g^{j+sm}]},$$

where $\eta^{[i]}$ in the right hand means the Gaussian period $\eta_j^{(f)}$ which contains ζ^i, i.e., $\eta^{[i]} = \sum_s \zeta^{ig^{sm}}$. Using the Gauss formula and the trivial relation $\sum_{i=0}^{m-1} \eta_i^{(f)} = -1$ repeatedly, we can reduce $g(x) = \Pi_{j=0}^{m-1}(x - \xi^{\sigma^j}) \in \mathbb{Z}[x, \eta_0^{(f)}, \eta_1^{(f)}, \ldots, \eta_{m-1}^{(f)}]$ to a polynomial $g(x)$ of $\mathbb{Z}[x]$. The remainding is only to check whether $g(x^\ell)$ has an irreducible factor of degree m.

We here give an example to illustrate our algorithm.

Example 1. Let $p = 5437, \ell = 31$ and $r = 1$. Then $n = 2718$, $\rho_{2718} = \rho_6 = 1$ and $v_6(x) = (x-1)(x+5) \in \mathbb{F}_{31}[x]$. Now $g = 5$ and $e_0 = (\zeta^5 - \zeta^{-5})/(\zeta - \zeta^{-1}) = 1 + \eta_{327}^{(2)} + \eta_{654}^{(2)}$, where $\zeta = \zeta_{5437}$ and $\eta_i^{(2)}$ is the Gaussian period of 2 terms. So

$$\begin{aligned}
\xi_0 &= N_{\mathbb{Q}(\zeta)^+/K_6}(e_0) \\
&= 4313206656944\eta_0^{(906)} + 4318106573460\eta_1^{(906)} + 4322874423442\eta_2^{(906)} \\
&\quad +4332036559191\eta_3^{(906)} + 4673220060409\eta_4^{(906)} + 4302990157453\eta_5^{(906)},
\end{aligned}$$

where $\eta_i^{(906)}$ is the Gaussian period of 906 terms.

Now, to examine whether $h(x) = (x+5) | w_6(x)$, we put $\alpha(x) = (x^6 - 1)/h^{\triangle}(x) = 6(5 + 6x + x^2 - 5x^3 - 6x^4 - x^5)$, so that $\boldsymbol{a} = \Phi(\alpha(x)) = 6(5, 6, 1, -5, -6, -1)$. Here we may consider $\boldsymbol{a} = (5, 6, 1, -5, -6, -1)$. Put $\boldsymbol{b} = \boldsymbol{a}^\sigma + (6, 6, 6, 6, 6, 6) = (5, 11, 12, 7, 1, 0)$. Then $\sqrt[31]{\xi(\boldsymbol{a})} \in E_{K_6}$ if and only if $\sqrt[31]{\xi(\boldsymbol{b})} \in E_{K_6}$. Hence we have

$$\begin{aligned}
ll\xi(\boldsymbol{b}) &= \xi_0^5 \xi_1^{11} \xi_2^{12} \xi_3^7 \xi_4 \\
&= -625445791755999710030414670886834821401637367721915868046 5\eta_0^{(906)} \\
&\quad -6763964819275024893167115701761960432558589567472683935938\eta_1^{(906)} \\
&\quad -6193152508641797868472023527278775422576039963176680635248\eta_2^{(906)} \\
&\quad -6227327731106592730040756696702447201998647791566600467761\eta_3^{(906)} \\
&\quad -6234129729181136596192064753782974987571735120573354167785\eta_4^{(906)} \\
&\quad -6241006540845803026912245003275911831096087870246353410713\eta_5^{(906)}.
\end{aligned}$$

We calculate the minimal polynomial $g(x)$ of $\xi(\boldsymbol{b})$ over $\mathbb{Q}$. Then

$$
\begin{aligned}
g(x) = 1 - &37914039246610352215088352391670418089817473990254831297910x \\
&-52640663545217914581877701877797657992550443567446555416593/ \\
&548686612147881645821650051877097330551416795839586592078x^2 \\
&-154275569908394591335361358545259896427515799142841111292857/ \\
&4003974092063920341744578774674834644409493766684006148078x^3 \\
&-52640663545217914581877701877797657992550443567446555416593/ \\
&548686612147881645821650051877097330551416795839586592078x^4 \\
&-37914039246610352215088352391670418089817473990254831297910x^5 + x^6.
\end{aligned}
$$

Therefore we have

$$(1 - 6x - 5422x^2 - 10894x^3 - 5422x^4 - 6x^5 + x^6) \,|\, g(x^{31}),$$

which shows that $x + 5$ is a factor of $w_6(x)$. Thus we have $w_{2718}(x) = w_6(x) = (x - 1)(x + 5)$ and 31-rank of E^+_{5437}/C^+_{5437} is 1.

Remark 6.4. *In example* 1, *for every* $m|n = 2718$, *we obtain that* $w_m(x) = (x-1)(x+5)$ *or* $w_m(x) = x - 1$ *according as* $6|m$ *or not. We here show an interesting example. Let* $p = 7753$ *and* $\ell = 5$. *Then* $n = 3876$ *and* $w_{3876}(x) = w_{12}(x) = (x - 1)(x + 2)(x^2 + x + 1)$. *Hence* $w_3(x) = (x - 1)(x^2 + x + 1)$ *and* $w_4(x) = (x - 1)(x + 2)$ *by Proposition* 5.2, *so that* $5|h_{K_3}$ *and* $5|h_{K_4}$.

§ 7. The polynomial $w_n(x)$ for the case $\ell = 2$

In this section we illustrate a method by which we can determine the 2-rank of $E^+_{p^r}/C^+_{p^r}$. This method is a similar one in the preceding sections.

Let $e_i = \sin(2g_{i+1}\pi/p^r)/\sin(2g_i\pi/p^r)$ be the cyclotomic unit in $\mathbb{Q}(\zeta_{p^r})^+$ defined in §1. Let $\mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}$. Let c_i be 0 or 1 according as e_i is positive or not. We define the polynomials u_n and v_n in $\mathbb{F}_2[x]$ as $u_n(x) = \sum_{j=0}^{n-1} c_j x^{n-1-j}$ and $v_n(x) = \gcd(u_n(x), x^n + 1)$. We note that $x^n + 1 = x^n - 1$ in this case. For a polynomial $f(x) = \sum_{i=0}^{n-1} a_j x^j$ in $\mathbb{F}_2[x]$, we define $f^*(x)$ as in §3, i.e., $f^*(x) = x^{n-1}f(1/x)$. Then $v_n^*(x) = \gcd(u_n^*(x), x^n+1)$. For any $m|n$, we put $t = n/m$ and define polynomials u_m and v_m in $\mathbb{F}_2[x]$ as $u_m(x) = \sum_{j=0}^{m-1}(\sum_{k=0}^{t-1} c_{j+km})x^{m-1-j}$ and $v_m(x) = \gcd(u_m(x), x^m + 1)$ respectively.

The following theorem was given by Bentzen [1].

Theorem 7.1. $2|h^+_{p^r}$ *if and only if* $\deg\ \gcd(v_n(x), v_n^*(x)) > 0$.

Here we give another proof of Theorem 7.1. Our proof is based upon the following results in [14].

Lemma 7.2. (Lemma 1 [14]) *Let $C^+_{p^r,0}$ be the subgroup of $C^+_{p^r}$ of totally positive cyclotomic units. Then we have*

$$\operatorname{Ker} v_n^*(A) \simeq C^+_{p^r,0}/(C^+_{p^r})^2.$$

Theorem 7.3. (Theorem 1 [14]) *Let $E_U^{(2)}$ be the subgroup of $C^+_{p^r}$ of 2-primary cyclotomic units, i.e., $E_U^{(2)} = \{\eta \in C^+_{p^r} ; \alpha^2 \equiv \eta \pmod 4$ for some integer $\alpha \in \mathbb{Q}(\zeta_{p^r})^+\}$. Then we have*

$$\operatorname{Ker} v_n(A) \simeq E_U^{(2)}/(C^+_{p^r})^2.$$

Now, Corollary of Theorem 1 [14] shows that $h^+_{p^r}$ is even if and only if $\operatorname{Ker} v_n(A) \cap \operatorname{Ker} v_n^*(A) \neq 1$. Since $\dim_{\mathbb{F}_2} \operatorname{Ker} v_n(A) \cap \operatorname{Ker} v_n^*(A) = \deg \gcd(v_n(x), v_n^*(x))$, it follows from Lemma 7.2 and Theorem 7.3 that $2|h^+_{p^r}$ if and only if $\deg\ \gcd(v_n(x), v_n^*(x)) > 0$. This completes the proof of Theorem 7.1.

Theorem 7.4. *Let p be an odd prime and $\ell = 2$. Then, among the divisors of $x^n + 1$ in $\mathbb{F}_2[x]$, there exists a unique monic polynomial $w_n(x)$ such that*

$$\operatorname{Ker}\ w_n(A) = \{\boldsymbol{y} \in \mathbb{F}_2^n ;\ \sqrt{\xi(\boldsymbol{y})} \in E^+_{p^r}\},$$

where $w_n(x)$ is a divisor of $\gcd(v_n(x), v_n^*(x))$ and $x + 1 \nmid w_n(x)$. And the 2-rank of $E^+_{p^r}/C^+_{p^r}$ is equal to the degree of $w_n(x)$.

Remark 7.5. *$w_n(x)$ is not necessarily equal to $\gcd(v_n(x), v_n^*(x))$. As an example, we have $v_n(x) = (x^3+x+1)(x^3+x^2+1) = \gcd(v_n(x), v_n^*(x))$ and $w_n(x) = x^3+x^2+1$ for $p = 4327$.*

Corollary 7.6. *Let m be a divisor of n. Then, among the divisors of $x^m + 1$ in $\mathbb{F}_2[x]$, there exists a unique monic polynomial $w_m(x)$ such that*

$$\operatorname{Ker}\ w_m(A) = \{\boldsymbol{y} \in \mathbb{F}_2^m ;\ \sqrt{\xi(\boldsymbol{y})} \in E_{K_m}\}.$$

Here $w_m(x)$ is a divisor of $\gcd(v_m(x), v_m^*(x))$. It satisfies $w_m(x) = \gcd(w_n(x), x^m + 1)$ and $x + 1 \nmid w_m(x)$. The 2-rank of E_{K_m}/C_{K_m} is equal to the degree of $w_m(x)$.

In case $\ell = 2$, w_n again dominates all the w_m for the proper divisors $m|n$ by Corollary 7.6. On the other hand, $w_n(x)$ does not have $x + 1$ as a divisor in case $\ell = 2$. This is quite different from the fact $x - 1|w_n(x)$ in case $\ell > 2$.

Proof of Theorem 7.4 For the simplicity, we put $E = E_{p^r}^+$ and $C = C_{p^r}^+$. Suppose that $2|h_{p^r}^+$. Since $E^2 \cap C \subseteq E_U^{(2)}$, we have $\operatorname{Ker} w_n(A) \subseteq \operatorname{Ker} v_n(A)$ by Theorem 7.3. It follows from Proposition 3.4 that $w_n|v_n$. Similarly $\operatorname{Ker} w_n(A) \subseteq \operatorname{Ker} v_n^*(A)$ implies $w_n|v_n^*$. Therefore w_n is a divisor of $\gcd(v_n, v_n^*)$. We denote by $(E/C)_2$ the 2-elementary subgroup of E/C. Then, in a similar way as in Theorem 5.3, we have

$$(E/C)_2 \simeq E^2 \cap C/C^2 \simeq \operatorname{Ker} w_n(A).$$

We notice that $\sum_{i=0}^{n-1} c_i \equiv 1 \pmod 2$ implies $(1, 1, \ldots, 1) \notin \operatorname{Ker} v_n(A)$ and $x + 1 \nmid v_n(x)$, so $\operatorname{Ker} w_n(A) \cap \mathcal{N} = \{(0, 0, \ldots, 0)\}$. Therefore we have $x + 1 \nmid w_n(x)$ and

$$2\text{-rank}\,(E/C)_2 = \dim_{\mathbb{F}_2} \operatorname{Ker} w_n(A) = \deg w_n.$$

This completes the proof of Theorem 7.4.

In the case $\ell = 2$, Theorem 7.4 shows that $\gcd(v_n(x), v_n^*(x))$ plays a role as an approximate polynomial $\hat{w}_n(x)$ of $w_n(x)$. Thus, for each factor of $\gcd(v_n(x), v_n^*(x))$ in $\mathbb{F}_2[x]$, we examine whether it is a factor of $w_n(x)$ by Proposition 5.1 and the following

Proposition 7.7. *Let p be an odd prime. Let K_m be the subfield of $\mathbb{Q}(\zeta_{p^r})^+$ of degree m. Let ξ be a unit of K_m. Suppose that $\mathbb{Q}(\xi) = K_m$. We denote by $g(x)$ the minimal polynomial of ξ over $\mathbb{Q}$. Then $\sqrt{\xi} \in K_m$ if and only if $g(x^2)$ has a unique irreducible factor $h(x)$ in $\mathbb{Z}[x]$ of degree m such that $g(x^2) = (-1)^m h(x)h(-x)$.*

The proof of Proposition 7.7 is same as one of Proposition 6.3. So we omit it.

Remark 7.8. *In the case $\ell = 2$ and $r = 1$, Bentzen* [1] *calculated the polynomial $w_n(x)$ for $p < 6000$. Our calculation of $w_n(x)$ was done for $p < 10000$ and it coincides with his table for $p < 6000$.*

Example 2. Let $p = 7687, \ell = 2$ and $r = 1$. Then $n = 3843$ and $v_n(x) = x^{11} + x^{10} + x^6 + x^3 + 1$. So we have $\gcd(v_n(x), v_n^*(x)) = x^2 + x + 1 \in \mathbb{F}_2[x]$. Now $g = 6$ and $e_0 = (\zeta^6 - \zeta^{-6})/(\zeta - \zeta^{-1}) = \eta_0^{(2)} + \eta_{2527}^{(2)} + \eta_{4545}^{(2)}$, where $\zeta = \zeta_{7687}$ and $\eta_i^{(2)}$ is the Gaussian period of 2 terms. Since $\rho_n = \rho_{63}$, we must consider the cyclotomic units in K_{63}. But it suffices to consider the cyclotomic units in K_3 because $x^2 + x + 1 | x^3 + 1$ in $\mathbb{F}_2[x]$. So

$$\begin{aligned}\xi_0 = N_{\mathbb{Q}(\zeta)^+/K_3}(e_0) = {} & 12329504535330953686\eta_0^{(2562)} + 11893174231611985867\eta_1^{(2562)} \\ & + 12286294258110801841\eta_2^{(2562)},\end{aligned}$$

where $\eta_i^{(2562)}$ is the Gaussian period of 2562 terms.

Now, since $w_n(x) \,|\, \gcd(v_n(x), v_n^*(x))$, we may examine whether $h(x) = x^2 + x + 1$ is a factor of $w_3(x) = w_n(x)$. Then $\alpha(x) = (x^3 - 1)/h^*(x) = -1 + x$, so that $\boldsymbol{a} = \Phi(\alpha(x)) = (1, 1, 0)$. Hence we have

$$\xi(\boldsymbol{a}) = \xi_0\xi_1 = -114579034093\eta_0^{(2562)} - 110525592358\eta_1^{(2562)} - 114176445562\eta_2^{(2562)}.$$

We calculate the minimal polynomial $g(x)$ of $\xi(\boldsymbol{a})$ over $\mathbb{Q}$. Then

$$g(x) = -1 + 36508973025053741394x - 339281072013x^2 + x^3.$$

Therefore we have

$$g(x^2) = (-1 + 6042265554x - 592761x^2 + x^3)(1 + 6042265554x + 592761x^2 + x^3),$$

which shows that $w_{3843}(x) = w_3(x) = x^2 + x + 1$, so that 2-rank of E_{7687}^+/C_{7687}^+ is 2.

§ 8. Numerical results

We here treat with $\mathbb{Q}(\zeta_p)^+$ $(r = 1)$ and tabulate all the non-trivial polynomials $w_n(x)$ for the pairs (ℓ, p) in the range $2 \le \ell < 10^4$, $3 \le p < 10^4$, and $\ell \ne p$ except the one case $(\ell, p) = (131, 7411)$. The number of non-trivial polynomial $w_n(x)$ is 345 in all. For this exceptional case denoted by † in the table, we can obtain $\hat{w}_n(x) = (x - 1)(x + 31)$, but we can not determine $w_n(x) = (x - 1)(x + 31)$. We recall that the triviality of $w_n(x)$ means $w_n(x) = x - 1$ for $\ell > 2$ and $w_n(x) = 1$ for $\ell = 2$ respectively. In the table we denote by m the least divisor of n such that $\rho_m = \rho_n$, where $\rho_n = \deg v_n(x) - 1$ or $\rho_n = \deg v_n(x)$ according as $\ell > 2$ or $\ell = 2$. We notice that $w_n(x)$ is trivial for the pair (ℓ, p) lying in above range and not appearing in the table. Hence, if there exists an odd prime $p < 10^4$ such that (ℓ, p) does not appear in the table for every $\ell < 10^4$, then h_p^+ has no prime divisors $< 10^4$. The number of such odd prime $p < 10^4, p \ne 7411$ is 925 as against the number of all odd primes $p < 10^4$ is 1228.

First we used three personal computers for about 270 hours to calculate approximate polynomials $\hat{w}_n(x)$ in 2000. We used a program which was written in C with inline-assembler. Each PC consisted on Pentium 3, 800 MHz with 512 MB memory. Second we used a personal computer(Pentium 4, 3.2 GHz with 1 GB memory) for about 6 hours to calculate $w_n(x)$ from $\hat{w}_n(x)$ a few years later. We used a Mathematica program named “nt003-44”. However, by working only nt003-44, we could not obtain all the $w_n(x)$ with one exceptional case $(\ell, p) = (131, 7411)$. In fact, for the following 28 pairs, since the coefficients of a defining equation $g(x)$ of $\xi(\boldsymbol{a})$ are very huge, i.e., exceeding 5000 digits, we could not find an irreducible divisor $h(x)$ with degree m of $g(x^\ell)$

by nt003-44:

$$(\ell, p) = (23, 4049), (29, 5209), (29, 9689), (31, 8431), (37, 3433), (47, 829), (61, 3121),\\ (61, 6361), (67, 8713), (71, 953), (73, 5581), (73, 9857), (79, 4603), (97, 4481),\\ (97, 6337), (101, 5701), (109, 7417), (109, 8017), (113, 8317), (113, 9521),\\ (131, 7411), (151, 3301), (211, 1231), (313, 6577), (421, 7841), (541, 9551),\\ (883, 3547), (1451, 5051).$$

For these 27 pairs excluding $(131, 7411)$, we used the Chinese Remainder Theorem for the coefficients of $g(x^\ell)$ in additon to nt003-44, and determined the coefficients of $h(x)$ and checked that $h(x)$ divides $g(x^\ell)$. We could therefore obtain $w_n(x)$ in above 27 cases. For the case $(\ell, p) = (131, 7411)$, we could not obtain $g(x)$ itself, so we could not adapt the Chinese Remainder Theorem for it to get $w_n(x)$.

Table of the non-trivial polynomials $w_n(x)$ for $p < 10^4$ and $\ell, 2 \le \ell < 10^4$

ℓ	p	m	$w_n(x)$	ℓ	p	m	$w_n(x)$
2	163	3	x^2+x+1	2	4801	6	x^2+x+1
2	277	6	x^2+x+1	2	5197	6	x^2+x+1
2	349	6	$(x^2+x+1)^2$	2	5479	3	x^2+x+1
2	397	6	x^2+x+1	2	5531	7	x^3+x+1
2	491	7	x^3+x+1	2	5659	3	x^2+x+1
2	547	3	x^2+x+1	2	5779	3	x^2+x+1
2	607	3	x^2+x+1	2	5953	3	x^2+x+1
2	709	6	$(x^2+x+1)^2$	2	6037	3	x^2+x+1
2	827	7	x^3+x+1	2	6079	3	x^2+x+1
2	853	3	x^2+x+1	2	6163	3	x^2+x+1
2	937	3	x^2+x+1	2	6247	3	x^2+x+1
2	941	10	$x^4+x^3+x^2+x+1$	2	6301	7	x^3+x+1
2	1009	63	x^2+x+1	2	6553	21	x^2+x+1
2	1399	3	x^2+x+1	2	6637	3	x^2+x+1
2	1699	3	x^2+x+1	2	6709	3	x^2+x+1
2	1777	6	x^2+x+1	2	6833	7	x^3+x^2+1
2	1789	6	x^2+x+1	2	7027	3	x^2+x+1
2	1879	3	x^2+x+1	2	7297	6	x^2+x+1
2	1951	3	x^2+x+1	2	7489	3	x^2+x+1
2	2131	3	x^2+x+1	2	7589	7	x^3+x+1
2	2161	5	$x^4+x^3+x^2+x+1$	2	7639	3	x^2+x+1
2	2311	21	x^2+x+1	2	7687	63	x^2+x+1
2	2689	3	x^2+x+1	2	7841	7	$(x^3+x+1)(x^3+x^2+1)$
2	2797	6	x^2+x+1	2	7867	3	x^2+x+1
2	2803	3	x^2+x+1	2	7879	3	x^2+x+1
2	2927	7	x^3+x+1	2	8011	3	x^2+x+1
2	3037	6	x^2+x+1	2	8191	63	x^2+x+1
2	3271	3	x^2+x+1	2	8209	3	x^2+x+1
2	3301	5	$x^4+x^3+x^2+x+1$	2	8629	3	x^2+x+1
2	3517	3	x^2+x+1	2	8647	3	x^2+x+1
2	3727	3	x^2+x+1	2	8731	3	x^2+x+1
2	3931	5	$x^4+x^3+x^2+x+1$	2	8831	5	$x^4+x^3+x^2+x+1$
2	4099	3	x^2+x+1	2	8887	3	x^2+x+1
2	4219	3	x^2+x+1	2	9109	6	x^2+x+1
2	4261	6	$(x^2+x+1)^2$	2	9283	3	x^2+x+1
2	4297	6	$(x^2+x+1)^2$	2	9319	3	x^2+x+1
2	4327	7	x^3+x^2+1	2	9337	3	x^2+x+1
2	4357	6	x^2+x+1	2	9391	3	x^2+x+1
2	4561	30	$(x^2+x+1)^2$	2	9421	6	x^2+x+1
2	4567	3	x^2+x+1	2	9601	3	x^2+x+1
2	4639	3	x^2+x+1	2	9649	6	x^2+x+1
2	4789	126	x^2+x+1	2	9721	3	x^2+x+1

ℓ	p	m	$w_n(x)/(x-1)$	ℓ	p	m	$w_n(x)/(x-1)$
3	229	2	$x+1$	3	5741	2	$x+1$
3	257	2	$x+1$	3	5821	2	$x+1$
3	401	8	x^2+x-1	3	6053	2	$x+1$
3	521	26	x^3+x^2-x+1	3	6133	6	$x+1$
3	641	40	x^2+x-1	3	6637	6	$x+1$
3	733	2	$x+1$	3	6737	4	x^2+1
3	761	2	$x+1$	3	6997	2	$x+1$
3	1129	6	$x+1$	3	7057	6	$x+1$
3	1229	2	$x+1$	3	7481	2	$x+1$
3	1373	2	$x+1$	3	7537	2	$x+1$
3	1489	6	$x+1$	3	7573	6	$x+1$
3	1901	2	$x+1$	3	7673	2	$x+1$
3	2089	6	$x+1$	3	7753	2	$x+1$
3	2213	2	$x+1$	3	7873	6	$(x+1)^2$
3	2557	6	$x+1$	3	8017	2	$x+1$
3	2677	2	$x+1$	3	8069	2	$x+1$
3	2713	6	$x+1$	3	8297	4	x^2+1
3	2753	8	x^2-x-1	3	8581	858	$x+1$
3	2777	4	$x+1$	3	8597	2	$x+1$
3	2857	6	$x+1$	3	8713	6	$x+1$
3	2917	6	$x+1$	3	8761	6	$(x+1)^2$
3	3137	2	$x+1$	3	8837	2	$x+1$
3	3221	2	$x+1$	3	9133	2	$x+1$
3	3229	2	$x+1$	3	9281	40	$x+1$
3	3877	2	$x+1$	3	9293	2	$x+1$
3	3889	6	$x+1$	3	9413	26	$(x+1)(x^3+x^2-x+1)$
3	4001	40	$x+1$	3	9697	4	x^2+1
3	4241	4	x^2+1	3	9749	2	$x+1$
3	4409	2	$x+1$	3	9833	2	$x+1$
3	4481	40	$x+1$	5	401	20	$x+1$
3	4493	2	$x+1$	5	457	4	$x-2$
3	4597	2	$x+1$	5	641	4	$x-2$
3	4649	2	$x+1$	5	857	4	$x-2$
3	4729	2	$x+1$	5	977	4	$x-2$
3	4933	18	$x+1$	5	1093	2	$x+1$
3	5081	2	$x+1$	5	1297	8	x^2-2
3	5261	2	$x+1$	5	1429	2	$x+1$
3	5281	6	$x+1$	5	1873	8	x^2-2
3	5297	2	$x+1$	5	2081	2	$x+1$
3	5333	2	$x+1$	5	2153	2	$x+1$
3	5477	2	$x+1$	5	2473	4	$x-2$
3	5521	6	$x+1$	5	3121	20	$x+1$
3	5641	4	x^2+1	5	3181	2	$x+1$

ℓ	p	m	$w_n(x)/(x-1)$	ℓ	p	m	$w_n(x)/(x-1)$
5	3253	2	$x+1$	7	2437	3	$x-2$
5	3697	4	$x+2$	7	2557	6	$(x-2)(x-3)$
5	4073	4	$x+2$	7	2917	6	$x-3$
5	4357	2	$x+1$	7	3217	3	$x-2$
5	4441	12	$(x+1)(x-2)$	7	3313	6	$x-3$
5	4457	4	$x+2$	7	3571	3	$x+3$
5	4657	4	$x+2$	7	4219	3	$x+3$
5	4793	4	$x+2$	7	4229	2	$x+1$
5	4889	4	$x+1$	7	4339	3	$x+3$
5	4937	4	$x+2$	7	4597	6	$x-3$
5	4993	24	$x+2$	7	4783	3	$x-2$
5	6113	2	$x+1$	7	4861	6	$x+2$
5	6449	104	$x+2$	7	5273	2	$x+1$
5	6481	24	$x+1$	7	5417	2	$x+1$
5	6521	4	$x+2$	7	5953	6	$x+3$
5	6949	2	$x+1$	7	6037	6	$x-3$
5	7229	2	$x+1$	7	6709	6	$x-3$
5	7529	4	$x+2$	7	6991	3	$x-2$
5	7753	12	$(x+2)(x^2+x+1)$	7	6997	6	$x-3$
5	7817	2	$x+1$	7	7057	84	$x+1$
5	8161	12	$x+2$	7	7351	21	$x-2$
5	8297	4	$x-2$	7	7489	48	$x-2$
5	8377	4	$x+2$	7	7621	3	$x-2$
5	8501	10	$x+1$	7	8017	6	$x+2$
5	8689	24	$x+1$	7	8287	3	$x-2$
5	9161	4	$x+2$	7	8563	3	$x-2$
5	9181	10	$x+1$	7	8629	6	$x-2$
5	9377	4	$x+2$	7	8893	6	$x+2$
5	9601	20	$x+2$	7	9013	6	$x+2$
5	9829	2	$x+1$	7	9029	2	$x+1$
7	313	3	$x-2$	7	9049	6	$x+1$
7	577	6	$x+1$	7	9133	6	$x-3$
7	877	6	$(x+2)(x-2)$	7	9277	3	$x-2$
7	1009	6	$x+1$	7	9319	3	$x+3$
7	1069	6	$x-3$	7	9421	6	$x-3$
7	1129	6	$x+3$	7	9613	6	$x+2$
7	1381	6	$x-3$	7	9697	24	$x-2$
7	1567	3	$x+3$	11	191	5	$x-5$
7	1601	2	$x+1$	11	631	5	$x+2$
7	1831	3	$x-2$	11	641	40	$x-4$
7	1889	16	x^2-x-1	11	821	10	$x+3$
7	1987	3	$x-2$	11	1297	2	$x+1$
7	2029	2	$x+1$	11	1861	5	$x-5$

ℓ	p	m	$w_n(x)/(x-1)$	ℓ	p	m	$w_n(x)/(x-1)$
11	2351	5	$x-4$	19	4591	9	$x+3$
11	2381	10	$x+3$	19	5557	3	$x+8$
11	2621	10	$x-2$	19	8017	3	$x+8$
11	3001	10	$(x+2)(x+4)$	19	8389	6	$x+7$
11	3581	5	$x-4$	23	4049	22	$x-10$
11	4201	5	$x-3$	23	5413	11	$x-3$
11	5101	10	$x+4$	29	5209	28	$x-4$
11	5441	10	$x-2$	29	6257	4	$x+12$
11	5501	55	$x-4$	29	9689	28	$x+3$
11	6581	10	$x-3$	31	5119	3	$x+6$
11	8681	10	$x-2$	31	5437	6	$x+5$
11	9421	10	$(x+2)(x+5)$	31	8431	15	$x-14$
13	1063	3	$x+4$	31	9001	10	$x+2$
13	1459	3	$x+4$	31	9127	3	$x-5$
13	2617	4	$x+5$	31	9907	3	$x+6$
13	3041	4	$x+5$	37	2113	12	$x-8$
13	3469	6	$x-4$	37	3433	12	$x-14$
13	4729	12	$x+2$	37	7561	6	$x-11$
13	5827	3	$x+4$	37	8269	3	$x-10$
13	6073	12	$x+6$	41	2417	8	$x+14$
13	6229	6	$x+3$	41	6421	10	$x+10$
13	6529	12	$x+2$	41	7937	4	$x-9$
13	6781	6	$x+3$	47	829	46	$x+4$
13	7333	6	$x+3$	61	3121	20	$x+28$
13	7369	12	$x-6$	61	6361	60	$x+8$
13	8101	2	$x+1$	67	8713	33	$x-26$
13	9241	84	$x-3$	71	953	7	$x-32$
17	1697	4	$x+4$	73	5557	6	$x-9$
17	2417	4	$x-4$	73	5581	9	$x-16$
17	4817	8	$x-2$	73	9511	3	$x+9$
17	6577	4	$x-4$	73	9857	8	$x+22$
17	6673	8	$x-2$	79	4603	39	$x-25$
17	6961	8	$x-2$	97	4481	32	$x-28$
17	9041	4	$x-4$	97	6337	48	$x+25$
17	9817	4	$x-4$	101	5701	10	$x-6$
19	1153	72	$x+3$	109	7417	12	$x+41$
19	1459	9	$x-6$	109	8017	12	$x-8$
19	1489	3	$x+8$	113	8317	14	$x+28$
19	2659	3	$x-7$	113	9521	28	$x+2$
19	3313	9	$x-7$	$131^\dagger$	$7411^\dagger$	65	$x+31^\dagger$
19	3529	18	$x+8$	151	3301	150	$x-4$
19	3547	9	$x+8$	211	1231	15	$x+77$
19	4177	18	$x+4$	313	6577	8	$x-125$

ℓ	p	m	$w_n(x)/(x-1)$	ℓ	p	m	$w_n(x)/(x-1)$
421	7841	5	$x+142$	883	3547	9	$x-286$
541	9551	5	$x-124$	1451	5051	5	$x+430$

References

[1] S. Bentzen, Duality of cyclotomic units and 2-torsion of U/C, Aarhus University Preprint Series 1989/90, no. 39.

[2] S. Bentzen, Unit signatures and the 2-class group of cyclotomic fields of prime power conductor, Aarhus University Preprint Series 1989/90, no. 41.

[3] J. Buhler, R. Crandall, R. Ernvall, T. Metsänkylä and M. A. Shokrollahi, Irregular primes and cyclotomic invariants to twelve million, J. Symb. Comp., **31** (2001), 89−96.

[4] G. Cornell and M. Rosen, The ℓ-rank of the real class group of cyclotomic fields, Compositio Math., **53** (1984), 133−141.

[5] G. Gras and M.N. Gras, Calcul du nombre de classes et des unités des extensions abéliennes réelles de **Q**, Bull. Sci. math., **101** (1977), 97−129.

[6] H. Hasse, Über die Klassenzahl abelscher Zahlkörper, Akademie-Verlag, Berlin, 1952 ; Springer-Verlag, 1985.

[7] S. Jakubec, On the divisibility of class number of real abelian fields of prime conductor, Abh. Math. Sem. Univ. Hamburg, **63** (1993), 67−86.

[8] E. E. Kummer, Über eine Eigenschaft der Einheiten der aus den Wurzeln der Gleichung $\alpha^\lambda = 1$ gebildeten complexen Zahlen, und über den zweiten Factor der Klassenzahl, Monatsber. Akad. Wiss., Berlin, 1870, 855−880. Reprinted in Collected Papers , vol. I, Springer-Verlag, 1975, 919−944.

[9] H. W. Leopoldt, Über Klassenzahlprimteiler reeller abelscher Zahlkörper als Primteiler verallgemeinerter Bernoullischer Zahlen, Abh. Math. Sem. Univ. Hamburg, **23** (1959), 36−47.

[10] F. van der Linden, Class number computations of real abelian number fields, Math. Comp., **39** (1982), 693−707.

[11] T. Metsänkylä, An application of the p-adic class number formula, Manuscripta Math., **93** (1997), 481−498.

[12] R. Schoof, Class numbers of real cyclotomic fields of prime conductor, Math. Comp. **72** (2003), 913−937.

[13] L. C. Washington, Introduction to Cyclotomic Fields. Springer-Verlag, 1982; Second edition 1997.

[14] K. Yoshino, A criterion for the parity of the class number of an abelian field with prime power conductor, Nagoya Math. J. **145** (1997), 163−177.

[15] K. Yoshino, A condition for divisibility of the class number of real p th cyclotomic field by an odd prime distinct from p, Abh. Math. Sem. Univ. Hamburg **69** (1999), 37−57.