Calculation of Prime Divisors of Class Numbers of Real Cyclotomic Fields

実円分体の類数の素因子の計算

Youichi Koyama(Kanazawa Institute of Technology)

Ken-ichi Yoshino(Kanazawa Medical University)

The Content

§1. Introduction

Notation

p : an odd prime, r : a positive integer

$n = \varphi(p^r)/2 = p^{r-1}(p-1)/2$

$\zeta := \cos(2\pi/p^r) + i\sin(2\pi/p^r)$: a primitive p^rth root of 1

$\mathbb{Q}(\zeta)$: p^rth cyclotomic field

$\mathbb{Q}(\zeta)^+ = \mathbb{Q}(\zeta) \cap \mathbb{R} = \mathbb{Q}(\cos 2\pi/p^r)$: its maximal real subfield

g : a primitive root modulo p^r, i.e., a generator of multiplicative cyclic group $(Z/p^rZ)^*$

$g_i : g^i \equiv g_i \pmod{p^r}, \quad 0 < g_i < p^r$

$$e_i := \frac{\zeta^{g_{i+1}} - \zeta^{-g_{i+1}}}{\zeta^{g_i} - \zeta^{-g_i}} = \frac{\sin \frac{2g_{i+1}\pi}{p^r}}{\sin \frac{2g_i\pi}{p^r}} \quad (i = 0, 1, \ldots, n-1)$$

e_i has a period n and the relation $e_0 e_1 \ldots e_{n-1} = -1$.

$C_{p^r}^+$: the subgroup of $E_{p^r}^+$ generated by cyclotomic units $e_0, e_1, \ldots, e_{n-1}$

$E_{p^r}^+$: the group of units of $\mathbb{Q}(\zeta)^+$

$h_{p^r}^+$: the class number of $\mathbb{Q}(\zeta)^+$

Then it is well known that

$$h_{p^r}^+ = [E_{p^r}^+ : C_{p^r}^+].$$

- It is very hard to compute $h_{p^r}^+$ itself.

The value of integer h_p^+ is not still known for $p \geq 71$.

$$\boxed{\text{Question: Which prime divisors appear in } h_{p^r}^+ \text{ ?}}$$

For a prime ℓ, we consider when $h_{p^r}^+$ is divisible by ℓ.

History of challenging the question

- E. E. Kummer (1870) investigated this problem and gave a necessary condition for h_p^+ to be divisible by an odd prime $\neq p$.
- H. W. Leopoldt (1959) gave a generalization of Kummer's result a necessary condition of $\ell | h_K$ for a real abelian field K, where an "abelian field" means $K \subseteq \mathbb{Q}(\zeta_f)$ and h_K is the class number of K. He showed that if $\ell | h_K$ and $\ell \nmid [K : \mathbb{Q}]$, then $\ell | B_{k,\chi}$ for some k and χ, where $B_{k,\chi}$ is a generalized Bernoulli number. However, the converse is not necessarily valid in general.
- S. Jakubec and T. Metsänkylä gave an extension and a simplification of Leopoldt's result.

- The case $\ell = 2$ (The class number parity of $h_{p^r}^+$)

This case is completely determined as follows.

Let $c_i \in \mathbb{F}_2 = \mathbb{Z}/2\mathbb{Z}\,(i \in \mathbb{Z})$ be

$$c_i = \begin{cases} 0 & \text{if } e_i > 0, \\ 1 & \text{if } e_i < 0. \end{cases}$$

Define $f(x)$ and $f^*(x)$ in $\mathbb{F}_2[x]$ as

$$\begin{aligned} f(x) &:= c_0 + c_1 x + \cdots + c_{n-1} x^{n-1}, \\ f^*(x) &:= x^{n-1} f(1/x) = c_0 x^{n-1} + c_1 x^{n-2} + \cdots + c_{n-1}. \end{aligned}$$

Theorem 1 (Bentzen 1989)

$$2 | h_{p^r}^+ \iff \gcd(f(x), f^*(x), x^n + 1) \neq 1.$$

- <u>The case $\ell = p$</u>

There is the famous conjecture.

Kummer-Vandiver conjecture : p never divides $h_{p^r}^+$ for any prime p.

The conjecture has been verified for all $p < 4 \times 10^6$.

<u>Main Theorem</u>

Let p be an odd prime and ℓ ($\neq p$) an odd prime. Let $q_n(x)$ be the characteristic polynomials defined in §3. Then

$$\ell \,|\, h_{p^r}^+ \iff q_n(x) \neq x - 1 \ (\mu_n > 0).$$

Moreover, for the subfield $K_m \subseteq \mathbb{Q}(\zeta)^+$,

$$\ell \,|\, h_{K_m} \iff \mu_m > 0.$$

For an odd prime distinct from p, we put $\mathbb{F}_\ell := \mathbb{Z}/\ell\mathbb{Z}$.

For any integers a and b such that $(p, a) = 1$, we denote by $R(a, b)$ the least positive solution such that $ax \equiv b \pmod{p^r}$.

For $k = 1, 2, \ldots, (\ell - 1)/2$ and for any $j \in \mathbb{Z}$, set

$$\varepsilon_j^{(k)} := \begin{cases} 1 & \text{if either } R(\ell, \ell - 2k) - g_{n-j} \text{ or } R(\ell, \ell - 2k) - g_{2n-j} \\ & \text{is odd and positive,} \\ 0 & \text{otherwise.} \end{cases}$$

We notice that $R(\ell, \ell - 2k) - g_{n-j} + R(\ell, \ell - 2k) - g_{2n-j} = 2R(\ell, \ell - 2k) - p^r$ is odd and so $\varepsilon_j^{(k)}$ is well defined. We put

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

Define $f_n(x)$ and $p_n(x)$ in $\mathbb{F}_\ell[x]$ as

$$f_n(x) := \sum_{j=0}^{n-1} c_j x^j,$$
$$p_n(x) := \gcd(f_n(x), x^n - 1).$$

§2. Polynomial gcd computation method

Let $A := circ(\underbrace{0, 1, 0, \ldots, 0}_{n})$ be the circular matrix, i.e.,

$$A = \begin{pmatrix} 0 & 1 & 0 & \cdots & 0 & 0 \\ 0 & 0 & 1 & \cdots & 0 & 0 \\ \multicolumn{6}{c}{\dotfill} \\ 0 & 0 & 0 & \cdots & 0 & 1 \\ 1 & 0 & 0 & \cdots & 0 & 0 \end{pmatrix}.$$

For $f(x) = \sum_{j=0}^{n-1} a_j x^j \in \mathbb{F}_\ell[x]$, $f(A)$ is also a circular matrix and

$$\begin{aligned} f(A) &= a_0 E + a_1 A + \cdots + a_{n-1} A^{n-1}, \\ &= circ(a_0, a_1, \ldots, a_{n-1}). \end{aligned}$$

Then $f(A)$ is a linear transformation. If A and B are circular, then $A \pm B$ and AB are also circular.

We define

$$\operatorname{Ker} f(A) := \{\boldsymbol{x} \in \mathbb{F}_\ell^n \,;\, f(A)\boldsymbol{x}^t = \boldsymbol{0}\},$$

where $\boldsymbol{x}^t$ is the transpose of $\boldsymbol{x} = (x_0, x_1, \ldots, x_{n-1})$.

<u>Proposition 2</u> For $h(x) \in \mathbb{F}_\ell[x]$

$$\dim \operatorname{Ker} h(A) = \deg \gcd(h(x), x^n - 1).$$

Proposition 2 shows that $\operatorname{Ker} f_n(A) = \operatorname{Ker} p_n(A)$.

Put $R := \mathbb{F}_\ell[x]/(x^n - 1)$ and $\mathbb{F}_\ell^n := \oplus_{i=0}^{n-1} \mathbb{F}_\ell$. Then we define

$$\Phi : R \longrightarrow \mathbb{F}_\ell^n \quad ; \sum_{i=0}^{n-1} a_i x^i \mapsto (a_0, a_1, \ldots, a_{n-1}).$$

Then Φ is an isomorphism as a $\mathbb{F}_\ell$-vector space.

The group action of $G(\mathbb{Q}(\zeta)^+/\mathbb{Q})$ to $\mathbb{F}_\ell^n$

Let $G = G(\mathbb{Q}(\zeta)^+/\mathbb{Q})$ be the Galois group of $\mathbb{Q}(\zeta)^+$ over $\mathbb{Q}$ and σ the generator of G such that $\zeta^\sigma = \zeta^g$.

For $\boldsymbol{a} = (a_0, a_1, \ldots, a_{n-1}) \in \mathbb{F}_\ell^n$ we define

$$\begin{aligned} \boldsymbol{a}^\sigma &= (a_{n-1}, a_0, \ldots, a_{n-2}), \\ \boldsymbol{a}^{\sigma^2} &= (a_{n-2}, a_{n-1}, \ldots, a_{n-3}), \end{aligned}$$

and so on. Then $\mathbb{F}_\ell^n$ is naturally regarded as a ring.

For a G-subspace $\mathcal{L}$, $\Phi^{-1}(\mathcal{L})$ is an ideal of R and so there exists $\alpha \in R$ such that $\Phi^{-1}(\mathcal{L}) = \alpha R$.

For a polynomial $h(x) = \sum_i b_i x^i \in \mathbb{F}_\ell[x]$,

$$\begin{aligned} h^*(x) : &= x^{n-1} h(1/x) = \sum_{i=0}^{n-1} b_i x^{n-1-i}, \\ h^\triangle(x) &= x^{\deg h} h(1/x). \end{aligned}$$

We note that $h^*(x) = x^{n-1-\deg h} h^\triangle(x)$.

Proposition 3 For $h(x) \in \mathbb{F}_\ell[x]$ with $\deg h < n$, put $\mathcal{L} = \operatorname{Ker} h(A)$ and

$$\alpha(x) := \frac{x^n - 1}{\gcd(h^*(x), x^n - 1)}.$$

Then we have $\Phi^{-1}(\mathcal{L}) = \alpha R$.

Proposition 4 Let $\mathcal{L}$ be a non-trivial G-subspace of $\mathbb{F}_\ell^n$. Then, putting $\Phi^{-1}(\mathcal{L}) = \alpha R$ and

$$h(x) := \frac{x^n - 1}{\gcd(\alpha^*(x), x^n - 1)},$$

we have

$$\mathcal{L} = \operatorname{Ker} h(A).$$

Conversely, using this $h(x)$, we have

$$\alpha(x) = \frac{x^n - 1}{\gcd(h^*(x), x^n - 1)}.$$

§3. Characteristic polynomial $q_n(x)$

For $\boldsymbol{y} = (y_0, \ldots, y_{n-1}) \in \mathbb{F}_\ell^n$, we put $\eta(\boldsymbol{y}) = e_0^{y_0} \cdots e_{n-1}^{y_{n-1}}$. Since $\{\boldsymbol{y} \in \mathbb{F}_\ell^n \,;\, \sqrt[\ell]{\eta(\boldsymbol{y})} \in E_{p^r}^+\}$ is a G-subspace of $\mathbb{F}_\ell^n$, Proposition 4 shows that there exists a polynimial $q_n(x) \in \mathbb{F}_\ell^n[x]$ such that

$$\operatorname{Ker} q_n(A) = \{\boldsymbol{y} \in \mathbb{F}_\ell^n \,;\, \sqrt[\ell]{\eta(\boldsymbol{y})} \in E_{p^r}^+\},$$

where $A = circ(0, 1, 0, \ldots, 0)$.

Here, if we choose $q_n(x)$ to be monic, $q_n(x)$ is uniquely determined and satisfies

$$x - 1 \mid q_n(x) \mid p_n(x).$$

This means that $p_n(x)$ is a upper bound of $q_n(x)$. Put $\rho_n := \deg p_n(x) - 1$ and $\mu_n := \deg q_n(x) - 1$.

Main Theorem

Let p be an odd prime and ℓ ($\neq p$) an odd prime. Then

$$\ell \,|\, h_{p^r}^{+} \qquad \Longleftrightarrow \; q_n(x) \neq x-1 \; (\mu_n > 0).$$

Moreover, for $K_m \subseteq \mathbb{Q}(\zeta)^+$,

$$\ell \,|\, h_{K_m} \Longleftrightarrow \mu_m > 0\,.$$

Remarks

f: the conductor of cyclotomic field

- Our method yields nothing in case $f = 2^r$. That is, we don't know any criterion how to find prime divisors of $h_{2^r}^{+}$.

- If f is a composite integer, we can not obtain such a criterion which determines all the prime divisors of h_f^+. Now, in case $f = pq$, we have $[E_f^+ : E_C^+] = h_f^+$. The group E_C^+ of cyclotomic units in this case is given by

$$E_C^+ =< -1, |1-\zeta|^2, \frac{\sin \frac{2\pi a}{f}}{\sin \frac{2\pi}{f}}, \frac{\sin \frac{2\pi b}{p}}{\sin \frac{2\pi}{p}}, \frac{\sin \frac{2\pi c}{q}}{\sin \frac{2\pi}{q}} >,$$

where a, b, c run through the following ranges respectively : $0 < a < f/2$, $(a, f) = 1$, $0 < b < p/2$, $(b, p) = 1$, $0 < c < q/2$, $(c, q) = 1$. Since there are the variety of cyclotomic units, we have many difficulties in making criterion. So we can not get any criteion in this case at present.

G. Cornell and M. Rosen study the ℓ-rank of the real class group of cyclotomic fields and show the following result.

Proposition (G. Cornell and M. Rosen)
Let ℓ be an odd prime. Let p and q be odd primes such that $p, q \equiv 1 \bmod \ell$. If $x^\ell \equiv p \bmod q$ and $y^\ell \equiv q \bmod p$ have solutions in $\mathbb{Z}$, then $\ell \mid h_{pq}^+$.

Using above Proposition, we have the following examples.

$$3 \mid h_{13\cdot 103}^+ \text{ and } 3 \nmid h_{13}^+ \cdot h_{103}^+, \quad 5 \mid h_{11\cdot 241}^+ \text{ and } 5 \nmid h_{11}^+ \cdot h_{241}^+,$$
$$7 \mid h_{127\cdot 449}^+ \text{ and } 7 \nmid h_{127}^+ \cdot h_{449}^+.$$

The characteristic polynomial $q_m(x)$ of subfield

For a divisor m of n, we denote by K_m the subfield of $\mathbb{Q}(\zeta)^+$ of degree m and by h_{K_m} the class number of K_m. So, in particular, we have $K_n = \mathbb{Q}(\zeta)^+$ and $h_{K_n} = h_{p^r}^+$. And we define two polynomials in $\mathbb{F}_\ell[x]$ as follows.

$$\begin{aligned} f_m(x) : &= \sum_{k=0}^{m-1} \Big(\sum_{j=0}^{n/m-1} c_{k+jm} \Big) x^j, \\ p_m(x) : &= \gcd(f_m(x), x^m - 1). \end{aligned}$$

Moreover we put $\rho_m := \deg p_m(x) - 1$.

Now let C_{K_m} be the group of cyclotomic units in K_m, i.e., $C_{K_m} = C_{p^r}^+ \cap E_{K_m} =< \eta_0, \eta_1, \ldots, \eta_{m-1} >$, where $\eta_i = N_{\mathbb{Q}(\zeta)^+/K_m}(e_i) = \prod_j e_{i+mj}$. For $\boldsymbol{y} = (y_0, \ldots, y_{m-1}) \in \mathbb{F}_\ell^m$, put $\eta(\boldsymbol{y}) = \eta_0^{y_0} \cdots \eta_{m-1}^{y_{m-1}}$. Since $\{\boldsymbol{y} \in \mathbb{F}_\ell^m\,;\ \sqrt[\ell]{\eta(\boldsymbol{y})} \in E_{K_m}\}$ is a G-subspace of $\mathbb{F}_\ell^m$, Proposition 4 shows that there exists a polynomial $q_m(x) \in \mathbb{F}_\ell[x]$ such that

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

If we choose $q_m(x)$ to be monic, $q_m(x)$ is uniquely determined and satisfies the condition

$$x - 1 \,|\, q_m(x) \,|\, p_m(x).$$

Put $\rho_m := \deg p_m(x) - 1$ and $\mu_m := \deg q_m(x) - 1$.

It turns out that $q_n(x)$ dominates all the $q_m(x)$.

<u>Proposition 5</u> Let m be divisors of $n = \varphi(p^r)/2$. Then

$$\begin{aligned} p_m(x) &= \gcd(p_n(x), x^m - 1), \\ q_m(x) &= \gcd(q_n(x), x^m - 1). \end{aligned}$$

<u>Theorem 6</u> Let ℓ be an odd prime distinct from p. Let m and m' be the divisors of $n = \varphi(p^r)/2$. If $q_m(x) \neq q_{m'}(x)$ for some m, m' such that $m|m'$, then $\ell \,|\, h_{K_{m'}}/h_{K_m}$.

<u>Theorem 7</u> Put $n_i = \varphi(p^{i+1})/2\,(i \geq 0)$. Then we have $q_{n_i}(x)|q_{n_{i+1}}(x)$ for every $i \geq 0$ and there is an integer $s \in \mathbb{N}$ such that $q_{n_i}(x) = q_{n_s}(x)$ for every $i \geq s$.

§4. Algorithm and example

In this section we illustrate our method which determines the characteristic polynomials $q_n(x)$. Our algorithm consists on two steps: The first step is to calculate the approximate polynomial $\hat{q}_m(x)$ by using $p_n(x)$, where $\hat{q}_m(x)$ is regarded as a upper bound of $q_m(x)$. The second step is to calculate the characteristic polynomial $q_m(x)$ by using $\hat{q}_m(x)$.

Now we find the least divisor m of n such that $\rho_m = \rho_n$. Since $q_n(x) =$

$q_m(x)$, we may determine $q_m(x)$.

First we calculate the approximate polynomial $\hat{q}_m(x)$ of $q_m(x)$ such that $q_m(x) \,|\, \hat{q}_m(x) \,|\, p_m(x)$ by using the following Proposition 8.

Decompose $p_m(x)$ into irreducible factors as

$$p_m(x) = h_1^{r_1} h_2^{r_2} \cdots h_s^{r_s},$$

where $h_1(x) = x - 1$.

Put $h(x) = h_i^{f_i}\,(f_i \leq r_i)$ and

$$\alpha(x) = \frac{x^m - 1}{\gcd(h^*(x), x^m - 1)}.$$

And we put $\Phi(\alpha) = \boldsymbol{c} \in \mathbb{F}_\ell^m$. For seven pairs of (q, b) in Proposition 8, we examine whether $f(b)^{\frac{q-1}{\ell}} \equiv 1 \,(\mathrm{mod}\; q)$ is satisfied. If seven congruence equations are all satisfied, we regard $h(x) = h_i^{f_i}$ as a factor of $\hat{q}_m(x)$.

<u>Proposition 8</u> Let ℓ be an odd prime distinct from p. Let q be an auxiliary prime such that $q \equiv 1(\mathrm{mod}\; p\ell)$. Let $\mathcal{Q}|q$ be a prime ideal of the first degree of $\mathbb{Q}(\zeta_p)$. We choose an integer $b \in \mathbb{Z}$ such that $\zeta_p \equiv b(\mathrm{mod}\; \mathcal{Q})$, $b^p \equiv 1(\mathrm{mod}\; q)$ and $b \not\equiv 1(\mathrm{mod}\; q)$. Then, for $\boldsymbol{c} = (c_0, c_1, \cdots, c_{m-1}) \in \mathbb{F}_\ell^m$, we have

$$\sqrt[\ell]{\eta(\boldsymbol{c})} \in E_{K_m} \implies f(b)^{\frac{q-1}{\ell}} \equiv 1(\mathrm{mod}\, q)$$

for all $b \in \mathbb{Z}$ such that $b^p \equiv 1(\mathrm{mod}\; q)$ and $b \not\equiv 1(\mathrm{mod}\; q)$.

Second we calculate the characteristic polynomial $q_m(x)$ by $\hat{q}_m(x)$ such that $x - 1 \,|\, q_m(x) \,|\, \hat{q}_m(x)$.

We decompose $\hat{q}_m(x)$ into irreducible factors and examine whether each factors truely divides $q_m(x)$ by using the following

Proposition 9 Let ℓ be an odd prime distinct from p. For a divisor m of n, let K_m be the subfield of $\mathbb{Q}(\zeta)^+$ of degree m. For $\xi \in K_m$ satisfying $\mathbb{Q}(\xi) = K_m$, we denote by $g(x)$ the minimal polynomial of ξ over $\mathbb{Q}$. Then we have

$$\sqrt[\ell]{\xi} \in K_m \iff {}^{\exists}h(x) \in \mathbb{Z}[x] \text{ such that } h(x) \mid g(x^\ell) \text{ and } \deg h = m.$$

¿From a computational point of view, our practical technique is proved to be sufficiently effective.

Example

- $p = 631$, $\ell = 11 (n = 315, g = 3)$

Then $\rho_5 = \rho_{315} = 1$ for K_5 and $f_5(x) = -(x-1)(x+2)(x^2-3x-1), p_5(x) = (x-1)(x+2)$. Since $x-1 \mid q_5(x) \mid p_5(x)$, $q_5(x)$ is equal to either $(x-1)(x+2)$ or $x-1$.

Since $e_0 = 1 + \eta_{98}^{(2)}$, where $\eta_i^{(t)}$ is the Gaussian period of t terms, $\eta_0 = N_{\mathbb{Q}(\zeta)^+/K_5}(e_0) = \prod_{i=0}^{62} e_{5i} = -27\eta_0^{(126)} - 23\eta_1^{(126)} - 23\eta_2^{(126)} - 24\eta_3^{(126)} - 25\eta_4^{(126)}$. It suffices to examine whether or not $x+2$ divides $q_5(x) = q_{315}(x)$. Then

$$\alpha(x) = \frac{x^5 - 1}{x + 6} = x^4 + 5x^3 + 3x^2 + 4x + 9.$$

Hence $\boldsymbol{a} = \Phi(\alpha(x)) = (9, 4, 3, 5, 1)$. So, by Gaussian periods, $\eta(\boldsymbol{a}) = \eta_0^9\eta_1^4\eta_2^3\eta_3^5\eta_4$ is represented as

$$\begin{aligned}&1825781034834690\eta_0^{(126)} + 1778816751439277\eta_1^{(126)} + 2077816469455803\eta_2^{(126)}\\&+1729782845381458\eta_3^{(126)} + 1725978229949424\eta_4^{(126)}.\end{aligned}$$

Therefore the minimal polynomial of $\eta(\boldsymbol{a})$ over $\mathbb{Q}$ is

$$\begin{aligned}g(x) = {}&x^5 - 5167802153534793x^4 + 4202294020565334127059 47x^3\\&-270930328704651338120831399706 2x^2 - 5891565028952171549607 1x - 1.\end{aligned}$$

Then we obtain

$$-1-122x-527x^2+266x^3-36x^4+x^5 \mid g(x^{11}),$$

so that $\sqrt[11]{\eta(\boldsymbol{a})} \in E_{K_5}$. This implies that $x+2 \mid q_5(x)$. Therefore we have $q_5(x)=(x-1)(x+2)$. Thus $11 \mid h_{631}^{+}$.

Remark In above example, we get $q_{315}(x)=q_5(x)=(x-1)(x+2)$. So, for every $m \mid 315$,

$$q_m(x)=\begin{cases} (x-1)(x+2) & \text{if } 5 \mid m, \\ x-1 & \text{if } 5 \nmid m. \end{cases}$$

Table 1 $q_n(x)$ for $3 \le \ell \le 11$, $5 \le p < 700$

ℓ	p	ρ	m	$q_m(x)=q_n(x)$
3	229	1	2	$(x-1)(x+1)$
3	257	1	2	$(x-1)(x+1)$
3	401	3	8	$(x-1)(x^2+x-1)$
3	521	4	26	$(x-1)(x^3+x^2-x+1)$
3	641	6	40	$(x-1)(x^2+x-1)$
5	401	4	20	$(x-1)(x+1)$
5	457	2	4	$(x-1)(x-2)$
5	641	1	4	$(x-1)(x-2)$
7	313	2	3	$(x-1)(x-2)$
7	577	4	6	$(x-1)(x+1)$
11	191	1	5	$(x-1)(x-5)$
11	631	1	5	$(x-1)(x+2)$
11	641	4	40	$(x-1)(x-4)$

Table 2 Odd prime divisors $< 10^4$ of h_p^+ ($p < 1600$)

p	divisors	p	divisors	p	divisors
191	11	761	3	1129	3, 7
229	3	821	11	1153	19
257	3	829	47	1229	3
313	7	857	5	1231	211
401	3, 5	877	7	1297	5, 11
457	5	953	71	1373	3
521	3	977	5	1381	7
577	7	1009	7	1429	5
631	11	1063	13	1459	13, 19
641	3, 5, 11	1069	7	1489	3, 19
733	3	1093	5	1567	7

For other prime $p < 1600$, h_p^+ has no odd prime divisors $< 10^4$.

References

[1] S. Bentzen, Duality of cyclotomic units and the 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] G. Gras, Critère de parité du nombre de classes des extensions abéliennes réelles de **Q** de degré impair, Bull. Soc. Math. France, **103** (1975), 177−190

[4] 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

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

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

[7] J. Masley, Class numbers of real cyclic number fields with small conductor, Compositio Math., **37** (1978), 297−319

[8] R. Schoof, Class numbers of real cyclotomic fields of prime conductor, Preprint

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

[10] 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

[11] 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