On prime factors of class number of cyclotomic fields

Roland Quême

2006 jan 09

Contents

1 Some definitions .................................................. 2

2 On Kummer and Stickelberger relation ......................... 3

3 Polynomial congruences mod $p$ connected to the $p$-class group $C_p$ ........................................... 6
   3.1 Stickelberger relation for prime ideals $q$ of inertial degree $f = 1$ .................. 6
   3.2 Stickelberger relation for prime ideals $q$ of inertial degree $f > 1$ .................. 7
   3.3 Polynomial congruences mod $p^2$ connected to the $p^2$-class group $C_{p^2}$ ..... 9

4 On prime factors $h \neq p$ of the class number of the $p$-cyclotomic field .................. 11
   4.1 The general case ............................................. 12
   4.2 The case of complex quadratic fields contained in $K$ .................................... 15
   4.3 The case of biquadratic fields contained in $K$ ........................................... 17

5 A numerical MAPLE algorithm .................................. 18

Abstract

Let $p$ be an odd prime. Let $K = \mathbb{Q}(\zeta)$ be the $p$-cyclotomic number field. Let $v$ be a primitive root mod $p$ and $\sigma : \zeta \to \zeta^n$ be a $\mathbb{Q}$-isomorphism of the extension $K/\mathbb{Q}$ generating the Galois group $G$ of $K/\mathbb{Q}$. Following the conventions of Ribenboim in [8], for $n \in \mathbb{Z}$, the notation $v_n$ is understood by $v_n = v^n$ mod $p$ with $1 \leq v_n \leq p - 1$. Let $P(X) = \sum_{i=0}^{p-2} X^i v_{n-i} \in \mathbb{Z}[X]$ be the Stickelberger polynomial. $P(\sigma)$ annihilates the class group $C$ of $K$. There exists a polynomial $Q(X) \in \mathbb{Z}[G]$ such that $P(\sigma) \times (\sigma - v) = p \times Q(\sigma)$ and such that $Q(\sigma)$ annihilates the $p$-class group $C_p$ of $K$. 

1
These result allow:

1. to describe the structure of the relative class group $C^-$,
2. to give some explicit congruences in $\mathbb{Z}[v] \mod p$ for the $p$-class group of $K$ (the subgroup of exponent $p$ of $C$),
3. to give some explicit congruences in $\mathbb{Z}[v] \mod h$ for the $h$-class group of $K$ for the prime divisors $h \neq p$ of the class number $h(K)$.
4. We detail at the end the case of class number of quadratic and biquadratic fields contained in the cyclotomic field $K$.
5. As application, we give a MAPLE algorithm which describes the structure of the relative class group $C^-$ of the cyclotomic field $K$ for all the prime numbers $p < 500$.

This article is at elementary level.

Remark: we have not found in the literature some formulations corresponding to theorems 3.2 p. 7, 4.1 p. 12, 4.3 p. 13, 4.6 p. 16, 4.7 p. 17 and 4.8 p. 18 and to MAPLE algorithm described in section 5 p. 18.

1 Some definitions

In this section we give some definitions and notations on cyclotomic fields and $p$-class group used in this paper.

1. Let $p$ be an odd prime. Let $\mathbb{F}_p$ be the finite field of cardinal $p$ and $\mathbb{F}_p^*$ its multiplicative group. Let $\zeta$ be a root of the polynomial equation $X^{p-1} + X^{p-2} + \cdots + X + 1 = 0$. Let $K$ be the $p$-cyclotomic field $K = \mathbb{Q}(\zeta)$ and $O_K$ its ring of integers. Let $K^+$ be the maximal totally real subfield of $K$. Let $v$ be a primitive root $\mod p$. In this paper, following Ribenboim conventions in Ribenboim [8] for any $n \in \mathbb{Z}$, we note $v_n = v^n \mod p$ with $1 \leq v_n \leq p - 1$. Let $G$ be the Galois group of the extension $K/\mathbb{Q}$. Let $\sigma : \zeta \rightarrow \zeta^v$ be a $\mathbb{Q}$-isomorphism of the extension $K/\mathbb{Q}$ generating $G$. Let $\lambda = \zeta - 1$. The prime ideal of $K$ lying over $p$ is $\pi = \lambda O_K$.

2. Let $C$ be the class group of $K$. Let $C_p$ be the $p$-class of $K$ (the subgroup of exponent $p$ of $C$). Let $C_p^+$ be the $p$-class group of $K^+$. Then $C_p = C_p^+ \oplus C_p^-$ where $C_p^-$ is called the relative $p$-class group. Let $r^-$ be the rank of $C_p^-$. Then $C_p^-$ is the direct sum of $r^-$ subgroups $\Gamma_k$ of order $p$ annihilated by $\sigma - \mu_k \in \mathbb{F}_p[G]$ with $\mu_k \in \mathbb{F}_p^*$, $\mu_k = v_{2m_k + 1}$ where $m_k$ is a natural integer $m_k$, $1 \leq m_k \leq \frac{p - 3}{2}$.

$$C_p^- = \bigoplus_{k=1}^{r^-} \Gamma_k.$$
2 On Kummer and Stickelberger relation

Stickelberger relation was already known by Kummer under the form of Jacobi resolvents for the cyclotomic field $K$, see for instance Ribenboim [8] (2.6) p. 119. In this section we derive some elementary properties from Stickelberger relation.

1. Let $q \neq p$ be an odd prime. Let $\zeta_q$ be a root of the minimal polynomial equation $X^{q-1} + X^{q-2} + \cdots + X + 1 = 0$. Let $K_q = \mathbb{Q}(\zeta_q)$ be the $q$-cyclotomic field. Let $K_{pq} = \mathbb{Q}(\zeta_p, \zeta_q)$. Then $K_{pq}$ is the compositum $KK_q$. The ring of integers of $K_{pq}$ is $\mathcal{O}_{K_{pq}}$.

2. Let $q$ be a prime ideal of $\mathcal{O}_K$ lying over the prime $q$. Let $f$ be the order of $q \mod p$ and $m = N_{K_p/Q}(q) = q^f$. If $\psi(\alpha) = a$ is the image of $\alpha \in \mathcal{O}_K$ under the natural map $\psi: \mathcal{O}_K \to \mathcal{O}_K/q$, then for $\psi(\alpha) = a \neq 0$ define a character $\chi_{q}^{(p)}$ on $F_m = \mathcal{O}_K/q$ by

$$
\chi_{q}^{(p)}(a) = \{\alpha/q\}^{-1}_p = \{\alpha/q\}_p,
$$

where $\{\alpha/q\} = \zeta^c$ for some natural integer $c$, is the $p^{th}$ power residue character mod $q$. We define the Gauss sum

$$
g(q) = \sum_{x \in F_m} (\chi_{q}^{(p)}(x) \times \zeta_q^{Tr_{F_m/F_q}(x)}) \in \mathcal{O}_{K_{pq}}.
$$

It follows that $g(q) \in \mathcal{O}_{K_{pq}}$. Moreover $g(q)^p \in O_K$, see for instance Mollin [6] prop. 5.88 (c) p. 308.

3. The Stickelberger relation is classically:

$$
g(q)^p O_K = q^S,
$$

with $S = \sum_{t=1}^{p-1} t \times \varpi_t^{-1}$, where $\varpi_t \in Gal(K/Q)$ is given by $\varpi_t : \zeta \to \zeta^t$ (see for instance Mollin [6] thm. 5.109 p. 315).

The four following lemmas are derived in an elementary way from the Stickelberger relation.

**Lemma 2.1.** If $q \not\equiv 1 \mod p$ then the Gauss sum $g(q) \in \mathbb{Z}[\zeta]$.

*Proof.*

1. Let $u$ be a primitive root mod $q$. Let $\tau : \zeta_q \to \zeta_q^u$ be a $\mathbb{Q}$-isomorphism generating $Gal(K_q/Q)$. The $\mathbb{Q}$-isomorphism $\tau$ is extended to a $K_p$-isomorphism of $K_{pq}$ by $\tau : \zeta_q \to \zeta_q^u$, $\zeta_p \to \zeta_p$. Then $g(q)^p \in \mathbb{Z}[\zeta]$ and so

$$
\tau(g(q))^p = g(q)^p.
$$
and it follows that there exists a natural integer $\rho$ with $\rho < p$ such that

$$\tau(g(q)) = \zeta_\rho^p \times g(q).$$

Then $N_{K_p/K}(\tau(g(q))) = \zeta^{(q-1)\rho} \times N_{K_p/K}(g(q))$ and so $\zeta^{(q-1)\rho} = 1$.

2. If $q \not\equiv 1 \mod p$, it implies that $\zeta^\rho = 1$ and so that $\tau(g(q)) = g(q)$ and thus that $g(q) \in \mathcal{O}_K$.

\[\square\]

**Lemma 2.2.** Let $S = \sum_{t=1}^{p-1} \tau_t^{-1} \times t$ where $\tau_t$ is the $\mathbb{Q}$-isomorphism of the extension $K/\mathbb{Q}$ given by $\tau_t : \zeta \rightarrow \zeta^t$ of $K$. Let $P(\sigma) = \sum_{i=0}^{p-2} \sigma^i \times v_{-i} \in \mathbb{Z}[G]$. Then $S = P(\sigma)$.

**Proof.** Let us consider one term $\tau_t^{-1} \times t$. Then $v_{-1} = v_{p-2}$ is a primitive root mod $p$ and so there exists one and one $i$ such that $t = v_{-i}$. Then $\tau_{v_{-i}} : \zeta \rightarrow \zeta^{v_{-i}}$ and so $\tau_{v_{-i}}^{-1} : \zeta \rightarrow \zeta^{v_i}$ and so $\tau_{v_{-i}}^{-1} = \sigma^i$ (observe that $\sigma^{p-1} \times v_{-(p-1)} = 1$), which achieves the proof. \[\square\]

**Lemma 2.3.**

(5) \[P(\sigma) = \sum_{i=0}^{p-2} \sigma^i \times v_{-i} = v_{-(p-2)} \times \left\{ \prod_{k=0}^{p-2} (\sigma - v_k) \right\} + p \times R(\sigma),\]

where $R(\sigma) \in \mathbb{Z}[G]$ with $\deg(R(\sigma)) < p - 2$.

**Proof.** Let us consider the polynomial $R_0(\sigma) = P(\sigma) - v_{-(p-2)} \times \left\{ \prod_{k=0}^{p-2} (\sigma - v_k) \right\}$ in $\mathbb{F}_p[G]$. Then $R_0(\sigma)$ is of degree smaller than $p - 2$ and the two polynomials $\sum_{i=0}^{p-2} \sigma^i v_{-i}$ and $\prod_{k=0}^{p-2} (\sigma - v_k)$ take a null value in $\mathbb{F}_p[G]$ when $\sigma$ takes the $p - 2$ different values $\sigma = v_k$ for $k = 0, \ldots, p-2, \ k \neq 1$. Then $R_0(\sigma) = 0$ in $\mathbb{F}_p[G]$ which leads to the result in $\mathbb{Z}[G]$. \[\square\]

**Lemma 2.4.**

(6) \[P(\sigma) \times (\sigma - v) = p \times Q(\sigma),\]
where $Q(\sigma) = \sum_{i=1}^{p-2} \delta_i \times \sigma^i \in \mathbb{Z}[G]$ is given by

\[
\begin{align*}
\delta_{p-2} &= \frac{v-(p-3) - v-(p-2)v}{p}, \\
\delta_{p-3} &= \frac{v-(p-4) - v-(p-3)v}{p}, \\
& \vdots \\
\delta_i &= \frac{v-(i-1) - v-iv}{p}, \\
& \vdots \\
\delta_1 &= \frac{1 - v-1v}{p},
\end{align*}
\]

with $-p < \delta_i \leq 0$.

Proof. We start of the relation in $\mathbb{Z}[G]$

\[
P(\sigma) \times (\sigma - v) = v-(p-2) \times p \times R(\sigma) \times (\sigma - v) = p \times Q(\sigma),
\]

with $Q(\sigma) \in \mathbb{Z}[G]$ because $\prod_{k=0}^{p-2}(\sigma - v_k) = 0$ in $\mathbb{F}_p[G]$ and so $\prod_{k=0}^{p-2}(\sigma - v_k) = p \times R_1(\sigma)$ in $\mathbb{Z}[G]$. Then we identify in $\mathbb{Z}[G]$ the coefficients in the relation

\[
(v-(p-2)\sigma^{p-2} + v-(p-3)\sigma^{p-3} + \cdots + v-1\sigma + 1) \times (\sigma - v) = \\
p \times (\delta_{p-2}\sigma^{p-2} + \delta_{p-3}\sigma^{p-3} + \cdots + \delta_1\sigma + \delta_0),
\]

where $\sigma^{p-1} = 1$.

Remarks:

1. Observe that we have more generally for the indeterminate $X$ the algebraic identity in $\mathbb{Z}[X]$

\[
P(X)(X - v) = p \times Q(X) + v(X^{p-1} - 1).
\]

2. Observe that, with our notations, $\delta_i \in \mathbb{Z}, \ i = 1, \ldots, p-2$, but generally $\delta_i \not\equiv 0 \mod p$.

3. We see also that $-p < \delta_i \leq 0$. Observe also that $\delta_0 = \frac{v-(p-2)-v}{p} = 0$. 

\[\textcircled{5}\]
3 Polynomial congruences mod $p$ connected to the $p$-class group $C_p$

We give some explicit polynomial congruences in $\mathbb{Z}[v] \mod p$ connected to the relative $p$-class group $C_p^\sigma$ of $O_K$. We apply successively the Stickelberger relation to prime ideals $q$ of inertial degree $f = 1$ and of inertial degree $f > 1$. We recall that $r^-$ is the $p$-rank of the relative $p$-class group $C_p^\sigma$ of $K$.

3.1 Stickelberger relation for prime ideals $q$ of inertial degree $f = 1$

Theorem 3.1. $\prod_{k=1}^{r^-}(\sigma - v_{2m_k+1})$ divides $Q(\sigma)$ in $\mathbb{F}_p[G]$ and

\[ Q(v_{2m_k+1}) = \sum_{i=1}^{p-2} v_{(2m_k+1)\times i} \times \left( \frac{v_{-(i-1)} - v_{-i} \times v}{p} \right) \equiv 0 \mod p, \]

where $m_k$ is defined in relation (1) p. 2.

Proof. From Kummer, the group of ideal classes of $K$ is generated by the classes of prime ideals of degree 1 (see for instance Ribenboim [8] (3A) p. 119). Let $q$ a prime ideal of inertial degree 1 whose class Cl$(q) \in C_p^\sigma$ is annihilated by $\sigma - \mu_k$ with $\mu_k = v_{2m_k+1}$. We start of $g(q)^pO_K = q^{P(\sigma)}$ and so $g(q)^{p(\sigma-v)}O_K = q^{P(\sigma)(\sigma-v)} = q^{pQ(\sigma)}$ and thus $g(q)^{(\sigma-v)}O_K = q^{Q(\sigma)}$. It can be shown that $g(q)^{(\sigma-v)} \in K$, see for instance Ribenboim [9] F. p. 440. Therefore $Q(\sigma)$ annihilates the ideal class Cl$(q)$ and the congruence follows. \qed

Remarks:

1. Observe that $\delta_i$ can also be written in the form $\delta_i = -[\frac{v_{-i} \times x}{p}]$ where $[x]$ is the integer part of $x$, similar form also known in the literature.

2. Observe that it is possible to get other polynomials of $\mathbb{Z}[G]$ annihilating the relative $p$-class group $C_p^\sigma$: for instance from Kummer’s formula on Jacobi cyclotomic functions we induce other polynomials $Q_d(\sigma)$ annihilating the relative $p$-class group $C_p^\sigma$ of $K$: If $1 \leq d \leq p - 2$ define the set

\[ I_d = \{ i \mid 0 \leq i \leq p - 2, \ v_{(p-1)/2-i} + v_{(p-1)/2-i+\text{ind}_v(d)} > p \} \]

where the index $\text{ind}_v(d)$ is the minimal integer $s$ such that $d = v_s$. Then the polynomials $Q_d(\sigma) = \sum_{i \in I_d} \sigma^i$ for $d = 1, \ldots, p - 2$ annihilate the $p$-class $C_p$ of $K$, see for instance Ribenboim [8] relations (2.4) and (2.5) p. 119.
3. See also in a more general context Washington, [11] corollary 10.15 p. 198.

4. It is easy to verify the consistency of relation (9) with the table of irregular primes and Bernoulli numbers in Washington, [11] p. 410.

5. See section 5 p. 18 with an algorithm improving this result.

3.2 Stickelberger relation for prime ideals \( q \) of inertial degree \( f > 1 \)

Let \( q \) be a prime ideal of \( O_K \) with \( Cl(q) \in C_p \). In this section we apply Stickelberger relation to the prime ideals \( q \) of inertial degree \( f > 1 \) with the method used for the prime ideals of inertial degree 1 in section 3 p. 6. Observe, from lemma 2.1 p. 3 that \( f > 1 \) implies that \( g(q) \in O_K \), property used in this section (by opposite \( g(q) \not\in K \) when \( f = 1 \)).

**A definition:** we say that the prime ideal \( c \) of a number field \( M \) is \( p \)-principal if the component of the class group \( \langle Cl(c) \rangle \) in \( p \)-class group \( D_p \) of \( M \) is trivial.

**Theorem 3.2.** Let \( q \) be an odd prime with \( q \not= p \). Let \( f \) be the order of \( q \) mod \( p \) and \( m = \frac{p - 1}{f} \). Let \( q \) be a prime ideal of \( O_K \) lying over \( q \) with \( Cl(q) \in C_p^- \). If \( f > 1 \) then

1. \( g(q) \in O_K \) and \( g(q)O_K = q^{P_1(\sigma)} \) where

\[
(10) \quad P_1(\sigma) = \sum_{i=0}^{m-1} \left( \sum_{j=0}^{f-1} v_{-(i+jm)} \right) / p \times \sigma^i \in \mathbb{Z}[G].
\]

2. There exists a natural integer \( n \) with \( 1 \leq n \leq p - 2 \) such that \( \sigma - v_n \) divides \( P_1(\sigma) \) in \( \mathbb{F}_p[G] \) and \( \sigma - v_n \) annihilates \( Cl(q) \).

**Proof.**

1. \( N_{K/Q}(q) = q^f \) and \( q = q^{a^m} = \cdots = q^{(f-1)^m} \). From Stickelberger relation \( g(q)^{P(\sigma)} = q^{P(\sigma)} \) where \( P(\sigma) = \sum_{i=0}^{m-1} \sum_{j=0}^{f-1} \sigma^i v_{-(i+jm)} \). Observe that, from hypothesis, \( q = q^{a^m} = \cdots = q^{(f-1)^m} \) so Stickelberger’s relation implies that \( g(q)^{P(\sigma)} = q^{P(\sigma)} \) with

\[
P(\sigma) = \sum_{i=0}^{m-1} \sum_{j=0}^{f-1} \sigma^i v_{-(i+jm)} = p \times \sum_{i=0}^{m-1} \left( \sum_{j=0}^{f-1} v_{-(i+jm)} / p \right) \times \sigma^i,
\]

where \( (\sum_{j=0}^{f-1} v_{-(i+jm)}) / p \in \mathbb{Z} \) because \( v_m - 1 \not\equiv 0 \) mod \( p \).
2. Let $P_1(\sigma) = \frac{P(\sigma)}{p}$. Then from below $P_1(\sigma) \in \mathbb{Z}[G]$. From lemma 2.1 we know that $g(q) \in O_K$. Therefore

$$g(q)^p O_K = q^{P_1(\sigma)}, \quad g(q) \in O_K,$$

and so

$$g(q) O_K = q^{P_1(\sigma)}, \quad g(q) \in O_K.$$

Then $P_1(\sigma)$ annihilates $Cl(q)$ and thus there exists $1 < n \leq p - 2$ such that $(\sigma - v_n) | P_1(\sigma)$.

Remarks

1. For $f = 2$ the value of polynomial $P_1(\sigma)$ obtained from this lemma is $P_1(\sigma) = \sum_{i=1}^{(p-3)/2} \sigma^i$.

2. Let $q$ be a prime not principal ideal of inertial degree $f > 1$ with $Cl(q) \in C_p$. The two polynomials of $\mathbb{Z}[G]$, $Q(\sigma) = \sum_{i=0}^{p-2} \left(\frac{v-(i-1)-v-i}{p}\right) \times \sigma^i$ (see thm 3.1) and $P_1(\sigma) = \sum_{i=0}^{m-1} \left(\frac{f-1}{p} v-(i+jm)\right) \times \sigma^i$ (see lemma 3.2) annihilate the ideal class $Cl(q)$. When $f > 1$ the lemma 3.2 supplement the theorem 3.1.

3. This result explains that, when $f$ increases, the proportion of $p$-principal ideals $q$ increases.

It is possible to derive some explicit congruences in $\mathbb{Z}$ from this theorem.

**Corollary 3.3.** Let $q$ be an odd prime with $q \neq p$. Let $f$ be the order of $q$ mod $p$ and let $m = \frac{p-1}{f}$. Let $q$ be an prime ideal of $O_K$ lying over $q$. Suppose that $f > 1$.

1. If the ideal $q$ is non $p$-principal there exists a natural integer $l$, $1 \leq l < m$ such that

   $$(11) \quad \sum_{i=0}^{m-1} \left(\frac{\sum_{j=0}^{f-1} v-(i+jm)}{p}\right) \times v^l f_i \equiv 0 \mod p,$$

2. If for all natural integers $l$ such that $1 \leq l < m$

   $$(12) \quad \sum_{i=0}^{m-1} \left(\frac{\sum_{j=0}^{f-1} v-(i+jm)}{p}\right) \times v^l f_i \not\equiv 0 \mod p,$$

then $q$ is $p$-principal

**Proof.**
1. Suppose that \( q \) is not \( p \)-principal. Observe at first that congruence (11) with \( l = m \) should imply that 
\[
\sum_{i=0}^{m-1} \frac{\sum_{j=0}^{f-1} v_{-(i+jm)}}{p} \equiv 0 \pmod{p^2},
\]
which is not possible because \( v_{-(i+jm)} = v_{-(i'+j'm)} \) implies that \( j = j' \) and \( i = i' \) and so that 
\[
\sum_{i=0}^{m-1} \sum_{j=0}^{f-1} v_{-(i+jm)} \equiv 0 \pmod{p^2},
\]
which is not possible because \( v_{-(i+jm)} = v_{-(i'+j'm)} \) implies that \( j = j' \) and \( i = i' \) and so that 
\[
\sum_{i=0}^{m-1} \sum_{j=0}^{f-1} v_{-(i+jm)} = \frac{p(p-1)}{2}.
\]

2. The polynomial \( P_1(\sigma) \) of lemma 3.2 annihilates the non \( p \)-principal ideal \( q \) in \( \mathbf{F}_p[G] \) only if there exists \( \sigma - v_n \) dividing \( P_1(\sigma) \) in \( \mathbf{F}_p[G] \). From \( q^{p^{-m}-1} = 1 \) it follows also that \( \sigma - v_n \mid \sigma^m - 1 \). But \( \sigma - v_n \mid \sigma^m - v_{nm} \) and so \( \sigma - v_n \mid v_{nm} - 1 \), thus \( nm \equiv 0 \pmod{p-1} \), so \( n \equiv 0 \pmod{f} \) and \( n = lf \) for some \( l \). Therefore if \( q \) is non \( p \)-principal there exists a natural integer \( l, 1 \leq l < m \) such that 
\[
\sum_{i=0}^{m-1} \frac{\sum_{j=0}^{f-1} v_{-(i+jm)}}{p} \times v^{lf}i \equiv 0 \pmod{p},
\]

3. The relation (12) is an immediate consequence of previous part of the proof.

3.3 Polynomial congruences \( \pmod{p^2} \) connected to the \( p^2 \)-class group \( C_{p^2} \)

Let \( C_{p^2}^- \) be the subgroup of exponent \( p^2 \) (so with elements of order dividing \( p^2 \)) of the relative class group \( C^- \) of \( K \).

1. We have seen in relation (11) p. 2 that the relative \( p \)-class group \( C_p^- \) can be seen as a direct sum \( C_p^- = \bigoplus_{i=1}^{r} \Gamma_i \) where \( \Gamma_i \) is a cyclic subgroup of \( C_p^- \) annihilated by \( \sigma - \mu_i \) with \( 2 \leq \mu_i \leq p-2 \).

2. \( C_{p^2}^- \) can be seen as a direct sum 
\[
C_{p^2}^- = \bigoplus_{i=1}^{r} \Delta_i,
\]
where \( \Delta_i \) is a cyclic group with \( \Gamma_i \subset \Delta_i \) and whose order divides \( p^2 \).

3. Suppose that \( \Delta_i \) is of order \( p^2 \). Show that \( \Delta_i \) is annihilated by \( \sigma - (\mu_i + a_ip) \) with \( a_i \) natural integer \( 1 \leq a_i \leq p-1 \):

(a) From Kummer, there exist some prime ideals \( Q_i \) of \( \mathcal{O}_K \) with \( Cl(Q_i) \in \Delta_i \), \( Cl(Q_i^p) \in \Gamma_i \) and \( < Q_i^{p(\sigma-\mu_i)} > \) principal as seen in previous sections. Therefore \( < Q_i^{\sigma-\mu_i} > \) is of order \( p \).
Proof.

(a) \( Cl(Q_i^{\mu}) \in \Delta_i \). In the other hand \( Cl(Q_i^\sigma) \in \Delta_i \); if not \( Cl(Q_i^\sigma) \) should have at least one component \( c_j \in \Delta_j, j \neq i \) and so \( Cl(Q_i^{\mu+\sigma}) \) should have a component \( c_j^p \in \Delta_j^p = \Gamma_j, j \neq i \), contradiction. Therefore \( Cl(Q_i^{\sigma-\mu}) \in \Delta_i \).

Then, from \( Q_i^{\rho(\sigma-\mu_i)} \) principal, it follows that \( Cl(Q_i^{\sigma-\mu_i}) \in \Gamma_i \) because \( \Delta_i \) is cyclic of order \( p^2 \).

(b) Thus there exists \( a_i, 1 \leq a_i \leq p - 1 \), such that \( Cl(Q_i^{\sigma-\mu_i}) = Cl(Q_i^{\sigma-\mu}) \) and so \( Q_i^{\sigma-\mu_i-a_i} \) is principal.

In this section we examine the case of subgroups \( \Delta_i \) of order \( p^2 \). Let us note \( \Delta \) for one of this groups annihilated by \( \sigma - (\mu + ap), a \neq 0 \).

**Theorem 3.4.** \( \mu \) verifies the two congruences

\[
\sum_{i=0}^{p-2} \mu^i \delta_i \equiv 0 \mod p \text{ with } \delta_i = \frac{v_{-(i-1)} - v_{-i}v}{p},
\]

(15)

\[
\sum_{i=0}^{p-2} \mu^{p-2+i} \delta_i + (\mu^{p-1} - 1) \sum_{i=1}^{p-2} i \mu^{i-1} \delta_i \equiv 0 \mod p^2.
\]

**Proof.**

1. There exists prime ideals \( Q \) of \( O_K \) with \( Cl(Q) \in \Delta \), hence \( Q^{\sigma^2} \) principal and \( Q^p \) not principal. From Stickelberger relation \( g(Q)^pO_K = Q^{P(\sigma)} \) where \( P(\sigma) \) has been defined in lemma [2.2] p. [4]. Then \( g(Q)^p(\sigma-v)O_K = Q^{P(\sigma)(\sigma-v)} \), hence from lemma [2.4] p. [4] we get \( g(Q)^p(\sigma-v)O_K = Q^{P(\sigma)} \), hence \( g(Q)^{\sigma-v}O_K = Q^{Q(\sigma)} \). We know, for instance from Ribenboim [9] F. p. 440 that \( g(Q)^{\sigma-v} \in K \) so \( Q^{Q(\sigma)} \) is principal. But \( Q^{\sigma-\mu+ap} \) is principal hence \( Q^{Q^{2(\mu+ap)}} \) is principal, and thus

(16) \( Q(\mu + ap) \equiv 0 \mod p^2 \).

2. From lemma [2.4] p. [4] \( Q(\sigma) = \sum_{i=0}^{p-2} \sigma^i \delta_i \) where \( \delta_i = \frac{v_{-(i-1)} - v_{-i}v}{p} \). From relation (16)

\[
\sum_{i=0}^{p-2} (\mu + ap)^i \delta_i \equiv 0 \mod p^2,
\]

hence

\[
\sum_{i=0}^{p-2} \mu^i \delta_i + ap \sum_{i=1}^{p-1} i \mu^{i-1} \delta_i \equiv 0 \mod p^2.
\]

From theorem [3.1] p. [6] applied to the ideal \( Q^p \in \Gamma \) of order \( p \),

\[
\sum_{i=0}^{p-2} \mu^i \delta_i \equiv 0 \mod p.
\]
$\mathbb{Q}^{p-1-1}$ is principal, therefore $\mathbb{Q}^{(\mu+ap)^{p-1}-1}$ is principal and so $(\mu+ap)^{p-1}-1 \equiv 0 \mod p^2$, hence $\mu^{p-1} + (p-1)\mu^{p-2}ap - 1 \equiv 0 \mod p^2$, hence $\mu^{p-1} - 1 - \mu^{p-2}ap \equiv 0 \mod p^2$, hence $a \equiv \frac{\mu^{p-1}-1}{\mu^{p-2}p} \mod p$, and so

$$\sum_{i=0}^{p-2} \mu^i \delta_i + \frac{\mu^{p-1}-1}{\mu^{p-2}} \sum_{i=1}^{p-1} i\mu^{i-1} \delta_i \equiv 0 \mod p^2$$

and finally

$$(17) \quad \sum_{i=0}^{p-2} \mu^{p-2+i} \delta_i + (\mu^{p-1} - 1) \sum_{i=1}^{p-2} i\mu^{i-1} \delta_i \equiv 0 \mod p^2,$$

which achieves the proof.

\[Q.E.D.\]

**Example:**

1. This congruence mod $p^2$ is valid for no irregular prime numbers $p < 4001$ with rank $r$ of $C_p$ verifying $r > 1$ (verified with a MAPLE program). Therefore the class group of $K$ has no cyclic subgroups of order $p^2$ for the primes $p = 157, 353, 379, 467, 491, 547, 587, 617, 647, 673, 691, 809, 929, 1151, 1217, 1291, 1297, 1307, 1663, 1669, 1733, 1789, 1847, 1933, 1997, 2003, 2087, 2273, 2309, 2371, 2383, 2423, 2441, 2591, 2671, 2789, 2909, 2939, 2957, 3391, 3407, 3511, 3517, 3533, 3539, 3559, 3593, 3617, 3637, 3833, 3851, 3881.

2. (see table of irregular prime in Washington [11] p. 410). Our result is consistent for the primes $p = 157, 353, 467, 491$ with Schoof [10] table 4.2 p. 1239 describing structure of class groups of some $p$-cyclotomic fields.

**4 On prime factors $h \neq p$ of the class number of the $p$-cyclotomic field**

In previous sections we considered the relative $p$-class group $C_p^-$ of $K$. By opposite, in this section we apply Stickelberger relation to all the primes $h \neq p$ dividing the class number $h(K)$. A first subsection is devoted to the general case of the relative class group $C^-$ of $K$, a second to the class group of the quadratic subfield of $K$ and a third subsection to the class group to the biquadratic subfield of $K$ when $p \equiv 1 \mod 4$. 

11
4.1  The general case

1. The class group \( C \) of \( K \) is the direct sum of the class group \( C^+ \) of the maximal totally real subfield \( K^+ \) of \( K \) and of the relative class group \( C^- \) of \( K \).

2. Remind that \( v \) is a primitive root mod \( p \) and that \( v_n \) is to be understood as \( v^m \mod p \) with \( 1 \leq v_n \leq p - 1 \). Let \( h(K) \) be the class number of \( K \). Let \( h \neq p \) be an odd prime dividing \( h(K_p) \), with \( v_h(h(K)) = \beta \). Let \( d = \text{Gcd}(h - 1, p - 1) \). Let \( C(h) \) be the \( h \)-Sylow subgroup of the class group of \( K \) of order \( h^\beta \). Then \( C(h) = \bigoplus_{j=1}^\rho C_j(h) \) where \( \rho \) is the \( h \)-rank of the abelian group \( C(h) \) of order \( h^\beta \) and \( C_j(h) \) are cyclic groups of order \( h^{\beta_j} \) where \( \beta = \sum_{i=1}^\rho \beta_j \).

3. From Kummer (see for instance Ribenboim [8] (3A) p. 119), the prime ideals of \( O_K \) of inertial degree 1 generate the ideal class group. Therefore there exist in the subgroup \( C_h \) of exponent \( h \) of \( C(h) \) some prime ideals \( q \) of inertial degree 1 such that \( \text{Cl}(q) \in \bigoplus_{j=1}^\rho c_j \) where \( c_j \) is a cyclic group of order \( h \) and \( \text{Cl}(q) \notin \bigoplus_{j \in J} c_j \) where \( J \) is a strict subset of \( \{1, 2, \ldots, \rho\} \).

4. Let \( P(\sigma) = \sum_{k=0}^{\rho-2} \sigma^kv_{-k} \) be the Stickelberger polynomial. From lemma 2.2 p. 4 Stickelberger relation is \( q^{P(\sigma)} = g(q)^pO_K \) where \( g(q)^p \in O_K \). Therefore \( q^{P(\sigma)} \) is principal, a fortiori is \( C(h) \)-principal (or \( \text{Cl}(q)^{P(\sigma)} \) has a trivial component in \( C(h) \)). There exists a minimal polynomial \( V(X) \in \mathbb{F}_h(X) \) of degree \( \delta \leq \rho \) such that \( q^{V(\sigma)} \) is \( C(h) \)-principal, if not the remainder of the division of \( P(X) \) by \( V(X) \) of degree smaller than \( \delta \) would annihilate also \( q \). Therefore the irreducible polynomial \( V(X) \) divides \( P(X) \) in \( \mathbb{F}_h[X] \) for the indeterminate \( X \).

5. If \( \text{Cl}(q) \in C^- \) then \( q^{\sigma^{(p-1)/2}+1} \) is principal.

6. Let \( D(X) \in \mathbb{F}_h(X) \) defined by \( D(X) = \text{Gcd}(P(X), X^{(p-1)/2} + 1) \mod h \).

We obtain the following:

**Theorem 4.1.** Suppose that the prime \( h \neq p \) divides the class number \( h(K) \). Let \( D(X) = \text{Gcd}(P(X), X^{(p-1)/2} + 1) \mod h \). Then

1. \( V(X) \) divides \( D(X) \) in \( \mathbb{F}_h[X] \). The \( h \)-rank \( \rho \) of \( C(h) \) is greater or equal to the degree \( \delta \) of \( V(X) \) and \( h^\rho | h(K) \).

2. If \( h \) is coprime with \( p - 1 \) and with the class number \( h(E) \) of all intermediate fields \( F \subset E \subset K \), \( E \neq K \) then \( f | \rho \) where \( f \) is the order of \( h \mod p - 1 \).

**Proof.**

1. Reformulation of previous paragraph.

2. Immediate consequence of theorem 10.8 p. 187 in Washington [11] for the cyclic extension \( K/E \).
Remark: See the section 5 p. 18 for a MAPLE program applying the theorem 4.1 p. 12.

Corollary 4.2. If \( C(h) \) is cyclic then:

1. \( V(X) = X - \nu \) with \( \nu \in F_h^* \).
2. In \( F_h(X) \)
   
   \[
   V(X) \mid X^d - 1, \quad d = \gcd(h - 1, p - 1),
   \]

   \[
   V(X) \mid \{ \sum_{i=0}^{d-1} X^i \times \sum_{j=0}^{(p-1)/d-1} \nu^{-(i+jd)} \}/p \}.
   \]

3. Let \( M \) be the smallest subfield of \( K \) such that \( h \mid h(M) \). Let \( n = [M : \mathbb{Q}] \). If \( h \) is coprime with \( n \) then \( h - 1 \equiv 0 \mod n \).

Proof.

1. \( \rho = 1 \) implies that \( V(\sigma) = \sigma - \nu \).
2. \( X - \nu \mid X^{h-1} - \nu^{h-1} \) and so \( \sigma^{h-1} - \nu^{h-1} \) annihilates \( C(h) \). From \( \nu^{h-1} \equiv 1 \mod h \) it follows that \( \sigma^{h-1} - 1 \) annihilates \( C(h) \). \( \sigma^{p-1} - 1 \) annihilates \( C(h) \) and so \( \sigma^d - 1 \) annihilates \( C(h) \) and so \( X - \nu \) divides \( X^d - 1 \) in \( F_h[X] \). Then apply theorem 4.1. Observe that \( \sum_{i=0}^{(p-1)/d-1} \nu^{-(i+jd)} \equiv 0 \mod p \) and that we have assumed that the prime \( h \neq p \) in this section.
3. Let \( E \) be the smallest intermediate field \( E, \mathbb{Q} \subset E \subset K \) with \( h \mid h(E) \) and \( [E : \mathbb{Q}] = n \). Then we apply theorem 10.8 p. 187 of Washington [11] to the cyclic extension \( M/\mathbb{Q} \), thus \( h \equiv 1 \mod n \) and \( n \mid p - 1 \) because \( f \mid \rho \) where \( \rho = 1 \).

\( \square \)

It is possible to enlarge previous results with another annihilation polynomial:

Theorem 4.3. The polynomial \( \Pi(\sigma) = \sum_{i=0}^{p-2} v_{-i} \) even \( \sigma^i \) annihilates the non-\( p \)-part of the class group \( C \) of the \( p \)-cyclotomic field \( K \).

Proof.

1. Apply Stickelberger relation to field \( \mathbb{Q}(\zeta_{2p}) = \mathbb{Q}(\zeta_p) \). Let \( \varpi_{2t+1} : \zeta_{2p} \rightarrow \zeta_{2p}^{2t+1} \). The Stickelberger polynomial can be written

   \[
   S_2 = \sum_{2t+1=1, \ t\neq p}^{2p-1} \varpi_{2t+1}^{-1} \times (2t + 1).
   \]
2. Observe at first that $\zeta_{2p} = -\zeta_p$. 

If $t > (p - 1)/2$

then $\varpi_{2t+1} : \zeta_{2p} \to -\zeta_{2t+1-p}$, hence $\varpi_{2t+1} : -\zeta_p \to -(-\zeta_p)^{2t+1-p}$, hence $\varpi_{2t+1} : -\zeta_p \to -(-\zeta_p)^{2t+1-p}$ because $2t+1-p$ is even, hence $\varpi_{2t+1} : \zeta_p \to \zeta_{2t+1-p}$, hence $\varpi_{2t+1} = \varpi_{2t+1-p}$, hence

$$\varpi_{2t+1}^{-1} \times (2t + 1) = \varpi_{2t+1-p}^{-1} \times (2t + 1 - p) + p \times \varpi_{2t+1-p}^{-1}.$$ 

3. The Stickelberger polynomial is

$$S_2 = \sum_{t=0}^{(p-3)/2} \varpi_{2t+1}^{-1} \times (2t + 1) + \sum_{t=(p+1)/2}^{p-1} \varpi_{2t+1-p}^{-1} \times (2t + 1),$$

hence

$$S_2 = \sum_{t=0}^{(p-3)/2} \varpi_{2t+1}^{-1} \times (2t + 1) + \sum_{t=(p+1)/2}^{p-1} \varpi_{2t+1-p}^{-1} \times (2t + 1 - p) + p \sum_{t=(p-1)/2}^{p-1} \varpi_{2t+1-p},$$

hence

$$S_2 = \sum_{t=1}^{p-1} \varpi_t^{-1} t + p \sum_{t=(p-1)/2}^{p-1} \varpi_{2t+1-p},$$

hence, with $P(\sigma)$ defined in lemma 2.2 p. [4]

$$S_2 = P(\sigma) + p \sum_{t=(p-1)/2}^{p-1} \varpi_{2t+1-p},$$

With $2t + 1 - p = v_{-i}$ we get

(19) $$S_2 = P(\sigma) + p \sum_{t=(p-1)/2}^{p-1} \sigma^i.$$ 

4. The polynomial $P(\sigma)$ annihilates the class group C of K. Therefore the polynomial $p \times \sum_{t=0, v_{-i} \text{ even}}^{p-2} \sigma^i$ annihilates also C. If $h \neq p$ then $\Pi(\sigma)$ annihilates $C(h)$, which achieves the proof.
Remark: Numerical MAPLE computations seem to show more: the polynomial
\[ Gcd(\Pi(\sigma), \sigma^{(p-1)/2} + 1) = \frac{\sigma^{(p-1)/2} + 1}{\sigma - \nu} = \prod_{m=1}^{(p-3)/2} (\sigma - \nu_{2m+1}). \]
Therefore \( \Pi(\sigma) \) annihilates also the relative \( p \)-class group \( C_{p}^{-} \).

**Lemma 4.4.** Let \( E \) be a subfield of \( K \) with \( [K : \mathbb{Q}] = d \). Let \( h \) be an odd prime number dividing \( h(L) \). Then in \( \mathbb{F}_h[X] \)
\[
V(X) \vert \sum_{i=0}^{d-1} X^i, \\
V(X) \vert \{ \sum_{i=0}^{d-1} X^i \times \frac{\sum_{j=0}^{(p-1)/d-1} \nu^{-(i+jd)}}{p} \}.
\]

(20)

**Proof.** \( \sigma^d - 1 \) annihilates \( C(h) \). The Stickelberger polynomial
\[
P(X) = \sum_{i=0}^{p-2} X^i \nu_{-i} = p \times \sum_{i=0}^{d-1} X^i \times \frac{\sum_{j=0}^{(p-1)/d-1} \nu^{-(i+jd)}}{p},
\]
and from \( p \neq h \) it follows that
\[
V(X) \vert \{ \sum_{i=0}^{d-1} X^i \times \frac{\sum_{k=0}^{(p-1)/d-1} \nu^{-(i+jd)}}{p} \}
\]
in \( \mathbb{F}_p[G] \).

Remark: Compare lemma 4.4 for \( h \neq p \) with lemma 3.2 p. 7 proved when \( h = p \).

### 4.2 The case of complex quadratic fields contained in \( K \)

In this paragraph we formulate directly previous result when \( h \) divides the class number of the complex quadratic field \( \mathbb{Q}(\sqrt{-p}) \subset K, p \equiv 3 \mod 4, p \neq 3 \).

**Theorem 4.5.** *Hilbert 145 theorem*

Suppose that \( p \equiv 3 \mod 4, p \neq 3 \). If \( h \) is an odd prime with \( h \mid h(\mathbb{Q}(\sqrt{-p})) \) then
\[
\sum_{i=0}^{p-2} (-1)^i \nu_{-i} \equiv 0 \mod h.
\]

(21)

**Proof.** Let \( Q \) be the prime of \( \mathbb{Q}(\sqrt{-p}) \) lying above \( q \). The ideals \( Q \neq \sigma(Q) \) and so \( Q^{\sigma+1} \) is principal because \( Q^{\sigma^2} = Q \). Therefore \( Q^{\sum_{i=0}^{p-2} (-1)^i \nu_{-i}} \) is principal and \( \sum_{i=0}^{p-2} (-1)^i \nu_{-i} \equiv 0 \mod h \).
Remarks:

1. The theorem 4.7 can also be obtained from Hilbert Theorem 145 see Hilbert [3] p. 119. See also Mollin, [6] theorem 5.119 p. 318.

2. From lemmas 2.4 p. 4 we could prove similarly:

   Suppose that \( p \equiv 3 \text{ mod } 4, \ p \neq 3 \). If \( h \) is an odd prime with \( h \mid h(\mathbb{Q}(\sqrt{-p})) \) then

   \[
   2 \times \sum_{i=0}^{(p-3)/2} (-1)^i v_{-i} - p \equiv 0 \text{ mod } h. \tag{22}
   \]

3. Numerical evidences easily computable show more: If \( p \neq 3 \) is prime with \( p \equiv 3 \text{ mod } 4 \) then the class number \( h(\mathbb{Q}(\sqrt{-p})) \) verifies

   \[
   h(\mathbb{Q}(\sqrt{-p})) = -\frac{\sum_{i=0}^{p-2} (-1)^i v_{-i}}{p}. \tag{23}
   \]

   This result has been proved by Dirichlet by analytical number theory, see Mollin remark 5.124 p. 321. It is easy to verify this formula, for instance in tables of class numbers of complex quadratic fields in :

   (a) H. Cohen [2] p. 502-505, all the table for \( p \leq 503 \).

   (b) in Wolfram table of quadratic class numbers [12] for large \( p \).

4. When \( p \equiv 1 \text{ mod } 4 \) this method cannot be applied to the quadratic field \( \mathbb{Q}(\sqrt{p}) \subset K \) because \( \sum_{i=0}^{p-2} (-1)^i v_{-i} \) is trivially null.

**Theorem 4.6.** Suppose that \( p \equiv 3 \text{ mod } 4, \ p \neq 3 \). If \( h \) is an odd prime with \( h \mid h(\mathbb{Q}(\sqrt{-p})) \) then

   \[
   \sum_{i=0, \ v_{-i} \ even}^{p-2} (-1)^i \neq 0, \tag{24}
   \]

   \[
   \sum_{i=0, \ v_{-i} \ even}^{p-2} (-1)^i \equiv 0 \text{ mod } h.
   \]

**Proof.** We apply previous theorem 4.3 p. 13 observing that in that case \( \sigma^2(\mathbb{Q}) = \mathbb{Q} \) when \( \mathbb{Q} \) is a non-principal ideal of the quadratic field \( \mathbb{Q}(\sqrt{-p}) \), hence \( \sigma + 1 \) annihilates \( \mathbb{C}(h) \) and \( \sum_{i=0, \ v_{-i} \ even}^{p-2} (-1)^i \equiv 0 \text{ mod } h \). This sum has \( \frac{p-1}{2} \) elements, thus of odd cardinal and cannot be null.
Theorem 4.7. Suppose that \( p \equiv 3 \mod 4, p \neq 3 \). Let \( \delta \) be an integer \( 1 \leq \delta \leq p-2 \). Let \( I_\delta \) be the set

\[
I_\delta = \{ i \mid 0 \leq i \leq p-2, \ v_{(p-1)/2-i} + v_{(p-1)/2-i+\text{ind}_v(\delta)} > p \},
\]

where, as seen above, \( \text{ind}_v(\delta) \) is the notation index of \( \delta \) relative to \( v \). If \( h \) is an odd prime with \( h \mid h(\mathbb{Q}(\sqrt{-p})) \) then

\[
\sum_{i \in I_\delta} (-1)^i \neq 0,
\]

\[
\sum_{i \in I_\delta} (-1)^i \equiv 0 \mod h.
\]

Proof. \( I_\delta \) has an odd cardinal. Then see relation (25).

Remark:

1. Observe that results of theorems 4.6 and 4.7 are consistent with existing tables of quadratic fields, for instance Arno, Robinson, Wheeler [1]. Numerical verifications seem to show more :

\[
\sum_{i=0, v_{-i} \text{ even}}^{p-2} (-1)^i \equiv 0 \mod h(\mathbb{Q}(\sqrt{-p})).
\]

2. Observe that if \( p \equiv 1 \mod 4 \) then \( \sum_{i=0, v_{-i} \text{ even}}^{p-2} (-1)^i = 0 \).

4.3 The case of biquadratic fields contained in \( K \)

The following example is a generalization for the biquadratic fields \( L \) which are included in the \( p \)-cyclotomic field \( K \) with \( p \equiv 1 \mod 4 \).

Theorem 4.8. Let \( p \) be a prime with \( 2^2 \mid p-1 \). Let

\[
S = \left( \sum_{i=0}^{(p-3)/2} (-1)^i v_{2i} \right)^2 + \left( \sum_{i=0}^{(p-3)/2} (-1)^i v_{2i+1} \right)^2.
\]

Let \( L \) be the field with \( \mathbb{Q}(\sqrt{p}) \subset L \subset K \), \( [L : \mathbb{Q}(\sqrt{p})] = 2 \). Let \( h \) be an odd prime number with \( h \mid h(L) \) and \( h \not\mid h(\mathbb{Q}(\sqrt{p})) \). Then \( S \neq 0 \) and \( S \equiv 0 \mod h \).

Proof. \( V(\sigma) \mid \sigma^4 - 1 \) and \( h(\mathbb{Q}(\sqrt{p})) \) and so \( V(\sigma) \mid \sigma^2 + 1 \). \( P(\sigma) = \sum_{i=0}^{(p-3)/2} \sigma^{2i} v_{-2i} + \sigma \sum_{i=0}^{(p-3)/2} \sigma^{2i} v_{2i+1} \). Relation (28) follows.
Remarks:
1. S does not depend of the primitive root $v \mod p$ chosen.
2. Numerical computations seem to show more: $P(\sigma) \equiv 0 \mod p^2$ and so
   \begin{equation}
   \frac{\sum_{i=0}^{(p-3)/2} (-1)^i v_{2i})^2 + \sum_{i=0}^{(p-3)/2} (-1)^i v_{2i+1})^2}{p^2} \equiv 0 \mod h.
   \end{equation}
3. This result is a generalization for biquadratic fields of theorem 145 of Hilbert for quadratic fields.

5 A numerical MAPLE algorithm

This section contains a MAPLE algorithm connected to the structure of the relative class group $C^-$. For each prime number $p < 500$, the algorithm computes
1. a primitive root $v \mod p$,
2. the Stickelberger polynomial $P(X)$ has been defined in lemma 2.2 p. 4 and $Q(X)$ in lemma 2.3 p. 4. For the prime numbers $h$ with $3 \leq h \leq p^2$ and the primitive root $v \mod p$, the algorithm computes the polynomial $GCD(X) \in \mathbb{F}_h[X]$ for the indeterminate $X$ given by formulas:
   \begin{enumerate}
   \item[(a)] if $h \neq p$ then
   \item[(b)]
   \begin{equation}
   GCD(X) = \text{Gcd}(P(X), X^{(p-1)/2} + 1) \mod h,
   \end{equation}
   \item[(c)] if $h = p$ then
   \begin{equation}
   GCD(X) = \text{Gcd}(Q(X), X^{(p-1)/2} + 1) \mod h,
   \end{equation}
   \end{enumerate}

The results are compared with the corresponding tables of class numbers of cyclotomic fields $K = \mathbb{Q}(\zeta_p)$ for the primes $p < 500$ in Schoof [10]. We observe that:
1. The set of odd prime numbers $h$ with $\text{degree}(GCD(X)) > 0$ is strictly the set of odd prime divisors $h$ of $K$ in Schoof table p. 1142.
2. The rank $\rho$ of the $h$-Sylow subgroup $C(h)$ in Schoof tables 4.2 p. 1239 ($h$ not dividing $p - 1$) and 4.3 p. 1240 ($h$ dividing $p - 1$) is the degree of the polynomial $GCD(X)$ found here. Observe that when $h(K^+) \not\equiv 0 \mod p$ and $h = p$ this fact can be proved by means out of reach of this article at elementary level (Ribet theorem).
3. Let \( GCD(X) = \prod_{i=1}^{n} A_i(X)^{n_i} \) be the prime decomposition of \( GCD(X) \) in the euclidean field \( F_h[X] \). We observe that to each prime polynomial \( A_i(X) \) corresponds a subgroup of \( C(h) \) of \( h \)-rank \( d_i \times n_i \) where \( d_i \) is the degree of \( A_i(X) \). In particular if \( d_i = n_i = 1 \) then the subgroup corresponding to \( A_i(X) \) is cyclic. Note that for all prime \( p \) with \( h(K^+) \not\equiv 0 \mod p \) and \( h = p \) it is a consequence of Ribet theorem.

4. We observe that when \( h \neq p \) there exists some cases where \( n_i > 1 \) for instance for \( p = 101 \) and \( h = 5 \) with \( n_1 = 2 \). In these cases this implies that the minimal polynomial \( V(X) \) annihilating \( C_h \) is different of \( GCD(X) : V(X) \mid GCD(X) \) and \( \deg(V(X)) < \deg(GCD(X)) \).

A question: for all the odd primes \( p < 500 \) and all the odd primes \( h < p^2 \) we have observed that the degree of \( GCD(X) \) is equal to the rank \( \rho \) of the \( h \)-Sylow subgroup \( C(h) \) of the relative class group \( C \) of \( K \) with \( GCD(X) = 1 \iff h(K) \not\equiv 0 \mod h \): this gives important informations on the structure of the relative class group \( C^\perp \) of \( K \): the precise set of odd primes \( h \) dividing \( h(K) \) and for each of them the rank \( \rho \) of the \( h \)-group \( C(h) \). Can we generalize this property to all the odd primes \( p \) and all the odd primes \( h \) or at least at some predefined subsets of them?

The MAPLE algorithm

```
restart;
> p:=3:
> while p<499 do
> p:=nextprime(p):
> for v from 2 to p-2 do:
> i_v:=1:
> for i from 2 to p-2 do:
> if v&^i mod p = 1 then i_v:=0: fi:
> od:
> if i_v=1 then
> T:= X^((p-1)/2)+1 :
> S:=0:
> Q:=0:
> for i from 0 to p-2 do:
> vmi:=v&^(p-1-i) mod p:
> vmim1:=v&^(p-1-(i-1)) mod p:
> delta_i:=iquo(vmim1-v*vmi,p):
> S:=S+X^i*vmi:
> Q:=Q+X^i*delta_i:
> od:
> for h from 3 to p^2 do:
> if isprime(h)=true then
> if h<>p then
> GCD:=Gcd(T,S) mod h:
> deg_GCD:=degree (GCD):
> if deg_GCD>0 then
> GCD_Factors:=Factors(GCD) mod h:
> fi:
> fi:
> fi:
> fi:
> fi:
```

19
In the following page the table of results obtained.
\[
\begin{array}{cccccc}
\text{p} & \text{h} & \rho & v & \text{GCD}(X) \\
\hline
23 & 3 & 1 & 3 & X + 1 & 57 & 1 & 3 & X + 1 \\
31 & 3 & 1 & 3 & X + 1 & 157 & 5 & 1 & 5 & X + 3 \\
37 & 37 & 1 & 2 & X + 5 & 157 & 13 & 1 & 5 & X + 6 \\
41 & 11 & 2 & 6 & X^2 + 10X + 6 & 157 & 157 & 2 & 5 & (X + 95)(X + 91) \\
43 & 211 & 1 & 3 & X + 73 & 157 & 1093 & 1 & 5 & X + 800 \\
47 & 5 & 1 & 5 & X + 1 & 157 & 1873 & 1 & 5 & X + 935 \\
47 & 139 & 1 & 3 & X + 31 & 163 & 181 & 1 & 2 & X + 65 \\
59 & 3 & 1 & 2 & X + 1 & 163 & 23167 & 1 & 2 & X + 8783 \\
59 & 59 & 1 & 2 & X + 36 & 167 & 11 & 1 & 5 & X + 1 \\
59 & 233 & 1 & 2 & X + 8 & 167 & 499 & 1 & 5 & X + 491 \\
61 & 41 & 1 & 2 & X + 36 & 173 & 5 & 1 & 2 & X + 2 \\
61 & 1861 & 1 & 2 & X + 997 & 173 & 18825 & 1 & 2 & X + 997 \\
67 & 67 & 1 & 2 & X + 24 & 179 & 3 & 1 & 3 & X + 1 \\
71 & 7 & 1 & 7 & X + 1 & 179 & 1069 & 1 & 2 & X + 552 \\
73 & 89 & 1 & 5 & X + 12 & 181 & 5 & 1 & 2 & X + 3 \\
79 & 5 & 1 & 3 & X + 1 & 181 & 37 & 1 & 2 & X + 29 \\
79 & 53 & 1 & 3 & X + 28 & 181 & 41 & 1 & 2 & X + 2 \\
83 & 3 & 1 & 2 & X + 1 & 181 & 61 & 1 & 2 & X + 6 \\
89 & 113 & 1 & 3 & X + 95 & 181 & 1321 & 1 & 2 & X + 149 \\
97 & 577 & 1 & 5 & X + 46 & 181 & 2521 & 1 & 2 & X + 2015 \\
97 & 3457 & 1 & 5 & X + 1558 & 191 & 11 & 1 & 19 & X + 3 \\
101 & 5 & 1 & 2 & (X + 3)^2 & 191 & 13 & 1 & 19 & X + 1 \\
101 & 101 & 1 & 2 & X + 66 & 193 & 6529 & 1 & 5 & X + 4193 \\
101 & 601 & 1 & 2 & X + 323 & 193 & 15361 & 1 & 5 & X + 13057 \\
103 & 5 & 1 & 5 & X + 1 & 193 & 29761 & 1 & 5 & X + 29163 \\
103 & 103 & 1 & 5 & X + 58 & 197 & 5 & 1 & 2 & X + 3 \\
103 & 1021 & 1 & 5 & X + 9 & 197 & 1877 & 1 & 2 & X + 981 \\
107 & 3 & 1 & 2 & X + 1 & 197 & 2475 & 1 & 2 & X + 1064 \\
107 & 743 & 1 & 2 & X + 50 & 199 & 3 & 1 & 3 & X + 1 \\
107 & 9859 & 1 & 2 & X + 4936 & 199 & 19 & 1 & 3 & X + 4 \\
107 & 17 & 1 & 6 & X + 4 & 199 & 727 & 1 & 3 & X + 590 \\
109 & 1009 & 1 & 6 & X + 41 & 211 & 11 & 1 & 2 & X + 3 \\
113 & 113 & 1 & 3 & X + 5 & 211 & 7 & 1 & 2 & X + 4 \\
113 & 57 & 1 & 3 & X + 1 & 211 & 41 & 1 & 2 & X + 16 \\
113 & 13 & 1 & 3 & X + 9 & 211 & 71 & 1 & 2 & X + 15 \\
113 & 43 & 1 & 3 & X + 4 & 211 & 181 & 1 & 2 & X + 5 \\
113 & 547 & 1 & 3 & X + 169 & 211 & 281 & 2 & 2 & (X + 199)(X + 101) \\
113 & 883 & 1 & 3 & X + 336 & 211 & 421 & 1 & 2 & X + 93 \\
127 & 3079 & 1 & 3 & X + 1925 & 211 & 1051 & 1 & 2 & X + 884 \\
131 & 3 & 3 & 2 & X^3 + 2X^2 + 1 & 211 & 12251 & 1 & 2 & X + 1580 \\
131 & 5 & 1 & 2 & X + 1 & 223 & 7 & 1 & 3 & X + 1 \\
131 & 53 & 1 & 2 & X + 6 & 223 & 43 & 1 & 3 & X + 36 \\
131 & 131 & 1 & 2 & X + 34 & 227 & 5 & 1 & 2 & X + 1 \\
131 & 1301 & 1 & 2 & X + 283 & 227 & 2939 & 3 & 2 & (X + 1420)(X + 509)(X + 2006) \\
137 & 137 & 1 & 3 & X + 8 & 229 & 13 & 1 & 6 & X + 6 \\
139 & 3 & 1 & 2 & X + 1 & 229 & 17 & 1 & 6 & X + 13 \\
139 & 47 & 1 & 2 & X + 9 & 229 & 457 & 1 & 6 & X + 126 \\
139 & 277 & 2 & 2 & (X + 191)(X + 218) & 229 & 7753 & 1 & 6 & X + 4310 \\
139 & 967 & 1 & 2 & X + 241 & 233 & 233 & 1 & 3 & X + 193 \\
149 & 3 & 2 & 2 & X^2 + 1 & 233 & 1433 & 1 & 3 & X + 1091 \\
149 & 149 & 1 & 2 & X + 43 & 239 & 3 & 1 & 7 & X + 1 \\
151 & 7 & 1 & 6 & X + 1 & 239 & 5 & 1 & 7 & X + 1 \\
151 & 11 & 2 & 6 & X^2 + 6X + 3 & 239 & 9 & 1 & 7 & X + 1 \\
151 & 281 & 1 & 6 & X + 90 & 239 & 10 & 1 & 7 & X + 1 \\
\end{array}
\]
\begin{verbatim}
p h ρ v GCD(X) p h ρ v GCD(X)
241 47 2 7 X^2 + 29X + 1
241 13921 1 7 X + 9053
241 15601 1 7 X + 7049
251 7 1 6 X + 1
251 11 1 6 X + 4
257 257 1 3 X + 76
263 13 1 5 X + 1
263 15601 1 5 X + 204
263 787 1 5 X + 510
269 13 1 2 X + 5
271 11 1 6 X + 9
271 271 1 6 X + 2
271 31 1 6 X + 2
271 271 1 6 X + 9
271 271 1 6 X + 196
271 811 1 6 X + 271
277 17 1 5 X + 13
277 829 1 5 X + 150
281 7 1 6 X + 1
281 17 1 3 X + 8
281 41 1 3 X + 24
281 401 1 3 X + 250
283 3 1 3 X + 1
283 283 1 3 X + 236
289 11 1 6 X + 9
293 3 1 2 X + 1
293 233 1 10 X + 136
293 6113 1 3 X + 9053
293 14621 1 3 X + 2522
307 3 1 5 X + 1
307 37 1 5 X + 33
307 137 1 5 X + 38
307 307 1 5 X + 16
307 443 1 5 X + 13
307 613 1 5 X + 49
307 919 1 5 X + 144
307 1429 1 5 X + 1294
311 19 1 17 X + 1
311 41 1 17 X + 18
311 311 1 17 X + 158
313 37 2 10 X^2 + 14
313 233 1 10 X + 136
317 13 1 2 X + 5
317 2521 1 2 X + 60
331 33 6 2 (X + 1)^2(X^4 + 2X^3 + X^2 + 2X + 1)
331 67 1 3 X + 64
337 7 2 10 X^2 + X + 6
337 17 2 10 (X + 10)(X + 7)
337 353 1 10 X + 36
347 5 1 2 X + 1
347 347 1 2 X + 52
349 5 1 2 X + 2
349 13 1 2 X + 6
349 2089 1 2 X + 1733
349 17749 1 2 X + 9289
353 353 2 3 (X + 299)(X + 51)
353 6113 1 3 X + 2060
353 9473 1 3 X + 5067
359 19 1 7 X + 1
367 3 1 6 X + 1
367 733 1 6 X + 686
373 11 1 2 X + 5
373 1489 1 2 X + 990
373 3917 1 2 X + 176
373 4969 1 2 X + 159
379 13 1 2 X + 3
379 127 1 2 X + 13
379 379 2 3 (X + 348)(X + 91)
383 17 1 5 X + 1
383 283 1 5 X + 150
383 383 1 5 X + 236
389 41 1 2 X + 32
389 1553 1 2 X + 1130
397 23 2 5 X^2 + 5X + 5
397 23 2 5 X^2 + 13X + 18
397 109 1 5 X + 32
397 4861 1 5 X + 3655
397 9901 1 5 X + 8544
397 9901 1 5 X + 8544
401 401 1 3 X + 141
401 64849 1 3 X + 46775
409 5 2 21 X^2 + 3
409 17 1 21 X + 2
409 73 1 21 X + 66
409 409 1 21 X + 48
409 1321 1 21 X + 1304
419 3 1 2 X + 1
419 1103 1 2 X + 494
421 5 1 2 X + 2
421 29 1 2 X + 18
421 37 1 2 X + 23
421 421 1 2 X + 72
421 2521 1 2 X + 60
421 39509 1 2 X + 7582
421 39901 1 2 X + 8081
421 70309 1 2 X + 65038
431 3 1 7 X + 1
431 7 1 7 X + 1
431 11 1 7 X + 5
431 701 1 7 X + 210
433 433 1 5 X + 371
433 3457 1 5 X + 2700
433 12097 1 5 X + 31
433 21601 1 5 X + 10658
433 47521 1 5 X + 36247
\end{verbatim}
| $p$  | $h$  | $\rho$ | $v$  | $GCD(X)$                                |
|------|------|--------|------|-----------------------------------------|
| 439  | 3    | 2      | 15   | $(X + 1)^2$                             |
| 439  | 1    | 1      | 15   | $X + 1$                                 |
| 439  | 203  | 1      | 15   | $X + 283$                               |
| 443  | 3    | 2      | 2    | $X^3 + X^2 + 2X + 1$                    |
| 443  | 5    | 1      | 2    | $X + 1$                                 |
| 443  | 79   | 1      | 2    | $X + 8$                                 |
| 443  | 157  | 1      | 2    | $X + 67$                                |
| 443  | 12377| 1      | 2    | $X + 6026$                              |
| 449  | 168449| 1      | 3    | $X + 33570$                            |
| 457  | 5    | 2      | 13   | $X^2 + 4X + 2$                          |
| 457  | 41   | 1      | 13   | $X + 14$                                |
| 457  | 577  | 1      | 13   | $X + 9$                                 |
| 457  | 1217 | 1      | 13   | $X + 692$                               |
| 457  | 43777| 1      | 13   | $X + 37577$                            |
| 457  | 63841| 1      | 13   | $X + 2827$                             |
| 461  | 5    | 2      | 2    | $(X + 2)^2$                             |
| 461  | 461  | 1      | 2    | $X + 13$                                |
| 461  | 661  | 1      | 2    | $X + 258$                               |
| 461  | 161461| 1   | 2    | $X + 134936$                           |
| 463  | 7    | 2      | 3    | $(X + 2)(X + 1)$                        |
| 463  | 29   | 1      | 3    | $X + 20$                                |
| 463  | 89   | 1      | 3    | $X + 64$                                |
| 463  | 463  | 1      | 3    | $X + 8$                                 |
| 463  | 631  | 1      | 3    | $X + 62$                                |
| 463  | 673  | 1      | 3    | $X + 223$                               |
| 463  | 1123 | 1      | 3    | $X + 49$                                |
| 463  | 4423 | 1      | 3    | $X + 387$                               |
| 463  | 8779 | 1      | 3    | $X + 5520$                              |
| 467  | 7    | 1      | 2    | $X + 1$                                 |
| 467  | 467  | 1      | 2    | $(X + 239)(X + 236)$                    |
| 479  | 5    | 1      | 13   | $X + 1$                                 |
| 479  | 48757| 1      | 13   | $X + 34844$                             |
| 479  | 62141| 1      | 13   | $X + 43049$                             |
| 487  | 7    | 2      | 3    | $(X + 4)(X + 1)$                        |
| 487  | 37   | 2      | 3    | $(X + 33)(X + 12)$                     |
| 487  | 919  | 1      | 3    | $X + 267$                               |
| 487  | 2647 | 1      | 3    | $X + 1070$                             |
| 487  | 10909| 1      | 3    | $X + 3031$                             |
| 487  | 58321| 1      | 3    | $X + 58241$                            |
| 491  | 3    | 1      | 2    | $X + 1$                                 |
| 491  | 11   | 2      | 2    | $(X + 4)(X + 5)$                        |
| 491  | 29   | 1      | 2    | $X + 16$                                |
| 491  | 491  | 3      | 2    | $(X + 203)(X + 419)(X + 418)$           |
| 499  | 3    | 1      | 7    | $X + 1$                                 |
| 499  | 167  | 1      | 7    | $X + 98$                                |

References

[1] S. Arno, M.L. Robinson, F.S. Wheeler *Imaginary quadratic fields with small odd class number*, Acta Arith. 83, 1998, 295-300.

[2] H. Cohen, A course in computational number theory, Springer-Verlag, 1993.

[3] D. Hilbert, *The Theory of Algebraic Numbers*, Springer, 1998
[4] K. Ireland, M. Rosen, *A Classical Introduction to Modern Number Theory*, Springer-Verlag, 1982.

[5] H. Koch, *Algebraic Number Theory*, Springer, 1997.

[6] R.A. Mollin, *Algebraic Number Theory*, Chapman and Hall/CRC, 1999.

[7] W. Narkiewicz, *Elementary and Analytic Theory of Numbers*, Springer-Verlag, 1990.

[8] P. Ribenboim, *13 Lectures on Fermat’s Last Theorem*, Springer-Verlag, 1979.

[9] P. Ribenboim, *Classical Theory of Algebraic Numbers*, Springer, 2001.

[10] R. Schoof, *Minus class groups of the fields of the l-roots of unity*, Mathematics of Computation, vol 267,223, jul 1998, p. 1225-1245.

[11] L.C. Washington, *Introduction to cyclotomic fields, second edition*, Springer, 1997.

[12] *Class number of quadratic fields*,
http://www.mathworld.wolfram.com/ClassNumber.html

Roland Quème
13 avenue du château d’eau
31490 Brax
France
mailto: roland.queme@wanadoo.fr
home page: http://roland.queme.free.fr/

********************************************************************
V10 - MSC Classification : 11R18; 11R29
********************************************************************