A class number congruence for cyclotomic fields and their subfields

by

TAUNO METSÄNKYLÄ (Turku)

1. Introduction. Consider the cyclotomic field \( \mathbb{Q}(\zeta) \) generated by \( \zeta = \exp(2\pi i/p) \), where \( p = 2m+1 \) is a prime > 3. As usual, write the class number of \( \mathbb{Q} \) in the form \( H = H_1 H_2 \), where \( H_1 \) is an integer and \( H_2 \) denotes the class number of the maximal real subfield \( \mathbb{Q}_p \) of \( F \). Carlitz [5] recently derived a congruence

\[
H_1 = H_2 \sigma(p) \pmod{p} \quad (\sigma \text{ an integer}),
\]

thus giving, among other things, a new proof for the known fact (Kummer's theorem) that \( H_1 = 0 \pmod{p} \) implies \( H_1 = 0 \pmod{p} \). It is remarkable that Carlitz's proof uses, apart from the explicit expression of \( H_1 \), only a few elementary results from the theory of cyclotomic fields.

Borevich and Shafranovich proved Kummer's theorem in [3] by a new \( p \)-adic method, due to D. O. Faddeev. In this paper we shall show that this \( p \)-adic method easily gives a congruence for \( H_2 \), from which we can deduce a congruence of the form (1) (see Theorem 1 and its Corollary). Furthermore, we shall prove that our congruence implies that of Carlitz, and vice versa.

We shall also generalize Theorem 1 to the subfields of \( F \). This generalization yields, as a special case, the well-known congruence connecting the class number and fundamental unit of a real quadratic field (see Section 4).

2. Preliminaries. Recall that the prime factorization of \( p \) in \( \mathbb{Q} \) is \( p = p_1^{r_1} \cdots p_n^{r_n} \), where \( p_1 = (1 - \zeta) \). Let \( F_p \) denote the \( p \)-adic completion of \( \mathbb{Q} \). Then \( Q_p \), the \( p \)-adic completion of \( Q \), can be embedded in \( F_p \) in a natural way, and \( [F_p:Q_p] = [F:Q] = p-1 \). Moreover, the automorphisms \( \sigma_s \) (s = 0, ..., p - 2) of the extension \( F/Q \), defined by

\[
\sigma_s(\zeta) = \zeta^s \quad (s \text{ a primitive root } \pmod{p}),
\]

can be extended to \( F_p/Q_p \) in a natural way. (For the proof of these and the following results in this Section, see [3], Chapter 5, Section 6.)
Let us denote by $\mathbb{Z}$ the ring of rational integers and by $\mathbb{Z}_p$ and $\mathbb{Z}_p^*$ the rings of $p$-adic and $p$-adic integers, respectively. Choose the unique prime element $\lambda$ of $\mathbb{Z}_p$ satisfying the conditions

$$\lambda^{p-1} + p = 0, \quad \lambda = \zeta - 1 \pmod{\lambda^p}$$

and note that the system $\{1, \zeta, \ldots, \zeta^{p-2}\}$ is a fundamental basis of $\mathbb{F}_p/\mathbb{Q}_p$.

**Lemma 1.** In $\mathbb{F}_p$, the maximal subfield whose elements are left fixed by $\sigma_0$ is the subfield generated by $\{1, \lambda, \ldots, \lambda^{p-2}\}$.

Consider the function $\log \phi$ over the field $\mathbb{F}_p$. It is defined for all principal units (i.e., for units $\varepsilon$ with $\varepsilon = 1 \pmod{\lambda}$) of $\mathbb{Z}_p$ and satisfies the equation

$$\log(\varepsilon_1 \varepsilon_2) = \log \varepsilon_1 + \log \varepsilon_2.$$  

**Lemma 2.** For every unit $\varepsilon$ of $\mathbb{F}_p$, $\varepsilon^{p-1}$ is a principal unit of $\mathbb{Z}_p$ and $\log \varepsilon^{p-1}$ can be represented in the form

$$\log \varepsilon^{p-1} = \sum_{k=1}^{p-1} \alpha_k \varepsilon^{2k} \quad (\alpha_k \in \mathbb{Z}_p).$$

**Lemma 3.** Put

$$L(1+x) = \sum_{n=1}^{p-1} (-1)^{n-1} x^n/n, \quad E(x) = \sum_{n=1}^{p-1} x^n/n!.$$ 

Then the following congruences hold in the ring $\mathbb{Z}_p$:

1. $L(\varepsilon^{p-1}) = \log \varepsilon^{p-1} \pmod{\lambda^p}$ (a unit of $\mathbb{F}_p$),
2. $E(\varepsilon \lambda^k) = \varepsilon^k \pmod{\lambda^p}$ (for $k = 1, 2, \ldots$).

**3. Congruences for $H$.** The so-called cyclotomic units of $\mathbb{F}_p$ are the units

$$e_i = \sigma_{i-1} \left( \varepsilon(\xi) \right) \quad (i = 1, \ldots, m-1),$$

where $\varepsilon(\xi)$ is the positive unit

$$\varepsilon(\xi) = \left\{ \frac{1 - \xi^{2k}}{1 - \xi^k} \right\}_{1, \xi^k, \ldots, \xi^{k-1}}.$$ 

Let $(\varepsilon_j = \varepsilon_j(\xi))_{j = 1, \ldots, m-1}$ denote a system of positive fundamental units of $\mathbb{F}_p$ and put

$$a_i = \prod_{j=1}^{m-1} \varepsilon_j^{(i,j)} \quad (i = 1, \ldots, m-1)$$

with $r(i, j) \in \mathbb{Z}$. Then it is known that

$$H_i = |\det(r(i, j))| \quad (i, j = 1, \ldots, m-1).$$

(Cf. [3], pp. 361–362. Our system of cyclotomic units is not the same as the corresponding system in [3] but is more appropriate for generalization.)

In what follows we shall assume the sequence of fundamental units to be so chosen that the determinant on the right is positive.

We apply Lemma 2 to the above units. Since every $p$-adic integer is congruent $\pmod{p}$ to some rational integer, we may then write

$$\log e_i^{p-1} = \sum_{k=1}^{m-1} v_{ik} r^{2k} \pmod{\lambda^p} \quad (i = 1, \ldots, m-1),$$

$$\log e_i^{p-1} = \sum_{k=1}^{m-1} w_{ik} r^{2k} \pmod{\lambda^p} \quad (j = 1, \ldots, m-1)$$

with $v_{ik}, w_{ik} \in \mathbb{Z}$. By (4) and (2), this yields

$$\sum_{k=1}^{m-1} v_{ik} r^{2k} = \sum_{k=1}^{m-1} \sum_{j=1}^{m-1} r(i, j) w_{jk} r^{2k} \pmod{\lambda^p} \quad (i = 1, \ldots, m-1).$$

Hence we have the following "basic" congruence for $H_i$:

$$\det(v_{ik}) = H_i \det(w_{ik}) \pmod{p} \quad (i, j, k = 1, \ldots, m-1).$$

The computation of the numbers $v_{ik}$ can be accomplished by a procedure completely similar to that in [3], pp. 374–376, by starting from the formulas

$$e_i = \sigma_{i-1} \left( \frac{\xi^{1/2} - 1}{\xi - 1} \right)^{1/2} \quad (i = 1, \ldots, m-1).$$

The result is

$$v_{ik} = B_{2k}(1 - r^{2k}) r^{(-i-1)k} \pmod{2k(2k+1)} \quad (i, j, k = 1, \ldots, m-1),$$

where $B_{2k}$ denotes the $2k$-th Bernoulli number in the even suffix notation. Observing that

$$(1 - r^3)(1 - r^4) \ldots (1 - r^{p-1}) = -\frac{1}{2} \pmod{p}$$

we therefore get

**Theorem 1.** The class number $H_i$ of $\mathbb{F}_p$ satisfies the congruence

$$-\frac{1}{2} \det(r^{(i-1)k}) \prod_{n=1}^{m-1} \frac{B_{2n}}{2n(2n+1)} = H_i \det(w_{ik}) \pmod{p} \quad (i, j, k = 1, \ldots, m-1),$$

where the $w_{ik}$ are rational integers defined by (6). The determinant on the left side of (9), being of Vandermonde type, equals, except for sign, the product of all $r^{2k} - r^{2k}$, where $1 \leq i < k \leq m-1$. Hence this determinant is not divisible by $p$. 

According to a classical result of Vandiver ([11], see also [10]),
\[ H_1 = (-1)^{m-1} \sum_{n=1}^{m} B_{(m-n)\rho-1} \pmod{p}. \]

Using Kummer's congruence and von Staudt's theorem for Bernoulli numbers ([3]), we may put this relation in the form
\[ H_1 = (-1)^{m-1} \sum_{n=1}^{m-1} (B_{n\rho}/2n) \pmod{p}, \]
which combined with (9) gives
\[ H_1 = 0 \pmod{p} \]

**Corollary.** We have
\[ H_1 = -2^{2-m} H_{m-1} \det \{ (2k)! w_{jk} \} \pmod{p}, \]
where \( D = \det (x^{k-1}) \) \((i, j, k = 1, \ldots, m-1)\).

As mentioned in the Introduction, it follows from this congruence that
\[ H_1 = 0 \pmod{p}. \]

4. **Comparison with Carlitz's congruence.** Let us suppose that the unit \( \zeta(x) \) is written in the canonical form by means of the basis \( \{ 1, \xi, \ldots, \xi^{p-2} \} \) of \( F \), so that \( \zeta(x) \) is a polynomial over \( \mathbb{Z} \) \((j = 1, \ldots, m-1)\).

Write briefly \( \zeta'(x) \) for \( \zeta(x)/x(x) \), where \( \zeta'(x) \) denotes the derivative of \( \zeta(x) \), and set
\[ \zeta' = \sum_{n=0}^{p-2} a_{p} \xi^{n} \pmod{p}, \]

Carlitz's congruence can now be presented in the form
\[ H_1 = -2^{2-m} H_{m-1} \det \{ \sum_{n=0}^{p-2} a_{p} \xi^{n} \pmod{p} \}
\]

\((j, k = 1, \ldots, m-1)\), where \( D \) is the determinant defined in the above Corollary. We shall prove the following lemma which indicates that this congruence implies (11), and conversely.

**Lemma 4.**
\[ (-2k)! w_{jk} = \sum_{n=0}^{p-2} a_{p} \xi^{n} \pmod{p} \]

\((j, k = 1, \ldots, m-1)\).

**Proof.** Making use of the fact that \( \zeta(x) \) is real, and of Lemma 3(ii), we obtain from (13)
\[ \zeta(x/y) = \frac{1}{y} \sum_{n=0}^{p-2} a_{p} \xi^{n} \zeta(\xi^{n}) = \frac{1}{y} \sum_{n=0}^{p-2} a_{p} \xi^{n} \zeta(\xi^{n} \tilde{x}^{n}) \]

\[ = \sum_{n=0}^{p-2} a_{p} \xi^{n} \zeta(\xi^{n} \tilde{x}^{n}) \pmod{p}. \]

(here and below \( j \) is fixed, \( 1 \leq j \leq m-1 \)). Thus our lemma is proved after we have shown that the definition (6) of \( \omega_{jk} \) implies
\[ (13) \]
\[ \zeta(x/y) = \sum_{n=0}^{m-1} 2k \omega_{jk} \tilde{x}^{n-1} \pmod{p}. \]

To verify (13), put
\[ \xi = \sum_{n=0}^{p-2} a_{n} \xi^{n} \pmod{p} \]

and denote
\[ P(x) = \sum_{n=0}^{p-2} a_{n} \xi^{n}, \quad R(x) = \xi \cdot P(x) \pmod{p} \]

so that
\[ P(\lambda) = \xi, \quad R(\lambda) = \xi \cdot P(\lambda) \pmod{p}. \]

Obviously, \( P(x), R(x) \in \mathbb{Z}[x] \), and the constant term of \( R(x) \) is, by Lemma 2, congruent to \( 1 \pmod{p} \). It follows then from the identity
\[ (1 + x) \frac{d}{dx} L(1 + x) = 1 + (-1)^{p-2} \xi^{p-1} \]

that
\[ \frac{d}{dx} L(R(x)) = R'(x) + \xi^{p-1} S(x) + p T(x) \]

with \( S(x), T(x) \in \mathbb{Z}[x] \).

Applying Lemma 3(i) to (6) we may write
\[ L(\xi^{p-1}) = \sum_{n=0}^{p-2} b_{p} \xi^{n} \pmod{p}, \]

where
\[ b_{2k} = \omega_{2k}(\pmod{p}) \]

and the other \( b_{n} \) are \( 0 \pmod{p} \). Now, the equation
\[ L(R(x)) = \sum_{n=0}^{p-2} b_{n} \xi^{n} \]

holds for every \( \sigma_{k}(x) \), that is, for \( x = \lambda, \lambda \tilde{x}, \ldots, \lambda^{p-2} \), where \( \tilde{x} \) is a primitive \((p-1)\)-th root of unity. Hence we have the identity
\[ L(R(x)) = \sum_{n=0}^{p-2} b_{n} \xi^{n} \pmod{p}. \]
with \( F(x) \in \mathbb{Z}_2[x] \). After differentiating and setting \( x = \lambda \) we get, by (16),

\[
(K'/K)(\lambda) = \sum_{k=1}^{m-1} 2k\eta_k \lambda^{m-1} \pmod{\lambda^{p-1}}.
\]

On the other hand,

\[
(K'/K)(\lambda) = (p-1) (e_j/e_j) (\zeta) E'(\lambda),
\]

where, furthermore,

\[
E'(\lambda) = \sum_{n=1}^{p-2} a_n \lambda^{n-1} = \zeta \pmod{\lambda^{p-2}}
\]

because \( a_n = 1/n! \pmod{p} \) (see (14) and Lemma 3(ii)). Combining (16), (17), and (18) we obtain the congruence (13).

5. Generalization. We shall generalize Theorem 1 and Lemma 4 to the subfields \( K \) of \( F \). It is known (see, e.g., [6], [2]) that the class number of \( K \) is of the form \( h = h_1 h_2 \), where \( h_1 \) and \( h_2 \) are integral factors of \( H_1 \) and \( H_2 \), respectively, and \( h_3 \) is the class number of the maximal real subfield \( K_0 \) of \( K \) (where \( h_1 = 1 \) if \( K = K_0 \)). In the following we may assume that \( K \) is imaginary, since every real subfield of \( F \) is contained as a maximal real subfield in some imaginary subfield of \( F \). Let \( K \) be of degree \( a = 2u \) over \( Q \) and put \( p-1 = ab \), where \( b \) is odd.

The maximal subfield of \( F \) being pointwise invariant under the automorphism \( \sigma \) is the real field \( K_0 \). The following lemma can be proved similarly as Lemma 1.

**Lemma 1A.** In \( F \), the maximal subfield whose elements are left fixed by \( \sigma \) is the subfield generated by \( \{ 1, \lambda, \ldots, \lambda^{a-1} \} \).

Using this lemma, one can easily prove

**Lemma 2A.** For every unit \( \varepsilon \) of \( K_0 \), \( \varepsilon^{p-1} \) is a principal unit of \( Y_0 \) and \( \log \varepsilon^{p-1} \) can be represented in the form

\[
\log \varepsilon^{p-1} = \sum_{k=1}^{b-1} \eta_k \lambda^{2bk} \pmod{\lambda^{p-1}}.
\]

The cyclotomic units of \( K_0 \) are the units

\[
\varepsilon_i = e_i e_{i+u} \cdots e_{i+(b-1)u} \quad (i = 1, \ldots, u-1),
\]

where the \( e_i \) are defined by (3) ([6], p. 23). Let \( \{ e_1, \ldots, e_{u-1} \} \) denote a system of positive fundamental units of \( K_0 \) (this notation may be used without confusion because the fundamental units of \( F \) are not needed any more). Writing, by Lemma 2A,

\[
\log \varepsilon_i^{p-1} = \sum_{k=1}^{u-1} \eta_k \lambda^{2bk} \pmod{\lambda^{p-1}} \quad (i = 1, \ldots, u-1),
\]

(19)

\[
\log \varepsilon_i^{p-1} = \sum_{k=1}^{u-1} \eta_k \lambda^{2bk} \pmod{\lambda^{p-1}} \quad (j = 1, \ldots, u-1)
\]

with \( s_{ik}, \lambda^{2bk} \pmod{\lambda^{p-1}} \), we have then as an analogue of (7) the congruence

\[
\det(s_{ik}) = h \det(w_{jk}) \pmod{p} \quad (i, j, k = 1, \ldots, u-1).
\]

Indeed, the analogues of (4) and (5) hold in this case, too. (See, e.g., [6].

Note that there is no ambiguity of sign when we assume the sequence of the \( e_j \) to be suitably ordered, or in case \( u = 2 \), when we assume \( e_1 > 0 \).

The numbers \( s_{ik} \) may be computed by means of (8) as follows:

\[
\log \varepsilon_j^{p-1} = \sum_{k=1}^{b-1} \log \eta_k^{p-1} = \sum_{k=1}^{b-1} \sum_{l=0}^{m-1} w_{ik} \lambda^{2bk}.
\]

Because of

\[
(1 - \lambda^{2bk}) (1 - \lambda^{2b}) \cdots (1 - \lambda^{2b(u-1)}) = -1/2b \pmod{p},
\]

we thus arrive at

**Theorem 1A.** The class number \( h_0 \) of \( K_0 \) satisfies the congruence

\[
-\frac{1}{2b} \det(\lambda^{2b(u-1)}) \sum_{n=1}^{p-2} B_{2bn} \pmod{2n(2bn)!} = h_0 \det(w_{jk}) \pmod{p}
\]

(19)

\[
(h, k = 1, \ldots, u-1), \quad \text{where the } w_{jk} \text{ are rational integers defined by (19)}.
\]

The following lemma allows one to put (20) in a slightly different form.

**Lemma 4A.** Let the rational integers \( c_{jk} \) \((j = 1, \ldots, u-1; s = 0, \ldots, p-2) \) be determined by the expansions (13), written for the fundamental units \( e_i \) of \( K_0 \). Then

\[
-(2bk)! w_{jk} = \sum_{s=0}^{b-1} c_{js} \lambda^{(2bn-s)k} \pmod{p} \quad (j, k = 1, \ldots, u-1).
\]
Proof. From (12) it can be concluded that
\[ \zeta(q'/q)(\zeta) \equiv (2b)^{-1} \sum_{n=0}^{p-2} \sum_{l=0}^{2b-1} q_{l+1} c_{q}^{q'n} (\mod p^{2-1}) \]

(applying the automorphisms \(\sigma_{q}\) to the elements on the left). The right side of this congruence is, by Lemma 3(ii), congruent \(\mod p^{2-1}\) to
\[ \sum_{n=1}^{\infty} \left( (2b-1)! \right)^{-1} \sum_{l=0}^{p-2} c_{l+1} c_{q}^{q'n} (\mod p^{2-1}) \]

On the other hand, it follows from (19) that
\[ \zeta(q'/q)(\zeta) \equiv - \sum_{n=1}^{\infty} 2b n q_{l+1} (\mod p^{2-1}) \]

This can be verified similarly, as the corresponding congruence (13) in the proof of Lemma 4. Thus Lemma 4A is seen to be true.

Remarks. As in connection with Theorem 1, we find that the determinant on the left side of (20) is not divisible by \(p\). However, Theorem 1A does not imply any result analogous to the Corollary of Theorem 1, since the analogue of (19) is
\[ h_1 \equiv (-1)^{p-q-1} \prod_{n=1}^{q} \frac{B_{(2n-1)} p^{n-1}}{(2n-1) b+1} (\mod p) \]

provided \(K\) is a proper imaginary subfield of \(F\). This congruence has been demonstrated by Carlitz [4].

The author [9] has previously derived some congruences for \(h_2\), by generalizing certain considerations in Carlitz's paper [5]. To see that these congruences agree with the present results one has to observe that the polynomial
\[ \psi(x) = p^{-1} \sum_{n=1}^{2b-2} (x x_{n-1} - x_n) x_n \]

where \(x_n\) denotes the least positive residue of \(x \mod p\), is connected with Bernoulli numbers by the congruences
\[ 2p^{2m-1} \equiv B_{2m} (x^{2m-1} - 1) \ (\mod p) \ (m = 1, \ldots, m-1) \]

(cf. [7], pp. 280–281).

In [9] it is shown that the analogue of Kummer's theorem for proper subfields \(K\) of \(F\) reads as follows: if \(h_2 = 0 (\mod p)\), then \(h_2 | h_{2k} = 0 (\mod p)\). This could also be proved as an application of Theorem 1A.

6. Application to a real quadratic field. Let \(p \equiv 1 (\mod 4)\) and choose \(a = 4\), whence \(K_0\) is the quadratic field \(Q(\sqrt{p}\)). In this case (20) reduces to
\[ B_m/m! = \psi_{11}(\mod p) \]

where \(w_{11}\) is defined by
\[ \log e^{\omega_{11}} = w_{11} \lambda_{11} (\mod p^{2-1}) \]

\(\varepsilon (1)\) being the fundamental unit of \(K_0\). Let \(T\) and \(U\) be rational integers such that \(\varepsilon = \frac{1}{2}(T + UV)\). Clearly,
\[ e^{\omega_{11}} = 1 - (U/T)V_{11} (\mod p^{2-1}) \]

and so
\[ \log e^{\omega_{11}} = -(U/T)V_{11} (\mod p^{2-1}) \]

We may compute \(V_{11}\) by the known Gaussian sum formula ([3], p. 314) and by Lemma 3(ii) as follows:
\[ V_{11} = \sum_{n=0}^{p-2} (-1)^n \sigma_n (\zeta) = \sum_{n=0}^{p-2} \frac{\lambda_{11}^{n+1}}{n+1} \sum_{n=0}^{p-2} (-1)^n \lambda_{11}^{-n} = - \frac{p^{1-m}}{m!} (\mod p^{2-1}) \]

By substituting this in (22) we thus obtain
\[ w_{11} = U/T! V_{11} (\mod p) \]

which combined with (21) yields
\[ TR_m/m! = \psi_{11} (\mod p) \]

This congruence has been discovered by Kiselev [8] and, independently, by Ankeny, Artin, and Chowla [1]. A proof for it, resembling our proof, is also sketched in [3], pp. 377–378.

References

On pairings of the first $2n$ natural numbers

by

G. B. Huff (Athens, Ga.)

Introduction. In proposing a research problem [2], Mok-Kong Shen and Tsen-Pao Shen noted that the first $2n$ positive integers may be grouped in $n$ pairs, $(a_1, b_1), (a_2, b_2), \ldots, (a_n, b_n)$, with $a_i < b_i$ and conjectured that for $n > 2$, there exists a pairing such that the $2n$ numbers $b_i + a_i$ and $b_i - a_i$ are all different. We say that a pairing of any $2n$ distinct positive integers is acceptable if these conditions are satisfied.

A program devised by Mr. James C. Fortson for an IBM 360, Model 65, has produced all acceptable pairings of $\{1, 2, \ldots, 2n\}$ for $n < 9$. The printout shows that if $A(n)$ designates the number of acceptable pairings of $\{1, 2, \ldots, 2n\}$, then $A(1) = 1$, $A(2) = 0$, $A(3) = 1$, $A(4) = 8$, $A(5) = 22$, $A(6) = 51$, $A(7) = 342$, and $A(8) = 2669$. This suggests that the difficulty in an existence proof stems from the fact that too many acceptable pairings exist for large values of $n$ and that the problem may be simplified by putting on additional conditions.

M. Slater [4] has suggested that the Shen problem be attacked by requiring that $1 \leq a_i \leq n$ and conjectured that acceptable pairings satisfying this condition exist except for $n = 2, 3$, or 6. D. A. Klamer [1] noted that the Slater conjecture is related to the “problem of the reflecting queens” and used results of M. Kratichik to construct all favorable examples for $n = 4, 5, 7$, and 8. J. D. Sebastian [3] used a computer to construct a favorable example in each of the cases $n = 9, 10, 11, \ldots, 27$.

If $K_{2n}$ is a set of $2n$ distinct integers, a pairing of $K_{2n}$ is a collection of pairs $\{(a_i, b_i) \mid i \in [1, n]\}$ such that $a_i < b_i$ for all $i$, $\{a_i, b_i\} \subset K_{2n}$, and each element of $K_{2n}$ occurs in some pair. A pairing such that each of the sets $\{b_i + a_i\}$ and $\{b_i - a_i\}$ is a complete residue system, modulo $n$, is a good candidate to be acceptable. In this paper the Shen question is given an affirmative answer by studying pairings such that

\((*)\) each of the sets $\{a_i\}, \{b_i\}, \{b_i + a_i\}, \{b_i - a_i\}$ is a complete residue system, modulo $n$, and

\((\#)\) $b_i = 2a_i$, modulo $n$. 

---

Received on 16. 2. 1973