ANNALES ACADEMIAE SCIENTIARUM FENNICAE

Series A

I. MATHEMATICA

472

A CONGRUENCE FOR THE CLASS NUMBER OF A CYCLIC FIELD

BY

TAUNO METSÄNKYLÄ

HELSINKI 1970
SUOMALAINEN TIEDEAKATEMIA

doi:10.5186/aasfm.1971.472

Communicated 9 April 1970 by K. Inkeri

KESKUSKIRJAPAINO
HELSINKI 1970

A congruence for the class number of a cyclic field

1. Introduction. Let p be an odd prime and ζ a primitive p-th root of unity. In this paper we consider the subfields of the cyclotomic field F generated by ζ over the rational number field Q.

Put $p-1=ab$ with $1 \leqq b < p-1$ and denote by K the subfield of F whose degree over Q is a. Denote further by F_0 and K_0 the maximal real subfields of F and K, respectively. Then K and K_0 are cyclic fields and, in addition, K is real $(K=K_0)$ or imaginary depending on whether b is even or odd.

Moreover, suppose that the class numbers of F and K are

$$H = H_1 H_2 , \quad h = h_1 h_2 ,$$

respectively, where the first factors H_1 and h_1 are integers (the so-called relative class numbers of F/F_0 and K/K_0) and the second factors H_2 and h_2 are the class numbers of F_0 and K_0, respectively. It is known that H_1 is divisible by h_1 and H_2 divisible by h_2 (see, e.g., [2, p. 778] and [1, p. 219]).

Denote by r a primitive root (mod p) and by r_s the least positive residue of r^s (mod p). Define

$$\psi(x) = \sum_{s=0}^{p-2} q_s x^s$$

with integral coefficients $q_s = (r r_{s-1} - r_s)/p$. Carlitz [4] has proved that

$$\prod_{n=1}^{m-1} \psi(r^{2n-1}) \equiv \pm H_2 G' \pmod{p} , \tag{1}$$

where $m = \frac{1}{2}(p-1)$ and G' is an explicitly given integer (see [4], formula (2.16); note that the symbol G' here stands for Carlitz's CG_0^{-1}). Furthermore, this congruence gives, because of a connexion between its left side and H_1, a congruence

$$H_1 \equiv \pm H_2 G \pmod{p} ,$$

where G is an integer ([4, pp. 31—33]; see (16) below). From this one can see, among other things, the well-known fact that $H_2 \equiv 0 \pmod{p}$ implies $H_1 \equiv 0 \pmod{p}$.

We shall generalize (1) as follows.

Theorem 1. *If* K *is imaginary, then*

$$\prod_{n=1}^{u-1} \psi\,(r^{2bn-1}) \equiv \pm\, h_2 G_b \pmod p\,,$$

where $u = \frac{1}{2}\,a = (p - 1)/2b$ *and* G_b *is an integer* (see (13) below).

Theorem 2. *If* K *is real, then*

$$\prod_{n=1}^{a-1} \psi\,(r^{bn-1}) \equiv \pm\, h_2 \bar{G}_b \pmod p\,,$$

where $\bar{G}_b$ *is an integer* (see (15) below).

The proofs of these theorems are similar to that of (1). For $b = 1$ we have $G_b = G'$ so that theorem 1 contains the result (1) as a special case.

The theorems express a dependence between h_2 and H_1, discussed in more detail in section 6. Here we mention the following

Corollary. *If* K *is a proper subfield of* F, *then* $h_2 \equiv 0 \pmod p$ *implies* $H_1/h_1 \equiv 0 \pmod p$.

It should be mentioned that problems associated with the divisibility of the class numbers of cyclic fields are also investigated e.g. in [9] and [10] (see also references given in these papers).

2. A preliminary lemma. Let $f'(x)$ denote the derivative of the function $f(x)$. In the following we shall write briefly $(f'/f)\,(x)$ for $f'(x)/f(x)$.

Lemma. *Denote*

$$f_w(x) = (1 - x^{r^w})\,(1 - x^{-r^w})\,, \quad g_w(x) = f_{w+1}(x)/f_w(x)\,,$$

where w *is an integer. Then*

$$\zeta(g_w'/g_w)\,(\zeta) = 2r^w \sum_{s=0}^{p-2} (q_{s-w} - t)\, \zeta^{r^s}$$

with $t = \frac{1}{2}\,(r - 1)$.

Proof (cf. [7, p. 125]). We begin with the relation

$$(1 - \zeta) \sum_{s=1}^{p-1} s\zeta^s = -\, p \tag{2}$$

that can be easily verified. From this it follows that

$$(1 + \zeta) / (1 - \zeta) = - 1 - 2p^{-1} \sum_{s=0}^{p-2} r_s \zeta^{r^s} .$$

Making the substitution $(\zeta : \zeta^{r^w})$ and applying the result to

$$\zeta(f_w'/f_w)(\zeta) = - r^w(1 + \zeta^{r^w}) / (1 - \zeta^{r^w})$$

we obtain

$$\zeta(f_w'/f_w)(\zeta) = r^w(1 + 2p^{-1} \sum_{s=0}^{p-2} r_s \zeta^{r^{w+s}}) .$$

This yields further

$$\zeta(g_w'/g_w)(\zeta) = r^w(r - 1 + 2p^{-1} \sum_{s=0}^{p-2} (r r_{s-1} - r_s)\, \zeta^{r^{w+s}})$$

so that, by definition of q_s and because of

$$\sum_{s=0}^{p-2} \zeta^{r^s} = - 1 ,$$

we have

$$\zeta(g_w'/g_w)(\zeta) = r^w(2 \sum_{s=0}^{p-2} q_s \zeta^{r^{w+s}} - (r - 1) \sum_{s=0}^{p-2} \zeta^{r^s}) .$$

From this it is seen that the assertion of the lemma is true.

3. Relation between the fundamental and circular units. Consider first the case of imaginary K. Then b is odd and a even, $a = 2u$.

Put

$$\begin{aligned} e(\zeta) &= \{\prod_{k=0}^{2b-1} (1 - \zeta^{r^{ku+1}}) / (1 - \zeta^{r^{ku}})\}^{1/2} \\ &= \{\prod_{k=0}^{b-1} g_{ku}(\zeta)\}^{1/2} , \end{aligned} \tag{3}$$

where by the exponent $\frac{1}{2}$ is meant the positive square root (for $g_{ku}(\zeta)$, see the above lemma). The numbers

$$e(\zeta^{r^i}) \quad (i = 0 , \ldots , u - 2)$$

are the circular units (Kreiseinheiten, cf. [2, p. 461] or [5, p. 23]) of K_0. We denote by Δ the regulator of this unit system, i.e.

$$\Delta = |\det (\log e(\zeta^{r^{i+n}}))| \quad (i, n = 0 , \ldots , u - 2) .$$

Let $\varepsilon_j(\zeta)$ $(j = 1 , \ldots , u - 1)$ be a system of positive fundamental units of K_0; then the regulator of K_0 is

$$R = |\det(\log \varepsilon_j(\zeta^{r^n}))| \quad (j = 1, \ldots, u-1; \ n = 0, \ldots, u-2),$$

and it is known that

$$h_2 = \Delta / R$$

(see, e.g., [2, pp. 461—462]). By writing

$$e(\zeta^{r^i}) = \prod_{j=1}^{u-1} \varepsilon_j(\zeta)^{r_{ij}} \quad (i = 0, \ldots, u-2) \tag{4}$$

where the r_{ij}'s are rational integers, we further get for h_2 an »integral» expression

$$h_2 = \pm \det(r_{ij}) \quad (i = 0, \ldots, u-2; \ j = 1, \ldots, u-1). \tag{5}$$

Now, consider (4) with a fixed i as an equation in the field F. Replace ζ by an indeterminate x and note that the equation thus received holds for $x = \zeta, \zeta^2, \ldots, \zeta^{p-1}$. Hence we have

$$e(x^{r^i}) + (1 + x + \ldots + x^{p-1})\, \Phi(x) = \prod_{j=1}^{u-1} \varepsilon_j(x)^{r_{ij}},$$

where $\Phi(x)$ is a polynomial with rational integral coefficients. After differentiating logarithmically, multiplying by x and setting $x = \zeta$ we obtain

$$r^i \zeta^{r^i} (e'/e)(\zeta^{r^i}) + M_i \sum_{s=1}^{p-1} s\zeta^s = \sum_{j=1}^{u-1} r_{ij} \zeta (\varepsilon_j'/\varepsilon_j)(\zeta) \quad (i = 0, \ldots, u-2), \tag{6}$$

where $M_i = \Phi(\zeta) / e(\zeta^{r^i})$ is an integer of F. (Cf. [8, pp. 3—4].)

The second case where K is real is fully analogous to the above case. Here, one need only replace u by $a = 2u$ everywhere in this section and, in addition, b by $\frac{1}{2}b$ in (3).

4. Proof of theorem 1. We turn back to the case where K is imaginary, and consider the equation (6).

Put $\lambda = 1 - \zeta$ and let d_i $(i = 0, \ldots, u-2)$ be rational integers such that

$$M_i \equiv d_i \pmod{\lambda}.$$

Since $p = \varepsilon\lambda^{p-1}$, where ε is a unit of F, we have by (2)

$$\sum_{s=1}^{p-1} s\zeta^s \equiv 0 \pmod{\lambda^{p-2}}.$$

Consequently

$$(7) \qquad M_i \sum_{s=1}^{p-1} s\zeta^s \equiv d_i \sum_{s=0}^{p-2} r_s \zeta^{r^s} \pmod p .$$

Making use of our lemma we infer from (3) that

$$\zeta(e'/e)(\zeta) = \sum_{k=0}^{b-1} \sum_{s=0}^{p-2} r^{ku}(q_{s-ku} - t)\, \zeta^{r^s}$$

and, further,

$$(8) \qquad \zeta^{r^i}(e'/e)(\zeta^{r^i}) = \sum_{s=0}^{p-2} \sum_{k=0}^{b-1} r^{ku}\,(q_{s-i-ku} - t)\zeta^{r^s} \quad (i = 0\,, \ldots , u-2)\,.$$

We now write

$$\zeta(\varepsilon_j'/\varepsilon_j)(\zeta) = \sum_{s=0}^{p-2} c_{js}\zeta^{r^s} \quad (j = 1\,, \ldots , u-1)\,,$$

where the c_{js}'s are rational integers, and substitute this with (7) and (8) into (6). Thus we get

$$(9) \qquad \begin{aligned} &\sum_{s=0}^{p-2} \sum_{k=0}^{b-1} r^{i+ku}(q_{s-i-ku} - t)\, \zeta^{r^s} + d_i \sum_{s=0}^{p-2} r_s \zeta^{r^s} \\ &\equiv \sum_{s=0}^{p-2} \sum_{j=1}^{u-1} r_{ij} c_{js} \zeta^{r^s} \pmod p \quad (i = 0\,, \ldots , u-2)\,. \end{aligned}$$

Comparing coefficients we can then conclude that the following rational congruences hold:

$$(10) \qquad \begin{gathered} \sum_{k=0}^{b-1} r^{i+ku}(q_{s-i-ku} - t) + d_i r_s \equiv \sum_{j=1}^{u-1} r_{ij} c_{js} \pmod p \\ (i = 0\,, \ldots , u-2\,;\ s = 0\,, \ldots , p-2)\,. \end{gathered}$$

The next step consists of multiplying both sides of (10) by $r^{(2bn-1)s}$ $(n = 1\,, \ldots , u-1)$ and summing over s. By virtue of

$$\sum_{s=0}^{p-2} r^{(2bn-1)s} \equiv 0 \pmod p\,,$$

$$\sum_{s=0}^{p-2} r_s r^{(2bn-1)s} \equiv \sum_{s=0}^{p-2} r^{2bns} \equiv 0 \pmod p$$

this yields

$$(11) \qquad \begin{gathered} \sum_{s=0}^{p-2} \sum_{k=0}^{b-1} r^{i+ku+(2bn-1)s} q_{s-i-ku} \equiv \sum_{s=0}^{p-2} \sum_{j=1}^{u-1} r_{ij} c_{js} r^{(2bn-1)s} \pmod p \\ (i = 0\,, \ldots , u-2\,;\ n = 1\,, \ldots , u-1)\,. \end{gathered}$$

Here, the double sum on the left can be written in the form

$$\sum_{k=0}^{b-1} r^{i+ku} \sum_{s=0}^{p-2} r^{(2bn-1)(s+i+ku)} q_s =$$
$$\sum_{k=0}^{b-1} r^{2bn(i+ku)} \sum_{s=0}^{p-2} r^{(2bn-1)s} q_s \equiv b r^{2bni} \psi\, (r^{2bn-1}) \pmod p .$$

Defining, in addition,

$$C_{jn} = \sum_{s=0}^{p-2} c_{js} r^{(2bn-1)s} \quad (j, n = 1, \ldots, u-1)$$

we see that (11) reduces to

$$b r^{2bni} \psi\, (r^{2bn-1}) \equiv \sum_{j=1}^{u-1} r_{ij} C_{jn} \pmod p$$
$$(i = 0, \ldots, u-2 ; \quad n = 1, \ldots, u-1) .$$

From this, using (5) and denoting

$$D = \det\, (r^{2bni}) \quad (i = 0, \ldots, u-2 ; \quad n = 1, \ldots, u-1) ,$$
$$C = \det\, (C_{jn}) \quad (j, n = 1, \ldots, u-1) ,$$

we get that

$$b^{u-1} D \prod_{n=1}^{u-1} \psi\, (r^{2bn-1}) \equiv \pm\, h_2 C \pmod p. \tag{12}$$

The determinant D, being of Vandermonde type, equals, except for sign, the product of all $r^{2bi} - r^{2bn}$, where $1 \leqq i < n \leqq u-1$. Hence $D \not\equiv 0 \pmod p$, and we may set

$$G_b \equiv b^{1-u} D^{-1} C \pmod p . \tag{13}$$

Combined with (12) this proves theorem 1.

We remark that the numbers D^{-1} and C, occurring in (13), of course depend on b, i.e., on the subfield K in question.

5. Proof of theorem 2. Let the field K be a real one. Then we see, by the final statement of section 3, that (8), and further (9) and (10) hold with b replaced by $\frac{1}{2}b$ and u replaced by a. We multiply both sides of this new (10) by $r^{(bn-1)s}$ $(n = 1, \ldots, a-1)$ and sum over s. Proceeding as in the proof of theorem 1 we finally arrive at

$$(\tfrac{1}{2}\, b)^{a-1} \bar{D} \prod_{n=1}^{a-1} \psi\, (r^{bn-1}) \equiv \pm\, h_2 \bar{C} \pmod p , \tag{14}$$

where

$$\bar{D} = \det (r^{bni}), \quad \bar{C} = \det (\bar{C}_{jn}) , \quad \bar{C}_{jn} = \sum_{s=0}^{p-2} c_{js} r^{(bn-1)s}$$

$$(i = 0 , \ldots , a - 2 ; \; j , n = 1 , \ldots , a - 1) .$$

As before, $D \not\equiv 0 \pmod p$. Thus, by setting

(15) $$\bar{G}_b \equiv 2^{a-1} b^{1-a} \bar{D}^{-1} \bar{C} \pmod p$$

we see from (14) that theorem 2 is proved.

6. Residues of H_1 and h_1 (mod p). As is well-known,

$$H_1 = (-1)^m 2p \prod_{n=1}^{m} (2p)^{-1} \sum_{s=0}^{p-2} r_s Z^{(2n-1)s} ,$$

where Z is a primitive $(p-1)$-th root of unity. (See, e.g., [5] or [6, pp. 377,430]. In the literature the expression of H_1, as regards the sign, is frequently incorrect.) Furthermore, if K is a proper imaginary subfield of F , then

$$h_1 = (-1)^u 2 \prod_{n=1}^{u} (2p)^{-1} \sum_{s=0}^{p-2} r_s Z^{(2n-1)bs}$$

(see, e.g., [2, pp. 461,776]).

Assume now that r is a primitive root (mod p^2) so that $r^m + 1$ is divisible by p but not by p^2. When studying the residues of H_1 and h_1 (mod p) one has to observe that

$$(rZ^v - 1) \, p^{-1} \sum_{s=0}^{p-2} r_s Z^{vs} \equiv \psi (r^v) \pmod{\mathfrak{p}} ,$$

where v is any integer and $\mathfrak{p}$ a prime ideal factor of p in the $(p-1)$-th cyclotomic field $Q(Z)$. From this it can be easily deduced that

$$H_1 \equiv 2^{1-m} p (r^m + 1)^{-1} \prod_{n=1}^{m} \psi (r^{2n-1}) \pmod p ,$$

and further, as shown in [4, p. 32],

(16) $$H_1 \equiv - 2^{2-m} \prod_{n=1}^{m-1} \psi (r^{2n-1}) \pmod p .$$

Analogously, we find that

(17) $$h_1 \equiv 2^{1-u} (r^u + 1)^{-1} \prod_{n=1}^{u} \psi (r^{(2n-1)b}) \pmod p$$

and

(18) $$H_1 / h_1 \equiv - 2^{u-m+1} (r^u + 1) \prod_{n} \psi (r^{2n-1}) \pmod p ,$$

where the last product contains those $\psi(r^{2n-1})$ from (16) that do not occur in (17).

Now h_2, the class number of K_0, is by theorem 1 related with the product of those $\psi(r^{2n-1})$ from (16) where $2n - 1$ is of the form $2bn_1 - 1$ $(n_1 = 1, \ldots, u - 1)$. Since these $\psi(r^{2n-1})$ occur also on the right side of (18), we see that our corollary is true in the case of imaginary K.

On the other hand, if K is real, then $h_1 = 1$ and, by (16) and theorem 2, $h_2 \equiv 0 \pmod p$ implies $H_1 \equiv 0 \pmod p$, so that the corollary is proved also in this case. — Note that the latter case is trivial in view of the previously known facts about class numbers, mentioned in section 1. Indeed, if h_2 is divisible by p, then so is H_2 and hence also H_1.

We finally recall that, for $n = 1, \ldots, m - 1$, $\psi(r^{2n-1}) \equiv 0 \pmod p$ if and only if $B_{2n} \equiv 0 \pmod p$, where the B_i's are the Bernoulli numbers in the even suffix notation (see [6, pp. 431—432]). This together with (16) gives the known criterion, due to Kummer [7], for the divisibility of H_1 by p. It is seen from (17) that an analogous criterion for h_1 reads as follows: h_1 is divisible by p if and only if the numerator of at least one of the Bernoulli numbers $B_{(2n-1)b+1}$ $(n = 1, \ldots, u)$ is divisible by p. (Another proof for this is presented by Carlitz in [3].) Moreover, applying theorems 1 and 2 we find that if h_2 is divisible by p, then so is the numerator of at least one B_{2bn} $(n = 1, \ldots, u - 1)$ or B_{bn} $(n = 1, \ldots, a - 1)$ according to whether K is imaginary or real.

University of Turku
Turku, Finland

References

[1] Ankeny, N. C., Chowla, S., and Hasse, H.: On the class number of the maximal real subfield of a cyclotomic field. — J. Reine Angew. Math. 217 (1965), 217—220.

[2] Beeger, N. G. W. H.: Über die Teilkörper des Kreiskörpers $K(e^{2\pi i/l^h})$. — Proc. Akad. Wet. Amsterdam 21 (1919), 454—465, 758—779.

[3] Carlitz, L.: The first factor of the class number of a cyclic field. — Canad. J. Math. 6 (1954), 23—26.

[4] —»— A congruence for the second factor of the class number of a cyclotomic field. — Acta Arith. 14 (1968), 27—34.

[5] Hasse, H.: Über die Klassenzahl abelscher Zahlkörper. Berlin (1952).

[6] Hilbert, D.: Theorie der algebraischen Zahlkörper. — Jber. Deutsch. Math.-Verein. 4 (1897).

[7] Kummer, E.: Zwei besondere Untersuchungen über die Classen-Anzahl und über die Einheiten der aus λ-ten Wurzeln der Einheit gebildeten complexen Zahlen. — J. Reine Angew. Math. 40 (1850), 117—129.

[8] Metsänkylä, T.: Congruences modulo 2 for class number factors in cyclotomic fields. — Ann. Acad. Sci. Fenn., Ser. A I 453 (1969).

[9] Yokoi, H.: On the class number of a relatively cyclic number field. — Nagoya Math. J. 29 (1967), 31—44.

[10] Yokoyama, A.: On the relative class number of finite algebraic number fields. — J. Math. Soc. Japan. 16 (1967), 179—184.

Printed July 1970