ACTA ARITHMETICA
XIV (1968)

A congruence for the second factor of the class number of a cyclotomic field*

by

L. Carlitz (Durham, North Carolina)

1. Let $\zeta = e^{2\pi i/p}$, where p is a prime >3. Put $K = Q(\zeta)$, the cyclotomic field generated by ζ. If h denotes the class number of K, it is familiar that $h = h_1 h_2$, where

(1.1) $$h_1 = (2p)^{-(p-3)/2}\varphi(\beta)\varphi(\beta^3)\ldots\varphi(\beta^{p-2});$$

β is a primitive root of $x^{p-1}=1$ and

$$\varphi(\beta) = 1+g_1\beta+g_2\beta^2+\ldots+g_{p-2}\beta^{p-2},$$

where g denotes a fixed primitive root $(\operatorname{mod} p)$ and g_s is the least positive residue of $g^s\,(\operatorname{mod} p)$.

To define h_2 let $\varepsilon_1, \varepsilon_2, \ldots, \varepsilon_{m-1}$, where $p = 2m+1$, denote a fundamental set of units of K; it is well known that we may assume that the ε_s are real and positive. Next define the real positive unit

(1.2) $$e(\zeta) = \left\{\frac{(1-\zeta^g)(1-\zeta^{-g})}{(1-\zeta)(1-\zeta^{-1})}\right\}^{1/2};$$

then the units

$$e(\zeta),\ e(\zeta^g),\ \ldots,\ e(\zeta^{g^{m-2}})$$

are independent. Put

$$\Delta = |\log e(\zeta^{g^{r+s}})| \quad (r, s = 0, 1, \ldots, m-2)$$

and

$$R = |\log \varepsilon_r(\zeta^{g^s})| \quad (r, s = 0, 1, \ldots, m-2).$$

Then

(1.3) $$h_2 = |\Delta/R|.$$

* Supported in part by NSF grant GP-5174.

It is known that h_1 is divisible by p if and only if p divides the numerator of at least one of the Bernoulli numbers (in the even suffix notation)

$$B_2, B_4, \ldots, B_{p-3}.$$

Vandiver [2] has proved that

$$h_1 \equiv 2^{-m+1} p \prod_{s=1}^{m} B_{(2s-1)p^a+1} \pmod{p^a}, \tag{1.4}$$

where a is an arbitrary positive integer. Hasse [1] has recently given another proof of (1.4). Also it is well known that h_2 is divisible by p if and only if h_1 is divisible by p. For references see [3].

In the present note we show that

$$h_2 G \equiv h_1 \pmod{p}, \tag{1.5}$$

where G is a rational integer depending only on p. For the explicit definition see (3.9) below.

2. We shall use the fuller notation

$$\varepsilon_1(\zeta),\ \varepsilon_2(\zeta),\ \ldots,\ \varepsilon_{m-1}(\zeta) \qquad (p = 2m+1) \tag{2.1}$$

for a fundamental system of units; as above we assume that the units are real and positive. Since $e(\zeta)$ as defined by (1.2) is real and positive we may write

$$e(\zeta) = \varepsilon_1(\zeta)^{r_1} \varepsilon_2(\zeta)^{r_2} \ldots \varepsilon_{m-1}(\zeta)^{r_{m-1}}, \tag{2.2}$$

where the r_j are rational integers. Since (2.2) holds for ζ and all its conjugates we have

$$x^p e(x) + (1+x+x^2+\ldots+x^{p-1}) f(x) = \varepsilon_1(x)^{r_1} \varepsilon_2(x)^{r_2} \ldots \varepsilon_{m-1}(x)^{r_{m-1}},$$

where x is an indeterminate and $f(x)$ is a polynomial with rational integral coefficients. Differentiate logarithmically, multiply by x and then put $x = \zeta$. We get

$$\zeta \frac{e'(\zeta)}{e(\zeta)} + M\left(\zeta + 2\zeta^2 + \ldots + (p-1)\zeta^{p-1}\right) \equiv r_1 \zeta \frac{\varepsilon_1'(\zeta)}{\varepsilon_1(\zeta)} + r_2 \zeta \frac{\varepsilon_2'(\zeta)}{\varepsilon_2(\zeta)} + \ldots + r_{m-1} \zeta \frac{\varepsilon_{m-1}'(\zeta)}{\varepsilon_{m-1}(\zeta)} \pmod{p}, \tag{2.3}$$

where

$$M = f(\zeta)/e(\zeta).$$

Kummer showed that

$$\zeta \frac{e'(\zeta)}{e(\zeta)} = \frac{1}{2}(g-1) + \sum_{s=0}^{p-2} b_s \zeta^{g^s}, \tag{2.4}$$

where

$$b_s = (g g_{s-1} - g_s)/p \qquad (s = 0, 1, \ldots, p-2). \tag{2.5}$$

Since

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

(2.4) becomes

$$\zeta \frac{e'(\zeta)}{e(\zeta)} = \sum_{s=0}^{p-2} \left(b_s - \frac{g-1}{2}\right) \zeta^{g^s}. \tag{2.6}$$

It follows that

$$\zeta^{g^j} \frac{e'(\zeta^{g^j})}{e(\zeta^{g^j})} = \sum_{s=0}^{p-2} \left(b_{s-j} - \frac{g-1}{2}\right) \zeta^{g^s} \qquad (j = 0, 1, \ldots, m-2), \tag{2.7}$$

where $b_s = b_{s+p-1}$.

In place of (2.2) we now take

$$e(\zeta^{g^j}) = \varepsilon_1(\zeta)^{r_{j1}} \varepsilon_2(\zeta)^{r_{j2}} \ldots \varepsilon_{m-1}(\zeta)^{r_{j,m-1}} \qquad (j = 0, 1, \ldots, m-2); \tag{2.8}$$

then (2.3) becomes

$$\zeta^{g^j} \frac{e'(\zeta^{g^j})}{e(\zeta^{g^j})} + M_j \sum_{s=0}^{p-2} g_s \zeta^{g^{j+s}} \equiv \sum_{k=1}^{m-1} r_{jk} \zeta^g \frac{\varepsilon_k'(\zeta)}{\varepsilon_k(\zeta)} \pmod{p} \qquad (j = 0, 1, \ldots, m-2), \tag{2.9}$$

where M_j is an integer of K.

We now put

$$\zeta \frac{\varepsilon_k'(\zeta)}{\varepsilon_k(\zeta)} = \sum_{s=0}^{p-2} c_{ks} \zeta^{g^s} \qquad (k = 1, 2, \ldots, m-1), \tag{2.10}$$

where the c_{ks} are rational integers.

We recall that

$$(p) = (1-\zeta)^{p-1};$$

also since

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

it follows that

$$(1-\zeta)^{p-2} \Big| \sum_{s=0}^{p-2} g_s \zeta^{g^s}. \tag{2.11}$$

Hence if we put

$$M_j \equiv d_j \pmod{1-\zeta},$$

where d_j is a rational integer, if follows from (2.7), (2.8), (2.10) and (2.11) that

$$\sum_{s=0}^{p-2}\left(b_{s-j}-\frac{g-1}{2}\right)\zeta^{g^s}+d_j\sum_{s=0}^{p-2} g^{s-j}\zeta^{g^s} \equiv \sum_{k=1}^{m-1} r_{jk}\sum_{s=0}^{p-2} c_{ks}\zeta^{g^s} \pmod{p}$$
$$(j=0,1,\ldots,m-2).$$

Comparing coefficients we get

$$b_{s-j}-\tfrac{1}{2}(g-1)+d_j g^{s-j} \equiv \sum_{k=1}^{m-1} r_{jk} c_{ks} \pmod{p} \tag{2.12}$$
$$(j=0,1,\ldots,m-j;\ s=0,1,\ldots,p-2).$$

If we multiply both sides of (2.12) by $g^{(2n-1)s}$ and sum over s we get

$$g^{(2n-1)j}\sum_{s=0}^{p-2} b_s g^{(2n-1)s}-\tfrac{1}{2}(g-1)\sum_{s=0}^{p-2} g^{(2n-1)s}+d_j g^{-j}\sum_{s=0}^{p-2} g^{2ns} \tag{2.13}$$
$$\equiv \sum_{k=1}^{m-1} r_{jk}\sum_{s=0}^{p-2} c_{ks} g^{(2n-1)s} \pmod{p} \qquad (n=1,2,\ldots,m-1).$$

Since

$$\sum_{s=0}^{p-2} g^{(2n-1)s} \equiv \sum_{s=0}^{p-2} g^{2ns} \equiv 0 \pmod{p} \qquad (n=1,2,\ldots,m-1),$$

(2.13) reduces to

$$g^{(2n-1)j}\sum_{s=0}^{p-2} b_s g^{(2n-1)s} \equiv \sum_{k=1}^{m-1} r_{jk}\sum_{s=0}^{p-2} c_{ks} g^{(2n-1)s} \pmod{p} \tag{2.14}$$
$$(n=1,2,\ldots,m-1).$$

Now put

$$C_{kn}=\sum_{s=0}^{p-2} c_k g^{(2n-1)s} \qquad (k,n=1,2,\ldots,m-1), \tag{2.15}$$

so that (2.14) becomes

$$g^{(2n-1)j}\sum_{s=0}^{p-2} b_s g^{(2n-1)s} \equiv \sum_{k=1}^{m-1} r_{jk} C_{kn} \pmod{p}$$
$$(j=0,1,\ldots,m-2;\ n=1,2,\ldots,m-1).$$

It follows that

$$G_0\prod_{n=1}^{m-1}\sum_{s=0}^{p-2} b_s g^{(2n-1)s} \equiv |r_{jk}|\cdot C \pmod{p}, \tag{2.16}$$

where

$$G_0=|g^{(2n-1)j}| \qquad (j=0,1,\ldots,m-2;\ n=1,2,\ldots,m-1) \tag{2.17}$$

and

$$C=|C_{kn}| \qquad (k,n=1,2,\ldots,m-1). \tag{2.18}$$

Moreover, by (2.8), we have

$$h_2=|r_{jk}| \qquad (j=0,1,\ldots,m-2;\ k=1,2,\ldots,m-1). \tag{2.19}$$

3. Returning to (1.1) we have

$$(g\beta-1)\varphi(\beta)=p\psi(\beta), \tag{3.1}$$

where

$$\psi(\beta)=\sum_{s=0}^{p-2} b_s\beta^s \tag{3.2}$$

and b_s is defined by (2.5). Thus

$$(g\beta^{2n-1}-1)\varphi(\beta^{2n-1})=p\psi(\beta^{2n-1}).$$

Since

$$\prod_{n=1}^{m}(1-\beta^{2n-1}x)=1+x^m,$$

we get

$$(-1)^m(g^m+1)\prod_{n=1}^{m}\varphi(\beta^{2n-1})=p^m\prod_{n=1}^{m}\psi(\beta^{2n-1}). \tag{3.3}$$

We assume in what follows that g is a primitive root $(\bmod p^2)$, so that g^m+1 is divisible by p but not by p^2. Substituting from (3.3) in (1.1) we accordingly get

$$h_1=(-1)^m 2^{m+1}\frac{p}{g^m+1}\prod_{n=1}^{m}\psi(\beta^{2n-1}). \tag{3.4}$$

In the next place, in the cyclotomic field $Q(\beta)$ the principal ideal (p) is a product of $\varphi(p-1)$ prime ideals of the first degree:

$$(p) = \prod_{\substack{k=1\\(k,m-1)=1}}^{m-1} (p, \beta - g^k).$$

If we put $\mathfrak{p} = (p, \beta - g)$ it follows that

$$\beta \equiv g \pmod{\mathfrak{p}}$$

and therefore

$$\psi(\beta^{2n-1}) \equiv \psi(g^{2n-1}) \pmod{\mathfrak{p}}.$$

Hence (3.4) implies

$$h_1 \equiv (-1)^m 2^{m+1} \frac{p}{g^m+1} \prod_{n=1}^{m} \psi(g^{2n-1}) \pmod{p}. \tag{3.5}$$

The modulus is p rather than $\mathfrak{p}$ since both sides of (3.5) are rational integers.

For $n = m$ we have by (3.2) and (2.5)

$$p\psi(g^{2m-1}) = \sum_{s=0}^{p-2} (gg_{s-1} - g_s) g^{s(p-2)}.$$

Since $gg_{s-1} - g_s \equiv 0 \pmod{p}$, it follows that

$$\begin{aligned} p\psi(g^{2m-1}) &\equiv \sum_{s=0}^{p-2} (gg_{s-1} - g_s) g^{-s} \equiv \sum_{s=0}^{p-2} g^{-s+1} g_{s-1} - \sum_{s=0}^{p-2} g^{-s} g_s \\ &\equiv gg_{-1} - g^{-p+2} g_{p-2} \equiv (g - g^{-p+2}) g_{p-2} \\ &\equiv g^{-p+2}(g^{p-1}-1) g_{p-2} \equiv g^{p-1} - 1 \pmod{p^2} \end{aligned}$$

and therefore

$$\psi(g^{2m-1}) \equiv \frac{1}{p}(g^{p-1}-1) \pmod{p}. \tag{3.6}$$

Thus (3.5) reduces to

$$h_1 \equiv (-1)^m 2^{m+1} (g^m - 1) \prod_{n=1}^{m-1} \psi(g^{2n-1}) \pmod{p},$$

that is

$$h_1 \equiv (-1)^{m+1} 2^{m+2} \prod_{n=1}^{m-1} \psi(g^{2n-1}) \pmod{p}. \tag{3.7}$$

Comparing (3.7) with (2.16) we get

$$(-1)^{m+1} 2^{m+2} h_2 C \equiv \pm h_1 G_0 \pmod{p}, \tag{3.8}$$

with G_0, C defined by (2.17) and (2.18). Hence if we put

$$G \equiv (-1)^{m+1} 2^{m+2} G_0^{-1} C \pmod{p}, \tag{3.9}$$

we have

$$h_2 G \equiv \pm h_1 \pmod{p}. \tag{3.10}$$

In view of (1.3), the ambiguity of sign in (3.8) and (3.10) is unavoidable.

Since by (2.17)

$$G_0 \equiv \prod_{1 \leqslant j < k < m} (g^{2k-1} - g^{2j-1}) \pmod{p}, \tag{3.11}$$

it is clear that $G_0 \not\equiv 0 \pmod{p}$. If we put

$$G_1 \equiv \prod_{1 \leqslant j < k < m} (g^{2k-1} - g^{2j-1}) \pmod{p}, \tag{3.12}$$

then, except for sign, G_1 is congruent to the difference product of the quadratic nonresidues of p; hence G_1 is independent of g. Comparing (3.11) and (3.12) we have

$$G_1 \equiv G_0 \prod_{j=1}^{m-1} (g^{2m-1} - g^{2j-1}).$$

Now

$$\prod_{j=1}^{m-1} (g^{2m-1} - g^{2j-1}) \equiv \prod_{j=1}^{m-1} (g^{-1} - g^{2j-1}) \equiv g^{-m+1} \prod_{j=1}^{m-1} (1 - g^{2j}) \equiv -g \prod_{j=1}^{m-1} (1 - g^{2j});$$

since

$$\prod_{j=0}^{m-1} (x - g^{2j}) \equiv x^m - 1,$$

it follows that

$$\prod_{j=1}^{m-1} (1 - g^{2j}) \equiv m \equiv -\tfrac{1}{2}.$$

We have therefore

$$G_1 \equiv \tfrac{1}{2} g G_0 \pmod{p}. \tag{3.13}$$

4. It is of some interest to show directly that G in (3.8) is independent of the particular fundamental system of units. Let

$$\eta_j(\zeta) \quad (j = 1, 2, \ldots, m-1)$$

denote an arbitrary fundamental system of real positive units. Then we have

$$\eta_j(\zeta) = \varepsilon_1(\zeta)^{a_{j1}} \varepsilon_2(\zeta)^{a_{j2}} \ldots \varepsilon_{m-1}(\zeta)^{a_{j,m-1}} \quad (j = 1, 2, \ldots, m-1).$$

Exactly as above this implies

$$\eta_j(x) = \varepsilon_1(x)^{a_{j1}}\varepsilon_2(x)^{a_{j2}}\ldots\varepsilon_{m-1}(x)^{a_{j,m-1}}+(1+x+\ldots+x^{p-1})f_j(x),$$

where $f_j(x)$ is a polynomial with rational integral coefficients and the determinant $|a_{jk}| = \pm 1$. This implies

$$(4.1)\qquad \zeta\frac{\eta_j'(\zeta)}{\eta_j(\zeta)} = \sum_{k=1}^{m-1} a_{jk}\zeta\frac{\varepsilon_k'(\zeta)}{\varepsilon_k(\zeta)} + M_j(\zeta+2\zeta^2+\ldots+(p-1)\zeta^{p-1}).$$

Now put

$$\zeta\frac{\eta_j'(\zeta)}{\eta_j(\zeta)} = \sum_{s=0}^{p-1} c_{js}'\zeta^{p^s}\qquad (j = 1, 2, \ldots, m-1).$$

Then by (4.1) and (2.10) we have

$$(4.2)\qquad c_{js}' \equiv \sum_{k=1}^{m-1} a_{jk}e_{js}+d_jg^s \pmod p$$

$$(j = 1, \ldots, m-1;\ g = 0, 1, \ldots, p-2).$$

Multiplying both sides of (4.2) by $g^{(2n-1)s}$ and summing over s we get

$$(4.3)\qquad C_{jn}' \equiv \sum_{k=1}^{m-1} a_{jk}C_{kn} \pmod p,$$

where

$$C_{jn}' = \sum_{s=0}^{p-2} c_{js}'g^{(2n-1)s}.$$

It follows at once from (4.3) that

$$(4.4)\qquad C' = |C_{jn}'| \equiv \pm C \pmod p.$$

References

[1] H. Hasse, *Vandiver's congruence for the relative class number of the p-th cyclotomic field*, J. of Mathematical Analysis and Applications 15 (1966), pp. 87-90.

[2] H. S. Vandiver, *On the first factor of the class number of a cyclotomic field*, Bulletin of the American Mathematical Society 25 (1919), pp. 458-461.

[3] — and G. E. Wahlin, *Algebraic numbers II*, Report of the Committee on Algebraic Numbers, Washington 1928.

Reçu par la Rédaction le 10. 4. 1967

ACTA ARITHMETICA
XIV (1968)

L-functions and character sums for quadratic forms (I)

by

H. M. Stark (Ann Arbor, Mich.)

1. Let $Q(x)$ be a positive definite quadratic form in n variables $x = (x_1, x_2, \ldots, x_n)$ with integral coefficients, and let χ be a character $(\bmod k)$. We define

$$(1)\qquad L(s, \chi, Q) = \frac{1}{2}\sum_{x\neq 0}\chi(Q(x))Q(x)^{-s},$$

the series converges to an analytic function if $\operatorname{Re} s > n/2$. This generalization of the Epstein zeta function has been, in the case of binary quadratic forms, closely related to class-number problems for the last thirty years. Recently [5], a rapidly convergent expansion of $L(s, \chi, Q)$ at $s = 1$ was derived for a particular positive definite binary quadratic form with the real character $\chi(j) = \left(\frac{k}{j}\right)$, $k = 8$ and 12. On the basis of this expansion it was shown in [5] that the number of classes of binary quadratic forms of discriminant < -163 is greater than one. Still, the functions $L(s, \chi, Q)$ have not been sufficiently studied for their own sake. Even in [5], since only two different L-functions were studied with the corresponding characters having relatively small moduli (8 and 12), arithmetic was sometimes able to take the place of a general theory. In this paper, we introduce a general L-function for positive definite quadratic forms in n variables. Under certain restrictions, $L(s, \chi, Q)$ can be extended to an entire function in the complex s plane which satisfies a functional equation. In this paper we derive that functional equation and the character identity on which it depends. In [6], we will show how an alternate form of our character identity leads, in general, to an expansion of $L(s, \chi, Q)$ at $s = 1$ similar to that in [5], but with the arithmetic eliminated. Much of the difficulty in the following comes from allowing k to be even; but if we wish to apply these results to [5], it is clear that we must put up with the extra difficulty.