# THE FIRST FACTOR OF THE CLASS NUMBER OF A CYCLIC FIELD

LEONARD CARLITZ

**1. Introduction.** Let $p$ be a fixed prime $> 3$. The first factor of the field $R(\zeta)$, where $R$ is the rational field and $\zeta = e^{2\pi i/p}$, is determined by means of

$$h = (2p)^{-\frac{1}{2}(p-3)} f(Z) f(Z^3) \ldots f(Z^{p-2}), \tag{1.1}$$

where

$$f(x) = r_0 + r_1 x + r_2 x^2 + \ldots + r_{p-2} x^{p-2},$$

$Z = e^{2\pi i/(p-1)}$, $r$ is a primitive root (mod $p$), and $r_i$ is the least positive residue of $r^i$ (mod $p$). Vandiver **(4)** has proved that if $n$ is an arbitrary integer $\geqslant 1$, then

$$h \equiv 2^{-\frac{1}{2}(p-3)} p \prod_s B_{sp^n+1} \pmod{p^n}, \tag{1.2}$$

where $s = 1, 3, \ldots, p-2$, and the $B_m$ are the Bernoulli numbers in the even suffix notation.

Let $p - 1 = ab$, where $b$ is odd and greater than 1. Consider the cyclic field $K \subset R(\zeta)$ of degree $a$ over $R$. The class number of $K$ can be expressed in the form $h_a \cdot \Delta/R$, where **(1**, p. 332**)**

$$h_a = 2^{-\frac{1}{2}(a-2)} p^{-\frac{1}{2}a} \prod_u f(Z^{bu}), \tag{1.3}$$

where $u = 1, 3, \ldots, a-1$, and $f(x)$ and $Z$ have the same meaning as in (1.1). The numbers $h_a$ and $\Delta/R$ are the first and second factors, respectively, of the class number of $K$; since the second factor is not used below we omit the precise description of this number. Beeger **(2)** has proved that $h_a$ is a rational integer. In the present note we prove the formula

$$h_a \equiv 2^{-\frac{1}{2}(a-2)} \prod_u B_{bup^n+1} \pmod{p^n}, \quad n \geqslant 1, \tag{1.4}$$

where $u = 1, 3, \ldots, a-1$. The proof is similar to that of (1.2). Note that (1.3) does not include (1.1); also for $b > 1$, (1.4) does not reduce to (1.2).

**2. Proof of** (1.4). As in **(4)**, let

$$\mathfrak{p} = (Z - r, p) \tag{2.1}$$

denote one of the prime ideal factors of $(p)$ in the field $R(Z)$. Then for arbitrary $k$, $m$ we have

$$Z^{kp^m} \equiv r^{kp^m} \quad (\mathfrak{p}^{m+1}),$$

so that

Received December 19, 1952.

$$f(Z^k) = f(Z^{kp^m}) \equiv f(r^{kp^m}) \qquad (\mathfrak{p}^{m+1}). \tag{2.2}$$

Thus by (1.3) and (2.2)

$$p^{\frac{1}{2}a}h_a \equiv 2^{-\frac{1}{2}(a-2)} \prod_u f(r^{bup^m}) \qquad (\text{mod } p^{m+1}), \tag{2.3}$$

where $u = 1, 3, \ldots, a - 1$.

Now take $m = n + \frac{1}{2}a$, and (2.3) becomes

$$h_a \equiv 2^{-\frac{1}{2}(a-2)} p^{-\frac{1}{2}a} \prod_u f(r^{bup^m}) \qquad (\text{mod } p^{n+1}).$$

Since by Fermat's theorem

$$r^{kp^m} \equiv r^{kp^n} \qquad (\text{mod } p^{n+1}),$$

it follows that

$$h_a \equiv 2^{-\frac{1}{2}(a-2)} p^{-\frac{1}{2}a} \prod_u f(r^{bup^n}) \qquad (\text{mod } p^n). \tag{2.4}$$

In the next place, it follows from $r^i \equiv r_i \pmod p$ that

$$r^{ikp^n} \equiv r_i^{kp^n} \qquad (\text{mod } p^{n+1}),$$

so that

$$f(r^{bup^n}) = \sum_{i=0}^{p-2} r_i r^{ibup^n} \equiv \sum_{i=0}^{p-2} r_i^{bup^n+1} \qquad (\text{mod } p^{n+1}). \tag{2.5}$$

But since the numbers $r_0, r_i, \ldots, r_{p-2}$ are a permutation of the numbers $1, 2, \ldots, p - 1$, it is clear that (2.5) is the same as

$$f(r^{bup^n}) \equiv \sum_{k=1}^{p-1} k^{bup^n+1} \qquad (\text{mod } p^{n+1}). \tag{2.6}$$

Now using the well-known formula

$$\sum_{k=1}^{p-1} k^m = \frac{B_{m+1}(p) - B_{m+1}}{m+1},$$

where $B_{m+1}(x)$ denotes the Bernoulli polynomial of degree $m + 1$, it follows easily that

$$f(r^{bup^n}) \equiv pB_{bup^n+1} \qquad (\text{mod } p^{n+2}). \tag{2.7}$$

Substituting from (2.7) in (2.4) we get

$$h_a \equiv 2^{-\frac{1}{2}(a-2)} \prod_u B_{bup^n+1} \qquad (\text{mod } p^n),$$

which is the same as (1.4).

**3. Some special cases.** If we take $n = 1$, (1.4) becomes

$$h_a \equiv 2^{-\frac{1}{2}(a-2)} \prod_u B_{bup+1} \qquad (\text{mod } p). \tag{3.1}$$

But by Kummer's congruence (**3**, chap. 14)

$$\frac{B_{bup+1}}{bup+1} \equiv \frac{B_{bu+1}}{bu+1} \qquad (\text{mod } p), \tag{3.2}$$

so that (3.1) reduces to

https://doi.org/10.4153/CJM-1954-003-1 Published online by Cambridge University Press

$$(3.3) \qquad h_a \equiv 2^{-\frac{1}{2}(a-2)} \prod_u \frac{B_{bu+1}}{bu+1} \pmod{p}.$$

It follows at once from (3.3) that *the first factor of the class number of $K$ is divisible by $p$ if and only if the numerator of at least one of the numbers*

$$B_{bu+1} \qquad (u = 1, 3, \ldots, a-1)$$

*is divisible by $p$.*

Let $p \equiv 3 \pmod 4$, $a = 2$, $b = \frac{1}{2}(p-1)$. Thus $K$ is the quadratic field $R((-p)^{\frac{1}{2}})$. Since the class number of $K$ is now determined by

$$(3.4) \qquad h = -\frac{1}{p}\sum_{k=1}^{p-1} k\left(\frac{k}{p}\right),$$

where $(k/p)$ is the Legendre symbol, comparison of (3.4) with (1.3) shows that in this case $h_2 = -h$. Also we see at once that (1.4) reduces to

$$(3.5) \qquad h \equiv -B_{\frac{1}{2}(p-1)p^n+1} \pmod{p^n}.$$

In particular (3.5) includes the well-known formula

$$(3.6) \qquad h \equiv -2B_{\frac{1}{2}(p+1)} \pmod{p}.$$

(Since $1 \leqslant h < p$, it is clear that $B_{\frac{1}{2}(p+1)} \not\equiv 0 \pmod{p}$; indeed this is a consequence of the fact that $\frac{1}{2}(p-1)$ is odd, as is evident from (3.7).)

Again, in place of (3.4) let us use

$$(3.7) \qquad h = \left\{2 - \left(\frac{2}{p}\right)\right\}^{-1} \sum_{k=1}^{\frac{1}{2}(p-1)} \left(\frac{k}{p}\right).$$

Since it follows from

$$k^{\frac{1}{2}(p-1)} \equiv \left(\frac{k}{p}\right) \pmod{p}$$

that

$$k^{\frac{1}{2}(p-1)p^n} \equiv \left(\frac{k}{p}\right) \pmod{p^{n+1}},$$

it is evident that (3.7) implies

$$(3.8) \quad h \equiv \left\{2 - \left(\frac{2}{p}\right)\right\}^{-1} \sum_{k=1}^{\frac{1}{2}(p-1)} k^{\frac{1}{2}(p-1)p^n} \equiv \left\{2 - \left(\frac{2}{p}\right)\right\}^{-1} \frac{B_m(\frac{1}{2}(p+1)) - B_m}{m} \pmod{p^{n+1}},$$

where $m = \frac{1}{2}(p-1)p^n + 1$. Using the formula

$$B_m(\tfrac{1}{2}p) + B_m(\tfrac{1}{2}p + \tfrac{1}{2}) = 2^{1-m}B_m(p),$$

we get

$$B_m(\tfrac{1}{2}(p+1)) \equiv 2^{1-m}B_m - B_m \equiv \left\{\left(\frac{2}{p}\right) - 1\right\} B_m \pmod{p^{n+1}},$$

so that (3.8) yields

$$(3.9) \qquad h \equiv -\frac{B_m}{m} \equiv -\frac{B_m}{1 - \frac{1}{2}p^n} \pmod{p^{n+1}}.$$

https://doi.org/10.4153/CJM-1954-003-1 Published online by Cambridge University Press

It can be shown, using Kummer's congruence, that (3.5) implies (3.9); also for $n = 0$, (3.9) is identical with (3.6).

## References


1. N. G. W. H. Beeger, *Over de deelichamen van het cirkellichaam der $l^h$-de machtswortels uit de eenheid en hunne klassenaantallen* (1ste gedeelte), Konink. Akad. Wet. Amsterdam, *27* (1918), 324–336.
2. ———, *Over de deelichamen van het cirkellichaam der $l^h$-de machtswortels uit de eenheid en hunne klassenaantallen* (3de gedeelte), Konink. Akad. Wet. Amsterdam, *27* (1918), 822–827.
3. N. Nielsen, *Traité élémentaire des nombres de Bernoulli* (Paris, 1924).
4. H. S. Vandiver, *On the first factor of the class number of a cyclotomic field*, Bull. Amer. Math. Soc., *25* (1918–19), 458–461.


*Duke University*

https://doi.org/10.4153/CJM-1954-003-1 Published online by Cambridge University Press