TRANSACTIONS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 288, Number 1, March 1985

# A RECIPROCITY LAW FOR POLYNOMIALS WITH BERNOULLI COEFFICIENTS

BY

WILLEM FOUCHÉ

ABSTRACT. We study the zeros (mod $p$) of the polynomial $\beta_p(X) = \sum_k (B_k/k)(X^{p-1-k} - 1)$ for $p$ an odd prime, where $B_k$ denotes the $k$th Bernoulli number and the summation extends over $1 \leqslant k \leqslant p-2$. We establish a reciprocity law which relates the congruence $\beta_p(r) \equiv 0 \pmod p$ to a congruence $f_p(n) \equiv 0 \pmod r$ for $r$ a prime less than $p$ and $n \in \mathbf{Z}$. The polynomial $f_p(x)$ is the irreducible polynomial over $\mathbf{Q}$ of the number $\mathrm{Tr}_L^{\mathbf{Q}(\zeta)} \zeta$, where $\zeta$ is a primitive $p^2$th root of unity and $L \subset \mathbf{Q}(\zeta)$ is the extension of degree $p$ over $\mathbf{Q}$. These congruences are closely related to the prime divisors of the indices $I(\alpha) = (\mathcal{O} : \mathbf{Z}[\alpha])$, where $\mathcal{O}$ is the integral closure in $L$ and $\alpha \in \mathcal{O}$ is of degree $p$ over $\mathbf{Q}$. We establish congruences (mod $p$) involving the numbers $I(\alpha)$ and show that their prime divisors $r \neq p$ are closely related to the congruence $r^{p-1} \equiv 1 \pmod{p^2}$.

**0. Introduction.** If the Bernoulli numbers $B_k$, $k = 0, 1, \ldots,$ are given by the expansion

$$\frac{t}{e^t - 1} = \sum_{k=0}^{\infty} B_k \frac{t^k}{k!},$$

then one defines, for $p$ an odd prime, the polynomial

$$\beta_p(X) = \sum_{k=1}^{p-2} \frac{B_k}{k}(X^{p-1-k} - 1).$$

Note that the coefficients of this polynomial are $p$-integral (Kummer).

In this paper we prove the equivalence of the congruence $\beta_p(r) \equiv 0 \pmod p$, where $r$ is a prime such that $r < p$, to a polynomial congruence (mod $r$). In order to construct these polynomial congruences, we introduce a class of cyclic extensions of $\mathbf{Q}$.

Let $\zeta$ be a primitive $p^2$th root of unity ($p$ an odd prime). Then $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ contains a unique subgroup $H$ of order $p-1$. Let $L$ be the corresponding fixed field. We define

$$H_p = \mathrm{Tr}_L^{\mathbf{Q}(\zeta)} \zeta. \tag{0.1}$$

If one identifies $\mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ with $(\mathbf{Z}/p^2\mathbf{Z})^\times$ in the usual way, then one finds that $H \equiv \{\alpha^p \pmod{p^2}\colon 1 \leqslant \alpha \leqslant p-1\}$. Hence

$$H_p = \sum_{1 \leqslant \alpha \leqslant p-1} \zeta^{\alpha^p}. \tag{0.2}$$

Received by the editors July 5, 1983.
1980 *Mathematics Subject Classification*. Primary 12A35; Secondary 12A50.
*Key words and phrases*. Bernoulli numbers, Fermat quotients, discriminants, cyclic abelian extensions.

Since Heilbronn raised the problem of finding nontrivial upper bounds for these trigonometric sums, we shall refer to them as Heilbronn sums [**9**, **2**]. These sums are studied in [**2**] in connection with Fermat quotients; they are also closely related to certain $n$-dimensional Kloosterman sums (see, for example, [**9**, p. 342]).

Let $f_p(X)$ denote the irreducible polynomial of $H_p$ over $\mathbf{Q}$. A table of these polynomials and their discriminants ($p \leqslant 19$) appears in [**5**, p. 292], where they are studied in connection with problems in cyclotomy.

It will be shown that if $p$ and $r$ are distinct primes with $p$ odd, then the congruence $f_p(n) \equiv 0 \pmod r$ has an integral solution if and only if $\beta_p(r) \equiv r^{-1}[r/p] \pmod p$. (If $y \in \mathbf{R}$, then $[y]$ is the largest integer $\leqslant y$.) We shall establish this result by showing that both these congruences hold if and only if $r^{p-1} \equiv 1 \pmod{p^2}$ (Theorem 4.1).

Let $\mathcal{O}$ denote the ring of integers in $L$. If $\alpha \in \mathcal{O} - \mathbf{Z}$, then $\alpha$ is of degree $p$ over $\mathbf{Z}$; consequently, $\mathbf{Z}[\alpha]$ is a free abelian group of rank $p$ and the number $I(\alpha) = (O : \mathbf{Z}[\alpha])$ is well defined. We shall study the arithmetic properties of these numbers. In particular, it will be shown that

$$I^2(H_p) \equiv (-1)^{(p+1)/2} \pmod{p^2}; \tag{0.3}$$

and if $p \equiv 1 \pmod 4$, then $I(\alpha) > p$ for every $\alpha$ of degree $p$ over $\mathbf{Z}$. Finally, a prime $r$ divides $I(\alpha)$ for every $\alpha$ of degree $p$ over $\mathbf{Z}$ if and only if $r < p$ and $\beta_p(r) \equiv 0 \pmod p$.

**1. Local results.** In the sequel, $p$ will be an odd prime number, while $\mathbf{Q}_p$ will denote the field of $p$-adic numbers; $\mathbf{Z}_p$ is the ring of $p$-adic integers. If $A$ is a ring, we denote by $A^\times$ the multiplicative group consisting of the units of $A$. If $L$ is a field which is a finite extension of $\mathbf{Q}_p$, then we write $N(L^\times)$ for the image of $L^\times$ under the norm map from $L$ to $\mathbf{Q}_p$. If $m \in \mathbf{Z}_p$, then $m^{\mathbf{Z}}$ stands for the multiplicative group consisting of the integral powers of $m$ and $\mu_{p-1}$ denotes the group consisting of the roots of unity in $\mathbf{Q}_p$. Finally, for $i = 1, 2$, $U_i$ is the subgroup $1 + p^i\mathbf{Z}_p$ of $\mathbf{Z}_p^\times$.

It is well known that $\mathbf{Q}_p$ possesses exactly $p + 1$ cyclic extensions of degree $p$. We shall need an explicit description of the norm groups of these extensions. With this object in mind, we introduce the following subgroups of $\mathbf{Q}_p^\times$: Let $u_0 = 1, u_1, \ldots, u_{p-1}$ be $p$ distinct representatives of the quotient group $U_1/U_2$. Then it is clear that $G_i = (u_i p)^{\mathbf{Z}} \cdot \mu_{p-1} \cdot U_2$, $i = 0, \ldots, p-1$, and $G_p = p^{p\mathbf{Z}} \cdot \mu_{p-1} \cdot U_1$ are $p + 1$ distinct open subgroups of $\mathbf{Q}_p^\times$ of index $p$. These are the only subgroups of $\mathbf{Q}_p^\times$ having this property: If $H$ is a subgroup of $\mathbf{Q}_p^\times$ of index $p$, then, since $\mu_{p-1}$ is of order $p - 1$ which is prime to $p$, the group $\mu_{p-1}$ is contained in $H$. Therefore, in order to count the subgroups of $\mathbf{Q}_p^\times$ of index $p$, we need only consider the subgroups of $\mathbf{Q}_p^\times/\mu_{p-1} \cong \mathbf{Z} \oplus \mathbf{Z}_p$; it is trivial that the latter group contains exactly $p + 1$ subgroups of index $p$.

Let $\mathbf{C}_p$ denote an algebraic closure of $\mathbf{Q}_p$. Then, by local class field theory, the groups $G_i$ correspond to the cyclic extensions $L_i$ of $\mathbf{Q}_p$ in $\mathbf{C}_p$ of degree $p$ over $\mathbf{Q}_p$ in such a manner that for $i = 0, \ldots, p$, we have $N(L_i^\times) = G_i$. In particular, $L_0$ is the unique subfield of $\mathbf{C}_p$ such that $L_0$ is a finite abelian extension of $\mathbf{Q}_p$ and

$$N(L_0^\times) = p^{\mathbf{Z}} \cdot \mu_{p-1} \cdot U_2. \tag{1.1}$$

It we take the structure of the norm groups $G_i$ into account, we see that $L_0$ is the only extension $L$ of degree $p$ over $\mathbf{Q}_p$ such that for some element $\pi$ of $L$ it follows that $N\pi = p$.

Let $K$ be the extension in $\mathbf{C}_p$ of $\mathbf{Q}_p$ obtained by adjoining a primitive $p^2$th root of unity $\zeta$ to $\mathbf{Q}_p$ and let $L'$ be the subfield of $K$ of degree $p$ over $\mathbf{Q}_p$. If we write $\pi = N_{L'}^K(\zeta - 1)$, then $N_{\mathbf{Q}_p}^{L'}(\pi) = N_{\mathbf{Q}_p}^K(\zeta - 1) = p$. It follows from the remark in the preceding paragraph that $L' = L_0$.

Let $\psi$ be a nontrivial character on $\mathbf{Q}_p^\times/N(L_0^\times)$; then it follows from (1.1) that $\psi$ has conductor $p^2\mathbf{Z}_p$. Since there are precisely $p - 1$ nontrivial characters on $\mathbf{Q}_p^\times/N(L_0^\times)$, it follows from the conductor-discriminant formula (see e.g. [**10**, p. 240]) that

$$d = p^{2(p-1)}\mathbf{Z}_p, \tag{1.2}$$

where $d$ denotes the discriminant of the extension $L_0/\mathbf{Q}_p$. It is clear that $L_0$ is a fully ramified extension $\mathbf{Q}_p$; therefore

$$D = \mathfrak{P}^{2(p-1)}, \tag{1.3}$$

where $D$ denotes the different of the extension and $\mathfrak{P}$ is the maximal ideal in the ring of integers $\mathcal{O}$ of $L_0$.

For every $\alpha \in L_0$, we denote by $\omega(\alpha)$ the order of $\alpha$ at $\mathfrak{P}$. If $\pi$ is of order 1 at $\mathfrak{P}$ and $f(X)$ is the irreducible polynomial of $\pi$ over $\mathbf{Q}_p$, then it follows from (1.3) that

$$\omega(f'(\pi)) = 2(p - 1). \tag{1.4}$$

On account of (1.1) and (1.3) we now have for a unique $\varepsilon \in \mu_{p-1}$ and a unique $a(\pi) \in \mathbf{Z}_p$ that

$$N(f'(\pi)) = \varepsilon(1 + a(\pi)p^2)p^{2(p-1)}. \tag{1.5}$$

We shall show in §5 that $\varepsilon = -1$.

Finally, we now show that for $\alpha \in L_0^\times$, we have

$$\omega(\alpha - \sigma\alpha) > \omega(\alpha) \tag{1.6}$$

for every $\sigma$ in the Galois group of the extension $L_0$ over $\mathbf{Q}_p$. Indeed, it follows from (1.1) that, if $x \in L_0^\times$ is such that $Nx = 1$, then $x \in 1 + \mathfrak{P}$. The result now follows if we put $x = \sigma\alpha/\alpha$.

**2. Heilbronn sums.** In the sequel, $\zeta$, $L$, $\mathcal{O}$ and $H_p$ will be as defined in the Introduction. Let $\mathfrak{P}$ be the prime ideal in $\mathcal{O}$ that lies above $p$. If $\alpha \in \mathcal{O}$, we denote by $\omega(\alpha)$ the order of $\alpha$ at $\mathfrak{P}$.

Note that, if we imbed $L$ in an algebraic closure of $\mathbf{Q}_p$, then the field $L_0$ given by (1.1) is the completion of $L$ at $\mathfrak{P}$. Consequently, the different $D$ of the extension $L/\mathbf{Q}$ is given by (1.3).

The following proposition deals with two rather special properties of Heilbronn sums:

PROPOSITION 2.1. (a) $\omega(H_p + 1) = 1$.

(b) *If $r$ is a rational prime such that $r \neq p$ and $R$ is a prime ideal in $\mathcal{O}$ that lies above $r$, then, for some $\sigma \in \mathrm{Gal}(L/\mathbf{Q})$, it follows that $\sigma H_p \not\equiv H_p \pmod{R}$.*

PROOF. (a) Let $\pi = (\zeta - 1)$ be the prime ideal in $\mathbf{Z}[\zeta]$ that lies above $p$. Then every $p^2$th root of unity is $1 \pmod{\pi}$ and $H_p$ is the sum of $p-1$ distinct $p^2$th roots of unity (see (0.2)). Consequently

$$\omega(H_p + 1) \geqslant 1. \tag{2.1}$$

Since $\mathrm{Tr}_{\mathbf{Q}}^{L} D^{-1} \subseteq \mathbf{Z}$ and $p\mathcal{O} = \mathfrak{P}^p$, by (1.3), we have $\mathrm{Tr}_{\mathbf{Q}}^{L}(D^{-1}) = \mathrm{Tr}_{\mathbf{Q}}^{L}(\mathfrak{P}^{-2p}\cdot\mathfrak{P}^2) = p^{-2}\mathrm{Tr}_{\mathbf{Q}}^{L}(\mathfrak{P}^2) \subseteq \mathbf{Z}$; in particular

$$\mathrm{Tr}_{\mathbf{Q}}^{L}(\mathfrak{P}^2) \subseteq p^2\mathbf{Z}. \tag{2.2}$$

Suppose that $\omega(H_p + 1) > 1$, then, by (2.2), $\mathrm{Tr}_{\mathbf{Q}}^{L}(H_p + 1) \equiv 0 \pmod{p^2}$. On the other hand, $\mathrm{Tr}_{\mathbf{Q}}^{\mathbf{Q}(\zeta)}(\zeta) = 0$ and it follows from (0.1) that $\mathrm{Tr}_{\mathbf{Q}}^{L}(H_p + 1) = p$—a contradiction. The result now follows from (2.1).

A proof of (b) appears in [**2**].

**3. Bernoulli numbers and Fermat quotients.** Let $p$ be an odd prime. For $x$ an integer such that $(x, p) = 1$, let $q(x)$ denote the Fermat quotient $(x^{p-1} - 1)/p \pmod{p}$. It follows from the definition of $q(x)$ that

$$q(xy) \equiv q(x) + q(y) \pmod{p}, \quad (xy, p) = 1. \tag{3.1}$$

PROPOSITION 3.1. *Let $x$ be an integer such that $(x, p) = 1$. Then*

$$q(x) \equiv \beta_p(x) - \frac{1}{x}\left[\frac{x}{p}\right] \pmod{p}. \tag{3.2}$$

REMARK. Dickson [**1**, p. 112] attributes a formula similar to (3.2) to Nielsen (1915). The formula, as cited by Dickson, is incorrect, for the second term on the right-hand side of (3.2) is omitted. Since the original source is quite inaccessible (to the author), we have devised a proof of (3.2) in the formalism of $p$-adic measures as developed by Mazur [7].

PROOF. We shall adhere to the notation and conventions of Koblitz [**6**, Chapter 2] in our application of $p$-adic measures in the sequel. The following is a brief summary of the results that will be needed: For every $x \in \mathbf{Z}$ which is prime to $p$, there exists a $\mathbf{Z}_p$-valued $p$-adic measure $\mu_{1,x}$ such that for $k \in \mathbf{Z}$, we have

$$\mu_{1,x}(k + p\mathbf{Z}_p) = \frac{1}{x}\left[\frac{kx}{p}\right] + \frac{1}{2}\left(\frac{1}{x} - 1\right), \qquad k \geqslant 0, \tag{M1}$$

$$\int_{\mathbf{Z}_p} \alpha^{k-1}\mu_{1,x} = (1 - x^{-k})\frac{B_k}{k}, \qquad k \geqslant 1, \tag{M2}$$

and

$$\mu_{1,x}(\mathbf{Z}_p^\times) = 0. \tag{M3}$$

Here $\mathbf{Z}_p$ denotes the ring of $p$-adic integers, while $\mathbf{Z}_p^\times$ is the group of units in $\mathbf{Z}_p$. Note that, since $\mu_{1,x}$ is $\mathbf{Z}_p$-valued, for a $\mu_{1,x}$-integrable function $f$ on $\mathbf{Z}_p$, we have $\int_{\mathbf{Z}_p} f\mu_{1,x} \equiv 0 \pmod{p}$ whenever $f(x) \equiv 0 \pmod{p}$ on $\mathbf{Z}_p$. By (M2), we have

$$\int_{\mathbf{Z}_p} \alpha^{p-2}\mu_{1,x} = (1 - x^{-(p-1)})B_{p-1}/(p-1).$$

Since $pB_{p-1} \equiv -1 \pmod p$, on account of the von Staudt congruence, it follows that

$$\int_{\mathbf{Z}_p} \alpha^{p-2}\mu_{1,x} \equiv (1 - x^{-(p-1)})/p \pmod p.$$

By (3.1), if $x^{-1}$ denotes the inverse of $x \pmod{p^2}$, then $q(x^{-1}) \equiv -q(x) \pmod p$. We have shown that

$$q(x) \equiv \int_{\mathbf{Z}_p} \alpha^{p-2}\mu_{1,x} \pmod p. \tag{3.3}$$

By (M3), we have for $p > 3$

$$\beta_p(x) \equiv \sum_{k=1}^{p-2} \frac{B_k}{k}(x^{-k} - 1) \equiv B_1(x^{-1} - 1) - \int_{\mathbf{Z}_p} (\alpha + \cdots + \alpha^{p-3})\mu_{1,x} \pmod p.$$

Since the integrand is $0 \pmod p$ if $\alpha \in p\mathbf{Z}_p$ and $\mathbf{Z}_p^\times = \mathbf{Z}_p - p\mathbf{Z}_p$, we have, by (M3), that

$$\beta_p(x) \equiv B_1(x^{-1} - 1) - \int_{\mathbf{Z}_p^\times} (1 + \alpha + \cdots + \alpha^{p-3})\mu_{1,x} \pmod p. \tag{3.4}$$

By (3.3), the integral is congruent $(\mathrm{mod}\ p)$ to

$$\int_{\mathbf{Z}_p^\times} (1 + \alpha + \cdots + \alpha^{p-2})\mu_{1,x} - q(x). \tag{3.5}$$

If $\alpha \in \mathbf{Z}_p^\times - (1 + p\mathbf{Z}_p)$, the integrand is equal to $(1 - \alpha^{p-1})/(1 - \alpha) \equiv 0 \pmod p$; hence (3.5) is congruent to

$$\begin{aligned} \int_{1+p\mathbf{Z}_p} (p-1)\mu_{1,x} - q(x) &\equiv -\mu_{1,x}(1 + p\mathbf{Z}_p) - q(x) \\ &\equiv -\frac{1}{x}\left[\frac{x}{p}\right] - \frac{1}{2}\left(\frac{1}{x} - 1\right) - q(x) \end{aligned} \tag{3.6}$$

in view of (M1) (with $k = 1$). The result (3.2) (for $p > 3$) now follows upon subtracting (3.6) from $B_1(x^{-1} - 1) = -(x^{-1} - 1)/2$ in (3.4). The case $p = 3$ is easily checked.

As an application of (3.2), we prove the following

COROLLARY. *If* $p \equiv 1 \pmod 4$, *then*

$$\sum_{2 (\mathrm{mod}\ 4)} \frac{B_k}{k} = \frac{B_2}{2} + \frac{B_6}{6} + \frac{B_{10}}{10} + \cdots + \frac{B_{p-3}}{p-3} \not\equiv 0 \pmod p. \tag{3.7}$$

PROOF. Let $n_p$ be an integer such that $n_p^2 \equiv -1 \pmod p$ and $1 < n_p < p$. We shall prove

$$\sum_{2 (\mathrm{mod}\ 4)} \frac{B_k}{k} \equiv \frac{1}{4}\left[(n_p + 1) - (n_p^2 + 1)/p\right] \pmod p. \tag{3.8}$$

It is easily seen that for $l \in \mathbf{Z}$, we have $q(-1 + lp) \equiv l \pmod p$. Therefore, if we write $n_p^2 = -1 + lp$, we find that $q(n_p^2) \equiv l \equiv (n_p^2 + 1)/p \pmod p$.

Hence, by (3.1), it follows that $q(n_p) \equiv (n_p^2 + 1)/2p$. On account of (3.2),

$$\left(n_p^2 + 1\right)/2p \equiv \beta_p(n_p) \equiv \sum_{k=1}^{p-3} \frac{B_k}{k}\left(n_p^{-k} - 1\right)$$

$$\equiv \frac{1}{2}\left(n_p + 1\right) + \sum_{k \geqslant 2} \frac{B_k}{k}\left(n_p^{-k} - 1\right) \pmod p.$$

Since $B_k = 0$ if $k \geqslant 3$ is odd, and $n_p^{-k} \equiv 1$ or $-1 \pmod p$, according to whether $k \equiv 0$ or $2 \pmod 4$, we see that (3.8) holds.

Suppose now that (3.7) does not hold; then by (3.8), we have $n_p^2 + 1 \equiv p(n_p + 1) \pmod{p^2}$. Since both $n_p^2 + 1$ and $p(n_p + 1)$ are positive and less than $p^2$, it must follow that $n_p^2 + 1 = p(n_p + 1)$—which is impossible.

**4. Reciprocity law.** We shall prove the following

THEOREM 4.1. *Let $r$ and $p$ be distinct primes with $p$ odd. Let $F$ denote the family of irreducible polynomials of elements in $\mathcal{O}$. Then the following statments are equivalent*:

(a) $\beta_p(r) \equiv \frac{1}{r}\left[\frac{r}{p}\right] \pmod p$.

(b) $f_p(n) \equiv 0 \pmod r$ *for some* $n \in \mathbf{Z}$.

(c) *For every* $f(X) \in F$ *there exists an integer* $m$ *such that* $f(m) \equiv 0 \pmod r$.

In the course of the proof of Theorem 4.1 we shall characterise the numbers $\alpha \in \mathcal{O}$ for which the theorem remains valid if we replace $f_p(X)$ in (b) by $\operatorname{Irr}(\alpha, L/\mathbf{Q}, X)$. If $r$ is a prime number and $R$ a prime ideal in $\mathcal{O}$ that divides $r$, we write $\overline{\mathcal{O}}_R = \mathcal{O}/R$ and $\overline{\mathbf{Z}}_r = \mathbf{Z}/r\mathbf{Z}$. If $\alpha \in \mathcal{O}$, we denote the image of $\alpha$ under the natural map $\mathcal{O} \to \overline{\mathcal{O}}_R$ by $\alpha_R$. Finally, we write $G = \operatorname{Gal}(L/\mathbf{Q})$.

Note that since $p$ is the only prime that ramifies in the extension $L/\mathbf{Q}$ and the extension is of prime degree, every prime number $r \neq p$ either splits completely in $\mathcal{O}$ or remains prime when lifted to $\mathcal{O}$.

LEMMA 4.2. *Let $r$ be a prime number $\neq p$. The congruences $f(x) \equiv 0 \pmod r$, $f(X) \in F$, all have solutions in $\mathbf{Z}$ if and only if $r$ splits completely in $\mathcal{O}$.*

PROOF. Suppose $r$ does not split completely in $\mathcal{O}$. Then $R = r\mathcal{O}$ is prime and $\overline{\mathcal{O}}_R$ is a separable field extension of $\overline{\mathbf{Z}}_r$ of degree $p$. Choose $\mu$ in $\mathcal{O}$ such that $\mu_R$ generates $\overline{\mathcal{O}}_R$ over $\overline{\mathbf{Z}}_r$. Then, obviously, $\sigma\mu \not\equiv \mu \pmod R$ for at least one $\sigma \not\equiv \mathrm{id}$ in $G$ and $\mu \not\equiv n \pmod R$ for every $n \in \mathbf{Z}$; hence, the polynomial $\operatorname{Irr}(\mu, L/\mathbf{Q}, X)$ has no integral solutions modulo $r$. Conversely, if $r$ splits completely in $\mathcal{O}$, then $\overline{\mathcal{O}}_R = \overline{\mathbf{Z}}_r$ for every $R|r$ and the congruences all have solutions in $\mathbf{Z}$ modulo $r$.

DEFINITION. Let $\alpha \in \mathcal{O}$. Then $\alpha$ is *basic* if, for every rational prime $r \neq p$ and prime divisor $R$ or $r$ in $\mathcal{O}$, it follows that $\overline{\mathcal{O}}_R = \overline{\mathbf{Z}}_r[\alpha_R]$.

REMARK. It is clear that if $\alpha$ generates a power basis of $\mathcal{O}$ over $\mathbf{Z}$, then $\alpha$ is basic. However, this is not a fruitful approach to the construction of examples of basic numbers since it will be showin in §5 that $\mathcal{O}$ has no power basis whenever $p \equiv 1 \pmod 4$. (On the other hand, if $p = 3$, then $\mathcal{O} = \mathbf{Z}[H_3]$!)

LEMMA 4.3. *If $\alpha \in \mathcal{O}$, then the following statements are equivalent*:

(i) $\alpha$ *is basic.*

(ii) *If* $r$ $(\neq p)$ *is prime and* $\mathrm{Irr}(\alpha, L/\mathbf{Q}, n) \equiv 0 \pmod r$ *for some* $n \in \mathbf{Z}$, *then the congruences* $f(x) \equiv 0 \pmod r$, $f(X) \in F$ *all have solutions in* $\mathbf{Z}$.

(iii) *If* $r$ $(\neq p)$, $R|r$ *and* $\alpha \equiv n \pmod R$ *for some* $n \in \mathbf{Z}$, *then* $r$ *splits completely in* $\mathcal{O}$.

(iv) *If the prime* $r$ $(\neq p)$ *does not split in* $\mathcal{O}$, *then, for some* $\sigma \in G$, *it follows that* $\sigma\alpha \not\equiv \alpha \pmod{r\mathcal{O}}$.

PROOF. It is clear from Lemma 4.2 that (ii) and (iii) are equivalent. We shall prove (i) $\Rightarrow$ (iii) $\Rightarrow$ (iv) $\Rightarrow$ (i).

(i) $\Rightarrow$ (iii): If (i) holds and $\alpha \equiv n \pmod R$, then $\bar{\mathcal{O}}_R = \bar{\mathbf{Z}}_r[\alpha_R] = \bar{\mathbf{Z}}_r$; hence the residue class degree of $R$ over $r$ is 1 and $r$ splits completely in $\mathcal{O}$.

(iii) $\Rightarrow$ (iv): Suppose $r$ does not split in $\mathcal{O}$ and $r \neq p$. Then $R = r\mathcal{O}$ is prime; if $\sigma\alpha \equiv \alpha \pmod R$ for every $\sigma \in G$, then for some $n \in \mathbf{Z}$ we have $\alpha \equiv n \pmod R$, in contradiction to (iii).

(iv) $\Rightarrow$ (i): If $r$ splits completely in $\mathcal{O}$, then $\alpha_R \in \bar{\mathbf{Z}}_r$ and $\bar{\mathcal{O}}_R = \bar{\mathbf{Z}}_r = \bar{\mathbf{Z}}_r[\alpha_R]$ for every $R|r$. Suppose that $r$ does not split completely in $\mathcal{O}$. Then $R = r\mathcal{O}$ is prime and by (iv), we have $\alpha_R \notin \bar{\mathbf{Z}}_r$. Since $\bar{\mathcal{O}}_R/\bar{\mathbf{Z}}_r$ is a field extension of prime degree, we have that $\bar{\mathcal{O}}_R = \bar{\mathbf{Z}}_r[\alpha_R]$.

LEMMA 4.4. *The rational prime* $r$ *splits completely in* $\mathcal{O}$ *if and only if* $r^{p-1} \equiv 1 \pmod{p^2}$.

PROOF. This is immediate from the factorisation properties of rational primes when lifted to $\mathbf{Q}(\zeta)$.

PROOF OF THEOREM 4.1. It follows from Proposition 2.1(b) and Lemma 4.3(iv) that $H_p$ is basic; hence (b) and (c) are equivalent, on account of Lemma 4.3(ii). By Lemma 4.2, Lemma 4.4 and Proposition 3.1 statements (a) and (c) hold if and only if $r^{p-1} \equiv 1 \pmod{p^2}$. The proof is complete.

REMARKS. 1. In **[2]** it is shown that $q(2) \equiv 0 \pmod p$ if and only if $f_p(0) = -NH_p$ is even, $N$ being the norm from $L$ to $\mathbf{Q}$. Consequently, the following statements are equivalent:

(i) $2^{p-1} \equiv 1 \pmod{p^2}$;

(ii) $NH_p$ is even;

(iii) $\beta_p(2) \equiv 0 \pmod p$.

2. D. H. and E. Lehmer **[5]** show that if $f_p(n) \equiv 0 \pmod r$ for some $n \in \mathbf{Z}$, then $q(r) \equiv 0 \pmod p$. By Lemmas 4.3 and 4.4 this provides an alternative proof of the fact that $H_p$ is basic. They raised the question whether $f_p(X)$ could ever assume even values. We see from Remark 1 that it may happen and if it does, then $f_p(n)$ will be even when $n \equiv 0 \pmod p$; this happens for $p \leqslant 6.10^9$ exactly when $p = 1093$ or $p = 3511$ **[4]**.

**5. Discriminants.** If $\alpha \in \mathcal{O}$, we denote by $d(\alpha)$ the discriminant of the irreducible polynomial of $\alpha$ over $\mathbf{Q}$. Since $L$ is a totally real field, the absolute discriminant $d_L$ of the extension $L/\mathbf{Q}$ is positive; hence, by (1.2), $d_L = p^{2(p-1)}$. Consequently, if $\alpha \in \mathcal{O} - \mathbf{Z}$, and $I(\alpha) = (\mathcal{O} : \mathbf{Z}[\alpha])$, then

$$d(\alpha) = I^2(\alpha)\, p^{2(p-1)}. \tag{5.1}$$

Furthermore, if $\alpha \in \mathcal{O}$, then

$$d(\alpha) = (-1)^{p(p-1)/2} N_{\mathbf{Q}}^{L}(f'(\alpha)), \tag{5.2}$$

where $f(X) = \mathrm{Irr}(\alpha, L/\mathbf{Q}, X)$.

It is shown in [**5**] that if $r$ $(\neq p)$ is a prime divisor of $d(H_p)$, then $r^{p-1} \equiv 1 \pmod{p^2}$. It will be shown that the converse also holds, provided $r < p$. Indeed, we shall prove

PROPOSITION 5.1. (a) *If $\alpha \in \mathcal{O}$ is basic, then for every prime divisor $r \neq p$ of $d(\alpha)$, we have* $r^{p-1} \equiv 1 \pmod{p^2}$.

(b) *If $r$ is a prime number, then $r | I(\alpha)$ for every $\alpha \in \mathcal{O} - \mathbf{Z}$ if and only if $r < p$ and* $r^{p-1} \equiv 1 \pmod{p^2}$.

PROOF. (a) Let $G = \mathrm{Gal}(L/\mathbf{Q})$. If $r | d(\alpha)$ and $R | r$ in $\mathcal{O}$, then for some $\sigma, \tau \in G$ such that $\sigma \neq \tau$ we have $\sigma\alpha \equiv \tau\alpha \pmod R$. Suppose that $r \neq p$ and $r^{p-1} \not\equiv 1 \pmod{p^2}$. Then, by Lemma 4.4, we have that $R = r\mathcal{O}$ is prime. In particular, $R$ remains invariant under the action of $G$. Hence $\tau^{-1}\sigma\alpha \equiv \alpha \pmod R$. Since $G$ is cyclic and of prime degree, $\sigma\alpha \equiv \alpha \pmod R$ for every $\sigma \in G$, in contradiction to Lemma 4.3(iv).

(b) Let $r < p$ be such that $r^{p-1} \equiv 1 \pmod{p^2}$. Then, by Lemma 4.4, $r$ splits completely in $\mathcal{O}$. Let $R | r$ in $\mathcal{O}$; then $\mathcal{O}/R = \mathbf{Z}/r\mathbf{Z}$ possesses $r$ distinct residue classes, i.e. $\alpha \pmod R$ can assume at most $r$ distinct values. On the other hand $G$ possesses $p > r$ elements. On account of Dirichlet's Box Principle, we conclude that for some $\sigma, \tau \in G$ such that $\sigma \neq \tau$, we have $\sigma\alpha \equiv \tau\alpha \pmod R$. Hence $r | d(\alpha)$ and $r | I(\alpha)$ by (5.1).

Conversely, if $r | I(\alpha)$ for every $\alpha \in \mathcal{O} - \mathbf{Z}$, then $r | I(H_p)$ so that by (5.1) and (a) we have $r^{p-1} \equiv 1 \pmod{p^2}$. Finally, it follows from Hensel's theory of indices of numbers fields [**3**] that if $r | I(\alpha)$ for every $\alpha \in \mathcal{O} - \mathbf{Z}$, then $r$ cannot exceed $p - 1$, $p$ being the degree of the extension $L/\mathbf{Q}$ (see [**8**, Proposition 4.13, p. 165]).

The observations of §1 will enable us to prove the following

THEOREM 5.2 (a) *If $\pi \in \mathcal{O}$ is of order* 1 *at the prime ideal above $p$, then*

$$I^2(\pi) \equiv (-1)^{(p+1)/2} \pmod{p^2}.$$

(b) *If* $p \equiv 1 \pmod 4$, *then* $I(\alpha) > p$ *for every* $\alpha \in \mathcal{O} - \mathbf{Z}$.

REMARK. Note that (0.3) now follows from (a), Proposition 2.1(a) and the observation that $I(H_p + 1) = I(H_p)$.

PROOF. (a) As a first step we show, in the notation of §1, that $\varepsilon = -1$ in (1.5). Let $\pi \in L_0$ be such that $\omega(\pi) = 1$ and let $f(X)$ denote the irreducible polynomial of $\pi$ over $\mathbf{Q}_p$. Write $G = \mathrm{Gal}(L_0/\mathbf{Q}_p)$. Since $f'(\pi) = \prod_{\sigma \neq \mathrm{id}}(\pi - \sigma\pi)$, it follows from (1.4) that $\sum_{\sigma \neq \mathrm{id}} \omega(\pi - \sigma\pi) = 2(p-1)$. If we now take (1.6) into account, we find for every $\sigma \in G$ satisfying $\sigma \neq \mathrm{id}$, that

$$\omega(\pi - \sigma\pi) = 2. \tag{5.3}$$

For the remainder of the proof, $\sigma$ will denote a fixed generator of $G$. We define the sequence $v_1, v_2, \ldots$ by the formula $\sigma^k\pi = v_k\pi$, $k \geqslant 1$. By (5.3), we have for some

$a \in \mathbf{Z}_p^\times$ that $v_1 \equiv 1 + a\pi \pmod{\mathfrak{P}^2}$. We prove inductively that

$$v_k \equiv (1 + ka\pi) \pmod{\mathfrak{P}^2}, \qquad k \geqslant 1. \tag{5.4}$$

Suppose that (5.4) holds for $k = l$, $l \geqslant 1$. Since $\sigma^{l+1}\pi = v_{l+1}\pi$ and $\sigma^{l+1}\pi = \sigma(v_l\pi) = (\sigma v_l)v_1\pi$, we have

$$v_{l+1} = v_1(\sigma v_l) \equiv (1 + a\pi)(1 + la\sigma\pi) \equiv 1 + (l+1)a\pi \pmod{\mathfrak{P}^2};$$

the proof of (5.4) is complete. Since $G$ is cyclic and of order $p$,

$$f'(\pi) = \prod_{k=1}^{p-1} (\pi - \sigma^k\pi) = \Big\{\prod_k (1 - v_k)\Big\}\pi^{p-1} = \Big\{\prod_k (-ka\pi + O(\pi^2))\Big\}\pi^{p-1}$$
$$= (-1)^{p-1}(p-1)!a^{p-1}\pi^{2(p-1)} + O(\pi^{2p-1}) = (-1)\pi^{2(p-1)} + O(\pi^{2p-1}),$$

where for $k \geqslant 1$ the symbol $O(\pi^k)$ stands for an element in $\mathfrak{P}^k$. Consequently, $f'(\pi)/\pi^{2(p-1)} \equiv -1 \pmod{\mathfrak{P}}$. Since $N(-1 + \mathfrak{P}) \subset -1 + p\mathbf{Z}_p$ and $N(\pi^{2(p-1)}) \equiv p^{2(p-1)} \pmod{p^{2p-1}}$ it follows that

$$N(f'(\pi))/p^{2(p-1)} \equiv -1 \pmod{p}. \tag{5.5}$$

By (1.5), the same congruence holds with $\varepsilon$ in the place of $-1$ on the right-hand side of (5.5). Since the elements of $\mu_{p-1}$ are pairwise incongruent modulo $p$, we see that $\varepsilon = -1$. Consequently, if we imbed $L$ into $L_0$, we see that the congruence (5.5) holds modulo $p^2$ in $\mathbf{Z}$ provided $\pi$ lies in $L$. The proof of (a) is complete in view of (5.1) and (5.2).

(b) Let $\alpha \in \mathcal{O} - \mathbf{Z}$. Since $\mathcal{O}/\mathfrak{P} = \mathbf{Z}/p\mathbf{Z}$ and $\mathbf{Z}[\alpha + n] = \mathbf{Z}[\alpha]$ for every $n \in \mathbf{Z}$, we may assume that $\omega(\alpha) \geqslant 1$. If $p \equiv 1 \pmod 4$ and $\omega(\alpha) = 1$, it follows from (a) that $I^2(\alpha) \equiv -1 \pmod{p^2}$. In particular, $I(\alpha) \geqslant l$, where $l$ is the smallest positive number such that $l^2 \equiv -1 \pmod{p^2}$; it is trivial that $l > p$. If $\omega(\alpha) > 1$, then, by (1.6) we have for every $\sigma \in G$ that $\omega(\alpha - \sigma\alpha) \geqslant 3$. Let $f(X)$ denote the irreducible polynomial of $\alpha$ over $\mathbf{Q}$. Then $\omega(f'(\alpha)) \geqslant 3(p-1)$; consequently, $d(\alpha) \equiv 0 \pmod{p^{3(p-1)}}$. By (5.1), we find that $I(\alpha)$ is divisible by $p^k$, $k = (p-1)/2$. In particular, $I(\alpha) > p$.

## References


1. L. E. Dickson, *History of the theory of numbers*: Vol. 1, Stechert, New York, 1934.
2. W. L. Fouché, *Arithmetic properties of Heilbronn sums*, J. Number Theory **19** (1984), 1–6.
3. K. Hensel, *Arithmetische Untersuchungen über die gemeinsamen ausserwesentlichen Discriminantentheiler einer Gattung*, J. Reine Angew. Math. **113** (1894), 128–160.
4. D. H. Lehmer, *On Fermat's quotient, base* 2, Math. Comp. **36** (1981), 289–290.
5. D. H. Lehmer and E. Lehmer, *Cyclotomy for non-squarefree moduli*, Proc. Analytic Number Theory (Philadelphia, 1980), Lecture Notes in Math., vol. 899, Springer-Verlag, Berlin and New York, 1981, pp. 276–300.
6. N. Koblitz, *p-adic numbers, p-adic analysis, and zeta-functions*, Springer-Verlag, Berlin and New York, 1977.
7. B. Mazur, *Analyse p-adique*, Bourbaki report, 1972.
8. W. Narkiewicz, *Elementary and analytic theory of algebraic numbers*, Polish Scientific Publishers, Warsaw, 1973.
9. R. A. Smith, *On n-dimensional Kloosterman sums*, J. Number Theory **11** (1979), 324–343.
10. A. Weil, *Basic number theory*, 3rd ed., Springer-Verlag, Berlin and New York, 1974.


Department of Mathematics, University of the Orange Free State, Bloemfontein 9300, South Africa