ILLINOIS JOURNAL OF MATHEMATICS
Volume 23, Number 4, December 1979

UNITS OF IRREGULAR CYCLOTOMIC FIELDS

BY
LAWRENCE C. WASHINGTON[1]

In an interesting series of papers, P. Dénes proved a number of results on cyclotomic fields, especially concerning their units, under the unproved assumption that the so called p-character of the Bernoulli numbers is finite. By relating this p-character to p-adic L-functions, we prove its finiteness as a consequence of the nonvanishing of the p-adic regulator. We then show how the p-adic regulator and p-adic L-functions may be used to obtain simple proofs of some of Dénes' results. We also show that a formula of Dénes is essentially the same as Leopoldt's p-adic class number formula. Finally, we give an application to the second case of Fermat's Last Theorem.

Since the p-adic L-functions are essentially an embodiment of many of the classical congruences for Bernoulli numbers (e.g., Kummer's congruences), several of our proofs can probably be translated back to the original ones, which relied heavily on properties of Kummer's logarithmic differential quotient. But the use of the theory of p-adic L-functions seems to be much more natural and also leads to new interpretations of classical results, in addition to being essential to the proof that the p-character is finite.

1. The p-character of the Bernoulli numbers

Throughout this paper we shall assume $p \geq 5$. Let the Bernoulli numbers be defined by

$$\frac{te^t}{e^t-1} = \sum_{n=0}^{\infty} B_n \frac{t^n}{n!},$$

so $B_0 = 1$, $B_1 = \frac{1}{2}$, $B_2 = \frac{1}{6}$, $B_3 = 0$, etc. (Dénes [2]) defined the p-character of the Bernoulli numbers to be the integers $u_2, u_4, \ldots, u_{p-3}$ defined by

$$B_{ip^j} \equiv 0 \pmod{p^{2j+1}} \quad \text{for} \quad 0 \leq j < u_i,$$
$$B_{ip^{u_i}} \not\equiv 0 \pmod{p^{2u_i+1}},$$

where $i = 2, 4, \ldots, p-3$. If p is a regular prime, then $u_i = 0$ for all i. We shall show how these numbers relate to p-adic L-functions.

Let $\mathbf{Z}_p$ be the ring of p-adic integers. If $a \in \mathbf{Z}_p$ and $p \nmid a$, then there is a unique $(p-1)$st root of unity $\omega(a) \in \mathbf{Z}_p$ such that $\omega(a) \equiv a \pmod{p}$. We may regard ω as a p-adic valued Dirichlet character. Define $\langle a \rangle = a/\omega(a)$, so

Received November 21, 1977.

[1] Research supported in part by a National Science Foundation grant.

$\langle a\rangle \equiv 1 \pmod p$. As usual, we set $\omega(b)=0$ if $p \mid b$. Let $L_p(s,\chi)$ denote the p-adic L-function for the character χ (see [7]).

LEMMA 1. *Let i be an even integer, $2 \le i \le p-3$, and let*

$$L_p(1-s,\omega^i) = a_0 + a_1 s + a_2 s^2 + \cdots .$$

Then $a_m \in \mathbf{Z}_p$ for all $m \ge 0$ and $p \mid a_m$ for $m \ge 1$.

Proof. In [14] we show that

$$L_p(1-s,\omega^i) = \frac{-1}{ps}\sum_{a=1}^{p-1}\omega^i(a)\langle a\rangle^s \sum_{j=0}^{\infty}\binom{s}{j}\left(\frac{-p}{a}\right)^j B_j,$$

where

$$\binom{s}{j} = \frac{s(s-1)\cdots(s-j+1)}{j!}.$$

Now

$$\langle a\rangle^s = \sum_{j=0}^{\infty}\binom{s}{j}(\langle a\rangle - 1)^j.$$

The coefficient of s^m in this expansion is of the form $A/m!$ where $p^m \mid A$ because $\langle a\rangle \equiv 1 \pmod p$. Since the exponent of p in $m!$ is less than $m/(p-1)$, we find that $p^{m(p-2)/(p-1)}$ divides the coefficient of s^m. If $m \ge 2$ then $m(p-2)/(p-1) > 1$. Since all coefficients are in $\mathbf{Q}_p$, we find that p^2 must divide the coefficient of s^m for $m \ge 2$. Consequently,

$$\langle a\rangle^s \equiv 1 + s(\langle a\rangle - 1) \pmod{p^2}.$$

Similarly, using the fact that $pB_j \in \mathbf{Z}_p$ (von Staudt-Clausen), we find that

$$\sum_{j=0}^{\infty}\binom{s}{j}\left(\frac{-p}{a}\right)^j B_j \equiv 1 - \frac{p}{2a}s \pmod{p^2}.$$

Therefore,

$$L_p(1-s,\omega^i) \equiv \frac{-1}{ps}\sum_{a=1}^{p-1}\omega^i(a)(1+s(\langle a\rangle - 1))\left(1-\frac{p}{2a}s\right)$$

$$\equiv \frac{-1}{p}\sum_{a=1}^{p-1}\omega^i(a)\left(\langle a\rangle - 1 - \frac{p}{2a}\right) \pmod p.$$

This last sum is clearly in $\mathbf{Z}_p$ and contains no powers of s. This proves the lemma. Q.E.D.

THEOREM 1. *Let v_p be the p-adic valuation normalized by $v_p(p)=1$. Then $u_i = v_p(L_p(1,\omega^i)) < \infty$, $i = 2, 4, \ldots, p-3$.*

Proof. If $n \equiv i \pmod{p-1}$, then $L_p(1-n,\omega^i) = -(1-p^{n-1})B_n/n$ (see [7]).

Since $ip^j \equiv i \pmod{p-1}$ for $j \geq 0$, we have

$$L_p(1-ip^j, \omega^i) = -(1-p^{ip^j-1})\frac{B_{ip^j}}{ip^j}.$$

We also have $L_p(1-ip^j, \omega^i) = a_0 + a_1(ip^j) + \cdots \equiv a_0 \pmod{p^{j+1}}$, since $p \mid a_m$ for $m \geq 1$. Therefore,

$$(1-p^{ip^j-1})B_{ip^j} \equiv -ip^j a_0 \pmod{p^{2j+1}}.$$

But $ip^j - 1 \geq 2j+1$ and $B_{ip^j} \in \mathbf{Z}_p$ (since $p-1 \nmid ip^j$), so

$$B_{ip^j} \equiv -ip^j a_0 \pmod{p^{2j+1}}.$$

We now see that the finiteness of u_i is equivalent to the fact that $a_0 = L_p(1, \omega^i) \neq 0$, which was proved by Brumer [1]; and from the definition of u_i it follows that $u_i = v_p(L_p(1, \omega^i))$. (Actually, Brumer proved that the p-adic regulator R_p is nonzero, but the p-adic class number formula (see the text preceding Lemma 4 below) shows that $R_p \neq 0$ implies $L_p(1, \omega^i) \neq 0$). Q.E.D.

Theorem 1 is the result Dénes needed to complete his proofs. However, it is now clear why he was unable to prove it, since Brumer's work depends on p-adic analogues of Baker's deep results on logarithms of algebraic numbers.

2. Units and the class number formula

In this section we show how several of Dénes' results on units may be obtained directly from the fact that the p-adic regulator is non-zero for the field $\mathbf{Q}(\zeta_p)$ of pth roots of unity. We also obtain a theorem of Pollaczek and we give a new proof of a class number formula of Dénes.

Let $\zeta = \zeta_p$ be a primitive pth root of unity and let $\lambda = 1-\zeta$. Note that any element α of $\mathbf{Z}[\zeta] = \mathbf{Z}[\lambda]$ which is not in $\mathbf{Z}$ and is prime to p satisfies $\alpha \equiv a + b\lambda^c \pmod{\lambda^{c+1}}$ for some rational integers a, b, c with $p \nmid ab$, and where $c \not\equiv 0 \pmod{p-1}$ is uniquely determined by α. Also, if α is real, c must be even. This representation of α will be used several times in the following, and it will always be implicitly assumed that a, b, c satisfy the above conditions.

LEMMA 2. *Let $\varepsilon \neq \pm 1$ be a unit of $\mathbf{Z}[\zeta]$, and assume $\varepsilon \equiv a + b\lambda^c \pmod{\lambda^{c+1}}$ with $c \geq 2$. Then $\log_p \varepsilon \equiv a^{-1}b\lambda^c \pmod{\lambda^{c+1}}$, where $\log_p$ is the p-adic logarithm (see [7]).*

Proof. Let N be the norm from $\mathbf{Q}(\zeta)$ to $\mathbf{Q}$. Then $1 = N(\varepsilon) \equiv a^{p-1} \pmod{\lambda}$. Since $p-1 \nmid c$ (so (λ^c) is not a power of the ideal (p)) and since $a^{p-1}-1$ is a rational integer, $a^{p-1} \equiv 1 \pmod{\lambda^{c+1}}$. From

$$\log_p(1+x) = x - x^2/2 + \cdots + x^p/p - \cdots$$

we easily see that $\log_p(1+x) \equiv x \pmod{\lambda x}$ if $\lambda^2 \mid x$. Therefore,

$$\log_p(a) = \frac{1}{p-1}\log_p(a^{p-1}) \equiv 0 \pmod{\lambda^{c+1}}$$

and

$$\log_p(a+b\lambda^c) = \log_p(a) + \log_p(1+a^{-1}b\lambda^c) \equiv a^{-1}b\lambda^c \pmod{\lambda^{c+1}}.$$

But $(a+b\lambda^c)/\varepsilon \equiv 1 \pmod{\lambda^{c+1}}$, so $\log_p(a+b\lambda^c) - \log_p(\varepsilon) \equiv 0 \pmod{\lambda^{c+1}}$. Q.E.D.

Remark. Any unit ε of $\mathbf{Z}[\zeta]$ can be written in the form $\varepsilon = \zeta^a\varepsilon^+$ with ε^+ real. Since $\zeta^a \equiv 1 - a\lambda \pmod{\lambda^2}$ and the integer c^+ for ε^+ must be even, hence ≥ 2, it follows that $c = 1$ exactly when $a \not\equiv 0 \pmod{p}$, which is exactly when $\varepsilon \neq \varepsilon^+$. Hence, the hypothesis of the lemma is equivalent to the assumption that ε is real and $\varepsilon \neq \pm 1$.

The crucial step is the following lemma. It was proved by Dénes (under the assumption of the finiteness of the p-character of the Bernoulli numbers) using properties of Kummer's logarithmic differential quotient. However, the use of the p-adic regulator greatly simplifies the argument and yields a complete proof of the result.

LEMMA 3. *Let ε be a unit of $\mathbf{Z}[\zeta]$ which is congruent to a rational integer modulo a high power of λ. Then ε is the pth power of a unit of $\mathbf{Z}[\zeta]$ (the size of the power of λ will be refined later (Corollary to Theorem 2), so we do not give an explicit estimate here).*

Proof. If ε is not a pth power, then there exist units $\varepsilon_2, \ldots, \varepsilon_{(p-3)/2}$ such that the group H generated by $\varepsilon, \varepsilon_2, \ldots, \varepsilon_{(p-3)/2}$ has index $[E: H]$ prime to p, where E is the group of all units of $\mathbf{Z}[\zeta]$. Since ε is congruent to an integer modulo a high power of λ, it follows from Lemma 2 that $\log_p \varepsilon$, hence $R_p(\varepsilon, \varepsilon_2, \ldots, \varepsilon_{(p-3)/2})$ which is the regulator of H (see [7]), is divisible by a high power of λ. But

$$R_p(\varepsilon, \ldots, \varepsilon_{(p-3)/2}) = [E: H]R_p,$$

where R_p is the regulator for E. Since $R_p \neq 0$ (see [1]), we obtain a contradiction. So ε must be a pth power. Q.E.D.

THEOREM 2 (Dénes [3]). *There exists a basis $\{\eta_2, \eta_4, \ldots, \eta_{p-3}\}$ for the real units modulo $\{\pm 1\}$ of $\mathbf{Z}[\zeta]$ such that*

$$\eta_i \equiv a_i + b_i\lambda^{c_i} \pmod{\lambda^{c_i+1}}$$

with $c_i = i + (p-1)u_i'$ for some integer $u_i' \geq 0$. Also,

$$u_i' \leq u_i = v_p(L_p(1, \omega^i)).$$

(Note that $c_i \equiv i \pmod{p-1}$, so that $c_2, \ldots, c_{p-3}$ are distinct mod $p-1$.)

Proof. The proof of the existence of the units will be that given by Dénes, but we include it for the sake of completeness.

Take any basis $\{\alpha_2, \alpha_4, \ldots, \alpha_{p-3}\}$ for the real units modulo $\{\pm 1\}$. Let

$$\alpha_i \equiv \beta_i + \gamma_i \lambda^{d_i} \pmod{\lambda^{d_i+1}}.$$

Suppose $d_i \equiv d_j \pmod{p-1}$, say $d_i = d_j + k(p-1)$ with $k \geq 0$. If we replace α_i by $\alpha_i \alpha_j^{\varepsilon p^k}$ for a suitable integer e we obtain a new basis with the d_i corresponding to the new α_i strictly larger than the original d_i. This process can be continued as long as the numbers $d_2, \ldots, d_{p-3}$ are not distinct mod $p-1$. Since each step increases these numbers, the process must stop, since by Lemma 3 a unit with a large d_i is a pth power, hence cannot be a basis element. We therefore eventually obtain the units η_i.

If $\prod \eta_i^{g_i} \equiv a + b\lambda^c \pmod{\lambda^{c+1}}$, then $c = \min(c_i + (p-1)v_p(g_i))$ and the index i giving the minimum is determined by $c \equiv i \pmod{p-1}$. To prove that $u_i' \leq u_i$ it therefore suffices to find a unit

$$(*) \qquad \beta_i \equiv e_i + f_i \lambda^{u_i(p-1)+i} \pmod{\lambda^{u_i(p-1)+i+1}},$$

since then $u_i(p-1)+i = c_i + (p-1)v_p(g_i) \geq c_i = u_i'(p-1)+i$.

Let $\varepsilon = \zeta^{(r-1)/2}(1-\zeta^{-r})/(1-\zeta^{-1})$, where r is an odd primitive root modulo p. Then ε is a real unit in $\mathbf{Z}[\zeta]$. We may assume that

$$r^{p-1} \equiv 1 \pmod{p^{M+1}} \quad \text{where} \quad M = \max(v_p(L_p(1, \omega^i))),\ i = 2, 4, \ldots, p-3.$$

Let $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ be defined by $\sigma(\zeta) = \zeta^r$, and let

$$s_i = 1 + \sigma r^{-i} + \sigma^2 r^{-2i} + \cdots + \sigma^{p-2} r^{-(p-2)i} \pmod{p^{M+1}}.$$

Define $\beta_i = \varepsilon^{s_i}$. We claim that β_i satisfies $(*)$. Dénes proved this using properties of Kummer's logarithmic differential quotient. However, it is perhaps easier to proceed as follows.

$$\begin{aligned}
\log_p \beta_i &= \sum_{j=0}^{p-2} r^{-ji}(\log_p(1-\zeta^{-r\sigma^j}) - \log_p(1-\zeta^{-\sigma^j})) \\
&= \sum_j r^{-ji} \log_p(1-\zeta^{-r^{j+1}}) - \sum_j r^{-ji} \log_p(1-\zeta^{-r^j}) \\
&\equiv \sum_{a=1}^{p-1} \omega(a)^{-i} \log_p(1-\zeta^{-ra}) - \sum_a \omega(a)^{-i} \log_p(1-\zeta^{-a}) \\
&\equiv (\omega(r)^i - 1) \sum_{a=1}^{p-1} \omega(a)^{-i} \log_p(1-\zeta^{-a}) \pmod{p^{M+1}},
\end{aligned}$$

since $r^{p-1} \equiv 1 \pmod{p^{M+1}}$ implies $\omega(r) \equiv r \pmod{p^{M+1}}$. Now

$$L_p(1, \omega^i) = -\frac{\tau(\omega^i)}{p} \sum_{a=1}^{p-1} \omega(a)^{-i} \log_p(1-\zeta^{-a}),$$

where $\tau(\omega^i)$ is a Gauss sum (see [7] or [15]). Stickelberger's Theorem [8, p.

94] implies that $v_p(\tau(\omega^i)) = 1 - i/(p-1)$. Therefore, since $\omega(r)^i \not\equiv 1 \pmod{p}$, we have

$$v_p(\log_p \beta_i) = v_p\left(\frac{p}{\tau(\omega_i)} L_p(1, \omega^i)\right)$$

$$= \frac{i}{p-1} + v_p(L_p(1, \omega^i))$$

$$= \frac{i}{p-1} + u_i.$$

But $\beta_i \equiv a + b\lambda^c \pmod{\lambda^{c+1}}$ implies that $v_p(\log \beta_i) = c/(p-1)$, by Lemma 2 ($c \geq 2$ since β_i is real). Therefore $c = i + (p-1)u_i$. Q.E.D.

COROLLARY. *Let $M = \max_i v_p(L_p(1, \omega^i))$, where $i = 2, 4, \ldots, p-3$, and let ε be a unit of $\mathbf{Z}[\zeta]$. If ε is congruent to a rational integer modulo p^{M+1} then ε is the pth power of a unit of $\mathbf{Z}[\zeta]$.*

Proof. We may assume $\varepsilon \neq \pm 1$. Let

$$\varepsilon = \pm \prod \eta_i^{g_i} \equiv a + b\lambda^c \pmod{\lambda^{c+1}}, \quad \text{with} \quad c \geq (M+1)(p-1).$$

Then as noted above, $c = \min(c_i + (p-1)v_p(g_i))$ Consequently, for each i we have

$$i + (p-1)u_i' \leq i + (p-1)u_i < (M+1)(p-1) \leq c \leq c_i + (p-1)v_p(g_i)$$
$$= i + (p-1)u_i' + (p-1)v_p(g_i).$$

Therefore $v_p(g_i) > 0$ for each i, so ε is a pth power. Q.E.D.

Remark. When p is a regular prime, then it easily follows from Kummer's congruences for Bernoulli numbers that $M = 0$, so we obtain a proof of Kummer's Lemma. Note that the proof in this case is independent of Brumer's result since $M = 0$ automatically implies that $L_p(1, \omega^i)) \neq 0$ for each i, hence $R_p \neq 0$.

We can now modify $\eta_2, \ldots, \eta_{p-3}$ to obtain the following result of Pollaczek [11].

THEOREM 3. *There is a basis $\{\alpha_2, \alpha_4, \ldots, \alpha_{p-3}\}$ for the real units modulo $\{\pm 1\}$ of $\mathbf{Z}[\zeta]$ such that $\alpha_i^{\sigma - r^i}$ is the pth power of a unit of $\mathbf{Z}[\zeta]$, where r is a fixed primitive root modulo p and $\sigma \in \mathrm{Gal}(\mathbf{Q}(\zeta)/\mathbf{Q})$ is determined by $\sigma(\zeta) = \zeta^r$.*

Proof. We first note that $\sigma(\lambda^c) \equiv r^c \lambda^c \pmod{\lambda^{c+1}}$, so

$$\sigma(a + b\lambda^c) \equiv (a + b\lambda^c)^{r^c} \cdot (a^{1-r^c}) \pmod{\lambda^{c+1}}.$$

Let c_i be as in the statement of Theorem 2, and suppose we have

$$c_{i_2} > c_{i_4} > \cdots > c_{i_{p-3}}.$$

For typographical reasons let $d_k = c_{i_k}$ and $r_k = r^{d_k}$. Note that $d_k \equiv i_k \pmod{p-1}$.

From the above, we have

$$\eta_{i_2}^{\sigma - r_2} \equiv a^{1-r_2} \pmod{\lambda^{d_2+1}}.$$

Since $d_2 + 1 > c_i$ for all i, it follows by the same reasoning as in the proof of the corollary to Theorem 2 that $\eta_{i_2}^{\sigma - r_2}$ must be a pth power, and since $d_2 = i_2 \pmod{p-1}$ it follows that $\eta_i^{\sigma - r^i}$, for $i = i_2$, is a pth power. Let $\alpha_{i_2} = \eta_{i_2}$. Suppose we have $\alpha_i^{\sigma - r^i}$ equaling a pth power for $i = i_2, \ldots, i_{k-2}$. Let

$$\alpha_{i_k} = \eta_{i_k} \alpha_{i_2}^{h_2} \cdots \alpha_{i_{k-2}}^{h_{k-2}},$$

where $h_2, \ldots, h_{k-2}$ are to be determined. Let $\delta_j = r^{i_j} - r^{i_k}$. Then, for $i = i_k$,

$$\alpha_i^{\sigma - r^i} = \eta_i^{\sigma - r^i} \alpha_{i_2}^{h_2 \delta_2} \cdots \alpha_{i_{k-2}}^{h_{k-2} \delta_{k-2}} \beta^p$$

for some unit β. By the above,

$$\eta_{i_k}^{\sigma - r_k} \equiv \text{rational integer} \pmod{\lambda^{d_k+1}}.$$

Therefore, since $d_k + 1 > d_j$ for $k \leq j \leq p-3$, it follows that when $\eta_{i_k}^{\sigma - r_k}$ is expressed as a product of powers of $\alpha_{i_2}, \ldots, \alpha_{i_{k-2}}, \eta_{i_k}, \ldots, \eta_{i_{p-3}}$, the exponents of the η's are divisible by p. Since $r^{i_k} \equiv r_k \pmod{p}$, the same holds for $\eta_i^{\sigma - r^i}$ with $i = i_k$. Since $\delta_j \not\equiv 0 \pmod{p}$ for $j \neq k$, we may choose $h_2, \ldots, h_{k-2}$ so that the exponent of α_{i_m} on the right hand side is divisible by p for $m = 2, \ldots, k-2$. Therefore $\alpha_i^{\sigma - r^i}$ is a pth power for $i = i_k$. Continuing, we get the desired basis $\{\alpha_2, \ldots, \alpha_{p-3}\}$ Q.E.D.

Remarks. We first note that the units α_i constructed above still satisfy a congruence of the form $\alpha_i \equiv m_i + n_i \lambda^{c_i} \pmod{\lambda^{c_i+1}}$, where c_i is as in Theorem 2.

Secondly, we note that the units α_i essentially give a decomposition of the units modulo pth powers with respect to the idempotents of the group ring of the Galois group. The element s_i used in the proof of Theorem 2 is, up to a constant factor and modulo p, one of these idempotents; so it is reasonable to expect that the unit $\beta_i = \varepsilon^{s_i}$ constructed in that proof is of the desired form.

Finally, we note that Pollaczek's original proof may be considered more elementary in that he does not need the validity of Leopoldt's Conjecture for $\mathbf{Q}(\zeta)$. However, it seems that there might be a possibility of using Pollaczek's units to construct the units of Theorem 2. This would give another proof of Leopoldt's conjecture for $\mathbf{Q}(\zeta)$, since the existence of these latter units is easily seen to imply that the p-adic regulator does not vanish (see the proof of Lemma 4).

We now show that a formula of Dénes is essentially the same as

Leopoldt's p-adic class number formula [7]

$$\frac{2^{(p-3)/2}hR_p}{d^{1/2}} = \prod_{i=2}^{p-3} L_p(1, \omega^i), \quad i \text{ even}$$

where h is the class number, R_p is the p-adic regulator, and $d = p^{(p-3)/2}$ is the discriminant of $\mathbf{Q}(\zeta)^+$, the maximal real subfield of $\mathbf{Q}(\zeta)$.

LEMMA 4. $v_p(R_p) = v_p(d^{1/2}) + \sum_{\substack{i=2 \\ i \text{ even}}}^{p-3} u_i'$, *where* u_i' *is as defined in Theorem 2.*

Proof. *Let* $\eta_i \equiv a_i + b_i\lambda^{c_i} \pmod{\lambda^{c_i+1}}$ be as in Theorem 2. Then

$$\sigma^k(\eta_i) \equiv a_i + b_i r^{kc_i}\lambda^{c_i},$$

so by Lemma 2,

$$\log_p \sigma^k(\eta_i) \equiv a_i^{-1}b_i r^{kc_i}\lambda^{c_i} \pmod{\lambda^{c_i+1}}.$$

Therefore, since $\{\sigma^k \mid k = 0, 1, \ldots, \frac{1}{2}(p-3)\}$ restricts to $\mathrm{Gal}(\mathbf{Q}(\zeta)^+/\mathbf{Q})$, we have

$$R_p = \det(\log_p(\sigma^k\eta_i))_{i,k} \begin{pmatrix} i = 2, 4, \ldots, p-3 \\ k = 0, 1, \ldots, \frac{1}{2}(p-5) \end{pmatrix}$$

$$\equiv \left(\prod_{\substack{i=2 \\ i \text{ even}}}^{p-3} a_i^{-1}b_i\lambda^{c_i}\right) \det(r^{kc_i})_{i,k} \pmod{\lambda^{1+\sum c_i}}.$$

Now $\det(r^{kc_i}) = \prod_{i<j}(r^{c_j} - r^{c_i})$ (Vandermonde) which is $\not\equiv 0 \pmod p$ since $c_i \not\equiv c_j \pmod{p-1}$. Also a_i and b_i are prime to p. Therefore,

$$v_p(R_p) = \frac{1}{p-1}\sum c_i = \sum_{\substack{i=2 \\ i \text{ even}}}^{p-3} \frac{i}{p-1} + \sum_i u_i' = \frac{p-3}{4} + \sum u_i' = v_p(d^{1/2}) + \sum u_i'.$$

Q.E.D.

The following theorem of Dénes [4] now follows easily.

THEOREM 4. *Let* p^f *be the exact power of* p *dividing class number* h *of* $\mathbf{Q}(\zeta)^+$. Then

$$f = \sum_{\substack{i=2 \\ i \text{ even}}}^{p-3} (u_i - u_i').$$

COROLLARY. *If* $\mathbf{Q}(\zeta)$ *is properly irregular (i.e.,* $p \nmid h$*), then* $u_i = u_i'$ *for all* i.

3. Fermat's Last Theorem

In [12], Vandiver showed that if the class number of $\mathbf{Q}(\zeta)^+$ is prime to p and if B_{ip} is not divisible by p^3 for $i = 2, 4, \ldots, p-3$, then the second case of

Fermat's Last Theorem is true for p. Using the corollary to Theorem 2, we prove the following generalization.

THEOREM 5. *Let p be an irregular prime and assume p does not divide the class number of $\mathbf{Q}(\zeta)^+$. Let $n = \max_i v_p(L_p(1, \omega^i))$, where $i = 2, 4, \ldots, p-3$. Then $x^p + y^p = z^{p^n}$, $p \nmid xy$, $p \mid z$, $(x, y, z) = 1$ has no solutions in non-zero rational integers.*

Remark. $n = 1$ for $p < 125{,}000$ (see [13]).

Proof. The proof is similar to that given by Vandiver; however, it seems that perhaps another exposition would be desirable, so we include the details.

Let $\kappa = (1-\zeta)(1-\zeta^{-1})$. We shall show that

$$\omega^p + \theta^p = \eta\kappa^m\xi^{p^n} \tag{1}$$

is impossible if ω, θ, ξ are non-zero integers of $\mathbf{Q}(\zeta)^+$ with ω, θ, κ pairwise relatively prime; η is a real unit of $\mathbf{Q}(\zeta)$; and $m \geq \frac{1}{2}(p-1)(n+1)+p$. The case $m = \frac{1}{2}(p-1)p^n$ yields the theorem, since p^{p^n} and κ^m then differ by a unit; so we may let $\omega = x$, $\theta = y$, and $\xi = z/p$.

Suppose (1) has a solution. Then

$$\prod_{a=0}^{p-1} (\omega + \zeta^a\theta) = \eta\kappa^m\xi^{p^n}.$$

the standard argument shows that the numbers $\omega + \zeta^a\theta$, $a = 0, \ldots, p-1$ are congruent to 0 modulo $(1-\zeta)$ but are incongruent modulo (κ). Since $\omega + \theta$ is real, $\omega + \theta \equiv 0 \pmod{\kappa}$. We find that the numbers $(\omega + \zeta^a\theta)/(1-\zeta^a)$, $a = 1, \ldots, p-1$, and $\omega + \theta$ are pairwise relatively prime algebraic integers; so there exist ideals $A_0, \ldots, A_{p-1}$ of $\mathbf{Q}(\zeta)$ such that

$$\left(\frac{\omega + \zeta^a\theta}{1-\zeta^a}\right) = A_a^p, \qquad a = 1, \ldots, p-1 \quad \text{and} \quad (\omega + \theta) = \kappa^{m-(p-1)/2} A_0^{p^n}.$$

(Actually, we could have $A_a^{p^n}$ but this will not be needed.) Since

$$\omega \equiv -\theta \pmod{\kappa^{m-(p-1)/2}},$$

we have

$$\alpha = \left(\frac{\omega + \zeta^a\theta}{1-\zeta^a}\right)\left(\frac{\omega + \zeta^{-a}\theta}{1-\zeta^{-a}}\right)^{-1} \equiv 1 \pmod{\lambda^{2m-p}},$$

where $\lambda = 1-\zeta$. Note that $\bar{\alpha} = \alpha^{-1}$, where $\bar{\alpha}$ denotes the complex conjugate. Also, α is the pth power of an ideal, so $\mathbf{Q}(\zeta, \alpha^{1/p})/\mathbf{Q}(\zeta)$ can only be ramified at (λ). However, since $2m - p \geq p+1$, α is a local pth power at (λ). Therefore, the extension is unramified at all primes. Assume the extension is non-trivial. Let σ generate its Galois group: $\sigma(\alpha^{1/p}) = \zeta\alpha^{1/p}$. Since $\bar{\alpha} = \alpha^{-1}$, it follows easily that σ commutes with complex conjugation. Therefore, the

subfield of $\mathbf{Q}(\zeta, \alpha^{1/p})$ fixed by complex conjugation is Galois of degree p and unramified over $\mathbf{Q}(\zeta)^+$. But this is impossible since the class number of $\mathbf{Q}(\zeta)^+$ is prime to p. Consequently, we must have $\alpha^{1/p} \in \mathbf{Q}(\zeta)$. So

$$\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right)\left(\frac{\omega+\zeta^{-a}\theta}{1-\zeta^{-a}}\right)^{-1} = (\rho'_a)^p \quad \text{(as numbers of } \mathbf{Q}(\zeta)) \tag{2}$$

for some $\rho'_a \in \mathbf{Q}(\zeta)$. Also

$$\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right)\left(\frac{\omega+\zeta^{-a}\theta}{1-\zeta^{-a}}\right) = (A_aA_{-a})^p \quad \text{(as ideals of } \mathbf{Q}(\zeta))$$

and since $A_{-a} = \bar{A}_a$, it follows that A_aA_{-a} is an ideal of $\mathbf{Q}(\zeta)^+$ ($-a$ is actually the index $p-a$). Since the class number of this field is prime to p, we have A_aA_{-a} principal. Therefore,

$$\left(\frac{\omega+\zeta^a\theta}{1-\zeta^a}\right)\left(\frac{\omega+\zeta^{-a}\theta}{1-\zeta^{-a}}\right) = \beta(\rho''_a)^p \quad \text{(as numbers of } \mathbf{Q}(\zeta)), \tag{3}$$

where ρ''_a is an integer from $\mathbf{Q}(\zeta)^+$ and β is a unit which must be real since the left-hand side of the equation is also real. It follows easily from (2) and (3) that

$$\frac{\omega+\zeta^a\theta}{1-\zeta^a} = \eta_a\rho_a^p \tag{4}$$

where η_a is a real unit and ρ_a is an integer of $\mathbf{Q}(\zeta)$.

Since $A_0 = \bar{A}_0$, it follows that

$$\omega+\theta = \eta_0\kappa^{m-(p-1)/2}\rho_0^{p^n} \tag{5}$$

for some integer ρ_0 in $\mathbf{Q}(\zeta)^+$.

Using the fact that $\eta_a = \eta_{-a}$ since both are real, we obtain from (4) for indices a and $-a$, and from (5) that $\rho_a^p - \rho_{-a}^p = \eta'_a\lambda^{2m-p}\rho_0^{p^n}$, where η'_a is a unit from $\mathbf{Q}(\zeta)$. Therefore,

$$\prod_{i=0}^{p-1}(\rho_a - \zeta^i\rho_{-a}) \equiv 0 \pmod{\lambda^{2m-p}}.$$

Consequently, $\rho_a \equiv \zeta^i\rho_{-a}$, or $\zeta^{-i/2}\rho_a \equiv \zeta^{i/2}\rho_{-a} \pmod{\lambda^2}$ for some i. By changing the choice of ρ_a and ρ_{-a} in (4), since ρ_a is only determined up to a power of ζ, we may assume $\rho_a \equiv \rho_{-a} \pmod{\lambda^2}$. Also, since $(\omega+\zeta^a\theta)/(1-\zeta^a)$, $(\omega+\zeta^{-a}\theta)/(1-\zeta^{-a})$, and λ are pairwise relatively prime, ρ_a, ρ_{-a}, and λ are relatively prime. Therefore, as before,

$$\rho_a - \rho_{-a} \equiv 0 \pmod{\lambda^{2m-2p+1}} \tag{6}$$

and

$$\left(\frac{\rho_a - \zeta^i\rho_{-a}}{1-\zeta^i}\right) = C_i^{p^n}, \quad i = 1, \ldots, p-1,$$

for some ideal C_i of $\mathbf{Q}(\zeta)$. But the left-hand side of this last equation is real (note that $\overline{\rho_a} = \rho_{-a}$); so we have

$$\frac{\rho_a - \zeta^i \rho_{-a}}{1-\zeta^i} = \eta_i^{(a)} \mu_i^{p^n}$$

for some integer μ_i of $\mathbf{Q}(\zeta)^+$ and some unit $\eta_i^{(a)}$ which must also be real. From (6) we obtain $\rho_a \equiv \eta_i^{(a)} \mu_i^{p^n} \pmod{\lambda^{2m-2p}}$. From (4),

$$\frac{\omega + \zeta^a \theta}{1-\zeta^a} = \eta_a \rho_a^p \equiv \eta_a (\eta_i^{(a)})^p \mu_i^{p^{n+1}} \pmod{\lambda^{2m-2p}}.$$

Since from (5),

$$\frac{\omega + \zeta^a \theta}{1-\zeta^a} \equiv \omega \pmod{\lambda^{2m-p}},$$

it follows that

$$\omega \equiv \eta_a (\eta_i^{(a)})^p \mu_i^{p^{n+1}} \pmod{\lambda^{2m-2p}}. \tag{7}$$

Let $b \equiv \pm a \pmod{p}$. From (7), and from (7) with b in place of a, we obtain

$$\varepsilon = \frac{\eta_a (\eta_i^{(a)})^p}{\eta_b (\eta_i^{(b)})^p} \equiv \mu^{p^{n+1}} \pmod{\lambda^{2m-2p}},$$

for some $\mu \in \mathbf{Q}(\zeta)^+$, and we may assume μ is an integer of $\mathbf{Q}(\zeta)^+$. But the $p^{n+1} - st$ power of an integer of $\mathbf{Q}(\zeta)^+$ is congruent to a rational integer modulo $\lambda^{(p-1)(n+1)+2}$. Since $2m - 2p \geq (p-1)(n+1)$ by the choice of m, it follows that $\varepsilon \equiv z \pmod{p^{n+1}}$, where z is a rational integer. By the corollary to Theorem 2, $\varepsilon = \gamma^p$ for some unit γ, which may be assumed real (since every unit is a power of ζ times a real unit). Let $\rho_a^* = (\eta_i^{(a)})^{-1} \rho_a$. Then

$$\frac{\omega + \zeta^a \theta}{1-\zeta^a} = \eta_a (\eta_i^{(a)})^p (\rho_a^*)^p.$$

From this and the same equation for the index $-a$ (note that $\eta_i^{(a)}$ is real so it corresponds to a and $-a$), we have

$$\omega^2 + (\zeta^a + \zeta^{-a}) \omega\theta + \theta^2 = \eta_a^* (2 - \zeta^a - \zeta^{-a}) (\omega^*)^p \tag{8}$$

where $\eta_a^* = (\eta_a (\eta_i^{(a)})^p)^2$ is a real unit and $\omega^* = \rho_a^* \rho_{-a}^*$ is an integer of $\mathbf{Q}(\zeta)^+$. From (5),

$$\omega^2 + 2\omega\theta + \theta^2 = \eta_0^2 \kappa^{2m-p+1} \rho_0^{2p^n}. \tag{9}$$

From (8) with indices a and b and from (9), it follows that (let $\rho_b^* \rho_{-b}^* = \theta^*$)

$$\begin{aligned} \eta_a^* (\omega^*)^p - \eta_b^* (\theta^*)^p &= \frac{\eta_0^2 \kappa^{2m-p+1} (\zeta^{-b} - \zeta^{-a})(\zeta^{a+b} - 1) \rho_0^{2p^n}}{(1-\zeta^a)(1-\zeta^{-a})(1-\zeta^b)(1-\zeta^{-b})} \\ &= \delta \kappa^{2m-p} \rho_0^{2p^n}, \end{aligned}$$

where δ is a unit. Dividing by η_b^* and noting that $\eta_a^*/\eta_b^* = \varepsilon^2 = \gamma^{2p}$, we obtain

$$(\gamma^2\omega^*)^p + (-\theta^*)^p = \delta_1 \kappa^{2m-p}(\rho_0^2)^{p^n},$$

where δ_1 is a unit which must be real since everything else is real. Since $2m-p > m$, we have obtained an equation of the same form as (1).

Assume that ξ in (1) has the minimal possible number of distinct prime ideal factors, where m ranges over all permissible values. Since $(\rho_0) = A_0$ and $(\xi)^{p^{n-1}} = A_0^{p^{n-1}} A_1 \cdots A_{p-1}$ with the ideals A_a pairwise relatively prime, we must have $A_a = 1$ for $a = 1, \ldots, p-1$. Therefore, $(\omega + \zeta^a\theta)/(1-\zeta^a)$ is a unit for $a = 1, \ldots, p-1$. Let

$$\alpha = \left(\frac{\omega + \zeta^a\theta}{1-\zeta^a}\right)\left(\frac{\omega + \zeta^{-a}\theta}{1-\zeta^{-a}}\right)^{-1}.$$

Then α is a unit with $\alpha\bar{\alpha} = 1$. By a well-known theorem, α must be a root of unity: $\alpha = \pm\zeta^t$. But from the above we have $\pm\zeta^t = \alpha \equiv 1 \pmod{\lambda^{2m-p}}$. Since $2m-p > 1$, it follows that $\alpha = \pm\zeta^t = 1$. A short calculation now yields $\zeta^a = \zeta^{-a}$, which is impossible since $a \not\equiv 0 \pmod{p}$. (Use the fact that $\omega \neq -\theta$; it is here that the trivial solution must be excluded.) This contradiction proves the theorem. Q.E.D.

Remark. It seems that perhaps more direct relationships could be found between Fermat's Last Theorem and p-adic L-functions, maybe using Stickelberger's theorem.

Also, it should be noted that Inkeri [6] has proved that $x^{p^n} + y^{p^n} = z^{p^n}$ has no nontrivial solutions for n sufficiently large, with no assumptions on the class number, and Morishima [10] has proved our Theorem 5 but with a different value of n, namely $3t+2$ where $t = v_p(h(\mathbf{Q}(\zeta_p)))$. Empirically this value is larger, but it may be estimated more easily. It should be interesting to investigate the relations between these results.

Finally, we mention that similar results have been proved in the first case ($p \nmid xyz$) (see [5], [9], [16]).

References

1. A. Brumer, *On the units of algebraic number fields*, Mathematika, vol. 14 (1967), pp. 121–124.
2. P. Dénes, *Uber irreguläre Kreiskörper*, Publ. Math. Debrecen, vol. 3 (1953), pp. 17–23.
3. ———, *Über Grundeinheitssysteme der irregulären Kreiskörper von besonderen Kongruenzeigenschaften*, Publ. Math. Debrecen, vol. 3 (1954), pp. 195–204.
4. ———, *Über den zweiten Faktor der Klassenzahl und den Irreguläritatsgrad der irregulären Kreiskörper*, Publ. Math. Debrecen, vol. 4 (1956), pp. 163–170.
5. Y. Hellegouarch, *Sur un théorème de Maillet*, C. R. Acad. Sci. Paris Sér. A, vol. 273 (1971), pp. 477–478.
6. K. Inkeri, *Untersuchungen über die Fermatsche Vermutung*, Ann. Acad. Sci. Fenn. Ser. A I, Math.-Phys. no. 33 (1946), 60 pp.

7. K. IWASAWA, *Lectures on p-adic L-functions*, Princeton Univ. Press, Princeton, NJ, 1972.
8. S. LANG, *Algebraic number theory*, Addison-Wesley, Reading, Mass., 1970.
9. E. MAILLET, *Sur l'équation indéterminée* $ax^{\lambda^l} + by^{\lambda^l} = cz^{\lambda^l}$, Assoc. française pour l'Avancement des Sciences, vol. 26 (1897), II, pp. 156–168.
10 T. MORISHIMA, *Über die Fermatsche Vermutung, IV*, Proc. Jap. Acad., vol. 6 (1930), pp. 243–244.
11. F. POLLACZEK, *Über die irregulären Kreiskörper der l-ten und* l^2*-ten Einheitswurzeln*, Math. Zeitschr., vol. 21 (1924), pp. 1–38.
12. H. S. VANDIVER, *On Fermat's last theorem*, Trans. Amer. Math. Soc., vol. 31 (1929), pp. 613–642.
13. S. WAGSTAFF, JR., *The irregular primes to* 125000, Math. Comp., vol. 32 (1978), pp. 583–591.
14. L. WASHINGTON, *A note on p-adic L-functions*, J. Number Theory, vol. 8 (1976), pp. 245–250.
15. ———, *The calculation of* $L_p(1, \chi)$, J. Number Theory, vol. 9 (1977), pp. 175–178.
16. ———, *On Fermat's last theorem*, J. Reine Angew. Math., vol. 289 (1977), pp. 115–117.

UNIVERSITY OF MARYLAND
COLLEGE PARK, MARYLAND