PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 93, Number 1, January 1985

ON SOME CYCLOTOMIC CONGRUENCES OF F. THAINE

LAWRENCE C. WASHINGTON[1]

ABSTRACT. Some congruences involving cyclotomic integers, orginally obtained by F. Thaine, are proved and strengthened by using p-adic logarithms and p-adic L-functions.

In a recent paper, F. Thaine [**1**] obtained some congruences on cyclotomic numbers via his theory of combinatory polynomials. In the present paper we show, in the spirit of [**3**], that the p-adic logarithm yields a general method for attacking such problems. As an application we strengthen and give alternative proofs for Thaine's results. Classically, Kummer's logarithmic differential quotient has been used on this type of problem, but it seems that the p-adic logarithm is more natural and connects more easily with the theory of p-adic L-functions, as in the proof of Theorem 2.

Let p be an odd prime, ς a primitive pth root of unity, and $\pi = 1 - \varsigma$. Let a, b, and f be rational integers, and let

$$B = \prod_{k=1}^{p-1} (a + b\varsigma^k)^{k^r}.$$

Such expressions arise in the study of Fermat's Last Theorem [**1**].

THEOREM 1 (F. THAINE). *Let $1 \le r \le p-3$ and suppose $p \nmid ab(a+b)$. If there exists $q \in \mathbf{Z}$ with $B \equiv q \bmod p$, then*

$$(*) \qquad \sum_{k=1}^{p-1} k^{p-2-r} \left(\frac{-b}{a}\right)^k \equiv 0 \mod p.$$

Conversely, if $(*)$ holds, then there exists $q \in \mathbf{Z}$ with $B \equiv q^p \bmod p\pi^2$.

Let

$$A = \prod_{k=1}^{p-1} \left(\frac{1-\varsigma^k}{1-\varsigma}\right)^{k^r}.$$

Units similar to A appear in the study of Fermat's Last Theorem [**2**, Chapter 8].

THEOREM 2. *Let r be even, $2 \le r \le p-3$. If there exists $q \in \mathbf{Z}$ with $A \equiv q \bmod p$, then p divides the Bernoulli number B_{p-1-r}. Conversely, if $p | B_{p-1-r}$, then there exists $q \in \mathbf{Z}$ with $A \equiv q^p \bmod p\pi^2$.*

The first half of Theorem 2 was proved by Thaine. He conjectured a weaker form of the second half and proved it when 2 is a primitive root $\bmod p$.

Received by the editors February 16, 1984.
1980 *Mathematics Subject Classification*. Primary 10A40, 12A35; Secondary 12B30, 10B15.
[1]Research partially supported by NSF.

Actually, the assumption that r is even in Theorem 2 is not needed: $B_{p-1-r} = 0$, but A is a pth power of a real number, when r is odd, from which it follows easily that $A \equiv q^p \bmod p\pi^2$ is satisfied. It may seem surprising at first that $A \equiv q \bmod p$ implies the stronger $A \equiv q_1^p \bmod p\pi^2$. However, $A \equiv q \bmod p$ implies $A \equiv q_2 \bmod p\pi$ for some $q_2 \in \mathbf{Z}$. Since A is real, the congruence can be taken $\bmod p\pi^2$. Since A is a unit, hence has norm 1, it follows that $q_2^{p-1} \equiv 1 \bmod p\pi^2$, so $A \equiv q_2 \equiv q_1^p \bmod p\pi^2$ for some q_1.

Our main tool in the proofs of the theorems will be the p-adic logarithm. Let

$$\log_p(1+x) = x - \frac{x^2}{2} + \frac{x^3}{3} - \cdots,$$

which is defined for $\pi | x$. If $y \in \mathbf{Z}_p[\varsigma]$ with $\pi \nmid y$, then we let

$$\log_p y = \frac{1}{(p-1)} \log_p(1+x)$$

with $x = y^{p-1} - 1$. It is easy to show that $\log_p \varsigma = 0$ and that $\log_p(1+x) \equiv x \bmod \pi x$ if $\pi^2 | x$. If $y = 1 + a_1\pi + a_2\pi^2 + \cdots$, then $\varsigma^{-a_1} y \equiv 1 \bmod \pi^2$, hence $\log_p y = \log_p(\varsigma^{-a_1} y) \equiv 0 \bmod \pi^2$. It follows that $\log_p y \equiv 0 \bmod \pi^2$ for all y. If $y \in \mathbf{Z}$, then $\log_p y \equiv 0 \bmod p$. Using the congruence $\binom{p}{j}/p \equiv (-1)^{j-1}/j \bmod p$ for $1 \le j \le p-1$, one easily shows that if $\pi | x$ then

$$\log_p(1+x) \equiv \frac{(1+x)^p - 1}{p} \mod p\pi^2.$$

LEMMA. *Let $\gamma \in \mathbf{Z}[\varsigma]$ satisfy $\pi \nmid \gamma$, and let $g \in \mathbf{Z}$. If $\log_p \gamma \equiv 0 \bmod \pi^g$, then there exist $q, t \in \mathbf{Z}$ such that $\gamma \equiv \varsigma^t q^{p^s} \bmod \pi^g$, where $s = [(g-1)/(p-1)]$. If γ is congruent to a rational integer $\bmod \pi^2$, then $t = 0$.*

Conversely, if $\gamma \equiv \varsigma^t q^{p^s} \bmod \pi^g$ with s as above, then $\log_p \gamma \equiv 0 \bmod \pi^g$.

PROOF. If $\gamma = a_0 + a_1\pi + \cdots$, then $\varsigma^{-a_1/a_0}\gamma \equiv a_0 \bmod \pi^2$, so we shall henceforth assume γ is congruent to a rational integer $\bmod \pi^2$ and prove the first half of the lemma with $t = 0$. Let π^e be the largest power of π such that γ is congruent to a rational integer $\bmod \pi^e$, and write $\gamma = x + y\pi^e$ with $x \in \mathbf{Z}$, $p \nmid x$, and $y \in \mathbf{Z}[\varsigma]$ (if a largest e does not exist, let $e \ge g$ be arbitrary). We have

$$\log_p \gamma = \log_p x + \log_p\left(1 + \frac{y}{x}\pi^e\right). \tag{1}$$

Suppose $e < g$. In particular, e is then maximal, so $\pi \nmid y$. Since π^{p-1}/p is a unit and congruent to an integer $\bmod \pi$, it follows that $e \not\equiv 0 \bmod p-1$. By the hypothesis on γ and a property of $\log_p$ mentioned above, we have

$$0 \equiv \log_p x + \frac{y}{x}\pi^e \mod \pi^{e+1}.$$

Since $x \in \mathbf{Z}$, $v_\pi(\log_p x) \equiv 0 \bmod p-1$ so $v_\pi(\log_p x) \ne e = v_p(y\pi^e/x)$. This contradicts the above congruence, so we must have $e \ge g$. Therefore $\gamma \equiv x \bmod \pi^g$, and (1) yields $\log_p x \equiv 0 \bmod \pi^g$. But this implies that $x^{p-1} - 1 \equiv 0 \bmod \pi^g$, hence $\bmod p^{s+1}$, where s is as in the lemma. It follows that $x \equiv q^{p^s} \bmod p^{s+1}$, therefore $\bmod \pi^g$, for some $q \in \mathbf{Z}$. This proves the first half of the lemma.

Now suppose $\gamma \equiv \varsigma^t q^{p^s} \bmod \pi^g$. Let $\gamma_1 = \varsigma^{-t}\gamma$. Then $\gamma_1^{p-1} \equiv 1 \bmod \pi^g$, so

$$\log_p \gamma = \log_p \gamma_1 = \frac{1}{p-1} \log_p \gamma_1^{p-1} \equiv 0 \mod \pi^g.$$

This completes the proof of the lemma.

Let a, b be as in Theorem 1 and let $\alpha = b/(a+b)$. Then

$$\begin{aligned}\log_p(a+b\varsigma) &= \log_p(a+b) + \log_p(1-\alpha\pi) \equiv \log_p(a+b) + \frac{(1-\alpha\pi)^p - 1}{p} \\ &\equiv \log_p(a+b) + \frac{(1-\alpha+\alpha\varsigma)^p - 1}{p} \\ &\equiv \log_p(a+b) + \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j}(1-\alpha)^{p-j}\alpha^j\varsigma^j + \frac{\alpha^p - 1 + (1-\alpha)^p}{p} \mod p\pi^2.\end{aligned}$$

A similar result holds with ς replaced by ς^k, $1 \le k \le p-1$.

Let ω be the Teichmüller character, so $\omega(k) \equiv k \bmod p$, $\omega(k)^{p-1} = 1$. Note that $\omega^r(k) \equiv k^r \bmod p$. Let

$$g(\omega^r) = \sum_{k=1}^{p-1} \omega^r(k)\varsigma^k$$

be the Gauss sum. Then

$$\sum_{k=1}^{p-1} \omega^r(k)\varsigma^{jk} = \omega^{-r}(j)g(\omega^r).$$

It is known (see [**2**, Lemma 6.14]) that $v_\pi(g(\omega^r)) = p-1-r$ for $1 \le r \le p-2$. With B as in Theorem 1 we have

$$\begin{aligned}\log_p B &= \sum_{k=1}^{p-1} k^r \log_p(a+b\varsigma^k) \\ &\equiv \sum_{k=1}^{p-1} \omega^r(k)\log_p(a+b\varsigma^k) \mod p\pi^2,\end{aligned}$$

since $\log_p y \equiv 0 \bmod \pi^2$, as mentioned above. Since $\sum \omega^r(k) = 0$ it follows that

$$\log_p B \equiv \sum_{j=1}^{p-1} \frac{1}{p}\binom{p}{j}(1-\alpha)^{p-j}\alpha^j\omega^{-r}(j)g(\omega^r) \mod p\pi^2.$$

Since $1 \le r \le p-3$ we have $g(\omega^r) \equiv 0 \bmod \pi^2$. Therefore, using $\binom{p}{j}/p \equiv (-1)^{j-1}/j$ and $\omega^{-r}(j) \equiv j^{-r} \bmod p$, we obtain

$$\begin{aligned}\log_p B &\equiv \sum_{j=1}^{p-1} (-1)^{j-1}(1-\alpha)^{p-j}\alpha^j j^{p-2-r} g(\omega^r) \\ &\equiv -g(\omega^r)(a+b)^{-p} \sum_{j=1}^{p-1} \left(\frac{-b}{a}\right)^j j^{p-2-r} \mod p\pi^2.\end{aligned}$$

If $B \equiv q \bmod p$ then $\log_p B \equiv 0 \bmod p$. Since $v_\pi(g(\omega^r)) < p-1$, it follows that the sum $(*)$ in Theorem 1 is $0 \bmod p$. Conversely, if the sum is $0 \bmod p$ then $\log_p B \equiv 0 \bmod p\pi^2$, so $B \equiv \varsigma^t q^p \bmod p\pi^2$ for some q, t.

Since $\varsigma^k = (1-\pi)^k \equiv 1 - k\pi \bmod \pi^2$, we have

$$\begin{aligned} B &\equiv \prod_{k=1}^{p-1} (a+b-bk\pi)^{k^r} \equiv (a+b)^{\sum k^r} \prod \left(1 - \frac{bk^{r+1}\pi}{a+b}\right) \\ &\equiv (a+b)^{\sum k^r} \left(1 - \frac{b\pi}{a+b} \sum k^{r+1}\right) \equiv (a+b)^{\sum k^r} \mod \pi^2. \end{aligned}$$

Therefore $t = 0$ and $B \equiv q^p \bmod p\pi^2$. This proves Theorem 1.

Theorem 2 does not follow directly from Theorem 1 since it corresponds to the case $p|a+b$. Hence we use slightly different techniques. We have

$$\begin{aligned} \log_p A &= \sum_{k=1}^{p-1} k^r \log_p(1 - \varsigma^k/1 - \varsigma) \\ &\equiv \sum_{k=1}^{p-1} \omega^r(k) \log_p(1 - \varsigma^k) \mod p\pi^2. \end{aligned}$$

Let $L_p(s, \omega^{-r})$ denote the p-adic L-function attached to the character ω^{-r}. Then (see [**2**, Chapter 5])

$$\begin{aligned} &L_p(x, \omega^{-r}) \equiv L_p(y, \omega^{-r}) \mod p \qquad \text{for all } x, y \in \mathbf{Z}_p, \\ &L_p(1, \omega^{-r}) = -\frac{g(\omega^{-r})}{p} \sum_{k=1}^{p-1} \omega^r(k) \log_p(1 - \varsigma^k), \\ &L_p(2 + r - p, \omega^{-r}) = -(1 - p^{p-r-2}) \frac{B_{p-1-r}}{p-1-r} \equiv \frac{1}{r+1} B_{p-1-r} \mod p, \end{aligned}$$

where B_n denotes the nth Bernoulli number. Note that $v_\pi(p/g(\omega^{-r})) = p-1-r$ and that $2 \le p-1-r \le p-3$. It follows that

$$\log_p A \equiv -\frac{p}{g(\omega^{-r})} \frac{1}{r+1} B_{p-1-r} \mod p\pi^2.$$

Therefore $\log_p A \equiv 0 \bmod p \Rightarrow p|B_{p-1-r} \Rightarrow \log_p A \equiv 0 \bmod p\pi^2$. Also,

$$\begin{aligned} \frac{1 - \varsigma^k}{1 - \varsigma} &= 1 + \varsigma + \cdots + \varsigma^{k-1} = 1 + (1-\pi) + \cdots + (1-\pi)^{k-1} \\ &\equiv k - \frac{1}{2} k(k-1)\pi \mod \pi^2, \end{aligned}$$

so

$$\begin{aligned} A \equiv \prod k^{k^r} \prod \left(1 - \frac{k-1}{2}\pi\right)^{k^r} &\equiv \left(\prod k^{k^r}\right) \left(1 - k^r \sum \frac{k-1}{2}\pi\right) \\ &\equiv \prod k^{k^r} \mod \pi^2. \end{aligned}$$

Theorem 2 now follows easily from the lemma.

The proof of Theorem 2 may easily be extended to yield the following: choose integers $\omega_N^r(k) \equiv \omega^r(k) \bmod p^N$ and let

$$A_N = \prod_{k=1}^{p-1} \left(\frac{1-\zeta^k}{1-\zeta} \right)^{\omega_N(k)^r}.$$

Then

$$A_N \equiv q^{p^{N-1}} \bmod p^N \Rightarrow p^{2N-1} | B_{p^{N-1}(p-1-r)} \Rightarrow A_N \equiv q^{p^N} \mod p^N \pi^2.$$

Finally, we note that Theorem 1 is also true for $r = p-2$ if we replace the congruence $\bmod p\pi^2$ with a congruence $\bmod p\pi$. The proof is the same, except that $v_\pi(g(\omega^{p-2})) = 1$, so the congruences $\bmod p\pi^2$ must be changed to congruences $\bmod p\pi$ in the later stages of the proof.

REFERENCES

1. F. Thaine, *Polynomials generalizing binomial coefficients and their application to the study of Fermat's Last Theorem*, J. Number Theory **15** (1982), 304–317.
2. L. Washington, *Introduction to cyclotomic fields*, Springer-Verlag, New York, Heidelberg and Berlin, 1982.
3. ——, *Units of irreduglar cyclotomic fields*, Illinois J. Math. **23** (1979), 635–647.

DEPARTMENT OF MATHEMATICS, UNIVERSITY OF MARYLAND, COLLEGE PARK, MARYLAND 20742