FERMAT'S LAST THEOREM AND THE SECOND FACTOR IN THE CYCLOTOMIC CLASS NUMBER

BY H. S. VANDIVER

1. *Introduction.* As usual in the relation

$$x^l + y^l + z^l = 0, \tag{1}$$

where l is an odd prime and x, y, z are rational integers prime to each other and none zero, we shall refer to the case where xyz is prime to l as case I; if $xyz \equiv 0 \pmod{l}$ then we call this case II. I now give a sketch of a proof of a theorem which appears to be the principal result I have so far found concerning the first case of the last theorem.

THEOREM 1. *If* (1) *is possible in case* I, *then the second factor of the class number of the cyclotomic field defined by*

$$\zeta = e^{2i\pi/l}$$

is divisible by l.

From (1) in case I we have either

$$x + \zeta y = \eta\omega_1\omega_2 \cdots \omega_s\alpha^l, \tag{2}$$

or

$$x + \zeta y = \sigma\beta^l, \tag{2a}$$

where η and σ are units, α is a number, and β is an integer in $k(\zeta)$, while each ω is the lth power of an ideal in $k(\zeta)$, not a principal ideal, and, as shown by Pollaczek,*

$$\omega_i^{s-r\alpha_i} = \delta\gamma^l,$$

where δ is the unit in $k(\zeta)$, a_i is in the set $1, 2, \cdots, l-2$, r is a primitive root of l and we are employing the Kronecker-Hilbert notation of symbolic powers, s denoting the substitution (ζ/ζ^r). We also have (Pollaczek†) for a_i even

$$\omega_i/\omega_{-i} = \delta_i\gamma_i^l,$$

* Mathematische Zeitschrift, vol. 21 (1924), pp. 19 and 22.

† Loc. cit., p. 22.

where γ_i is a number in $k(\zeta)$, δ_1 is a unit and ω_{-i} is obtained from ω_i by the substitution (ζ/ζ^{-1}). Applying this to (2), we have

$$\frac{x+\zeta y}{x+\zeta^{-1}y} = \zeta^t \xi_1 \xi_2 \cdots \xi_\nu \theta^l, \tag{3}$$

where

$$\xi_j^{s-r^{2i+1}} = \eta_1 \theta_1^{\,l}, \tag{3a}$$

η_1 being a unit in $k(\zeta)$.

The writer* has shown that

$$\prod_{\nu=1}^{k-1} \prod_{a=1}^{[\nu l/k]} (x+\zeta^{[1:a]}y)^2 = \zeta^t \rho^{2l}, \tag{4}$$

where k is an integer, $1<k<l$, ρ is an integer in the field $k(\zeta)$, t is an integer such that

$$t \equiv \frac{-2kyq(k)}{x+y} \pmod{l},$$

$[1:a]$ is the least positive solution of $Xa \equiv 1 \pmod{l}$, and $q(k)=(k^{l-1}-1)/l$. We also have

$$x+y = c^l, \tag{5}$$

where c is a rational integer.

Let $\mathfrak{p}$ be a prime ideal divisor of one of the ω's in (2). In the relation (4) put $k=2$ and ζ^h for ζ. We now employ this relation in much the same manner as in a former paper of the writer.† If in (4) there is an a such that

$$h[1:a] \equiv 1 \pmod{l},$$

then set ζ^{-h} in lieu of ζ^h throughout the relation of (4). For $k=2$, a ranges over the integers $1, 2, \cdots, (l-1)/2$. Then we cannot have any exponent of ζ which is $\equiv 1 \pmod{l}$, for if so we would have

$$-h[1:a_1] \equiv 1 \pmod{l},$$

where a_1 is one of the a's. This gives

* Annals of Mathematics, vol. 26 (1925), p. 217.

† Annals of Mathematics, vol. 26 (1925), pp. 227–229.

$$[1:a_1] \equiv -[1:a] \pmod{l},$$

which is impossible.

Equating lth power characters of each member of (4) with respect to $\mathfrak{p}$ we obtain, since each binomial factor is prime to $x+\zeta y$,

$$\prod_a \left\{\frac{x+\zeta^{\pm h[1:a]}y}{\mathfrak{p}}\right\}^2 = \left\{\frac{\zeta^{\pm ht}}{\mathfrak{p}}\right\}; \tag{6}$$

when $k=2$ the sign of h is selected so that

$$h[1:a] \not\equiv 1 \pmod{l}.$$

From the theorem of Furtwängler* we obtain

$$\left\{\frac{\zeta}{\mathfrak{p}}\right\} = 1.$$

Also we note that

$$x + \zeta^i y = (x + \zeta y) + y\zeta(\zeta^{i-1} - 1).$$

Applying this to (5), after taking lth power characters with respect to $\mathfrak{p}$, and also to (6), we have, after comparison,

$$\prod_a \left\{\frac{C_a}{\mathfrak{p}}\right\} = 1, \tag{7}$$

where

$$C_a = \frac{\zeta^{\pm h[1:a]-1} - 1}{\zeta - 1}.$$

Set

$$\sigma = \frac{\zeta^t - 1}{\zeta - 1},$$

where t is any integer $\not\equiv 0 \pmod{l}$, and

$$\left\{\frac{\sigma}{\mathfrak{p}}\right\} = \zeta^T,$$

and write

* Wiener Berichte, Abteilung IIa, vol. 121 (1912), pp. 589–592.

$$T = \operatorname{ind}\left(\frac{\zeta^t - 1}{\zeta - 1}\right).$$

We then have (Vandiver*)

$$\operatorname{ind}\left(\frac{\zeta^t - 1}{\zeta - 1}\right) \equiv \frac{1}{2}(t-1)\operatorname{ind}\zeta - 2\sum_{n=1}^{l_1}\frac{(t^{2n}-1)\operatorname{ind}E_n(\zeta)}{r^{2n}-1} \pmod{l},$$

where

$$E_n = \prod_{i=0}^{l_1}\epsilon(\zeta^{r^i})^{r^{-2in}}, \quad \epsilon = \left(\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}\right)^{1/2}, \quad (l_1 = l - 3/2).$$

Applying this to (7), we obtain

$$\sum_{n=1}^{l_1}\sum_{a=1}^{l_1+1}\frac{((\pm h[1:a]-1)^{2n}-1)\operatorname{ind}E_n(\zeta)}{r^{2n}-1} \equiv 0 \pmod{l}.$$

Now expanding the left hand members in powers of h, we find

$$\pm hA_1R_1 + h^2A_2R_2 + \cdots (\pm h)^{l-4}A_{l-4}R_{l-4} \equiv 0 \pmod{l},$$

where the A's are expressions involving r and $\operatorname{ind}E_n(\zeta)$, and

$$R_i = \sum_{a=1}^{l_1+1}[1:a]^i.$$

For i even, this is known to be divisible by l and we obtain

$$hA_1R_1 + h^3A_3R_3 + \cdots + h^{l-4}A_{l-4}R_{l-4} \equiv 0 \pmod{l}.$$

Letting $h = 1, 2, \cdots, l_1$ in turn, we obtain l_1 congruences and the determinant in the AR's is an alternant which is prime to l, so that

$$A_jR_j \equiv 0 \pmod{l}, \qquad (j = 1, 3, \cdots, l-4).$$

We also have, if

$$b_1 = -\tfrac{1}{2}, \quad b_{2i} = (-1)^{i+1}B_i, \quad b_{2i+1} = 0, \qquad (i > 0),$$

where the B's are Bernoulli's numbers,

* Transactions of this Society, vol. 31 (1929), p. 634.

$$\frac{(1-2^i)b_i}{2^{i-1}i} \equiv R_{l-i} \pmod{l}, \qquad (i < l-1);$$

$$(1-2^{2n})B_n A_{l-2n} \equiv 0 \pmod{l}, \qquad (n = 2, 3, \cdots, l_1).$$

Let $n=2, 3, 4, 5, 6$, and 7. These give, except for small values of l for which (1) is known to be impossible in case I, $A_{l-2n} \equiv 0 \pmod{l}$. We have

$$A_{l-4} = \frac{2(l-3)}{r^{l-3}-1} \operatorname{ind} E_{l_1}(\zeta);$$

hence

$$\operatorname{ind} E_{l_1}(\zeta) \equiv 0 \pmod{l}.$$

Similarly,

$$A_{l-6} = 2\binom{l-3}{3} \frac{\operatorname{ind} E_{l_1}(\zeta)}{r^{l-3}-1} + \frac{2(l-5)\operatorname{ind} E_{l_1-1}(\zeta)}{r^{l-5}-1},$$

which gives

$$\operatorname{ind} E_{l_1-1}(\zeta) \equiv 0 \pmod{l}.$$

Similarly,

$$\operatorname{ind} E_{l_1-j}(\zeta) \equiv 0 \pmod{l}, \qquad (j = 2, 3, 4, 5).$$

Now take any (ω) which appears in (2). There exists an ideal $\mathfrak{a}$, not principal, such that $\mathfrak{a}^{l^a} = (\omega)$, but $\mathfrak{a}^{l^{a-1}}$ is not principal. In lieu of $\mathfrak{p}$ in the above argument we may now set $\mathfrak{a}$ since it is the product of prime ideals. Then we may write

$$\left\{\frac{E_{l_1-j}(\zeta)}{\mathfrak{a}}\right\} = 1, \qquad (j = 0, 1, 2, 3, 4, 5).$$

We now have, however (Vandiver*), where $\operatorname{ind} E_n(\zeta)$ is taken with respect to $\mathfrak{a}$ in lieu of $\mathfrak{p}$,

$$\operatorname{ind} E_n \equiv \frac{r^{2n}-1}{2}(-1)^{(s-1)/2} \frac{B_{(s+1)/2}}{l^a} D(\omega', l) \pmod{l},$$

where

* Transactions of this Society, vol. 32 (1930), p. 400.

$$D(\omega', t) = \left[\frac{d^t \log \omega'(e^v)}{dv^t}\right]_{v=0},$$

$$t = (l - 2n)l^a, \quad \mathfrak{a}^{l^a(l-1)} = \omega', \quad \omega' \equiv 1 \pmod{\lambda},$$

$$\lambda = (1 - \zeta), \quad s = (2n - 1)l^a.$$

The second factor of the class number $k(\zeta)$ will now be assumed prime to l. We may employ a result in another paper (Vandiver*) and we see that $B_{(s+1)/2}$ is divisible by l^a, but not by l^{a+1}, so that $D(\omega', t) \equiv 0 \pmod{l}$, from which we obtain easily, provided $\mathfrak{a}$ belongs to the ideal class corresponding to B_n in the sense of the theorem on page 206 of that paper,

$$\left[\frac{d^{l-2n} \log \omega(e^v)}{dv^{l-2n}}\right]_{v=0} \equiv 0 \pmod{l}. \tag{8}$$

From (3) and (3a) we may derive identities in e^v, and taking these in connection with (2) and (2a), we obtain

$$\left[\frac{d^k \log \xi_j(e^v)}{dv^k}\right]_{v=0} \equiv 0 \pmod{l}, \quad (l - 1 > k \neq 2i + 1),$$

and also

$$\left[\frac{d^3 \log (x + e^v y)}{dv^3}\right]_{v=0} \equiv 0 \pmod{l},$$

after using (8) for $n = l_1$. In a similar way we obtain this relation with (x, z) or (y, z) in lieu of (x, y). These relations will then give easily

$$x \equiv y \equiv z \pmod{l},$$

and this is impossible for $l > 3$. Hence the second factor of the class number is divisible by l. This completes the (abbreviated) proof of Theorem 1.

2. *Second Factor of $k(\zeta)$ Divisible by l.* The preceding methods yield some criteria also in the case where the second factor of the class number of $k(\zeta)$ is divisible by l. Using some results due to Pollaczek,† we shall find in this case that there exists a singu-

* Proceedings of the National Academy of Sciences, vol. 15 (1929), p. 206.

† Loc. cit., pp. 19–22.

lar primary unit in $k(\zeta)$ corresponding to certain ω's in (2). It may be shown from this that we must have some of the E's equal to lth powers of units in $k(\zeta)$. In fact we find this result:*

THEOREM 2. *If the relation* (1) *is satisfied in case* I, *then, if* η_j *is a unit in* $k(\zeta)$,

$$E_{l_1-j} = \eta_j^l, \qquad (j = 0, 1, 2, 3, 4, 5),$$

and

$$B_s \equiv 0 \pmod{l^2}, \quad (i = 1, 2, 3, 4, 5, 6; s = n_i(l_1 + 1) - i),$$

where the n's each range independently over all positive integral values.

Use of Theorems 1 and 2 enables us to extend theorems† which have already been found for case II of (1). For example, five theorems as mentioned in another paper can now all be given without restriction to case II only, which restriction appears in Theorems 1 and 4.

Elsewhere‡ the writer has shown that if (1) is satisfied with $y \equiv 0 \pmod{l}$, $xz \not\equiv 0 \pmod{l}$, $x+z \not\equiv 0 \pmod{n}$, with n any integer $\not\equiv 0$ or $1 \pmod{l}$, then

$$q(n)D_0 \equiv 0, \quad q(n)B_{s+1}D_s \equiv 0 \pmod{l}, \quad (s = 1, 3, \cdots, l-4);$$

and in addition one of the following two relations holds:

$$q(n)D_{l-2} \equiv 0, \qquad q(n)\left(D_{l-2} + \frac{I(\zeta)}{2}\right) \equiv 0 \pmod{l},$$

where

$$q(n) = \frac{n^{l-1} - 1}{l}, \quad D_s = \sum_{d=1}^{l-1} d^s I(\zeta^d - \beta^a), \quad \left\{\frac{\zeta}{\mathfrak{p}}\right\} = \zeta^{I(\zeta)},$$

where β is a primitive $(n-1)$th root of unity and $\mathfrak{p}$ is a prime ideal divisor of n.

---

* This result as far as the B's are concerned is an extension of a theorem previously given by the writer, Proceedings of the National Academy of Sciences, vol. 16 (1930), p. 298.

† Vandiver, Proceedings of the National Academy of Sciences, vol. 17 (1931), pp. 670–671.

‡ Transactions of this Society, vol. 29 (1927), p. 161.

Now if in lieu of the assumption of $x+z\not\equiv 0 \pmod{n}$, which appeared in the above theorem, we have proved that $x+z\equiv 0 \pmod{n}$, we may proceed as in a former paper* and obtain the result that (1) is impossible if $y\equiv 0 \pmod{l}$, $xz\not\equiv 0 \pmod{l}$, and $x+z\equiv 0 \pmod{n}$, under the additional assumption that

$$\left\{\frac{E_a}{\mathfrak{p}}\right\} \neq 1$$

holds, where a ranges over the values $a_1, a_2, \cdots, a_s$, these integers being the subscripts of the Bernoulli numbers in the set $B_1, B_2, \cdots, B_{l_1}$ which are divisible by l.

Putting the preceding results together, we obtain a new criterion for the impossibility of (1) if we note that case I of (1) is covered by our assumptions concerning E_a. We note also† that we may extend this to the case where

$$n \equiv 1 \pmod{l}.$$

The theorem last mentioned as well as Theorem 1 indicates that much of the writer's work concerning Fermat's Last Theorem is tending toward the possible conclusion that if the second factor of the class number of $k(\zeta)$ is prime to l, then Fermat's Last Theorem is true.

A curious point in connection with the second case of the theorem is the fact that it is not conclusive that any of the methods used so far absolutely depend on the fact that x, y, and z in (1) are rational integers. For example, in Theorem V of a former article I employ the fact that x, y, and z are rational integers during the proof, but it is not shown that a similar argument breaks down when x, y, and z are integers‡ in the field $k(\zeta+\zeta^{-1})$.

In view of these considerations it may happen that Fermat's Last Theorem is true for rational integers, but for integers in the field of $k(\zeta+\zeta^{-1})$ it is not true. Possibly the method of infinite descent properly belongs to the treatment of this generalization.

---

* Transactions of this Society, vol. 31 (1929), p. 634.

† Transactions of this Society, vol. 29 (1927), p. 162, §5.

‡ Fueter raised this question in connection with Theorem 5, during a conversation with me.

A bit of light is shown on the possibilities mentioned in the last paragraph if we consider the argument employed to prove Theorem IV in another article.* In this proof we started with the relation $\omega^l+\theta^l+\phi^l=0$, where ω, θ, and ϕ are integers in the field $k(\zeta+\zeta^{-1})$. This assumption enabled us to transpose θ^l in the above relation, factor, and obtain the relation (25a) of the last mentioned paper. However, if we had started with the equation

$$\omega^l + \theta^l = \eta\phi^l,$$

where ϕ is divisible by $(1-\zeta)$, we would obtain, by proceeding somewhat as in the derivation of (25a) in the article just referred to,

$$\omega \equiv \pm\, \theta \pmod{\mathfrak{p}};$$

and if

$$\omega \equiv \theta \pmod{\mathfrak{p}},$$

then, using (1), we have

$$2\omega^l \equiv \eta\phi^l \pmod{\mathfrak{p}}.$$

This gives the result that $2/\eta$ is congruent to an lth power modulo $\mathfrak{p}$. It seems necessary then to include among our assumptions the statement that such a congruence does not hold, and this was not necessary in the case where $\eta=1$.

THE UNIVERSITY OF TEXAS

* Transactions of this Society, vol. 31 (1929), pp. 631–632.