Journal of Number Theory **80**, 174–186 (2000)
Article ID jnth.1999.2438, available online at http://www.idealibrary.com on IDEAL®

On a Fermat-Type Diophantine Equation

Sankar Sitaraman[1]

Department of Mathematics, Howard University, Washington, DC 20059

Communicated by A. Granville

Received June 30, 1998

Let $p>3$ be an odd prime and ζ a pth root of unity. Let c be an integer divisible only by primes of the form $kp-1$, $(k,p)=1$. Let $C_p^{(i)}$ be the eigenspace of the ideal class group of $\mathbf{Q}(\zeta)$ corresponding to ω^i, ω being the Teichmuller character. Let B_{2i} denote the $2i$th Bernoulli number. In this article we apply the methods (following H. S. Vandiver (1934, *Bull. Amer. Math. Soc.*, 118–123)) which were used by the author (1994, Ph.D. Thesis, California Institute of Technology) to prove a special case Fermat's Last theorem, to study the equation $x^p+y^p=pc\,z^p$. In particular, we prove the following: Assume p is irregular, and $p \mid B_{p-3}$. Let q be an odd prime such that $q\equiv 1 \pmod p$, and there is a prime ideal Q over q in $\mathbf{Q}(\zeta)$ whose ideal class generates $C_p^{(3)}$, which is known to be cyclic. If $x^p+y^p=pc\,z^p$ has nontrivial integer solutions, then we show that $q \nmid (pc\,z^p/(x+y))$. We also give proof of the unsolvability of the above equation for regular primes $(p>3)$, using the results of H. S. Vandiver (1936, *Monatsh. Math. Phys.* **43**, 317–320).

INTRODUCTION

Let p be an odd prime. Since the proof of Fermat's Last Theorem [W, TW], i.e., that $x^p+y^p=z^p$ has no nontrivial solutions, it has been known that [R, DM] the same techniques can be used to prove the unsolvability of equations of the form $Ax^p+By^p=Cz^p$, where A, B, C are constants. But the same is not true for equations such as $x^p+y^p=pc\,z^p$, when there are a large number of unrestricted prime divisors in the coefficient pc. In this paper we consider the above equation when $p>3$ and c is divisible only by primes of the form $kp-1$, $(k,p)=1$.

Let ζ a pth root of unity. Let C_p be the p-Sylow subgroup of the ideal class group of $\mathbf{Q}(\zeta)$, with order h_p. Let C_p^+ and h_p^+ denote the p-Sylow subgroup of $\mathbf{Q}(\zeta+\zeta^{-1})$, and its order, respectively. The Teichmüller character $\omega\colon \mathbf{Z}_p\to\mathbf{Z}_p^*$ is given by $\omega(x)\equiv x \pmod p$, where $\omega(x)$ is a

[1] I thank D. Ramakrishnan for suggesting this problem and his encouragement. I also thank L. Washington for his valuable comments, and L. Shapiro and F. Ramaroson for helpful conversations. I am also grateful to the referee for his valuable suggestions for improving the paper.

0022-314X/00 $35.00

$(p-1)$st root of unity, and $x \in \mathbf{Z}_p$. Under the action of this character, C_p decomposes as a direct sum of $C_p^{(i)}$, where $C_p^{(i)}$ is the eigenspace corresponding to ω^i. It is known, by a result of Kurihara [Ku] (also independently observed by Greenberg), that $C_p^{(3)}$ is cyclic.

The main results of this paper are the following.

Theorem 1.2. *Let $p > 3$ be a regular prime, and c an integer divisible only by primes of the form $kp-1$, $(k, p) = 1$. Then $x^p + y^p = pc\,z^p$ has no nontrivial integer solutions.*

This theorem follows easily from the results of [V4]. It can be shown that the theorem is true for certain irregular primes as well using the same methods (cf. [Wa, Chap. 9]). In particular, for p such that $p \nmid h_p^+$, $p^3 \nmid \mathbf{B}_{pi}$ for all even $i \leqslant p-3$.

The following theorem also concerns irregular primes, but without the assumption that $p \nmid h_p^+$. Note that, in any ideal class of $\mathbf{Q}(\zeta)$, one has an infinite number of prime ideals of degree 1 by the Tchebotarev density theorem (cf. [C, p. 257, Wa, p. 333]). So given an ideal class that generates $C_p^{(3)}$ there are an infinite number of prime ideals of $\mathbf{Q}(\zeta)$ in this ideal class which lie over rational primes congruent to 1 modulo p.

Theorem 2.1. *Assume p is irregular, and $p \mid B_{p-3}$, and c is as in Theorem* 1.2. *Let q be an odd prime such that $q \equiv 1$* (mod p), *and there is a prime ideal Q over q in $\mathbf{Q}(\zeta)$ whose ideal class generates $C_p^{(3)}$. If $x^p + y^p = pc\,z^p$ has nontrivial solutions $x, y, z \in \mathbf{Z}$, then $q \nmid (pc\,z^p/(x+y))$.*

Remark. As mentioned in [BCEM], there are only two primes p below 4 million, namely 16843 and 2124679, for which $p \mid B_{p-3}$. But the proof of the above theorem can be extended to B_{p-5}, B_{p-7}, ... and so on to many more indices (exactly how many depends on p), assuming that for each index $p-i$ the corresponding $C_p^{(i)}$ and $C_p^{(p-i)}$ are cyclic and trivial, respectively.

Our proof of this result follows, with many modifications, the methods of [S]. In [S] we used a series of ideas of H. S. Vandiver [V1, V2] along with a theorem of M. Kurihara [Ku] and some consequences of the proof of Iwasawa's main conjecture for cyclotomic fields due to B. Mazur and A. Wiles [MW] to prove a special case of the Fermat–Wiles theorem.

After recalling some notations and preliminaries, we prove some elementary propositions about $x^p + y^p = pc\,z^p$ which effectively render the proof of its unsolvability amenable to the same methods used (classically) in the second case of Fermat's last theorem. Indeed, the proof follows easily from the results of Vandiver [V4] and it is included for the sake of completeness.

The proof of the main theorem then uses a modification of the methods used by Vandiver [V1], as described in [S2, Chap. 3]. To complete the proof we need to show that certain generalised VanderMonde matrices are non-singular mod p. this is done by establishing a congruence relation between these determinants and the Bernoulli numbers.

0. NOTATIONS AND PRELIMINARIES

$p>3$ is a prime, ζ is a primitive pth root of unity, $\lambda=1-\zeta$, and $\beta=(1-\zeta)(1-\zeta^{-1})$. $K=\mathbf{Q}(\zeta)$ is the cyclotomic field, $A=\mathbf{Z}[\zeta]$ its ring of integers, and A^* the group of units in A. $G=Gal(K/\mathbf{Q})$, σ is a generator of G and $\sigma(\zeta)=\zeta^r$, where r is a primitive generator of $(\mathbf{Z}/p\mathbf{Z})^*$. C is the ideal class group of K, h the order of C. C_p, h_p is the p-Sylow subgroup of C and its order, respectively. $K^+=\mathbf{Q}(\zeta+\zeta^{-1})=$ Maximal real subfield of K. A^+, C^+, h_p^+, and C_p^+ are defined similarly. If I is an ideal in A, then $[I]$ is its ideal class in C. The Bernoulli numbers $\mathbf{B}_m$ are defined by $t/(e^t-1)=\sum_{m=0}^{\infty}\mathbf{B}_m(t^m/m!)$.

The generalized Bernoulli numbers $\mathbf{B}_{m,\omega^j}$ are defined by $\sum_{a=1}^{p-1}(\omega^j(a)\,xe^x/(e^{(p-1)x}-1))=\sum_{m=0}^{\infty}\mathbf{B}_{m,\omega^j}(x^m/m!)$. The *Kummer Unit* δ is given by $\delta=\sqrt{(1-\zeta^r)(1-\zeta^{-r})/(1-\zeta)(1-\zeta^{-1})}$. The *cyclotomic unit* E_m is defined as $E_m=\prod_{k=1}^{p-1}(\sigma^{-k}(\delta))^{r^{mk}}$.

Note. This definition of E_m is not standard. For instance, the E_m defined in [Ri, p. 128] is actually the square root of the E_m defined above. But all the properties of E_m that we need will follow easily from those of $\sqrt{E_m}$ and vice versa.

For a prime ideal $L\neq(\lambda)$ of A, and $\alpha\in A$, $\alpha\notin L$, the *pth power residue symbol* $\{\alpha/L\}$ is defined by $\{\alpha/L\}=\zeta^a$, where ζ^a is the unique pth root of unity such that $\alpha^{(N(L)-1)/p}\equiv\zeta^a\pmod{L}$, $N(L)$ being the (absolute) norm of L. $\{\alpha/L\}$ is extended to all ideals prime to (λ) multiplicatively. Also, we have

$$\left\{\frac{\alpha}{J}\right\}\alpha^{1/p}=\left(\frac{K(\alpha^{1/p})/K}{J}\right)(\alpha^{1/p}),$$

where J is any ideal of A with $(\lambda)\nmid J$, and $((K(\alpha^{1/p})/K)/J)$ is the generalized Frobenius element.

1. PRELIMINARY PROPOSITIONS

Throughout this paper, $p>3$ and $c\in\mathbf{Z}$ is such that only primes of the form $kp-1$, $(k,p)=1$ can divide it. In this section we prove some preparatory results about the solutions to the equation $x^p + y^p = pc\, z^p$. We could also assume, without loss of generality, that c is not divisible by the pth power of any integer.

PROPOSITION 1.0. *If c is as above, and a prime l divides c, then $\{\zeta/(l)\} \neq 1$.*

Proof. $\{\zeta/(l)\} = 1 \Rightarrow p^2 \mid (N(l) - 1) \Rightarrow p^2 \mid (l^{p-1} - 1)$ which is impossible when $l + 1$ is divisible by p but not p^2 as in the case of primes dividing c.

PROPOSITION 1.1. *If $X^p + Y^p = v\beta^m cZ^p$ is satisfied with $X, Y, Z \in K^+$, where c is as above, $(1 - \zeta)$ and (Z) are relatively prime, v is a real unit, and $m \geqslant (p-1)/2$ then*

(a) $(X, Y) = 1$

(b) *The factors $X + \zeta^i Y$, $0 \leqslant i \leqslant p - 1$ of $X^p + Y^p$ are all pairwise relatively prime, except for $(1 - \zeta)$ which divides all of them. Also, $(X + Y, (X^p + Y^p)/p(X + Y)) = (1)$.*

(c) *Let $l \mid c$, l a prime number. Then $l \nmid ((X^p + Y^p)/p(X + Y))$.*

Proof. (a) If $(1 - \zeta)$ divides (X) and (Y) then we can divide it out of $(\beta^m) = (1 - \zeta)^{2m}$. Suppose $L \neq (1 - \zeta)$ is a prime ideal that divides both (X) and (Y). Then $L^p \mid (cZ^p)$, which means (because we assumed c is not divisible by any pth power) $L \mid (Z)$, contrary to the assumption that X, Y, Z are relatively prime.

The proof of (b) follows easily using (a) and the fact that $p \nmid (X^p + Y^p)/p(X + Y)$ (cf. [Wa, p. 168]).

(c) Now, let l be a prime dividing c, of the form $kp - 1$ and let L be a prime ideal of A that divides l. Then $l \mid (X^p + Y^p)/(X + Y) \Rightarrow L \mid (X + \zeta^i Y)$ for some $i \neq 0$. Since $l \equiv -1 \pmod{p}$, the decomposition group of L is of order two, which means it is generated by the conjugation automorphism. So L is fixed by conjugation and hence $L \mid (X + \zeta^{-1} Y)$ which combined with $L \mid (X + \zeta^i Y)$ gives $L \mid (X)$ and $L \mid (Y)$, a contradiction.

Suppose x, y, z are relatively prime integers such that

$$x^p + y^p = pc\, z^p. \tag{1.1}$$

Letting $Z = z/p^t$ $(t = v_p(z))$, $v = p^{tp+1}/\beta^m$, $m = (tp + 1)(p - 1)/2 \geqslant p(p-1)/2$, we can apply Proposition 1.1 to get, $(x, y) = 1$ and with u, v, $t \in \mathbf{Z}$, $(u, v) = 1$, $(v, p) = 1$, $(u, p) = 1$,

$$x + y = cp^{tp}u^p \tag{1.1a}$$

$$\frac{x^p + y^p}{p(x + y)} = v^p. \tag{1.1b}$$

Equation (1.1b) can be written as

$$\prod_{i=0}^{p-1} \left(\frac{x+\zeta^i y}{1-\zeta^i} \right) = v^p. \tag{1.1c}$$

The ideals $((x+\zeta^i y)/(1-\zeta^i))$ in (1.1c) are prime to each other and (λ). Thus we have

$$\left(\frac{x+\zeta y}{1-\zeta} \right) = I^p, \qquad \text{where } I \text{ an integral ideal.} \tag{1.1d}$$

Remark. This reduces the problem amenable to the classical methods used in the study of the second case of Fermat's last theorem. In fact, using the results of Vandiver [V4], the equation $x^p + y^p = pc\, z^p$ can be shown to have no solutions when p is regular and $p > 3$. The proof is included below for the sake of completeness, and it is along the lines of [Wa, Chap. 9]. Moreover, using those methods we can prove that $x^p + y^p = pc\, z^p$ has no nontrivial integral solutions if $p \nmid h_p^+$ and satisfies assumption II of [Wa, Chap. 9]. In particular, for p such that $p \nmid h_p^+$, $p^3 \nmid \mathbf{B}_{pi}$ $\forall$ even $i \leqslant p-3$.

THEOREM 1.2. *If $p > 3$ is a regular prime, c as defined above, then*

$$x^p + y^p = pc\, z^p \tag{1.2}$$

has no nontrivial integral solutions.

Proof. Assume there is a solution. We will get a contradiction using a descent argument as in [V4, Wa, Chap. 9]. Let $Z \in A^+ = \mathbf{Z}[\zeta + \zeta^{-1}]$ be such that it has the minimal number of distinct prime factors among all solutions of

$$\prod_{i=0}^{p-1} (X + \zeta^i Y) = \eta B \beta^m Z^p, \tag{1.2b}$$

where X, $Y \in A^+$, η is a real unit, $m \geqslant p(p-1)/2$, and the only primes dividing the integer B are of the form $kp-1$, $(k, p) = 1$.

If (1.2) has a nontrivial solution, then (1.2b) has a nontrivial solution, by letting $X = x$, $Y = y$, $Z = z/p^t$ $(t = v_p(z))$, $B = c$, $\eta = p^{tp+1}/\beta^m$, $m = (tp+1)(p-1)/2 \geqslant p(p-1)/2$ where t is as in (1.1a).

From (1.2b), it follows from Proposition 1.1 that for $i = 1, ..., p-1$,

$$\left(\frac{X+\zeta^i Y}{1-\zeta^i} \right) = I_i^p, \qquad \text{where } I_i \text{ an ideal of A.} \tag{1.2c}$$

and

$$(X+Y)=B(\beta)^{tp(p-1)/2}\,I_0^p, \qquad \text{where } I_0 \text{ is also an ideal of A.} \tag{1.2d}$$

The ideals I_i are prime to each other and to $(1-\zeta)$ for $0\leqslant i\leqslant (p-1)$. Also we have $(Z)=I_0I_1\cdots I_{p-1}$. These ideals must all be principal because p is a regular prime, and from (1.2d) I_0 in particular can be seen to be of the form (ρ_0), $\rho_0\in A^+$. So we have

$$X+Y=\eta_0\beta^{tp(p-1)/2}B\rho_0^p. \tag{1.2e}$$

Here η_0 is a real unit and ρ_0 is prime to β.

Now, in [Wa, pp. 169–171] it is shown that, given cyclotomic integers X, Y satisfying (1.2c) and $X+Y\equiv 0 \bmod (1-\zeta)^p$, we have

$$\left(\frac{X+\zeta^iY}{1-\zeta^i}\right)=\eta_i\rho_i^p \qquad \text{for} \quad 1\leqslant i\leqslant p-1, \tag{1.2f}$$

where the η_i are real units and the $\rho_i\in A$.

Note. Under the conditions satisfied for X, Y, Z here, we can also get (1.2f) using Proposition 1.0.

Now, changing i to $-i$ in the above equation (and assuming $\rho_i=\rho_{-i}$, then multiplying the resulting equation with it), we get $(X+\zeta^iY)(X+\zeta^{-i}Y)=X^2+Y^2+(\zeta^i+\zeta^{-i})\,XY=\beta_i\eta_i^2(\rho_i\overline{\rho_i})^p$. We also have, from (1.2e), $X^2+Y^2+2XY=\eta_0^2\beta^{2tp(p-1)/2}B^2\rho_0^{2p}$.

Here $\beta_i=(1-\zeta^i)(1-\zeta^{-i})=2-\zeta^i-\zeta^{-i}$.

From these two equations we get

$$-XY=\eta_i^2(\rho_i\overline{\rho_i})^p-\eta_0^2\beta^{tp(p-1)}B^2\rho_0^{2p}\beta_i^{-1}.$$

Now if $j\not\equiv 0$ (mod p) and $j\not\equiv \pm i$ (mod p) (*this is why we needed* $p>3$) we get another equation

$$-XY=\eta_j^2(\rho_j\overline{\rho_j})^p-\eta_0^2\beta^{tp(p-1)}B^2\rho_0^{2p}\beta_j^{-1}.$$

From these two equations we get

$$\eta_i^2(\rho_i\overline{\rho_i})^p-\eta_j^2(\rho_j\overline{\rho_j})^p=\eta_0^2\beta^{tp(p-1)}B^2\rho_0^{2p}(\beta_i^{-1}-\beta_j^{-1}). \tag{1.2g}$$

We can write $\beta_i^{-1}-\beta_j^{-1}=\delta'/\beta$, where δ' is a real unit. Then from (1.2g) we get, with δ a real unit,

$$\left(\frac{\eta_i}{\eta_j}\right)^2(\rho_i\overline{\rho_i})^p+(-\rho_j\overline{\rho_j})^p=\delta\beta^{(tp(p-1))-1}B^2(\rho_0^2)^p. \tag{1.2h}$$

Now, by applying (1.2f) for i and j we get

$$\frac{\eta_i}{\eta_j} \equiv \left(\frac{\rho_j}{\rho_i}\right)^p \qquad \bmod (1-\zeta)^{p-1}$$

because $\eta_i = ((X+\zeta^i Y)/(1-\zeta^i))\, \rho_i^{-p} \equiv (X+\zeta^i((X+Y)/(1-\zeta^i)))\, \rho_i^{-p} \equiv X\rho_i^{-p}$ $(\mathrm{mod}(1-\zeta)^{p-1})$ and similarly for η_j.

Thus η_i/η_j is congruent to a rational integer mod p, and because p is regular, this forces η_i/η_j to be a pth power (cf. [Wa, Theorem 5.36]).

Now let

$$X_1 = \left(\frac{\eta_i}{\eta_j}\right)^{2/p} \rho_i \overline{\rho_i}, \qquad Y_1 = -(\rho_j \overline{\rho_j}), \qquad \text{and} \qquad Z_1 = \rho_0^2.$$

Then from (1.2h) we have

$$X_1^p + Y_1^p = \delta \beta^{(tp(p-1))-1} B^2 Z_1^p. \tag{1.2i}$$

In this equation X_1, Y_1, $Z_1 \in A^+$, $(tp(p-1))-1 \geqslant p(p-1)/2$, δ is a real unit, and B^2 is divisible only by primes of the form $kp-1$, $(k, p)=1$. Moreover, X_1, Y_1, Z_1, and β are pairwise relatively prime because ρ_i, ρ_j, ρ_0, β are pairwise relatively prime, as shown above (see remarks surrounding Eqs. (1.2d) and (1.2e)). Thus (1.2i) is another equation satisfying the same condition as (1.2b) but in this case it has $(Z_1) = (\rho_0)^2 = I_0^2$ which will have a smaller number of prime divisors than Z unless $I_1 = \cdots = I_{p-1} = (1)$ which would force $(X+\zeta^i Y)/(1-\zeta^i)$ to be a unit for $1 \leqslant i \leqslant p-1$. This can be shown to be a contradiction (cf. [Wa, p. 173]). Hence Theorem 1.2.

2. THE MAIN THEOREM

THEOREM 2.1. *Assume p is irregular, $p \mid B_{p-3}$, and c as in Theorem* 1.2. *Let q be an odd prime such that $q \equiv 1$ (mod p), and $\exists Q$ over q in $\mathbf{Q}(\zeta)$ whose ideal class generates $C_p^{(3)}$.*

If $x^p + y^p = pc\, z^p$ has nontrivial integer solutions, then $q \nmid (pc\, z^p)/(x+y)$.

Proof. Remark: As noted in the Introduction, Tchebotarev density theorem gives infinitely many primes q with the above properties.

We first need a proposition.

Let L be a prime ideal of $\mathbf{Q}[\zeta]$, such that $L \mid (x+\zeta y/1-\zeta)$. Then by Proposition 1.1b, $L \nmid (x+y)$. So if L lies over the rational prime l, then $l \mid (x^p + y^p) \Rightarrow x^p + y^p \equiv 0 \pmod{l} \Rightarrow (-x/y)^p \equiv 1 \pmod{l}$. From this we get $l \equiv 1$ (mod p). Except for the last paragraph, the proof of the following proposition, following [V2, p. 217] is almost identical to that of Proposition 3.1 of [S]. It is presented here for completeness. Recall that when $n \in \mathbf{Z}$, n' is an integer such that $n\, n' \equiv 1 \pmod{l}$.

Proposition 2.0. *If Eq. (1.2) is satisfied with $x, y \in \mathbf{Z}$, $(x, y) = 1$, then $\exists \alpha \in A$ such that*

$$\prod_{n=1}^{(p-1)/2} \left(\frac{x + \zeta^{n'} y}{1 - \zeta^{n'}} \right) = \alpha^p. \tag{2.0a}$$

Proof. As shown above, we have

$$\left(\frac{x + \zeta y}{1 - \zeta} \right) = I^p, \qquad \text{where } I \text{ an integral ideal,} \tag{2.0b}$$

when x, y are as in the statement of this proposition. Applying a Stickelberger type relation (cf. [L, p. 13, Fact. 3]) with $n_1 = n_2 = 1$, and using the fact that all prime ideals dividing $(x + \zeta y/1 - \zeta)$ are of degree 1 (see remark above), we find that the product $\prod_{n=1}^{(p-1)/2} \sigma_{n'}(I)$ is principal Applying this to Eq. (2.0b), we get

$$\prod_{n=1}^{p-1/2} \left(\frac{x + \zeta^{n'} y}{1 - \zeta^{n'}} \right) = \eta \beta^p, \qquad \text{where } \eta \in A \text{ is a unit, and } \beta \in A. \tag{2.0c}$$

Applying σ_{-1} to (2.0c), we get

$$\prod_{n=(p+1)/2}^{p-1} \left(\frac{x + \zeta^{n'} y}{1 - \zeta^{n'}} \right) = \bar{\eta} (\bar{\beta})^p. \tag{2.0d}$$

Multiplying (2.0c) and (2.0d), and using (1.1b), we find that the ideal $(\beta \bar{\beta}) = (v)$. Hence $\beta \bar{\beta} = Ev$, where $E \in A$ is a unit. Taking the product of (2.0c) and (2.0d) again, we find that

$$\eta \bar{\eta} E^p = 1. \tag{2.0e}$$

But we know, by a basic result, that

$$\eta = \zeta^g \varepsilon, \tag{2.0f}$$

where $\varepsilon \in A^+ = \mathbf{Z}[\zeta + \zeta^{-1}]$ is a real unit and $g \in \mathbf{Z}$.

From (2.0e) and (2.0f) we get $\varepsilon^2 = E^{-p}$. Since p is odd, we can find integers a, b such that $2a = 1 + bp$, so that $\varepsilon^{2a} = \varepsilon\varepsilon^{bp} = E^{-ap}$. Hence $\varepsilon = (\varepsilon^{-b}E^{-a})^p$, and $\eta = \zeta^g(\varepsilon^{-b}E^{-a})^p$. Letting $\alpha = \varepsilon^{-b}E^{-a}\beta$, we get

$$\prod_{n=1}^{(p-1)/2}\left(\frac{x+\zeta^{n'}y}{1-\zeta^{n'}}\right) = \zeta^g\alpha^p. \tag{2.0g}$$

Let l be a prime number that divides c. Then by Proposition 1.1, $l \mid (x+y)$, but $l \nmid (x^p+y^p)/p(x+y)$. From this, we get $(x^p+y^p)/p(x+y) = v^p \equiv y^{p-1} \pmod{l} \Rightarrow y \equiv v_1^p \pmod{l}$, for some $v_1 \in \mathbf{Z}$. Now applying the pth power residue character $\{(\ )/(l)\}$ to both sides of (2.0g), we get $\{\zeta^g/(l)\} = 1$. If $g \not\equiv 0 \pmod{p}$, $\{\zeta/(l)\} = 1$, which is impossible for such l by Proposition 1.0. Hence Proposition 2.0.

From (2.0a) we have

$$\prod_{n=1}^{(p-1)/2}\left(\frac{x+\zeta^{n'}y}{1-\zeta^{n'}}\right) = \alpha^p.$$

Let q, Q be as in the statement of Theorem 2.1. Then we can assume, taking a conjugate if necessary, $Q \mid (x+\zeta y)$. (If the ideal class of Q generates $C_p^{(3)}$, then because $C_p^{(3)}$ is an eigenspace corresponding to the eigenvalue $\omega^3(\sigma)$ which is prime to p, the conjugate $\sigma(Q)$ will also be in an ideal class that generates $C_p^{(3)}$.) Then $Q \nmid (x+\zeta^i y)$ for $i \neq 1$. Now for $k \in \{1, 2, ..., (p-1)/2\}$, $-kn' \not\equiv 1 \pmod{p}$, $\forall 1 \leqslant n \leqslant (p-1)/2$.

Applying σ_k to both sides of (2.0a), we get

$$\prod_{n=1}^{(p-1)/2}\left(\frac{x+\zeta^{-kn'}y}{1-\zeta^{-kn'}}\right) = \alpha_1^p. \tag{2.1}$$

Now, $(x+\zeta^i y)/(1-\zeta^i) \equiv (xe_{i-1}/e_i) \pmod{Q}$, where we define $e_i = (1-\zeta^i)/(1-\zeta)$, because $Q \mid (x+\zeta y)$. So from (2.1) we get

$$\prod_{n=1}^{(p-1)/2}\left\{\frac{x}{Q}\right\}\left(\frac{e_{-kn'-1}}{Q}\right)\left\{\frac{e_{-kn'}}{Q}\right\}^{-1} = \left\{\frac{\alpha_1^p}{Q}\right\} = 1. \tag{2.2}$$

Fix $k_0 = -(p-1)/2$, and let $k_1 = -1$, $k_2 = -2$, ..., $k_{(p-3)/2} = -p-3/2$. Then we get

$$\prod_{n=1}^{(p-1)/2}\left\{\frac{e_{-k_0n'-1}}{Q}\right\}\left\{\frac{e_{-k_0n'}}{Q}\right\}^{-1} = \prod_{n=1}^{(p-1)/2}\left\{\frac{e_{-k_in'-1}}{Q}\right\}\left\{\frac{e_{-k_in'}}{Q}\right\}^{-1},$$

$$i = 1, 2, ..., \frac{p-3}{2}. \tag{2.3}$$

Define (mod p), $ind(\alpha) = a$, where $\{\alpha/Q\} = \zeta^a$. In this notation, we get from (2.3) that

$$\sum_{n=1}^{(p-1)/2} [ind(e_{-k_o n'-1}) - ind(e_{-k_i n'-1}) - ind(e_{-k_o n'}) + ind(e_{-k_i n'})] \equiv 0 \pmod{p}. \tag{2.4}$$

From [K, p. 277], we have the following relation between $ind(e_i)$ and the $ind(E_j)$,

$$ind(e_i) \equiv \sum_{m=1}^{p-3/2} \left(\left(\frac{i^{2m}-1}{r^{2m}-1} \right) ind(E_{2m}) \right) - \frac{i-1}{2} ind(\zeta),$$

where r is as defined in Section 0. In (2.4), for any k_i, let $-k_i n' = i_n$, $-k_0 n' = a_n$.

Then

$$\sum_{n=1}^{(p-1)/2} [(ind(e_{a_n-1}) - ind(e_{a_n})) - (ind(e_{i_n-1}) - ind(e_{i_n}))] \equiv 0 \pmod{p}. \tag{2.5}$$

Then using the above relation, we get

$$\sum_{n=1}^{(p-1)/2} \left[\sum_{m=1}^{(p-3)/2} \left[\frac{(a_n-1)^{2m} - a_n^{2m} - ((i_n-1)^{2m} - i_n^{2m})}{r^{2m}-1} \right] ind(E_{2m}) \right] \equiv 0 \pmod{p}.$$

Simplifying, and using the fact that $A_t \overset{\text{def}}{=} \sum_{n=1}^{(p-1)/2} (n')^t \equiv 0 \pmod{p}$ when t is even, we get

$$\sum_{\substack{u=1 \\ u \text{ odd}}}^{p-4} \left(\sum_{\substack{m=1 \\ 2m \geqslant u}}^{(p-3)/2} \binom{2m}{u} \frac{ind(E_{2m})}{r^{2m}-1} \right) A_u (k_0^u - k_i^u) \equiv 0 \pmod{p}. \tag{2.6}$$

Letting i vary over 1, 2, ..., $(p-3)/2$, we get a system of $(p-3)/2$ equations in $(k_0^u - k_i^u)$ whose matrix equation has only the trivial solution if the following generalized $(p-1)/2 \times (p-1)/2$ VanderMonde matrix A is non-singular mod p:

$$A = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 \\ 1 & 2 & 3 & \cdots & \left(\frac{p-1}{2}\right) \\ 1 & 2^3 & 3^3 & \cdots & \left(\frac{p-1}{2}\right)^3 \\ \vdots & \vdots & \vdots & \ddots & \vdots \\ 1 & 2^{p-4} & 3^{p-4} & \cdots & \left(\frac{p-1}{2}\right)^{p-4} \end{bmatrix}.$$

Let the determinant of $A = \varDelta$. Then $\varDelta = \pm\varGamma$ where

$$\varGamma = \begin{vmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 2 & 2^3 & 2^5 & \cdots & 2^{p-4} & 1 \\ 3 & 3^3 & 3^5 & \cdots & 3^{p-4} & 1 \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \left(\frac{p-1}{2}\right) & \left(\frac{p-1}{2}\right)^3 & \left(\frac{p-1}{2}\right)^5 & \cdots & \left(\frac{p-1}{2}\right)^{p-4} & 1 \end{vmatrix}.$$

Let B be the non-singular (mod p) VanderMonde matrix given by

$$B = \begin{bmatrix} 1 & 1 & 1 & \cdots & 1 & 1 \\ 2 & 2^3 & 2^5 & \cdots & 2^{p-4} & 2^{p-2} \\ 3 & 3^3 & 3^5 & \cdots & 3^{p-4} & 3^{p-2} \\ \vdots & \vdots & \vdots & \ddots & \vdots & \vdots \\ \left(\frac{p-1}{2}\right) & \left(\frac{p-1}{2}\right)^3 & \left(\frac{p-1}{2}\right)^5 & \cdots & \left(\frac{p-1}{2}\right)^{p-4} & \left(\frac{p-1}{2}\right)^{p-2} \end{bmatrix}.$$

If $\det(B)$ is b, then $\varGamma = (x_{(p-1)/2})b$ where $\{x_1, x_2, ..., x_{(p-1)/2}\}$ is the solution of the matrix equation

$$B[x_1, x_2, ..., x_{(p-1)/2}]^t = [1, 1, 1, ..., 1]^t \qquad \text{(Cramer's rule)}.$$

But $B[x_1, x_2, ..., x_{(p-1)/2}]^t = [1, 1, 1, ..., 1]^t \Rightarrow \sum_{k=1}^{(p-1)/2} x_k n^{2k-1} = 1$, for $n = 1, 2, ..., (p-1)/2 \Rightarrow \sum_{k=1}^{(p-1)/2} x_k n^{2k} = n$, for $n = 1, 2, ...,$ $(p-1)/2 \Rightarrow \sum_{k=1}^{(p-1)/2} x_k (\sum_{n=1}^{(p-1)/2} n^{2k}) = \sum_{n=1}^{(p-1)/2} n$.

Since $\sum_{n=1}^{(p-1)/2} n^{2k} \equiv 0 \pmod p$ for $k < (p-1)/2$, we get $x_{(p-1)/2} \equiv (p+1)/4 \pmod p$. Thus $\varGamma$ has to be nonzero mod p and hence $\varDelta$ is also nonzero mod p.

Thus the system of Eq. (2.6) has only trivial solutions. Considering the leading term only, we get

$$\frac{(p-3)\, A_{p-4}\, ind(E_{p-3})}{r^{p-3}-1} \equiv 0 \qquad (\mathrm{mod}\ p), \tag{2.7}$$

where $A_{p-4} = \sum_{n=1}^{(p-1)/2} (n')^{p-4}$ as defined earlier.

We have the following relation between A_j's and the Bernoulli numbers $\mathbf{B}_i$ (cf. [V3, p. 114]):

$$\sum_{n=1}^{(p-1)/2} n^{i-1} \equiv \frac{1-2^i}{2^{i-1} i} \mathbf{B}_i \quad (\mathrm{mod}\ p), \qquad i \geqslant 2, \quad (p-1) \nmid i. \tag{2.8}$$

Remark. The above congruence is also a consequence of Voronoi's congruences (cf, for instance, [Ri. p. 108, 5B]).

Let $i = 4$. From (2.8) we have

$$\frac{(1-2^4)}{2^3.4} \mathbf{B}_4 \equiv A_{p-4} \qquad (\mathrm{mod}\ p).$$

Combining (2.7) and (2.8), we get

$$\frac{(p-3)\, ind(E_{p-3})}{r^{p-3}-1} \mathbf{B}_4 \frac{1-2^4}{2^5} \equiv 0 \qquad (\mathrm{mod}\ p).$$

Since p is irregular, certainly $p > 5$, and we get $(p-3)\, ind(E_{p-3})/(r^{p-3}-1) \equiv 0$ (mod p). Hence $ind(E_{p-3}) \equiv 0$ (mod p), i.e., $\{E_{p-3}/Q\} = 1$. Now we need the following results from [S]:

Lemma 2.2 [S]. *$K(E_{p-3}^{1/p})$ is a nontrivial, unramified, abelian extension of K.*

Corollary. *For any principal ideal (α) of K, $\{E_{p-3}/(\alpha)\} = 1$.*

Lemma 2.4 [He, p. 434]. *Let $k \in \{5, ..., l-2\}$, and P_k be any ideal prime to (λ) whose class belongs to $C_p^{(k)}$. Then $\{E_{p-3}/P_k\} = 1$.*

Since $[Q]$ generates $C_p^{(3)}$ by assumption, we can use Lemma 2.4 and the corollary of Lemma 2.2 to show that $(E_{p-3})^{1/p}$ generates a trivial extension of $\mathbf{Q}[\zeta]$. This will contradict Lemma 2.2.

This concludes the proof of the main theorem.

Some Remarks. (1) By using the other terms from (2.6), we get $ind(E_{p-t}) \equiv 0$ (mod p) for $t = 5$, and depending on p, some other $t > 3$ as well. So for instance, if we assume that $C_p^{(5)}$ is cyclic and $C_p^{(p-5)}=0$, then the above theorem can be proved with $C_p^{(5)}$ in the place of $C_p^{(3)}$.

(2) Denoting by Γ_j the determinant of the matrix obtained by replacing the jth column of the VanderMonde matrix B by $[1, 1, ..., 1]^t$, (so $\Gamma=\Gamma_{(p-1)/2}$), we get $\Gamma_j \equiv (x_j)\, b$, where x_j and b are as defined before. But it is easy to see that $x_j \equiv \sum_{n=1}^{(p-1)/2} n^{p-2j}$. So we get

$$x_j \equiv \frac{1-2^{p-2j+1}}{2^{p-2j}(p-2j+1)}\,\mathbf{B}_{p-2j+1} \qquad (\bmod p)$$

from (2.8) above. Thus, if $2^t \not\equiv 1 \pmod p$, then $B_t \equiv 0$ iff $\Gamma_{(p+1-t)/2} \equiv 0 \pmod p$, where $t = 2, 4, ..., p-3$.

REFERENCES

[BCEM] J. Buhler, R. Crandall, R. Ernvall, and T. Metsankyla, Irregular primes and cyclotomic invariants to four million, *Math. Comp.* **61** (1993), 151–153.

[C] H. Cohn, "A Classical Invitation to Algebraic Numbers and Class Fields," Springer-Verlag, New York/Berlin, 1978.

[DM] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's Last Theorem, preprint.

[He] J. Herbrand, Sur les classes des corps circulaires, *J. Math. Phys.* **11** (1932), 417–441.

[K] E. E. Kummer, Über die Erganzungsätze zu den allgemeinen Reziprozitätsgesetzen, *J. Math.* **44** (1852), 95–106.

[Ku] M. Kurihara, Some remarks on conjectures about cyclotomic fields and *K*-groups of **Z**, *Compositio Math.* **81** (1992), 223–236.

[L] S. Lang, "Cyclotomic Fields, I and II," Springer-Verlag, New York/Berlin, 1990.

[MW] B. Mazur and A. Wiles, Class fields of abelian extensions of **Q**, *Invent. Math.* **76** (1984), 179–330.

[Ri] P. Ribenboim, "Thirteen Lectures on Fermat's Last Theorem," Springer-Verlag, New York/Berlin, 1979.

[R] K. Ribet, On the equation $a^p + 2^\alpha b^p + c^p = 0$, *Acta Arith.* **79** (1997), 7–16.

[S] S. Sitaraman, Vandiver revisited, *J. Number Theory* **57** (1996), 122–129.

[S2] S. Sitaraman, "Ph.D. Thesis," California Institute of Technology, 1994.

[V1] H. S. Vandiver, Fermat's last theorem and the second factor in the cyclotomic class number, *Bull. Amer. Math. Soc.* (1934), 118–123.

[V2] H. S. Vandiver, A property of cyclotomic integers and its relation to the Fermat's last theorem, *Ann. of Math.* **26** (1925), 217–232.

[V3] H. S. Vandiver, On power characters of singular integers in a properly irregular cyclotomic field, *Trans. Amer. Math. Soc.* **32** (1930), 391–408.

[V4] H. S. Vandiver, On trinomial Diophantine equations connected with the Fermat relation, *Monatsh. Math. Phys.* **43** (1936), 317–320.

[Wa] L. Washington, "Introduction to Cyclotomic Fields," 2nd ed., Springer-Verlag, New York/Berlin, 1997.

[W] A. Wiles, Modular elliptic curves and Fermat's last theorem, *Ann. of Math.* **141** (1995), 443–551.

[TW] R. Taylor and A. Wiles, *Ann. of Math.* **141** (1995), 552–572.