Note on a Fermat-type Diophantine Equation

Sankar Sitaraman
Department of Mathematics
Howard University, Washington, D.C. 20059

Abstract

Let $p > 5$ be a prime number and ζ a p-th 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 $p-$Sylow subgroup of ideal class group C of $\mathbf{Q}(\zeta)$ corresponding to ω^i, ω being the Teichmuller character.

In this article we extend the main theorem in [S1] and get the following: For any fixed odd positive integer $n < p - 4$, assume:

(a) At least one of $C_p^{(3)}, C_p^{(5)}, ...C_p^{(n)}$ is non-trivial.

(b) $C_p^{(i)} = 0$ for $p - n - 1 \leq i \leq p - 2$.

(c) $2^i \not\equiv 1 \ mod \ (p)$ for $1 \leq i \leq n + 1$.

Let q be an odd prime such that $q \equiv 1 \ mod \ (p)$, and such that there is a prime ideal Q over q in $\mathbf{Q}(\zeta)$ whose ideal class is of the form $I^p J$ where J is non-trivial, not a $p-$th power and $J \in C_p^{(3)} \oplus C_p^{(5)} \oplus .... \oplus C_p^{(n)}$.

For such p and q, if $x^p + y^p = pc\ z^p$ has a nontrivial solution $x, y, z \in \mathbf{Z}$, with $(x, y, z) = 1$, then $q \not| \frac{pc\ z^p}{x+y}$.

Let $t(n) = n^{224n^4}$. If $log p > t(n)$, then applying a result of C. Soulé [So], we show that the above result holds with only condition (a) because the others are automatically satisfied.

We also make a remark about the effect of Soulé's result on the p-divisibility of h_p^+ (the class number of the maximal real subgroup of $\mathbf{Q}(\zeta)$) which is relevant to the existence of integral solutions to $x^p + y^p = pcz^p$.

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 certain 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 is a large number of unrestricted prime divisors in the coefficient pc. Equations of the form $x^p + y^p = Cz^p$ have been considered by Gandhi [G], Inkeri [I], Morishima [MM], Vandiver [V3], and Yamaguchi [Y], among others. Morishima and Miyoshi [MM] and Inkeri [I] gave criteria for existence of integral solutions to $x^p + y^p = Cz^p$, when z is not divisible by p and C is such that $(C, p) = 1, (\phi(C), p) = 1$ and $(xyz, p) = 1$. When z is divisible by p, and C is such that $(\phi(C/p^m), p) = 1$, where $p^m || C$ with $m \geq 0$, Gandhi [G] and Yamaguchi [Y] showed the following: Let h_p^+ be the class number of the maximal real subgroup of $\mathbf{Q}(\zeta)$, ζ being a p-th root of unity, and let $\mathbf{B}_k$ be the k-th Bernoulli number, defined below. When p doesn't divide h_p^+ and p^3 doesn't divide $\mathbf{B}_{pi}$ for all even $i \leq p-3$, there are no integral solutions to $x^p + y^p = Cz^p$. [While Gandhi unlike Yamaguchi assumes implicitly that $(C, p) = 1$, his proof with minor modifications will work for any C].

In this paper we discuss the unsolvability of equations of the form $x^p + y^p = pc\ z^p$, which were discussed in [S1]. As in [S1], we make an asumption on the constant c stronger than that made by Gandhi et al., namely that it is an integer divisible only by primes of the form $kp - 1, (k, p) = 1$. We do not assume that p doesn't divide h_p^+ or that p^3 doesn't divide the $\mathbf{B}_{pi}$. But we do make some assumptions regarding some subgroups of the ideal class group of $\mathbf{Q}(\zeta)$, as described below.

Let C_p be the p-Sylow subgroup of $\mathbf{Q}(\zeta)$. The Teichmüller character $\omega : \mathbf{Z}_p \to \mathbf{Z}_p^*$ is given by $\omega(x) \equiv x \pmod{p}$, where $\omega(x)$ is a $p-1$-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. The Bernoulli numbers $\mathbf{B}_m$ are defined by $\frac{t}{e^t - 1} = \sum_{m=0}^{\infty} \mathbf{B}_m \frac{t^m}{m!}$. It is well known that (by the work of Herbrand and Ribet) $C_p^{(i)} \neq 0 \Leftrightarrow p | \mathbf{B}_{p-i}$.

The main theorem of this paper is the following:

Theorem I

For any fixed odd positive integer $n < p - 4$, and any integer c divisible only by primes of the form $kp - 1$ where $(k, p) = 1$, assume:

(a) At least one of $C_p^{(3)}, C_p^{(5)}, ...C_p^{(n)}$ is non-trivial.

(b) $C_p^{(i)} = 0$ for $p-n-1 \leq i \leq p-2$.

(c) $2^i \not\equiv 1 \ mod\ (p)$ for $1 \leq i \leq n+1$.

Let q be an odd prime such that $q \equiv 1 \ mod\ (p)$, and such that there is a prime ideal Q over q in $\mathbf{Q}(\zeta)$ whose ideal class is of the form $I^p J$ where J is non-trivial, not a $p-$th power and $J \in C_p^{(3)} \oplus C_p^{(5)} \oplus .... \oplus C_p^{(n)}$.

For such p and q, if $x^p + y^p = pc\ z^p$ has a nontrivial solution $x, y, z \in \mathbf{Z}$, with $(x, y, z) = 1$, then $q \not| \frac{pc\ z^p}{x+y}$.

Remark: Any q that divides $\frac{x^p+y^p}{x+y} = \frac{pc\ z^p}{x+y}$ necessarily has to be congruent to 1 modulo p. This is easily proved by looking at $\frac{x^p+y^p}{x+y}$ modulo q.

Assumption (a) and the part of (b) that says $C_p^{(i)} = 0$ for $p-n-1 \leq i \leq p-2$, i even can be stated equivalently using the result of Herbrand and Ribet mentioned above as: p divides one of the Bernoulli numbers $\mathbf{B}_{p-n}, \ldots, \mathbf{B}_{p-3}$ but none of $\mathbf{B}_2, \ldots, \mathbf{B}_{n+1}$. Assumptions (b) and (c) can be dropped if p is sufficiently large. The part of (b) that says p doesn't divide $\mathbf{B}_2, \mathbf{B}_4 \ldots, \mathbf{B}_{n+1}$ and (c) are automatically satisfied as soon as $p > 14\sqrt{n+1}(\frac{n+1}{6})^{n+1}$ (proposition 1). (b) and (c) are both satisfied when p is large enough to make Soulé's result hold (see below).

In section 2, we look at the consequences of applying Soulé's result [So] concerning the $C_p^{(i)}$ to our main result and also to the p-divisibility of h_p^+. Let $t(n) = n^{224n^4}$. If $logp > t(n)$, then we show using Soulé's result that the above result holds with only condition (a) because the other two are automatically satisfied.

In [S1, Theorem 2.1] we proved (following Vandiver [V1], [V2]) the above theorem when $n = 1$. Note that from the work of M. Kurihara [Ku] (also R. Greenberg, independently) it was known that $C_p^{(p-3)}$ is trivial and hence $C_p^{(3)}$ is cyclic.

When p is regular it can be shown that $x^p + y^p = pc\ z^p$ has no solutions [cf. [S1], Theorem 1.2 ; this is also implicit in the result of Yamaguchi mentioned above].

I would like to thank D. Ramakrishnan for suggesting this problem and his encouragement, L. Washington for his valuable suggestions and the referee for his/her valuable remarks and suggestions to improve the paper.

0. Notations and Preliminaries

Throughout this paper, $p > 5$ is a prime, ζ is a primitive p-th root of unity, $\lambda = 1 - \zeta$. The integer c is such that only primes of the form $kp - 1, (k, p) = 1$ can divide it; $n < p - 4$ is a fixed odd positive integer; r is a generator of the multiplicative group of $\mathbf{Z}/p\mathbf{Z}$.

The *Kummer Unit* δ is given by $\delta = \sqrt{\frac{(1-\zeta^r)(1-\zeta^{-r})}{(1-\zeta)(1-\zeta^{-1})}}$.

The *cyclotomic unit* E_m is defined as $E_m = \prod_{k=1}^{p-1} (\sigma^{-k}(\delta))^{r^{mk}}$.

For a prime ideal $Q \neq (\lambda)$ of $\mathbf{Z}(\zeta)$, and $\alpha \in \mathbf{Z}(\zeta)$, $\alpha \notin Q$, the *p-th power residue symbol* $\left\{\frac{\alpha}{Q}\right\}$ is defined by $\left\{\frac{\alpha}{Q}\right\} = \zeta^a$, where ζ^a is the unique p-th root of unity such that $\alpha^{(N(Q)-1)/p} \equiv \zeta^a \pmod{Q}$, $N(Q)$ being the (absolute) norm of Q. The symbol $\left\{\frac{\alpha}{Q}\right\}$ 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 $(\lambda) \not| J$, $K = \mathbf{Q}(\zeta)$, and $\left(\frac{K(\alpha^{1/p})/K}{J}\right)$ is the generalized Frobenius element.

The following proposition gives an estimate for how large p must be (in relation to n) so that p does not divide the numerator of $\mathbf{B}_i, i = 2, 4, \ldots, n+1$. It is based on the suggestions of the referee and L. Washington.

Proposition 1

If $p > 14\sqrt{n+1}(\frac{n+1}{6})^{n+1}$, then p doesn't divide $\mathbf{B}_i$ for $i \leq n+1, i$ even.

Proof: We have the following well known formula for Bernoulli numbers: $|\mathbf{B}_{2k}| = \frac{2(2k)!\zeta(2k)}{(2\pi)^{2k}}$, where $\zeta(s)$ is the Riemann zeta function. We also have $\zeta(2k) \leq 1 + \frac{1}{2k-1}$ (by comparing with the corresponding integral) and $(2k)! \leq \sqrt{2\pi}(2k)^{2k+\frac{1}{2}}e^{-2k}(1+\frac{1}{8k})$ (from the Proof of Stirling's formula). On the other hand, if we write $\mathbf{B}_{2k} = \frac{N_{2k}}{D_{2k}}$ with $(N_{2k}, D_{2k}) = 1$, then by the von Staudt - Clausen criterion $D_{2k} = \prod_{(q-1)|2k} q \leq \prod_{q \leq 2k+1} q = e^{\theta(2k+1)}$, where q denotes primes and $\theta(x) = \sum_{q \leq x} log q$ is the Chebyshev theta function. We have $\theta(x) < 1.0011x$ from the results of J.B. Rosser and L. Schoenfeld [RS]. Since the numerators of the Bernoulli numbers are all 1 for $2k \leq 10$, we may assume that $k \geq 6$, and hence $1 + 1/8k \leq 49/48$. Combining all the estimates, we get the upper bound $N_{2k} \leq 14\sqrt{2k}(k/3)^{2k}$. Letting $2k = n+1$, we get the proposition.

1. Proof of Theorem I

In the proof of the main theorem in [S1], we had the following :

Let $A_u = \sum_{n=1}^{\frac{p-1}{2}} n^{p-1-u}$ where $1 \leq u \leq p-4$, u odd. For Q a prime ideal in $\mathbf{Q}(\zeta)$ different from (λ), let $ind_Q(E_{2m})$ be the positive integer $a < p$ such that $\left\{\frac{E_{2m}}{Q}\right\} = \zeta^a$. Let r be a generator of the multiplicative group of $\mathbf{Z}/p\mathbf{Z}$.

Theorem II [S1, page 183]

Assume p is irregular, and c is as before. Let q be an odd prime such that

$q \equiv 1 \ mod\ (p)$, and let Q be a prime ideal in $\mathbf{Q}(\zeta)$ that lies over q.

If $x^p + y^p = pc\ z^p$ has nontrivial solutions $x, y, z \in \mathbf{Z}$, with $(x, y, z) = 1$, and $q | \frac{pc\ z^p}{x+y}$, then for odd u such that $1 \leq u \leq p-4$, we have

$$A_u \left(\sum_{m=\frac{u+1}{2}}^{\frac{p-3}{2}} \binom{2m}{u} \frac{ind_Q(E_{2m})}{r^{2m}-1} \right) \equiv 0 \ \ mod\ (p). \tag{1}$$

Corollary

For Q as in Theorem II, if $2^i \not\equiv 1\ mod\ (p)$ for $1 \leq i \leq n+1$, and p not dividing $\mathbf{B}_i$ for $i \leq n+1$, i even, then $ind_Q(E_{2m}) \equiv 0\ mod\ (p)$ for $2m = p-3, p-5, ..., p-n$.

Proof of corollary

We have, [cf. S1, page 183], $A_u \equiv \frac{1-2^{p-u}}{2^{p-1-u}(p-u)}\mathbf{B}_{p-u}\ mod\ (p)$. So if $2^i \not\equiv 1\ mod\ (p)$ for $1 \leq i \leq n+1$, and p doesn't divide $\mathbf{B}_i$ for $i \leq n+1$, i even, then $A_u \not\equiv 0\ mod\ (p)$ for $p-n-1 \leq u \leq p-4$, u odd. Then the corollary follows easily from (1) by induction.

Let Q be a prime ideal of degree 1 (as in the statement of Theorem I) lying over an odd prime q such that $q | \frac{pc\ z^p}{x+y}$. Then because of assumptions (b) and (c) (note that assumption (b) implies p doesn't divide $\mathbf{B}_i$ for $i \leq n+1$) we can apply the corollary of Theorem II to such Q and get that the indices $ind_Q(E_{2m})$ are congruent to $0\ \ mod\ (p)$ for $2m = p-3, p-5, ..., p-n$. We will show that this leads to a contradiction.

Now we have, also by assumption (b), $C_p^{(i)} = 0$ for $i = p-3, p-5, \ldots, p-n$. Then by Leopoldt's refelection theorem $C_p^{(3)}, C_p^{(5)}, ..., C_p^{(n)}$ are all cyclic. Suppose the subgroup $C_p^{(j)}$ is non-trivial generated by the ideal class of P_j, a prime ideal of degree 1, where $j \in \{3, 5, ..., n\}$. [At least one such j exists by assumption (a).]

We need the following two lemmas. Their proofs are same as those of lemma 2.2 of [S2], page 126, and lemma 2.4 (due to Herbrand) of [S2], page 127 respectively, with the only modification that 3 is replaced by j.

The lemmas (and the corollary) are valid for j, p such that $j \in \{3, 5, \ldots, p-2\}$, $p | \mathbf{B}_{p-j}$ and $C_p^{(p-j)} = 0$.

Lemma 1

$K(E_{p-j}^{1/p})$ is a nontrivial, unramified, abelian extension of K.

We also have,

Corollary

For any principal ideal (α) of K, $\left\{\frac{E_{p-j}}{(\alpha)}\right\} = 1$.

Lemma 2 [Herbrand] Let $k \in \{2, 3, ...p-2\}$, $k \neq j$, and P_k be any ideal prime to (λ) whose class belongs to $C_p^{(k)}$. Then $\left\{\frac{E_{p-j}}{P_k}\right\} = 1$.

Now, from the hypothesis of Theorem I, we can write $Q = I^p P_{j_1}^{a_1} \dots P_{j_k}^{a_k}(\alpha)$ where $j_1, \dots, j_k \in \{3, 5, \dots, n\}$ and $a_1, a_3, \dots, a_k$ are non-zero and prime to p. By the corollary to Theorem II, we have $ind_Q(E_{2m}) \equiv 0 \ mod\ (p)$ for $2m = p-3, p-5, ..., p-n$. i.e, $\left\{\frac{E_{2m}}{Q}\right\} = 1$ for $2m = p-3, p-5, ..., p-n$. Substituting for Q by $I^p P_{j_1}^{a_1} \dots P_{j_k}^{a_k}(\alpha)$ in this, and applying the lemma 2 and the Corollary to lemma 1, we get that $\left\{\frac{E_{p-j_i}}{P_{j_i}^{a_i}}\right\} = 1$ for $i = 1, \dots, k$. Since $a_i \not\equiv 0 \ mod\ (p)$, for at least one of the $i \in \{1, \dots, k\}$ and $k \geq 1$ by assumption (a), we have $\left\{\frac{E_{p-j}}{P_j}\right\} = 1$ for at least one index $j \in \{3, 5, \dots, n\}$. We show that, for such j, $(E_{p-j})^{\frac{1}{p}}$ generates a trivial extension of $K = \mathbf{Q}[\zeta]$ if $ind_Q(E_{p-j}) = 0$.

Indeed, let X be any ideal class in C_p. Represent it by a prime ideal P different from (λ). We can write P as $P_3^{b_3} P_5^{b_5} \dots P_n^{b_n} Q_1^{c_1} \dots Q_m^{c_m}(\alpha)$ where the ideal classes of the prime ideals $P_3, P_5, \dots, P_n$ generate $C_p^{(3)}, C_p^{(5)}, \dots, C_p^{(n)}$, and the ideal classes of $Q_1, Q_2, \dots, Q_m$ generate the other cyclic subgroups of C_p. Applying lemma 2 and the corollary of lemma 1 to $\left\{\frac{E_{p-j}}{P}\right\} = \left\{\frac{E_{p-j}}{P_3^{b_3} P_5^{b_5} \dots P_n^{b_n} Q_1^{c_1} \dots Q_m^{c_m}(\alpha)}\right\}$, and using the fact that $\left\{\frac{E_{p-j}}{P_j}\right\} = 1$, we get $\left\{\frac{E_{p-j}}{P}\right\} = 1$. Since $K((E_{p-j})^{\frac{1}{p}})$ is an unramified extension of K (by Lemma 1), it is contained in H_p, the Hilbert $p-$class field of K. $\left\{\frac{E_{p-j}}{P}\right\} = 1$ implies that the Frobenius $\left(\frac{H_p/K}{P}\right)$ induces the trivial automorphism of $K(E_{p-j}^{1/p})$ over K, for a prime ideal P representing any ideal class X in C_p. This is impossible unless $K(E_{p-j}^{1/p})$ is a trivial extension of K. This contradicts lemma 1, thus proving Theorem I.

2. Application of Soulé's result

Soulé [So] showed that if $\log p > t(n)$ then $C_p^{(p-n)}, C_p^{(p-n-2)}, \dots, C_p^{(p-3)}$ are all trivial.

For such p, the fact that p doesn't divide $\mathbf{B}_2, \dots, \mathbf{B}_{n+1}$ follows easily from proposition 1 because $exp(t(n)) = exp(n^{224n^4}) > 14\sqrt{n+1}(\frac{n+1}{6})^{n+1}$. Thus assumption (b) is satisfied.

Clearly for such p, $p > 2^i$ for $i = 1, 2, \dots, n+1$. Thus assumption (c) is satisfied as well, and Theorem I can be restated as follows:

For any fixed odd positive integer n, let $p > exp(n^{224n^4})$ be an irregular prime such that one of $C_p^{(3)}, C_p^{(5)}, ...C_p^{(n)}$ is non-trivial. Let q be an odd prime such that $q \equiv 1 \ mod\ (p)$, and such that there is a prime ideal Q over q in $\mathbf{Q}(\zeta)$ whose ideal class is of the form $I^p J$ where J is non-trivial, not a $p-$th power and $J \in C_p^{(3)} \oplus C_p^{(5)} \oplus .... \oplus C_p^{(n)}$.

For such p and q, if $x^p + y^p = pc\, z^p$ has a nontrivial solution $x, y, z \in \mathbf{Z}$, with $(x, y, z) = 1$, then $q \not| \frac{pc\ z^p}{x+y}$.

Note on p-divisibility of h_p^+.

The use of Soulé's theorem also helps to weaken the condition $(p, h_p^+) = 1$. In particular, given p such that $log(p) > t(n)$, it is enough to assume that p doesn't divide $\mathbf{B}_i$ for even i such that $\sqrt{logp} < i < p-n$. It then easily follows from Soulé's result that $(p, h_p^+) = 1$. Indeed, a simple computation using proposition 1 shows that for $2m < \sqrt{logp}$, p doesn't divide $\mathbf{B}_2, \dots, \mathbf{B}_{2m}$. We also have that, if p doesn't divide $\mathbf{B}_i$, i even, then $C_p^{(i)}$ is trivial, for $i = 2, 4, \dots, p-3$. [Let $r_i = p\text{-rank}(C_p^{(i)})$. If $C_p^{(i)}$ is nontrivial, then $r_i \geq 1$. By the reflection theorem for C_p, $r_i \leq p\text{-rank}(C_p^{(p-i)}) \leq r_i + 1$ and thus $C_p^{(p-i)}$ will be non-trivial. This by Herbrand's theorem means that $p|\mathbf{B}_i$]. Thus $C_p^{(i)} = 0$ for $i = 2, 4, \dots, p-n-2$. By Soulé's theorem we get that $C_p^{(p-n)}, C_p^{(p-n-2)}, \dots, C_p^{(p-3)}$ are all trivial. Thus $C_p^{(i)} = 0$ for $i = 2, 4, \dots, p-3$ and hence $(p, h_p^+) = 1$.

References

[DM] H. Darmon and L. Merel, Winding quotients and some variants of Fermat's Last Theorem, *J. Reine Angew. Math.* , **490** (1997), 81-100.

[G] J. M. Gandhi, On generalised Fermat's last theorem. II, *J. Reine Angew. Math.* **256** (1972), 163-167.

[I] K. Inkeri, On a Diophantine equation of modified Fermat type, *Acta Arith.* **54** (1989), *no.* 1, 1-7.

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

[MM] T. Morishima and T. Miyoshi, On the diophantine equation $x^p + y^p = cz^p$, *Proc. Amer. Math. Soc.* **16** (1965), 833-836.

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

[RS] J. B. Rosser and L. Schoenfeld, Sharper bounds for the Chebyshev functions $\theta(x)$ and $\psi(x)$, *Math. Comp.*, **29** (1975), 243–269.

[So] C. Soulé, Perfect forms and the Vandiver conjecture, *J. Reine Angew. Math.*, **517** (1999), 209–221.

[S1] S. Sitaraman, On a Fermat type diophantine equation, *J. Number Theory* **80** (2000), 174-186.
[S2] S.Sitaraman, Vandiver Revisited, *J. Number Theory* **57** (1996),122-129.

[V1] H.S. Vandiver, Fermat's last theorem and the second factor in the cyclotomic class number , *Bull. Amer. Math. Soc.* **40** (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 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, NewYork / 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, Ring theoretic properties of certain Hecke algebras, *Ann. of Math.* **141** (1995), 552-572.

[Y] I. Yamaguchi, On generalized Fermat's last theorem, *TRU Math.* **6** (1970), 29–32.