PACIFIC JOURNAL OF MATHEMATICS
Vol. 67, No. 1, 1976

SOME FORMS OF ODD DEGREE FOR WHICH THE HASSE PRINCIPLE FAILS

MASAHIKO FUJIWARA AND MASAKI SUDO

The object of this paper is to give a family of absolutely irreducible forms of odd degree for which the Hasse principle fails.

Let K be an algebraic number field and $f(X_1, \cdots, X_n)$ be a polynomial of n variables $X_1, \cdots, X_n$ over K. We say the Hasse principle over K, briefly H.P./K, holds for $f(X_1, \cdots, X_n)$ when $f(X_1, \cdots, X_n) = 0$ has a solution in K if and only if it has a solution in $K_\mathfrak{p}$ for all prime spots $\mathfrak{p}$. Here, if f is a form, a solution means a nontrivial one. Our aim in this paper is to push forward the method in [3] and thus producing a family of forms of odd degree for which H. P. fails. As is well known, the Hasse-Minkowski theorem assures the validity of H. P. for any quadratic forms. So far as forms of higher degree are concerned, the things are not so simple if the form is absolutely irreducible of odd degree (see [1], Chap. I, § 7). For forms of degree 3, there have been found several counter examples ([2], [4], [5], [6]). Such a form of degree 5 was discovered by the first author [3]. In this paper, we prove the following theorem. Let $\boldsymbol{P}$ be the set of primes which satisfy the conditions in § 2 of this paper. For example $\{p \in \boldsymbol{P};\ p \leqq 1000\} = \{17, 53, 89, 131, 149, 167, 179, 257, 311, 359, 431, 449, 467, 521, 563, 599, 683, 773, 887, 953, 977\}$.

THEOREM. H.P./$\boldsymbol{Q}$ *does not hold for the following form of degree* $10n + 5$

$F(x, y, z) = (x^3 + 5y^3)(x^2 + xy + y^2)^{5n+1} - pz^{10n+5}$, *where n is any nonnegative integer and p is in $\boldsymbol{P}$.*

This theorem gives counter examples, for H. P./$\boldsymbol{Q}$, of any odd degree divisible by 5. Though the method of the proof is basically analogous to that of [3], local solvability needs more careful and involved treatment.

In § 1 we prove that the equation $F = 0$, actually in a slightly more general setting, can be solved everywhere locally. It goes without saying that Hensel's lemma plays a central role there.

In § 2 we show that the equation does not have any integral, therefore rational, solution. The argument used there enables one to find as many primes in $\boldsymbol{P}$ as one may want. We remark here that, if $5n+1$ is not divisible by 3, the set $\boldsymbol{P}$ in our theorem can be enlarged to the set $\boldsymbol{P}'$ also defined in § 2. The primes in $\boldsymbol{P}'$ less than 1000 are, in addition to the primes in $\boldsymbol{P}$ listed above, 47, 137, 191, 227, 281, 353, 389, 479, 587, 641, 677, 821, 911, 983.

Finally, Facom 230 45S 0S2/VS installed at Tokyo Metropolitan University was made use of in order to find all the primes in $\boldsymbol{P}$ and $\boldsymbol{P}'$ less than 1000.

1. Local solvability. In this section we consider the question of the solvability of the following equation

$$(x^3+5y^3)(x^2+xy+y^2)^{5n+1}-az^{10n+5}=0\,, \tag{E}$$

where a is an integer and n is a nonnegative integer, in a local field $\boldsymbol{Q}_q$. Throughout this section, by a solution, we always mean a nontrivial one.

Solvability in $\boldsymbol{Q}_q$ for $q\neq 2, 3, 5$ is found in the remark at the end of § 1 of [3]. Therefore we will deal with the cases $q=2$ (Prop. 1), $q=3$ (Prop. 2 and 3), and $q=5$ (Prop. 4 and 5).

PROPOSITION 1. *For any integer a,* (E) *has a solution in $\boldsymbol{Q}_2$.*

Proof. Put $(x, y, z)=(1, -1, 0)$, then $F(1, -1, 0)=-4\equiv 0$ (mod 2) and $(\partial F/\partial x)(1, -1, 0)=3-4(5n+1)\not\equiv 0$ (mod 2). This assures a 2-adic solution of (E) by Hensel's lemma (Th. 3, § 5, Chap. I, [1]).

We now consider the solvability in $\boldsymbol{Q}_3$ in two cases, i.e., the case $a\not\equiv 0$ (mod 3) and the case $a\equiv 0$ (mod 3).

PROPOSITION 2. *Let $a\not\equiv 0$ (mod 3). (i) If 3 does not divide $5n+1$, then* (E) *has a solution in $\boldsymbol{Q}_3$ (ii) If 3 divides $5n+1$, then* (E) *has a solution in $\boldsymbol{Q}_3$ if and only if* (a) $a\equiv 1$, (b) $a\equiv 4$, (c) $a\equiv 5$, *or* (d) $a\equiv 8$ (mod 9).

We need the following two lemmas in order to prove the case (ii) of Proposition 2.

LEMMA 1. *At least one of the following four congruences*

$$x^3\equiv a \pmod{27} \tag{1}$$

$$x^3\equiv -a \pmod{27} \tag{2}$$

$$5x^3\equiv a \pmod{27} \tag{3}$$

$$5x^3\equiv -a \pmod{27} \tag{4}$$

has a solution whenever a *satisfies* (a), (b), (c) *or* (d) *of Proposition* 2.

Proof. The case (a). Then we have $a \equiv 1$, 10 or 19 (mod 27). If, say, $a \equiv 1$ (mod 27), (1) has the solutions $x \equiv 1, -8, 10$ (mod 27). The other two cases can be done similarly.

The case (b). Then we have $a \equiv 4$, 13, or 22 (mod 27). If, say, $a \equiv 4$ (mod 27), (3) has the solutions $x \equiv -4, 5, -13$ (mod 27). The other two cases can be done similarly.

The cases (c) and (d) can be treated likewise.

LEMMA 2. *The solutions of the congruence*

$$x^2 + 3x - 1 \equiv 0 \pmod{27} \tag{A}$$

are $x \equiv 4, -7$ (mod 27) *and the solutions of the congruence*

$$x^2 - 1 \equiv 0 \pmod{27} \tag{B}$$

are $x \equiv 1, -1$ (mod 27).

And at least one of the solutions found in Lemma 1 *for each* a *satisfying* (a), (b), (c), *or* (d) *satisfies the congruence* (A) *or* (B).

Proof. Straightforward.

Proof of Proposition 2. (i) As a has a form $3m \pm 1$ in this case, we put $(x, y, z) = (1, -1, \mp 1)$, then $F(1, -1, \mp 1) \equiv -4 \pm 3m + 1 \equiv 0$ (mod 3) (signs taken simultaneously), and $(\partial F/\partial z)(1, -1, \mp 1) = -a(10n + 5) \not\equiv 0$ (mod 3). This assures a 3-adic solution of (E) by Hensel's lemma and (i) of our proposition is proved.

(ii) (First step) We prove that (E) has no solution in the case $a \equiv \pm 2$ (mod 9).

We have only to show that any solution of the congruence

$$(x^3 + 5y^3)(x^2 + xy + y^2)^{5n+1} - az^{10n+5} \equiv 0 \pmod{3^{10n+5}} \tag{5}$$

is divisible by 3 (Th. 2, § 5, Chap. I, [1]).

As $x^3 \equiv 0$ or ± 1 (mod 9) for any integer x, it is easy to see that $F(x, y, z) \not\equiv 0$ (mod 9) for any x, y, z with $3 \nmid z$. Consequently a solution (x, y, z) of (5) must be such that $3 | z$. If either one of x or y is divisible by 3, then both are. Therefore we can assume that $3 \nmid x, y$ and $3 | z$. Then we can easily show that each of $x^2 + xy + y^2$ and $x^3 + 5y^3$ are divisible by at most 3^1. Thus the first term of (5) is divisible by at most 3^{5n+2}, whereas the second term of (5) is divisible by 3^{10n+5}. This is a contradiction.

(Second step) We prove that (E) has a solution in the cases (a), (b), (c) and (d) in our proposition. We consider two cases $3 \| 5n + 1$

and $3^2 \mid 5n+1$.

Case 1. $3 \| 5n+1$. Suppose x_0 is a common root of the congruences (1) and (A), as $x_0 \not\equiv 0 \pmod 3$, $F(x_0, 3, 1) \equiv (x_0^3 + 5\cdot 3^3)(x_0^2 + x_0\cdot 3 + 3^2)^{5n+1} - a \equiv x_0^3(3^2+1)^{5n+1} - a \pmod{27} \equiv x_0^3 - a \equiv 0 \pmod{27}$ and $(\partial F/\partial y)(x_0, 3, 1) = 15\cdot 3^2(x_0^2 + x_0\cdot 3 + 3^2)^{5n+1} + (x_0^3 + 5\cdot 3^3)(5n+1)(x_0^2 + x_0\cdot 3 + 3^2)^{5n}(x_0 + 2\cdot 3) \equiv 0 \pmod 3 \not\equiv 0 \pmod{3^2}$.

Thus we obtain a 3-adic solution of (E). (2) and (A) can similarly be done by taking $(x, y, z) = (x_0, 3, -1)$ for above x_0.

Suppose y_0 is a common root of the congruences (3) and (A), as $y_0 \not\equiv 0 \pmod 3$, $F(3, y_0, 1) \equiv (3^3 + 5y_0^3)(3^2 + 3y_0 + y_0^2)^{5n+1} - a \equiv 5y_0^3(3^2+1)^{5n+1} - a \equiv 5y_0^3 - a \equiv 0 \pmod{27}$ and $(\partial F/\partial x)(3, y_0, 1) = 3^3(3^2 + 3y_0 + y_0^2)^{5n+1} + (3^3 + 5y_0^3)(5n+1)(3^2 + 3y_0 + y_0^2)^{5n}(2\cdot 3 + y_0) \equiv 0 \pmod 3 \not\equiv 0 \pmod{3^2}$. For (4) and (A), $(x, y, z) = (3, y_0, -1)$, for above y_0, will suffice to assure a 3-adic solution.

Suppose x_0 is a common root of the congruences (1) and (B), then $F(x_0, 3^2, 1) \equiv (x_0^3 + 5\cdot 3^6)(x_0^2 + x_0\cdot 3^2 + 3^4)^{5n+1} - a \pmod{27} \equiv x_0^3(1 + 3^2 x_0)^{5n+1} - a \equiv x_0^3 - a \equiv 0 \pmod{27}$ and $(\partial F/\partial y)(x_0, 3^2, 1) \equiv 0 \pmod 3 \not\equiv 0 \pmod{3^2}$. For (2) and (B), take $(x, y, z) = (x_0, 3^2, -1)$ for above x_0.

Suppose y_0 is a common root of the congruences (3) and (B), $F(3^2, y_0, 1) \equiv (3^6 + 5y_0^3)(3^4 + 3^2 y_0 + y_0^2)^{5n+1} - a \equiv 5y_0^3(1 + 3^2 y_0)^{5n+1} - a \equiv 5y_0^3 - a \equiv 0 \pmod{27}$ and $(\partial F/\partial x)(3^2, y_0, 1) \equiv 0 \pmod 3 \not\equiv 0 \pmod{3^2}$. For (4) and (B), take $(x, y, z) = (3^2, y_0, -1)$ for above y_0. Thus we obtain a 3-adic solution of (E) by Hensel's lemma.

Case 2. $3^2 \mid 5n+1$. Let x_0 be a solution of the congruence (1) or (2), then, as $x_0^2 \equiv 1 \pmod 3$, $F(x_0, 0, \pm 1) \equiv x_0^3(x_0^2)^{5n+1} \mp a \equiv x_0^3\{(x_0^2 - 1) + 1\}^{5n+1} \mp a \equiv x_0^3 \mp a \equiv 0 \pmod{27}$ (signs taken simultaneously according to (1) or (2)), and $(\partial F/\partial z)(x_0, 0, \pm 1) = -a(10n+5) = -a\{2(5n+1) + 3\} \equiv 0 \pmod 3 \not\equiv 0 \pmod{3^2}$.

This assures a 3-adic solution of (E) by Hensel's lemma.

If y_0 is a solution of the congruence (3) or (4), then take $(0, y_0, \pm 1)$ according to (3) or (4) and we can easily show $F(0, y_0, \pm 1) \equiv 0 \pmod{27}$ and $(\partial F/\partial z)(0, y_0, \pm 1) \equiv 0 \pmod 3 \not\equiv 0 \pmod{3^2}$.

Thus we obtain a 3-adic solution of (E). Therefore Proposition 2 is completely proved.

PROPOSITION 3. *Let* $a \equiv 0 \pmod 3$. (i) *If* $a \equiv \pm 3 \pmod 9$, (E) *has no solution in* $\boldsymbol{Q}_3$. (ii) *If* $a \equiv 0 \pmod 9$ ($a = 3^r a'$, r is an integer $\geqq 2$, $3 \nmid a'$), *then* (E) *has a solution in* $\boldsymbol{Q}_3$ *if* r *is a multiple of* $10n+5$ *and* $a' \equiv \pm 1$ *or* $\pm 5 \pmod 9$.

Proof. (i) We consider the following congruence

$$(6) \qquad (x^3 + 5y^3)(x^2 + xy + y^2)^{5n+1} - az^{10n+5} \equiv 0 \pmod{3^{10n+6}} .$$

We have only to show that any solution of (6) is divisible by 3. First suppose (x, y, z) is a solution such that $3 \nmid z$. Since the second term of (6) is precisely divisible by 3^1, if x or y is divisible by 3, then both are. So we can assume that neither x nor y are divisible by 3. Then it is easy to see that $3 \| x^3 + 5y^3$ and $3 \| x^2 + xy + y^2$. Therefore the first term of (6) is precisely divisible by 3^{5n+2}. This is a contradiction. Thus the solution, if it exists, must be such that $3 | z$. In this case we have $3^{10n+6} | az^{10n+5}$. If neither x nor y are divisible by 3, we will have a contradiction by the same discussion as above. If x or y is divisible by 3, then both are. Therefore any solution (x, y, z) of the congruence (6) is divisible by 3 and our assertion is proved.

(ii) Consider the equation

$$(7) \qquad (x^3 + 5y^3)(x^2 + xy + y^2)^{5n+1} - a'z^{10n+5} = 0 .$$

By Proposition 2, (7) has a 3-adic solution (x, y, z). Put $a = 3^{l(10n+5)}a'$ for some integer l. Then $(3^l x, 3^l y, z)$ is a 3-adic solution of (E).

We now enter the discussion of the solvability in $\boldsymbol{Q}_5$. We consider two cases, i.e., the case $a \not\equiv 0 \pmod 5$ and the case $a \equiv 0 \pmod 5$.

PROPOSITION 4. *Let* $a \not\equiv 0 \pmod 5$. *Then* (E) *has a solution in* $\boldsymbol{Q}_5$.

Proof. If $a \equiv \pm 1 \pmod 5$, we put $(x, y, z) = (\pm 1, 0, 1)$, then $F(\pm 1, 0, 1) \equiv (\pm 1) - (\pm 1) \equiv 0 \pmod 5$ (signs taken simultaneously) and $(\partial F/\partial y)(\pm 1, 0, 1) \equiv \pm 1(5n + 1)(\pm 1) \not\equiv 0 \pmod 5$. This assures a 5-adic solution of (E) by Hensel's lemma

If $a \equiv \pm 2 \pmod 5$, put $(x, y, z) = (2, 0, \pm 1)$ if n is even, then $F(2, 0, \pm 1) \equiv 0 \pmod 5$ (signs taken simultaneously), and $\partial F/\partial y (2, 0, \pm 1) \not\equiv 0 \pmod 5$. For odd n, put $(x, y, z) = (2, 0, \mp 1)$.

PROPOSITION 5. *If* $a \equiv 0 \pmod 5$ $(a = 5^r a'$, r is a positive integer, $5 \nmid a')$, *then* (E) *has a solution in* $\boldsymbol{Q}_5$ *if* r *is a multiple of* $10n + 5$.

Proof. Put $a = 5^{l(10n+5)}a'$ for some integer l and consider the equation

$$(8) \qquad (x^3 + 5y^3)(x^2 + xy + y^2)^{5n+1} - a' z^{10n+5} = 0 .$$

By Proposition 4, (8) has a 5-adic solution (x, y, z). Then $(5^l x, 5^l y, z)$ is a 5-adic solution of (E).

REMARK 1. In connection with Proposition 3 (ii), we can tell a little more. *If* $a \equiv 0 \pmod 9$ ($a = 3^{l(10n+5)+r}a'$, *r is an integer* s.t. $10n + 5 > r > 0$, *l is a nonnegative integer and a' is not divisible by* 3), *then*

(E) *has no solution in* $\boldsymbol{Q}_3$ *unless* $r = 5n + 2$.

2. In relation to Proposition 5, we can also tell more. *If* $a \equiv 0 \pmod 5$ ($a = 5^{l(10n+5)+r}a'$, *r is an integer* s.t. $10n + 5 > r > 0$, *l is a nonnegative integer and a' is not divisible by* 5), *then*

(E) *has no solution in* $\boldsymbol{Q}_5$ *unless* $r = 1$.

Next we give some sufficient conditions for the equation (E) to have a solution in $\boldsymbol{Q}_5$ when $r = 1$ above.

(E) *has a solution in* $\boldsymbol{Q}_5$ *if*

(i) $a' \equiv 1$ *or* $-1 \pmod{125}$

or

(ii) *the congruences*

$$x^2 + 25x \equiv 1 \text{ or } -1 \pmod{125}$$

and

$$x^3 \equiv a' \text{ or } -a' \pmod{125}$$

have a common root.

Remark 1 can be easily proved and 2 can also be done similarly as in Proposition 2.

Summing up all the results of Proposition 1 up to Proposition 5 and Remarks 1 and 2, we obtain the following.

PROPOSITION 6. (I) *For any integer a, the form* (E) *has a q-adic solution except $q = 3$ and* 5.

(II) *Solvability of* (E) *in* $\boldsymbol{Q}_3$. (a) *In case* $a \not\equiv 0 \pmod 3$. (i) *If* 3 *does not divide* $5n + 1$, (E) *has a solution.* (ii) *If* 3 *divides* $5n + 1$, (E) *has a solution if and only if* $a \equiv 1, 4, 5$, or $8 \pmod 9$. (b) *In case* $a \equiv 0 \pmod 3$. (i) *If* $a \equiv 3$ *or* $6 \pmod 9$, (E) *has no solution.* (ii) *If* $a \equiv 0 \pmod 9$ *and* $a = 3^r a'$ (r is a multiple of $10n + 5$, $3 \nmid a'$), *then* (E) *has a solution if and only if* $a' \equiv \pm 1$ *or* $\pm 5 \pmod 9$. (iii) *If r is not a multiple of* $10n + 5$ *in* (ii), *then* (E) *has no solution unless* $r \equiv 5n + 2 \pmod{10n + 5}$.

(III) *Solvability of* (E) *in* $\boldsymbol{Q}_5$. (1) *In case* $a \not\equiv 0 \pmod 5$. (E) *has a solution.* (2) *In case* $a \equiv 0 \pmod 5$. *Then* (i) *If* $a = 5^r a'$ *and r is a multiple of* $10n + 5$ ($5 \nmid a'$), (E) *has a solution.* (ii) *If*

r is not a multiple of $10n+5$ *in* (i), *then* (E) *has no solution unless* $r \equiv 1 \pmod{10n+5}$. (iii) *When* $a = 5^{l(10n+5)+1}a'$ (l is a nonnegative integer, $5 \nmid a'$), (E) *has a solution if* $a' \equiv \pm 1 \pmod{125}$, *or the congruences* $x^2 + 25x \equiv 1$ *or* $-1 \pmod{125}$ *and* $x^3 \equiv a'$ or $-a' \pmod{125}$ *have a common zero.*

2. Global nonsolvability. In this section, we assume p to be a prime satisfying $(-3/p) = -1$, foreseeing that the condition will be included in the definition of $\boldsymbol{P}$ and $\boldsymbol{P}'$.

Let (x, y, z) be a nontrivial integral solution of

$$F(x, y, z) = (x^3 + 5y^3)(x^2 + xy + y^2)^{5n+1} - pz^{10n+5} = 0 \tag{1}$$

in our theorem. Then we can assume x and y are coprime. Let d denote the largest common divisor of

$$x^3 + 5y^3 \tag{2}$$

and

$$x^2 + xy + y^2 . \tag{3}$$

Assume q^n divides both (2) and (3). Then q^n divides $(2)-(3)\cdot x = 5y^3 - x^2y - xy^2 = y(5y^2 - x^2 - xy)$. Here we can assume q divides neither x nor y, for if q divides one of x, y then it divides the other. Hence q^n divides $5y^2 - x^2 - xy$. Thus q^n divides $(x^2 + xy + y^2) + (5y^2 - x^2 - xy) = 6y^2$.

Therefore q^n divides 6. If 2 divides d then both x and y must be even by (2) and (3). Therefore $d = 1$ or 3. In the following, we show that $d = 3$ is impossible. When n is zero, this fact is proved in p. 273 [3]. So we assume $n \geqq 1$. Assume $d = 3$, then we get, by the second term of (1),

$$3^{10n+5} \mid (x^3 + 5y^3)(x^2 + xy + y^2)^{5n+1} . \tag{4}$$

We note here that $3^4 \mid (x^3 + 5y^3)$ or $3^4 \mid (x^2 + xy + y^2)$ leads to a contradiction (p. 273 [3]). Therefore, by (4), there are three possibilities to be considered.

(i) If $3 \,\|\, (x^2 + xy + y^2)$, then $3^{5n+1} \,\|\, (x^2 + xy + y^2)^{5n+1}$.

So we have $3^{5n+4} \mid (x^3 + 5y^3)$. This is a contradiction since $5n + 4 \geqq 4$.

(ii) If $3^2 \,\|\, (x^2 + xy + y^2)$, then $3^{10n+2} \,\|\, (x^2 + xy + y^2)^{5n+1}$.

So we get $3^3 \mid (x^3 + 5y^3)$ by (4). This is against our assumption $d = 3$. (iii) If $3^3 \,\|\, (x^2 + xy + y^2)$, we have $3^{15n+3} \,\|\, (x^2 + xy + y^2)^{5n+1}$ and $3 \,\|\, (x^3 + 5y^3)$. So the first term of (1) is precisely divisible by 3^{15n+4}, but the second term of (1) is divided at least by 3^{20n+10}. This is a contradiction. Therefore we have proved $d = 1$. Then, using the assumption $(-3/p) = -1$ and the same argument as in p. 274 [3] we see that the equation $x^3 + 5y^3 = pu^{10n+5}$ has a nontrivial integral solution (x, y, u) such that $(x, y) = 1$. Put $u^{2n+1} = Z$. Then the equation

$$\begin{cases} x^3 + 5y^3 = pZ^5 \\ (x, y) = 1 \end{cases}$$

must have an integral solution.

The next lemma is a slight generalization of Lemma 2 of [3].

LEMMA 3. *Let K be a cubic field over $\boldsymbol{Q}$ and p a prime which is unramified and factors in K as a product of a prime divisor $\mathfrak{p}$ of degree 1 and a remaining factor $\mathfrak{q}$. If ζ is an integer of K with* $\mathrm{Sp}(\zeta) = 0$ *and $\mathfrak{q} \mid \zeta$, then p divides ζ.*

Proof. Let $\mathfrak{q}^n \| \zeta$, where n is a positive integer. By the assumption we have $\zeta^3 + a\zeta + b = 0$ for some $a, b \in \boldsymbol{Z}$. Since $-b = N(\zeta)$, we have $p^{2n} \mid b$. Since $a\zeta = -\zeta^3 - b$, it follows that $(\mathfrak{q}, a) \neq 1$ and so $p \mid a$. Therefore ζ^3 is divisible by p, and we have $\mathfrak{p} \mid \zeta^3$, $\mathfrak{p} \mid \zeta$. Thus we obtain $p \mid \zeta$.

Denoting $\sqrt[3]{5}$ by θ, the field $\boldsymbol{Q}(\theta)$ has $1, \theta, \theta^2$ as an integral basis, has class number 1 and has $1 - 4\theta + 2\theta^2$ as its fundamental unit.

When $(-3/p) = -1$ and $p > 5$, p remains prime in $\boldsymbol{Q}(\sqrt{-3})$. Therefore, by the remark at the end of § 1 of [3], p does not remain prime in $\boldsymbol{Q}(\sqrt[3]{5})$. Since the composite field of $\boldsymbol{Q}(\sqrt{-3})$ and $\boldsymbol{Q}(\sqrt[3]{5})$ is the Galois closure of $\boldsymbol{Q}(\sqrt[3]{5})$, it is easy to see that p does not completely split in $\boldsymbol{Q}(\sqrt[3]{5})$. Thus, p factors in $\boldsymbol{Q}(\sqrt[3]{5})$ as a product of a prime divisor $\mathfrak{p}_1$ of degree 1 and a prime divisor $\mathfrak{p}_2$ of degree 2.

By Lemma 3, if $\mathfrak{p}_2$ divides $x + y\theta$, p divides $\theta(x + y\theta)$, for $\mathrm{Sp}(\theta(x + y\theta)) = 0$. So p divides $x + y\theta$ and thus both x and y. This contradicts $(x, y) = 1$.

Therefore by following the arguments in p. 275, [3], $x + y\theta$ must take the form of one of the following types: $\pi_1\zeta^5$, $\pi_1\varepsilon\zeta^5$, $\pi_1\varepsilon^2\zeta^5$, $\pi_1\varepsilon^3\zeta^5$, $\pi_1\varepsilon^4\zeta^5$, where ζ is an integer of $\boldsymbol{Q}(\theta)$, ε is the fundamental unit $1 - 4\theta + 2\theta^2$ in $\boldsymbol{Q}(\theta)$, and π_1 is an integer generating $\mathfrak{p}_1$. Write $\pi_1 = I + J\theta + K\theta^2$, where I, J and K are rational integers. In the following we will define a set $\boldsymbol{P}'$ consisting of primes and its subset $\boldsymbol{P}$ and then show that $x + y\theta$ can never take any one of those five forms if p in (1) belongs to $\boldsymbol{P}'$.

Put $\zeta = u + v\theta + w\theta^2$ where $u, v, w \in \boldsymbol{Z}$. Then

$$\zeta^5 = (u + \theta(v + w\theta))^5 = u^5 + 5A\ ,$$

where A is an integer of $\boldsymbol{Q}(\theta)$.

As $\varepsilon = 1 - 4\theta + 2\theta^2$, $\varepsilon^2 = -79 + 12\theta + 20\theta^2$, $\varepsilon^3 = -359 + 528\theta - 186\theta^2$ and $\varepsilon^4 = 8641 + 104\theta - 3016\theta^2$, putting $(I + J\theta + K\theta^2)\varepsilon^i = a_i + b_i\theta + c_i\theta^2$ $(i = 0, \cdots, 4)$, we obtain $c_0 = K$, $c_1 = 2I - 4J + K$, $c_2 = 20I + 12J - 79K$, $c_3 = -186I + 528J - 359K$, $c_4 = -3016I + 104J + 8641K$.

Now let $\boldsymbol{P}'$ be the set of all primes p that satisfy the following conditions

$$5 < p, \left(\frac{-3}{p}\right) = -1, 5 \nmid c_i (i = 0, \cdots, 4) \text{ or equivalently } 5 < p ,$$

$(-3/p) = -1$ and $5 \nmid K, 2I + J + K, 2J + K, -I + 3J + K, -I - J + K$. And let $\boldsymbol{P}$ be the set of all primes in $\boldsymbol{P}'$ that satisfy the condition $p \not\equiv \pm 2 \pmod 9$.

Let p be an element of $\boldsymbol{P}'$. If $x + y\theta$ takes one of the abovementioned forms then, for some i,

$$\begin{aligned} x + y\theta &= (a_i + b_i\theta + c_i\theta^2)\zeta^5 = (a_i + b_i\theta + c_i\theta^2)(u^5 + 5A) \\ &= a_iu^5 + 5B + (b_iu^5 + 5C)\theta + (c_iu^5 + 5D)\theta^2 , \end{aligned}$$

where B, C, D are rational integers. Since 5 does not divide c_i, this equality shows that 5 divides u. Consequently 5 divides $x + y\theta$ and thus both x and y. This contradicts our assumption $(x, y) = 1$. Therefore we have proved $x^3 + 5y^3 = pZ^5$ has no nontrivial integral solution with $(x, y) = 1$ when p belongs to $\boldsymbol{P}'$. Therefore (1) does not have a nontrivial integral solution for any p in $\boldsymbol{P}'$.

On the other hand, the equation (1) has obviously a nontrivial solution in $\boldsymbol{R}$ and has already been shown, in Proposition 6, to have solutions everywhere locally for each p in $\boldsymbol{P}$ (even in $\boldsymbol{P}'$ if $3 \nmid 5n + 1$). Therefore, we have completely proved the theorem.

References

1. Z. I. Borevich and I. R. Shafarevich, *Number Theory*, Academic Press 1966.
2. J. W. S. Cassels and M. J. T. Guy, *On the Hasse principle for cubic surfaces*, Mathematika, **13** (1966), 111-120.
3. M. Fujiwara, *Hasse principle in algebraic equations*, Acta Arithmetica, **22** (1973), 267-276.
4. L. J. Mordell, *On the conjecture for the rational points on a cubic surface*, J. London Math. Soc., **40** (1965), 149-158.
5. E. S. Selmer, *The diophantine equation* $ax^3+by^3+cz^3=0$, Acta Math., **85** (1951), 203-362.
6. H. P. F. Swinnerton-Dyer, *Two special cubic surfaces*, Mathematika, **9** (1962), 54-56.

Received April 26, 1976 and in revised form July 8, 1976.

OCHANOMIZU UNIVERSITY
AND
SEIKEI UNIVERSITY