JOURNAL OF RESEARCH of the National Bureau of Standards — B. Mathematical Sciences
Vol. 79B, Nos., 1 and 2, January–June 1975

The Diophantine Equation $p^2x^4 + 3px^2y^2 + y^4 = z^2$, p an Odd Prime*

T. N. Sinha **

(February 7, 1975)

The object of this paper is to prove:
THEOREM 1. *The equation*

$$p^2x^4 + 3px^2y^2 + y^4 = z^2$$

where p *is an odd prime, has no solutions in integers with* $xy \neq 0$ *if* $p=5$ *or* $p \equiv 3, 7 \pmod{20}$ *or* $p \equiv 13 \pmod{40}$.

Key words: Diophantine equation, Infinite descent, Quadratic residues.

In this paper we indicate certain values of p, where p is an odd prime, such that the equation

$$p^2x^4 + 3\,px^2y^2 + y^4 = z^2 \tag{1}$$

has no integer solutions with $xy \neq 0$, and note some applications for the case $p=5$.

1. It is known that for $p=1$ the equation (1) has no solution in integers with $xy \neq 0$ [1].[1] We now let p stand for an odd prime and consider the integer solutions of (1). We need only consider the solutions with $x \geqslant 0$, $y \geqslant 0$, $z \geqslant 0$ and $(x, y)=1$. If $p \mid y$, then $p \mid z$, and dividing through by p^2 we get equation which is the same as (1) with x, y interchanged. Hence we assume that $p \nmid y$ (and so $y \neq 0$). Then it follows that x, y, z are prime each to each, and z is odd. Multiplying through by 4 we write (1) as

$$5(y^2)^2 + (2z)^2 = (2px^2 + 3y^2)^2$$

Since p is an odd prime we have $(y^2, 2z, 2px^2 + 3y^2) = 1$ or 2 according as y is odd or even. Hence [3]

$$y^2 = drs,\ 2z = \pm\frac{d}{2}(r^2 - 5s^2),\ 2px^2 + 3y^2 = \frac{d}{2}\ (r^2 + 5s^2) \tag{2}$$

where $d=1$ or 4 according as r, s are integers of the same parity or of opposite parity, $(r, 5s) = 1$, $r \geqslant 1$, $s \geqslant 1$. From the first equation in (2) we have $r=R^2$, $s=S^2$, $y=\sqrt{d}\,RS > 0$, where R, S are integers, $(R, 5S)=1$, $R \geqslant 1$, $S \geqslant 1$. Writing $D=\sqrt{d} > 0$, so that $D=1$ or 2 according as

---

AMS Subject Classification: 10B10.
* An invited paper.
** Present Address: Department of Mathematics, Bhagalpur University, Bhagalpur (Bihar)-India.
[1] Figures in brackets indicate the literature references at the end of this paper.

R and S are of the same or of opposite parity we have from (2)

$$px^2 = \frac{D^2}{4}(R^2-5S^2)(R^2-S^2),\ y = DRS,\ z = \pm\frac{D^2}{4}(R^4-5S^4) \tag{3}$$

as the solution of (1) in px^2, y and z. If $R=S$, then $x=0$, $y^2=\pm s$. Suppose now that $R \neq S$, and consider the first equation in (3). It is clear that either $R > \sqrt{5}S$ or $R < S$; also that either $p \mid (R^2-S^2)$ or $p \mid (R^2-5S^2)$. We now prove

LEMMA 1. *Let* $p \mid (R^2-S^2)$. *Then*

(*i*) *if* $R > \sqrt{5}S$, *the first equation in* (3) *is impossible if* $p \equiv 3 \pmod 4$ *or* $p \equiv 5 \pmod 8$.

(ii) if $R < S$, there cannot occur a minimum value of $z > 0$.

For, letting $\delta = (R-S, R+S)$ we have $\delta \leq 2$, and $\delta' = (R^2-5S^2, R^2-S^2) = (4S^2, R^2-S^2) = \delta^2$. Since $p \mid (R^2-S^2)$ we have $R \mp S \equiv 0 \pmod p$ and so from the first equation in (3) we have either

(a) $R \mp S = p\,\delta\,u^2,\ R \pm S = \delta\,v^2,\ R^2-5S^2 = \delta^2 w^2,\ (R > \sqrt{5}S)$

or

(b) $S \mp R = p\,\delta\,u^2\cdot S \pm R = \delta\,v^2,\ 5S^2 - R^2 = \delta^2 w^2,\ (R < S)$

where u, v, w are positive integers, relatively prime pairwise, $u+v$, $v \not\equiv 0 \pmod p$, and w is odd. The case (a) gives

$$3p\,u^2v^2 = p^2u^4 + v^4 + w^2$$

Hence $p \mid (v^4+w^2)$. This is impossible if $p \equiv 3 \pmod 4$. Also, if $p \equiv 5 \pmod 8$, the number $3pu^2v^2$ is not a sum of three squares, because this number is of the form $4^k(8N+7)$, $k \geq 0$. The result (i) of Lemma 1 follows.

The case (b) gives

$$p^2u^4 + 3pu^2v^2 + v^4 = w^2$$

which is the same as (1) and where

$$w^2 = \frac{1}{\delta^2}(5S^2-R^2) \leq 5S^2 - R^2 = (\sqrt{5}S+R)(\sqrt{5}S-R) \tag{4}$$

Now, since $1 \leq R \leq S-1$, we have

$$\sqrt{5}-1 < (\sqrt{5}-1)R^2 + 2R - 1 = \sqrt{5}R^2 - (R-1)^2$$

$$\leq \sqrt{5}(S-1)^2 - (R-1)^2 = (\sqrt{5}S^2 - R^2) - 2(\sqrt{5}S - R) + (\sqrt{5}-1)$$

and so
$$\sqrt{5}S - R < \frac{1}{2}(\sqrt{5}S^2 - R^2)$$

Also, plainly $\sqrt{5}S + R < \sqrt{5}S^2 + R^2$ for all R, S under consideration. However, when R, S are both odd, we have, since $2 \leqslant R+1 \leqslant S-1$,

$$\sqrt{5}+1 < \sqrt{5}(R+1)^2+(R-1)^2 \leqslant \sqrt{5}(S-1)^2+(R-1)^2$$
$$= (\sqrt{5}S^2+R^2)-2(\sqrt{5}S+R)+\sqrt{5}+1$$

and so
$$\sqrt{5}S+R < \frac{1}{2}(\sqrt{5}S^2+R^2)$$

Thus (with D defined above)
$$\sqrt{5}S \pm R < \frac{D}{2}(\sqrt{5}S^2 \pm R^2)$$

Hence the product of the two factors on the right hand side of (4) is

$$< \frac{D}{2}(\sqrt{5}S^2+R^2) . \frac{D}{2}(\sqrt{5}S^2-R^2) = \frac{D^2}{4}(5S^4-R^4) \leqslant z^2, \text{ by (3).}$$

By the method of infinite descent the result (ii) of Lemma 1 follows.

LEMMA 2. *If* $p|(R^2-5S^2)$, *the first equation in* (3) *is impossible if* $p \equiv \pm 3, \pm 7$ (*mod 20*).

For, if $p|(R^2-5S^2)$, then $p \neq 5$, since otherwise $5|R$, contrary to the fact that $(R, 5S)=1$. Hence $\left(\frac{5}{p}\right)=1$. But $\left(\frac{5}{p}\right)=-1$ for $p \equiv \pm 3, \pm 7$ (mod 20), [2]. Lemma 2 follows.

From the Lemmas 1 and 2 now follows directly

THEOREM 1. *The equation (1), where* p *is an odd prime, has no solutions in integers with* $xy \neq 0$, *if*

$$p=5 \text{ or } p \equiv 3, 7 \ (mod\ 20) \text{ or } p \equiv 13 \ (mod\ 40).$$

2. Applications for the case $p=5$.

THEOREM 2. *The equation*

$$x^4+3x^2y^2+y^4=5z^2 \tag{5}$$

has no solutions in integers with $x^2 \neq y^2$.

PROOF. We may suppose that $(x, y, z)=1$. Then x, y, z are prime each to each. Put $t=xy$ so that $(z, t)=1$. Then from the equation (5)

$$5z^2-t^2=(x^2+y^2)^2=U^2, \quad 5z^2-5t^2=(x^2-y^2)^2=25V^2>0 \tag{6}$$

From the second equation in (6) we have, with $\partial=(z+t, z-t) \leqslant 2$,

$$z \mp t=5\partial m^2, \quad z \pm t=\partial n^2 \tag{7}$$

where m, n are relatively prime positive integers. From (7) and the first equation in (6) we then have

$$5^2m^4+3.5\, m^2n^2+n^4=(U/\partial)^2$$

which is impossible by theorem 1.

THEOREM 3. *The cubic curve*

$$\zeta^2+3\zeta+1=5\zeta\eta^2 \tag{8}$$

has only the (finite) rational points $(1, \pm 1)$.

For, let (ζ, η) be a finite rational point on (8). Clearly $\zeta\eta \neq 0$. Write (with l, m, z, n integers)

$$\zeta=\frac{l}{m},\ (l, m)=1,\ m>0,\ l\neq 0;\ \eta=\frac{z}{n},\ n>0,\ z\neq 0.$$

Then from (8) $$n^2(l^2+3lm+m^2)=5lmz^2$$

IF $5\nmid n$, we have, since $(l^2+3lm+m^2, lm)=1$,

$$l^2+3lm+m^2=5z^2,\ lm=n^2$$

Since $m>0$, we have $l>0$. Thus $l=x^2$, $m=y^2$, where x, y are integers, $(x, y)=1$, $xy\neq 0$, and so

$$x^4+3x^2y^2+y^4=5z^2$$

By theorem 2, this equation has only the solutions $x^2=y^2=1$. Hence $l=m=1$ and so $\zeta=1, \eta=\pm 1$.

For $n=5n'$ we have similarly $lm=5n'^2$, $l=5x^2$, $m=y^2$, leading to

$$5^2x^4+3.5x^2y^2+y^4=z^2,\ xy\neq 0$$

which is impossible theorem 1. Theorem 3 follows.

COROLLARY. *On writing* $\frac{1}{X}=\zeta$, $\frac{Y}{X}=\eta$, $(X\neq 0)$ *we see that the cubic curve*

$$X(X^2+3X+1)=5Y^2$$

has only the (finite) rational points $(0, 0)$, $(1, \pm 1)$.

References

[1] Pocklington, H. C., Some diophantine impossibilities, Proc. Camb. Phil. Soc. **17,** 108-121, (1914).

[2] Uspensky, J. V., and Heaslet, M. A., Elementary Number Theory (McGraw-Hill Book Company, Inc., New York and London, 1939), p. 294.

[3] Dickson, L. E., Introduction to the theory of numbers (The University of Chicago Press, Chicago, Illinois, 1929), pp. 40–41.

(Paper 79B1 & 2-418)