$x^4 + dx^2y^2 + y^4 = z^2$: SOME CASES WITH ONLY TRIVIAL SOLUTIONS–AND A SOLUTION EULER MISSED

by EZRA BROWN

(Received 23 May, 1988)

0. Introduction. Mathematicians have studied the diophantine equation of the title ever since the days of Fermat, Leibniz and Euler. In this paper, we review the history of this problem, present several new classes of values of d for which the equation has only trivial solutions, and find a nontrivial solution for $d = 85$ (a case Euler missed). With these results, the question of whether

$$x^4 + dx^2y^2 + y^4 = z^2; \quad (x, y) = 1, \quad x, y > 0 \tag{1}$$

has nontrivial solutions is now answered for all d, $0 \leq d \leq 100$.

1. History. A solution $\{x, y, z\}$ of (1) with $x, y, z \geq 0$ is said to be *trivial* either if $xy = 0$, or if $d = n^2 - 2$ and $x = y = 1$. In about 1637 (see Dickson's *History* [**1**, p. 615]) Fermat gave his celebrated proof-by-descent that, for $d = 0$, equation (1) has only trivial solutions; his proof appeared, oddly enough, as a marginal note in his copy of Bachet's 1621 edition of Diophantus' *Arithmetica.* Leibniz proved in 1678 [**1**, p. 617] that $u^4 - v^4$ is never a square (except for $u = 0$ or 1), from which it follows that (1) has only trivial solutions if $d = 6$.

In a paper [**2**; **1**, p. 635] published years after his death, Euler proved that, for $d = 14$, (1) has only trivial solutions, and gave a number of methods for generating nontrivial solutions of (1) for 47 different values of d between 2 and 100. His most elegant result was that if

$$u^2 - \lambda v^2 = 4,$$

then

$$x = v, \; y = 2r, \quad \text{and} \quad z = v^2 \pm 2ur^2$$

is a solution to (1), for $d = \lambda r^2 \pm u$.

As an example, take $\lambda = 31$; since $3040^2 - 31(546)^2 = 4$, we have $u = 3040$, $v = 546$, $r = 10$ and $d = 60$. Thus, $x = 546$, $y = 20$ and $z = 309884$. If $g = (x, y)$, then g^2 divides z; this yields the solution

$$273^4 + 60 \,.\, 273^2 \,.\, 10^2 + 10^4 = 77471^2,$$

with $(x, y) = 1$.

The next major results on the problem were due to H. C. Pocklington [**3**] who proved a number of theorems, including the following:

THEOREM 1. *Equation* (1) *has only trivial solutions if d satisfies any of the following sets of conditions*:

(a) *d odd, $d \not\equiv 7$ (mod 8) and $d + 2$ is a power of a prime*;

(b) $d = 2N + 2$, $N \equiv 1 \pmod 8$, *N is divisible only by primes* $\equiv 3 \pmod 8$ *or only by primes* $\equiv 7 \pmod 8$, *and* $N + 2$ *is a power of a prime*;

(c) $d = 8N + 2$, $N \equiv 1 \pmod 4$, *N is divisible only by primes* $\equiv 3 \pmod 4$, *and* $2N + 1$ *is a power of a prime.*

More recently, Sinha [**4**] proved that (1) has only trivial solutions for $d = 2(2P + 1)$, where $P = 1$ or P is a Mersenne prime, and Zhang [**5**] proved that (1) has only trivial solutions if $d \equiv 3 \pmod 8$, $d - 2$ is a prime, and $d + 2 = pq$, where $p \equiv 3$ and $q \equiv 7 \pmod 8$ are primes.

Collecting these results reveals the current status of the problem for $0 \leq d \leq 100$.

(a) There are no nontrivial solutions of (1) for $d = 0$, 1, $3 - 7$, $9 - 11$, 14, 15, 18–22, 25, $28 - 30$, 35, 45, 51, 59, 65, 69, 74, 75, 81 and 91. (Pocklington is responsible for all of these except for 0 (Fermat), 1 (R. Adrain [**1**, p. 636]), 6 (Leibniz), 14 (Euler), 30 (Sinha) and 75 (Zhang).)

(b) There are nontrivial solutions of (1) for $d = 2$, 8, 12, 13, 16, 17, 23, 24, 26, 27, 31, 33, 36, 39, 41, 42, 44, 48, 49, 52, 55–57, 60, 61, 63, 64, 66–68, 71, 73, 77–79, 83, 84, 86, 87, 89, 90, 92, 94–96, 99 and 100 (all due to Euler).

(c) The status of $d = 32$, 34, 37, 39, 40, 43, 46, 47, 50, 53, 54, 58, 62, 70, 72, 76, 80, 82, 85, 88, 93, 97 and 98 is unknown.

In this paper, we show that for all d listed in (c) above, (1) has only trivial solutions, except for $d = 85$, which has a nontrivial solution. Some of the proofs are based on ideas that are due to Pocklington [**3**]; we even found the nontrivial solution in the curious case $d = 85$ by pursuing Pocklington's method to, and past, an apparent dead end. The other proofs use results on concordant forms.

3. Applications of concordant forms. Two quadratic forms are called *concordant* if they can be made squares for the same nonzero values of their variables, simultaneously, and *discordant* otherwise. Thus, $3^2 + 4^2 = 5^2$ and $3^2 + 7 \cdot 4^2 = 11^2$, so that $r^2 + s^2$ and $r^2 + 7s^2$ are concordant. We use this idea to obtain several new cases for which (1) has only trivial solutions.

THEOREM 2. *The equation* $x^4 + dx^2y^2 + y^4 = z^2$ *has only trivial solutions for* $d = 34$, 46, 50, 54, 58, 62, 70, 82 and 98.

Proof. If $x^4 + (4n + 2)x^2y^2 + y^4 = z^2$, (2)

then

$$(x^2 - y^2)^2 + (n + 1)(2xy)^2 = z^2;$$

since

$$(x^2 - y^2)^2 + (2xy)^2 = (x^2 + y^2)^2$$

identically, it follows that $r^2 + s^2$ and $r^2 + (n + 1)s^2$ are concordant forms. By a result of Brooks and Watson [**1**, p. 475], $r^2 + s^2$ and $r^2 + As^2$ are concordant only for 41 values of A between 1 and 100 and discordant for the other 59. Hence, (2) has no nontrivial solutions if $n + 1$ is one of these 59 values, in particular for $n + 1 = 9$, 12, 13, 14, 15, 16, 18, 21 and 25. The latter nine values of $n+1$ yield the nine values of $d = 4n+2$ in the statement of the theorem, for which (2) has therefore only trivial solutions.

4. Pocklington's method. In [**3**], Pocklington used some elementary methods to show that (1) has only trivial solutions in certain cases. He transformed (1) to one of the equations

$$(x^2 \pm y^2)^2 + (d+2)x^2y^2 = z^2 \tag{3}$$

which led to a consideration of certain simultaneous quadratic equations. He then showed that, in certain cases, these quadratic equations have no solution, either by congruential impossibilities or by descent. We use Pocklington's method to obtain the following theorem:

THEOREM 3. *The equation* $x^4 + dx^2y^2 + y^4 = z^2$ *has no nontrivial solutions in each of the following cases*:

(A) $d = 8k+7 = p-2 = q+2$, p *and* q *primes* (*new case*: 39).

(B) $d = 2p+2 = 6q-2$, $p \equiv q \equiv 5 \pmod 8$ *primes* (*new case*: 76).

(C) $d = 16(3k+2) = 6p+2 = 2q-2$, $p \equiv q+4 \equiv 5 \pmod 8$ *primes* (*new cases*: 32, 80).

(D) $d = 2p+2 = 6q-2$, $p \equiv 19 \pmod{24}$ *and* $q \equiv 7 \pmod 8$ *primes* (*new case*: 40).

(E) $d = pq+2 = rs-2$; $p \equiv s \equiv 5$, $q \equiv 7$, $r \equiv 3 \pmod 8$ *primes*; *and either* $(p/r) = -1$ *or* $(q/r) = 1$, *where* $(/)$ *is the familiar Legendre symbol* (*new cases*: 37, 93).

(F) $d = 43, 47, 53, 72, 88,$ *or* 97.

The proof requires the following lemmas, whose proofs are in Pocklington's paper [**3**].

LEMMA 1. *Let* $x^2 + Ny^2 = z^2$, *with* $(x, Ny) = 1$ *or* $(z, Ny) = 1$. *Then there exist integers* k, m, u *and* v *such that* $(ku, mv) = 1$ *and such that*:

(a) *if* Ny *is odd, then* $km = N$, $2x = ku^2 - mv^2$, $y = uv$ *and* $2z = ku^2 + mv^2$;

(b) *if* Ny *and* y *are even, then* $km = N$, $x = ku^2 - mv^2$, $y = 2uv$, *and* $z = ku^2 + mv^2$.

LEMMA 2. *If* $xy = uv$, *then there exist* α, β, γ, *and* δ *such that* $x = \alpha\beta$, $y = \gamma\delta$, $u = \alpha\gamma$, $v = \beta\delta$. *Moreover, if* $(x, y) = (u, v) = 1$, *then* α, β, γ, *and* δ *are pairwise relatively prime.*

Proof of Theorem 3. We shall give the details of parts A and E and the special case $d = 47$. The other cases are similar, and proofs are available on demand.

Proof of A. Let $d \equiv 7 \pmod 8$, $d = p-2 = q+2$, where p and q are primes. Then we may write (1) as

$$(x^2 + y^2)^2 + q(xy)^2 = z^2. \tag{4}$$

Assume that $(x, y) = 1$, x and y nonzero and $x^2 + y^2$ minimal. Note that if q divides $x^2 + y^2$, it follows that q also divides z, so that q divides x or y. Either way, it follows that (x, y, z) is greater than 1. Hence, $(q, x^2 + y^2) = 1$. There are two cases to consider:

https://doi.org/10.1017/S0017089500007862 Published online by Cambridge University Press

Case 1. If xy is odd, then by Lemma 1, there exist integers k, m, u and v with $(ku, mv)=1$ and

$$2(x^2+y^2)=ku^2-mv^2, xy=uv \quad \text{and} \quad km=q. \tag{5}$$

Now as $(x, y)=(u, v)=1$, by Lemma 2, there exist α, β, γ and δ relatively prime in pairs, such that $x=\alpha\beta$, $y=\gamma\delta$, $u=\alpha\gamma$ and $v=\beta\delta$. Substitution into (5) leads to the equation

$$\alpha^2(k\gamma^2-2\beta^2)=\delta^2(2\gamma^2+m\beta^2). \tag{6}$$

Put $g=(k\gamma^2-2\beta^2, 2\gamma^2+m\beta^2)$; as g divides $2(k\gamma^2-2\beta^2)-k(2\gamma^2+m\beta^2)$ $(=(mk+4)(-\beta^2))$ and similarly g divides $(mk+4)\gamma^2$, it follows that g divides $mk+4=q+4=p$, since $(\gamma^2, \beta^2)=(\gamma, \beta)=1$. Hence, $g=1$ or $g=p$.

Using (6) and the fact that $(\alpha^2, \delta^2)=1$, we have that

$$\begin{aligned} k\gamma^2-2\beta^2&=\pm g\delta^2,\\ m\beta^2+2\gamma^2&=\pm g\alpha^2 \end{aligned} \tag{7}$$

with the same sign in both equations (in view of (6)). Now $mk=q=d-2\equiv 5 \pmod 8$ and $p\equiv 1 \pmod 8$.

If m and k are positive, then $m\beta^2+2\gamma^2\equiv\alpha^2\equiv 1 \pmod 8$ which is impossible, unless $m=1$ and γ is even. But then $k\gamma^2-2\beta^2$ is even, which is also impossible, since γd^2 must be odd (as $(\gamma, \delta)=1$).

If m and k are negative, then the negative signs are chosen in (7), so that

$$2\beta^2-k\gamma^2=g\delta^2\equiv 1 \pmod 8.$$

But then k negative implies that $k=-1$ or $k=-q$; as β and γ are odd, it follows that

$$2\beta^2-k\gamma^2\equiv 3 \text{ or } 7 \pmod 8,$$

a contradiction. Hence, xy cannot be odd.

Case 2. If xy is even, then, say, y is even; the lemmas guarantee integers k, m, u, v, α, β, γ, δ with

$$\begin{gathered} x^2+y^2=ku^2-mv^2, \qquad xy=2uv, \qquad km=q;\\ x=\alpha\beta, \qquad y=2\gamma\delta, \qquad u=\alpha\gamma, \qquad v=\beta\gamma, \quad \alpha \text{ and } \beta \text{ odd};\\ \alpha, \beta, \gamma \text{ and } \delta \text{ pairwise relatively prime}, (u, v)=1; \end{gathered}$$

hence,

$$\alpha^2(k\gamma^2-\beta^2)=\delta^2(m\beta^2+4\gamma^2). \tag{8}$$

As before, if $g=(k\gamma^2-\beta^2, m\beta^2+4\gamma^2)$, then it follows that g divides $mk+4=p$, so that $g=1$ or $g=p$. Hence

$$\begin{aligned} m\beta^2+4\gamma^2&=\pm g\alpha^2\\ k\gamma^2-\beta^2&=\pm g\delta^2 \end{aligned} \tag{9}$$

https://doi.org/10.1017/S0017089500007862 Published online by Cambridge University Press

where both signs are the same as the sign of m. There are several subcases to consider.

(a) If $m = 1$ and $k = q$, then $1 + 4\gamma^2 \equiv \beta^2 + 4\gamma^2 = g\alpha^2 \equiv 1 \pmod 8$, so that γ is even. Thus, δ is odd and so

$$-1 \equiv q\gamma^2 - \beta^2 = g\delta^2 \equiv g \pmod 4, \text{ a contradiction.}$$

(b) If $m = q$ and $k = 1$ then $5 + 4\gamma^2 \equiv q\beta^2 + 4\gamma^2 = g\alpha^2 \equiv g \equiv 1 \pmod 8$, so γ is odd; thus, $g\delta^2 = k\gamma^2 - \beta^2 \equiv 0 \pmod 8$, so δ is even. Eliminating β leads to the equation $(mk + 4)\gamma^2 = p\gamma^2 = g(\alpha^2 + 4\delta^2)$. There are two possibilities:

(i) If $g = p$ then we have

$$\begin{aligned} \gamma^2 &= \alpha^2 + q\delta^2, \\ \alpha^2 &= \beta^2 + 4\delta^2; \end{aligned} \tag{10}$$

hence, there exist r and s with $\alpha = r^2 + s^2$, $\delta = rs$ and $\beta = r^2 - s^2$. Thus, from (10) we see that

$$(r^2 + s^2)^2 + q(rs)^2 = \gamma^2,$$

in which $r^2 + s^2 = \alpha \le \alpha\beta = x \le x^2 < x^2 + y^2$ (as $y > 0$), contrary to the minimality of $x^2 + y^2$.

(ii) If $g = 1$, then (9) leads to

$$\begin{aligned} q\beta^2 + 4\gamma^2 &= \alpha^2, \\ \gamma^2 &= \beta^2 + \delta^2, \end{aligned} \tag{11}$$

where δ is even. Hence, there exist s and t of opposite parity with

$$\gamma = s^2 + t^2,\ \delta = 2st,\ \beta = s^2 - t^2.$$

Thus, $2\gamma = (s - t)^2 + (s + t)^2$ and (11) leads to

$$4\gamma^2 + q\beta^2 = ((s - t)^2 + (s + t)^2)^2 + q((s - t)(s + t))^2 = \alpha^2,$$

in which $(s - t)(s + t)$ is odd; but no such solution can exist, as we showed in Case 1. Hence, $m = q$, $k = 1$ is impossible.

(c) and (d). The proof if $m = -1$ and $k = -q$ is similar to the one for $m = q$ and $k = 1$; the proof if $m = -q$ and $k = -1$ is similar to the one for $m = 1$ and $k = q$; we omit the tedious details.

Thus $(x^2 + y^2)^2 + q(xy)^2 = z^2$ is impossible in nonzero integers x and y, if q and p are primes such that $p - 4 = q \equiv 5 \pmod 8$. This proves part A of Theorem 3.

Proof of E. Suppose that $x^4 + dx^2y^2 + y^4 = z^2$ with $(x, y, z) = 1$, $x^2 + y^2$ minimal and $d = pq + 2 = rs - 2$, where $p \equiv s \equiv 5$, $q \equiv 7$, $r \equiv 3 \pmod 8$ are primes such that either $(p/r) = -1$ or $(q/r) = 1$. Then $d \equiv 5 \pmod 8$ implies that x and y have opposite parity; assume y is even. As in the proof of Part A, applying the lemmas leads to the equations

$$\begin{aligned} k\gamma^2 - \beta^2 &= \pm g\delta^2, \\ 4\gamma^2 + m\beta^2 &= \pm g\alpha^2, \end{aligned} \tag{12}$$

where $km = pq = rs - 4$, g is a divisor of rs, $x = \alpha\beta$, $y = 2\gamma\delta$, α and β are odd, and α, β, γ, and δ are relatively prime in pairs. Moreover, the signs chosen in (12) are the same as the sign of m. There are eight possibilities for k and m; we now give the details for k and m positive, the negative cases being analogous.

(a) $k = pq$, $m = 1$. Then $4\gamma^2 + \beta^2 = g\alpha^2$, so that g is a sum of two relatively prime squares; hence, $g = 1$ or $g = s$. But then, eliminating β leads to the equation $rs\gamma^2 = g(\alpha^2 + \delta^2)$, so that either r or rs is a sum of two relatively prime squares, which is impossible.

(b) $k = p$, $m = q$. Then we have

$$p\gamma^2 - \beta^2 = g\delta^2. \tag{13}$$

Hence, $-\beta^2 \equiv g\delta^2 \pmod{p}$, so that $(g/p) = (-1/p) = 1$ (as $p \equiv 5 \pmod 8$). Also,

$$4\gamma^2 + q\beta^2 = g\alpha^2, \tag{14}$$

so that $7 \equiv q \equiv q\beta^2 \equiv g\alpha^2 \equiv g \pmod 4$; thus, $g \equiv 3 \pmod 4$. This means that $g = r$ or $g = rs$, so that (13) becomes

$$p\gamma^2 \equiv \beta^2 \pmod{r};$$

hence, $(p/r) = 1$. Finally, (14) becomes

$$-4\gamma^2 \equiv q\beta^2 \pmod{r};$$

hence, $(q/r) = (-1/r) = -1$. But we assumed that either $(p/r) = -1$ or $(q/r) = 1$, so that this case is impossible.

(c) $k = q$, $m = p$. Then we have

$$\begin{aligned} q\gamma^2 - \beta^2 &= g\delta^2, \\ 4\gamma^2 + p\beta^2 &= g\alpha^2. \end{aligned} \tag{15}$$

If γ is even, then δ is odd, so that $-1 \equiv -\beta^2 \equiv g \equiv g\alpha^2 \equiv p\beta^2 \equiv p \equiv 1 \pmod 4$, which is impossible. Hence, γ is odd; but this implies that $g\delta^2 \equiv 7\gamma^2 - \beta^2 \equiv 6 \pmod 8$, which is impossible, since g is odd and $\delta^2 \equiv 0$ or $1 \pmod 4$.

(d) $k = 1$, $m = pq$. Then we have

$$\begin{aligned} \gamma^2 - \beta^2 &= g\delta^2, \\ 4\gamma^2 + pq\beta^2 &= g\alpha^2, \end{aligned} \tag{16}$$

so that $g \equiv pq\beta^2 \equiv 3 \pmod 4$, and so $g = r$ or $g = rs$. From (16) we have that $4\gamma^2 \equiv g\alpha^2 \pmod{pq}$, so that $(g/p) = (g/q) = 1$. Now by assumption, either $(p/r) = -1$ or $(q/r) = 1$; in either case, if $g = r$, then either $(g/p) = -1$ or $(g/q) = -1$, a contradiction. Hence, $g = rs$. Eliminating β and γ in turn from (16) leads to the equations

$$\begin{aligned} \gamma^2 &= \alpha^2 + pq\delta^2, \\ \alpha^2 &= \beta^2 + 4\delta^2. \end{aligned}$$

Hence there exist m and n such that $\alpha = m^2 + n^2$, $\delta = mn$ and $\beta = m^2 - n^2$, which implies that

$$(m^2 + n^2)^2 + pq(mn)^2 = \gamma^2.$$

Thus, we have a solution to (1) with $d=pq+2$; however,

$$m^2+n^2=\alpha\le\alpha\beta=x\le x^2<x^2+y^2,$$

contrary to the minimality of x^2+y^2. Hence, case (d) is impossible, and this completes the proof of Part E.

5. The case $d=47$. The case $d=47$ is different enough to warrant separate treatment.

Let $x^4+47x^2y^2+y^4=z^2$ with $(x, y, z)=1$. Then we may write

$$(x^2-y^2)^2+49(xy)^2=z^2; \tag{17}$$

assume that xy is positive, minimal and $x\neq y$.

First, suppose that $(x^2-y^2, 7)=1$. There are two cases to consider.

Case 1. xy is odd. By Lemma 1, there exist u and v such that $2(x^2-y^2)=ku^2-mv^2$ and $xy=uv$, where $km=49$ and $(ku, mv)=1$. As before, there exist α, β, γ, δ, odd and pairwise relatively prime, such that $x=\alpha\beta$, $y=\gamma\delta$, $u=\alpha\gamma$, $v=\beta\delta$, and so

$$2(\alpha^2\beta^2-\gamma^2\delta^2)=k\alpha^2\gamma^2-m\beta^2\delta^2, \quad \text{or}$$
$$\alpha^2(2\beta^2-k\gamma^2)=\delta^2(2\gamma^2-m\beta^2).$$

As in previous cases, this leads to the equations

$$\begin{aligned}2\gamma^2-m\beta^2&=\pm g\alpha^2\\ 2\beta^2-k\gamma^2&=\pm g\delta^2\end{aligned} \tag{18}$$

where $g=(2\beta^2-k\gamma^2, 2\gamma^2-m\beta^2)$. A judicious choice of linear combinations shows that g is a divisor of $mk-4=45$.

(a) If $m=1$ and $k=49$, then eliminating β in (18) reveals that

$$-45\gamma^2=\pm g(\delta^2+2\alpha^2);$$

hence the $-$ sign is used. Thus $\beta^2-2\gamma^2=g\alpha^2$, so that $g\equiv 7 \pmod 8$, i.e. $g=15$. This implies that $\beta^2\equiv 2\gamma^2 \pmod 3$, which is impossible, since $(\beta, \gamma)=1$.

(b) If $m=-1$ and $k=-49$, the $+$ sign must be used, so that $2\gamma^2+\beta^2=g\alpha^2$. Hence, $g\equiv 3 \pmod 8$, so $g=3$. But then eliminating β yields $15\gamma^2=\delta^2-4\alpha^2$, which is impossible (mod 4) with γ and δ odd.

If $m=49$ and $k=1$, we find that the story in case (a) repeats itself; similarly, if $m=-49$ and $k=-1$, the story in case (b) repeats itself. Finally, $m=k=\pm 7$ is impossible, as $(x^2-y^2, 7)=1$.

We conclude that if $(x^2-y^2, 7)=1$, then xy is even.

Case 2. xy is even. Without loss of generality, let y be even. As before, this leads to the existence of k, m, u, v, α, β, γ and δ such that

$$x^2-y^2=ku^2-mv^2, \qquad xy=2uv, \qquad km=49, \qquad (ku, mv)=1;$$
$$x=\alpha\beta, \qquad y=2\gamma\delta, \qquad u=\alpha\gamma, \qquad v=\beta\delta; \qquad \alpha \text{ and } \beta \text{ odd}$$
$$\alpha, \beta, \gamma, \delta \text{ pairwise relatively prime.}$$

https://doi.org/10.1017/S0017089500007862 Published online by Cambridge University Press

This eventually results in the equations

$$\begin{aligned} -k\gamma^2 + \beta^2 &= \pm g\delta^2, \\ 4\gamma^2 - m\beta^2 &= \pm g\alpha^2, \end{aligned} \tag{19}$$

where g is a divisor of 45. Again there are four cases ($m = k = \pm 7$ is impossible, as $(x^2 - y^2, 7) = 1$).

(a) $m = -49$, $k = -1$. Then the $+$ sign is used, and so

$$\gamma^2 + \beta^2 = g\delta^2, \quad \text{and} \quad 4\gamma^2 + 49\beta^2 = g\alpha^2.$$

If γ is odd, then $g\delta^2 \equiv 2 \pmod 4$, which is impossible, so γ is even; hence, $g \equiv 1 \pmod 8$. Also, g is a sum of two relatively prime squares, so $g = 1$. Thus,

$$\gamma^2 + \beta^2 = \delta^2, \quad \text{and} \quad 4\gamma^2 + 49\beta^2 = \alpha^2.$$

Hence, there exist s and t of opposite parity such that $\beta = s^2 - t^2$ and $\gamma = 2st$. If we set $q = s - t$ and $r = s + t$, it follows that $\beta = qr$, $\gamma = (r^2 - q^2)/2$, where q and r are both odd. Thus,

$$4\gamma^2 + 49\beta^2 = (r^2 - q^2)^2 + 49(rq)^2 = \alpha^2,$$

and $rq = \beta \le \alpha\beta = x < xy$ (as y is even and xy is positive). This contradicts the minimality of xy in the solution of (17).

(b) $m = -1$, $k = -49$ is similar to case (a).

(c) $m = 49$, $k = 1$. Eliminating β in (19) reveals that the $-$ sign is used, and we see that

$$\begin{aligned} \gamma^2 - \beta^2 &= g\delta^2, \\ 49\beta^2 - 4\gamma^2 &= g\alpha^2. \end{aligned}$$

If γ is even, this leads to contradictions modulo 4, so that γ is odd; as g is a factor of 45, it follows that δ is even. Hence,

$$g \equiv g\alpha^2 \equiv 49 - 4 \equiv 5 \pmod 8.$$

Thus, $g = 5$ or $g = 45$. If $g = 5$, eliminating γ implies that $9\beta^2 = \alpha^2 + 4\delta^2$, which is impossible modulo 3, since $(\alpha, \delta) = 1$; hence, $g = 45$. This yields the equations

$$\begin{aligned} \beta^2 &= \alpha^2 + 4\delta^2, \\ \gamma^2 &= \beta^2 + 45\delta^2. \end{aligned}$$

Hence there exist r and s of opposite parity such that $\beta = r^2 + s^2$, $\delta = rs$ and $\alpha = r^2 - s^2$. If we eliminate β, we discover that

$$\gamma^2 = \alpha^2 + 49\delta^2 = (r^2 - s^2)^2 + 49(rs)^2,$$

where $rs = \delta < 2\gamma\delta = y \le xy$, contradicting the minimality of xy in (17).

(d) $m = 1$, $k = 49$ is similar to case (c).

Hence, if $(x^2 - y^2)^2 + 49(xy)^2 = z^2$, then $(x^2 - y^2, 7) = 7$. Writing $z = 7w$, we see that

$$((x^2 - y^2)/7)^2 + (xy)^2 = w^2. \tag{20}$$

https://doi.org/10.1017/S0017089500007862 Published online by Cambridge University Press

As before, we assume xy minimal and positive. There are two possibilities, considering the parity of xy.

Case 3. If xy is even with, say, y even, then $x-y$ and $x+y$ are both odd, so that $(x, y) = 1$ implies $(x-y, x+y) = 1$. Thus, one of $x-y$ and $x+y$ is divisible by 7, but not both. Hence, there exist u and v, both odd, such that $x+y = 7u$ and $x-y = v$, with $(7u, v) = 1$ (the case $x-y = 7u$, $x+y = v$ is almost identical). Thus, $x^2 - y^2 = 7uv$, $4xy = 49u^2 - v^2$ and

$$w^2 = (uv)^2 + ((49u^2 - v^2)/4)^2, \tag{21}$$

where $xy = (49u^2 - v^2)/4$ is even. Moreover, $(w, uv, xy) = 1$, so there exist r and s of opposite parity such that

$$\begin{aligned}(49u^2 - v^2)/4 &= 2rs = xy,\\ uv &= r^2 - s^2 = (x^2 - y^2)/7.\end{aligned} \tag{22}$$

Hence, there exist α, β, γ and δ, relatively primary in pairs, such that $x = \alpha\beta$, $y = 2\gamma\delta$, $r = \alpha\gamma$, $s = \beta\delta$, and α and β are odd. If we substitute these expressions into (22), we find that $7(\alpha^2\gamma^2 - \beta^2\delta^2) = \alpha^2\beta^2 - 4\gamma^2\delta^2$, which implies that

$$(7\alpha^2 + 4\delta^2)\gamma^2 = (\alpha^2 + 7\delta^2)\beta^2.$$

As before, this leads to the equations

$$7\alpha^2 + 4\delta^2 = g\beta^2, \qquad \alpha^2 + 7\delta^2 = g\gamma^2$$

with g a divisor of 45. If δ is even, the above equations are impossible mod 4, so δ is odd. Thus, $g \equiv g\beta^2 \equiv 7\alpha^2 + 4\delta^2 \equiv 3 \pmod 8$. Hence, $g = 3$; but then the second equation becomes $\alpha^2 \equiv 3\gamma^2 \pmod 7$, which is impossible, as $(\alpha, \gamma) = 1$ and $(3/7) = -1$. Hence, xy is not even.

Case 4. If xy is odd, then $(x, y) = 1$ implies that $x+y$ and $x-y$ are even, exactly one of them is divisible by 4, and exactly one of them is divisible by 7. Thus there are two possibilities:

(a) $x+y = 14u$, $x-y = 4v$ with $(7u, 2v) = 1$;

(b) $x+y = 28u$, $x-y = 2v$ with $(14u, v) = 1$.

As the resolution of these two cases is similar, we shall only present the details of (a).

If $x+y = 14u$ and $x-y = 4v$ with $(7u, 2v) = 1$, then $x = 7u + 2v$, $y = 7u - 2v$, $xy = 49u^2 - 4v^2$, $x^2 - y^2 = 56uv$; hence

$$w^2 = ((x^2 - y^2)/7)^2 + (xy)^2 = (8uv)^2 + (49u^2 - 4v^2)^2.$$

Now $((x^2 - y^2)/7, xy) = 1$, so it follows that $(8uv, 49u^2 - 4v^2) = 1$, and so there exist r and s of opposite parity with $(r, s) = 1$ such that

$$49u^2 - 4v^2 = r^2 - s^2, \qquad 8uv = 2rs, \quad \text{and} \quad w = r^2 + s^2. \tag{23}$$

Looking modulo 4 reveals that s is even, so that there exist α, β, γ and δ, relatively prime in pairs with α and β odd, such that

$$r = \alpha\beta, \qquad s = 4\gamma\delta, \qquad u = \alpha\gamma, \qquad v = \beta\delta.$$

Working as before, we substitute into (23) and obtain the equation

$$(49\alpha^2 + 16\delta^2)\gamma^2 = (\alpha^2 + 4\delta^2)\beta^2$$

which leads to the equations

$$\begin{aligned} 49\alpha^2 + 16\delta^2 &= g\beta^2 \\ \alpha^2 + 4\delta^2 &= g\gamma^2 \end{aligned} \tag{24}$$

where g is a factor of 45.

Clearly, g must be a sum of two relatively prime squares, and $g \equiv 1 \pmod 8$ because α and β are odd; hence, $g = 1$ and we have that

$$49\alpha^2 + 16\delta^2 = \beta^2, \quad \text{and} \quad \alpha^2 + 4\delta^2 = \gamma^2.$$

Hence there exist m and n of opposite parity such that $(m, n) = 1$ and

$$\alpha = m^2 - n^2, \qquad \delta = mn \quad \text{and} \quad \gamma = m^2 + n^2.$$

This yields

$$49(m^2 - n^2)^2 + 16(mn)^2 = \beta^2. \tag{25}$$

As m and n are of opposite parity, we may write $m - n = a$ and $m + n = b$, where a and b are odd. Hence, $m^2 - n^2 = ab$ and $mn = (a^2 - b^2)/4$, and so (25) becomes

$$(a^2 - b^2)^2 + 49(ab)^2 = \beta^2, \tag{26}$$

with a and b odd. It cannot be the case that $(a^2 - b^2, 7) = 1$, by Case 1, so $(a^2 - b^2, 7) = 7$, and ab is odd, which is the current case. However,

$$ab = m^2 - n^2 = \alpha \le \alpha\beta = x \le xy;$$

if $xy = ab$, then $\beta = 1$ and the only solution of (26) is $ab = xy = 0$, $a^2 - b^2 = 1$ or -1. Otherwise, $ab < xy$, which contradicts the minimality of xy.

Hence, $x^4 + 47x^2y^2 + y^4 = z^2$ has no nontrivial solutions.

6. The curious case $d = 85$. The discovery of a nontrivial solution to (1) for $d = 85$ is a novelty—a case that Euler missed. We found the solution in a very natural way, simply by using Pocklington's method for $d = 85$. One of the subcases did not provide any contradictions, so we undertook a brief search; here is what happened.

If $x^4 + 85x^2y^2 + y^4 = z^2$, then we wrote

$$(x^2 + y^2)^2 + 83(xy)^2 = z^2; \tag{27}$$

using Pocklington's techniques led to the equations

$$x = \alpha\beta, \qquad y = 2\gamma\delta, \qquad z = k\alpha^2\gamma^2 + m\beta^2\gamma^2, \qquad k\gamma^2 - \beta^2 = \pm g\delta^2, \qquad 4\gamma^2 + m\beta^2 = \pm g\alpha^2,$$
$$km = 83,\ \alpha, \beta, \gamma, \delta \text{ relatively prime in pairs}; \quad g\alpha, \beta \text{ odd; and } g = 1, 3, 29 \text{ or } 87.$$

Three subcases ($k = 1$, -1 and 83) led to contradictions; the fourth subcase did not.

If $k = -83$ and $m = -1$, the possibility that γ could be odd implied that $g = 29$; eliminating α and γ, respectively, led to the equations

$$\begin{aligned} \beta^2 + 3\delta^2 &= \gamma^2, \\ 29\beta^2 + 4\delta^2 &= \alpha^2. \end{aligned} \tag{28}$$

A brief calculator search revealed the nontrivial solutions

$$\alpha = 99, \qquad \beta = 13, \qquad \gamma = 62, \qquad \delta = 35$$

to (28). This yields the solution

$$x = \alpha\beta = 99 \,.\, 13 = 1287$$

$$y = 2\gamma\delta = 2 \,.\, 62 \,.\, 35 = 4340$$

$$z = (\alpha\gamma)^2 + 83(\beta\delta)^2 = (99 \,.\, 62)^2 + 83(13 \,.\, 35)^2 = 54858119$$

to (27); indeed,

$$1287^4 + 85 \,.\, 1287^2 4340^2 + 4340^4 = 3009413220218161 = 54858119^2.$$

7. Conclusion. There is not enough evidence to make the conjecture that for all d, Pocklington's method will always yield either (a) a proof that (1) has no nontrivial solutions, or (b) a nontrivial solution to (1). It is tempting to do so, however.

REFERENCES

1. L. E. Dickson, *History of the Theory of Numbers*, vol. II, (reprinted, Chelsea, New York, 1966.)

2. L. Euler, De casibus quibus formulam $x^4 + mxxyy + y^4$ ad quadratum reducere licet, *Mém. acad. sci. St. Pétersbourg* **7** (1815/16, 1820), 10–22; *Opera Omnia,* ser. I, V, 365–47, Geneva, 1944.

3. H. C. Pocklington, Some diophantine impossibilities, *Proc. Cambridge Phil. Soc.* **17** (1914), 108–121.

4. T. N. Sinha, A class of quartic diophantine equations with only trivial solutions, *Amer. J. Math* **100** (1978), 585–590.

5. M. Z. Zhang, On the diophantine equation $x^4 + kx^2y^2 + y^4 = z^2$, *Sichuan Daxue Xuebao* **2,** (1983), 24–31.

Virginia Polytechnic Institute and State University
Blacksburg,
Virginia 24061