ON THE DIOPHANTINE EQUATION $z^2 = x^4 + Dx^2y^2 + y^4$

by J. H. E. COHN

(Received 23 November, 1992)

The equation of the title in positive integers x, y, z where D is a given integer has been considered for some 300 years [**4**, pp 634–639]. As observed by V. A. Lebesgue, and probably known to Euler, if x, y, z is one non-trivial solution i.e., one with $xy(x^2 - y^2) \neq 0$, another is given by $\bar{x} = 2xyz$, $\bar{y} = |x^4 - y^4|$, $\bar{z} = |z^4 - (D^2 - 4)x^4y^4|$. It then follows that there are infinitely many such with $(x, y) = 1$. The question that remains is to determine for which values of D such solutions exist.

Brown [**1**], extending a method due to Pocklington [**5**], has completed this determination for $0 \leq D \leq 100$. He was obviously unaware of [**2**] which dealt in a rather similar way with the values $D = n^2 - 2$ for $1 \leqslant n \leqslant 100$, including the value $D = 47$ which occupies a whole section of [**1**]. The method is technically elementary, and in his conclusion Brown wonders whether such methods will always either produce a solution or prove that one does not exist. This seems not to be the case, for as was pointed out in [**2**], if $n = 49$, corresponding to $D = 2399$ we obtain a pair of equations

$$51c^2 - 2401d^2 = 2a^2, \qquad c^2 - 47d^2 = 2b^2.$$

These are consistent in the sense that they are satisfied by the values $(a, b, c, d) = (7, 1, 7, 1)$, notwithstanding which our equation is shown to be impossible in view of the fact that no solutions exist in which a, b, c, d are pairwise coprime. The demonstration of this fact appears to require non-elementary methods, and in [**3**] this was done using two different quadratic fields.

This phenomenon first seems to occur for $D = 147$, and it is the object of this note to consider this case in detail. We find using Pocklington's method that no non-trivial solution exists provided that each of the three sets

$$149c^2 - d^2 = 4a^2, \qquad 145c^2 - d^2 = 4b^2 \tag{1}$$

$$149c^2 - 5d^2 = -4a^2, \qquad 29c^2 - d^2 = -4b^2 \tag{2}$$

$$149c^2 - 29d^2 = -4a^2, \qquad 5c^2 - d^2 = -4b^2 \tag{3}$$

of simultaneous quadratic equations has no solutions in pairwise coprime integers a, b, c, d. Although we shall demonstrate this, it does not seem to be possible using only elementary methods.

For any such solution both c and d would have to be odd in each case. We use the field $\mathbb{Q}[\sqrt{149}]$ with unique factorisation for which the fundamental unit is $\frac{1}{2}(61 + 5\sqrt{149})$ with norm -1.

From (1), we find $c^2 = a^2 - b^2$ and so for coprime λ and μ, $c = \lambda^2 - \mu^2$, $a = \lambda^2 + \mu^2$ and so $a + c = 2\lambda^2$ and $a - c = 2\mu^2$. But now in the field

$$\tfrac{1}{2}(d + c\sqrt{149}) \cdot \tfrac{1}{2}(d - c\sqrt{149}) = -a^2$$

gives for some coprime rational integers ρ, σ

$$d + c\sqrt{149} = \tfrac{1}{4}(61 + 5\sqrt{149})(\rho + \sigma\sqrt{149})^2, \; a = \tfrac{1}{4}\,|\rho^2 - 149\sigma^2|,$$

Glasgow Math. J. **36** (1994) 283–285.

whence $c \equiv -2\rho\sigma$, $a \equiv \pm(\rho^2+\sigma^2)$ (mod 5). But then

$$2\lambda^2 = a + c \equiv \pm(\rho \mp \sigma)^2, \qquad 2\mu^2 = a - c \equiv \pm(\rho \pm \sigma)^2 \pmod 5$$

imply that both λ and μ are divisible by 5, which is impossible.

From (2) we find $d^2 = 149b^2 - 29a^2$ where a must be even and b odd. Thus

$$\left(\frac{d+b\sqrt{149}}{2}\right)\left(\frac{d-b\sqrt{149}}{2}\right) = -29(\tfrac{1}{2}a)^2 = \left(\frac{35+3\sqrt{149}}{2}\right)\left(\frac{35-3\sqrt{149}}{2}\right)(\tfrac{1}{2}a)^2,$$

whence $4(d+b\sqrt{149}) = (3\sqrt{149}+35q)(\lambda+\mu\sqrt{149})^2$, with $a = \frac{1}{2}|\lambda^2 - 149\mu^2|$ for some rational integers λ, μ of like parity and $q = \pm 1$. Thus we find successively that

$$4d = 35q(\lambda^2+149\mu^2) + 894\lambda\mu$$
$$4b = 3(\lambda^2+149\mu^2) + 70q\lambda\mu$$
$$4(d-2qb) = 29\{q(\lambda^2+149\mu^2) + 26\lambda\mu\}$$
$$4(d+2qb) = 41q(\lambda^2+149\mu^2) + 1034\lambda\mu.$$

But $(d-2qb)(d+2qb) = 29c^2$, where the factors on the left have no common factor. Thus by the above,

$$q\rho^2 = \lambda^2 + 149\mu^2 + 26q\lambda\mu, \qquad q\sigma^2 = 41(\lambda^2+149\mu^2) + 1034\lambda\mu q,$$

where $29 \nmid \sigma$. But now $q\sigma^2 \equiv 12(\lambda+2q\mu)^2 \pmod{29}$, which is impossible since $(\pm 12 \mid 29) = -1$.

Finally, from (3) we find $d^2 = 149b^2 - 5a^2$, where a must be even and b odd. Thus

$$\tfrac{1}{2}(d+b\sqrt{149}) \cdot \tfrac{1}{2}(d-b\sqrt{149}) = -5(\tfrac{1}{2}a)^2 = (12+\sqrt{149})(12-\sqrt{149})(\tfrac{1}{2}a)^2,$$

whence $2(d+b\sqrt{149}) = (\sqrt{149}+12q)(\lambda+\mu\sqrt{149})^2$, with $a = \frac{1}{2}|\lambda^2 - 149\mu^2|$ for some rational integers λ, μ of like parity and $q = \pm 1$. Thus we find successively that

$$d = 6q(\lambda^2+149\mu^2) + 149\lambda\mu$$
$$2b = (\lambda^2+149\mu^2) + 24q\lambda\mu$$
$$d-2qb = 5\{q(\lambda^2+149\mu^2) + 25\lambda\mu\}$$
$$d+2qb = 7q(\lambda^2+149\mu^2) + 173\lambda\mu.$$

But $(d-2qb)(d+2qb) = 5c^2$, where the factors on the left have no common factor. Thus by the above,

$$q\rho^2 = \lambda^2 + 149\mu^2 + 25q\lambda\mu, \qquad q\sigma^2 = 7(\lambda^2+149\mu^2) + 173\lambda\mu q,$$

where $5 \nmid \sigma$. But now $q\sigma^2 \equiv 2(\lambda+2q\mu)^2 \pmod 5$, which is again impossible since $(\pm 2 \mid 5) = -1$.

REFERENCES

1. E. Brown, $x^4 + dx^2y^2 + y^4 = z^2$: some cases with only trivial solutions—and a solution Euler missed, *Glasgow Math. J.* **31** (1989), 297–307.

2. J. H. E. Cohn, Squares in arithmetical progressions I, *Math. Scand.* **52** (1983) 5–19.

3. J. H. E. Cohn, Squares in arithmetical progressions II, *Math. Scand.* **52** (1983) 20–23.
4. L. E. Dickson, *History of the theory of numbers*, *II*, (Chelsea Publishing Co., New York, 1952).
5. H. C. Pocklington, Some diophantine impossibilities, *Proc. Cambridge Phil. Soc.* **17** (1914) 108–121.

DEPARTMENT OF MATHEMATICS
ROYAL HOLLOWAY UNIVERSITY OF LONDON
EGHAM
SURREY, TW20 0EX
ENGLAND