MATH. SCAND. 68 (1991), 171–179

THE DIOPHANTINE EQUATION $X(X+1) = Y(Y^2+1)$.

J. H. E. COHN

The equation of the title seems to have occurred naturally in a combinatorial problem, and my colleague B. J. Wilson has asked me to solve it completely. In this note we prove that $Y = 0$, 1 and 3 provide the only solutions in integers X and Y.

The method we shall use is outlined in [1]; the process consists of showing that the cubic equation may be reduced to a finite set of equations, known as Thue equations, each of the form $F(x, y) = 1$ where $F(x, y)$ is a binary quartic form. These can be tackled by Skolem's p-adic method, of which an account appears in [1; p. 207]. There are a number of practical difficulties; often many quartics appear, there is no *a priori* guarantee of success in proving that all solutions have been determined, and the arithmetic is often highly non-trivial. Perhaps because of these difficulties, many of the examples in the literature to illustrate the method are capable of much shorter treatment in other ways, and both of the examples given in [1] can be reduced to $u^4 + v^4 = w^2$ by substitutions, whence neither has a solution apart from $y = 0$ in *rationals*, let alone integers.

Writing $u = 2X + 1$ our equation becomes $2u^2 = (2Y)^3 + 4(2Y) + 2$ with u odd, and we work in the algebraic number field $Q[\varphi]$ with defining polynomial $\varphi^3 + 4\varphi + 2$. Properties of the field which are easily obtained are:

a. the integers of the field have an integral basis 1, φ, φ^2

b. the discriminant is -364

c. since the defining equation has one real and two complex roots there is one fundamental unit of infinite order; it may be taken to be $\varepsilon = 1 + 2\varphi$

d. the class number is 1, and so there is unique prime factorisation

e. the rational primes 2, 7 and 13 wnich divide the discriminant, have the following factorisations into primes of the field:

$$2 = -\varphi^3/\varepsilon = -\varphi(\varphi^2 + 4)$$

$$7 = (1 - \varphi)^2(3 + \varphi^2) = \pi^2(3 + \varphi^2), \text{ say}$$

$$13 = (1 + \varphi^2)(1 + \varphi + \varphi^2)^2/\varepsilon = (1 + \varphi^2)\tau^2/\varepsilon, \text{ say.}$$

Received May 14, 1990.

Then the equation becomes

$$-\varphi(\varphi^2+4)u^2 = (2Y-\varphi)(4Y^2+2\varphi Y+\varphi^2+4)$$

and so

$$\begin{aligned} u^2 &= (1-2Y/\varphi)(1-\varphi^2 Y-2\varphi Y^2) \\ &= (1+(\varphi^2+4)Y)(1-\varphi^2 Y-2\varphi Y^2) \\ &= \alpha\beta \text{ say.} \end{aligned}$$

Now $\beta - \alpha\varphi^2(Y+\varphi) = 1-\varphi^3 = \pi\tau$. Thus α and β have common factor dividing $\pi\tau$, and so each is an associate of a square times one of $1, \pi, \tau$ and $\pi\tau$.

We show next that $(\alpha, \beta) = 1$. This will follow from the fact that each of π, τ occurs squared in the factorisation of its norm. Suppose that π divided α. Then we should find $\pi \mid (1+5Y)$, and hence also its norm $7 \mid (1+5Y)^3$, i.e. $Y \equiv -3 \pmod 7$. But $\pi^2 \mid 7$ and so $\alpha \equiv 1 - 3\varphi^2 - 12 \equiv 3(1-\varphi)(1+\varphi) \pmod{\pi^2}$ and so α is divisible by π precisely once since π does not divide $(1+\varphi)$. Similarly we would obtain $\beta \equiv 1 + 3\varphi^2 - 4\varphi \equiv \pi(1-3\varphi) \pmod{\pi^2}$ and now $\pi \parallel \beta$, since π does not divide $(1-3\varphi)$. But then $\pi^2 \parallel u^2$ and this cannot be since $7^2 \mid u^2$ and so $\pi^4 \mid u^2$. A similar argument shows that τ cannot divide (α, β). Thus we must have

$$1 + (\varphi^2+4)Y = \pm\varepsilon^n(a+b\varphi+c\varphi^2)^2.$$

Now for any solution of our equation $Y \geqq 0$, and so we can reject the lower sign since for the real root φ, $\varepsilon > 0$. Absorbing even powers of ε into the expression in the bracket it suffices to consider only $n = -1$ or $n = 0$.

Consider $n = -1$ first. Then

$$\begin{aligned} (1+2\varphi)(1+(\varphi^2+4)Y) &= a^2 + 2ab\varphi + b^2\varphi^2 + 2bc\varphi^3 + 2ac\varphi^2 + c^2\varphi^4 \\ &= a^2 + 2ab\varphi + b^2\varphi^2 - 2bc(4\varphi+2) + 2ac\varphi^2 \\ &\quad - c^2\varphi(4\varphi+2) \end{aligned}$$

and so

$$1 + 2\varphi + \varphi^2 Y = (a^2 - 4bc) + 2\varphi(ab - 4bc - c^2) + \varphi^2(b^2 + 2ac - 4c^2)$$

whence

$$\begin{aligned} 1 &= a^2 - 4bc \\ 1 &= ab - 4bc - c^2 \\ Y &= b^2 + 2ac - 4c^2. \end{aligned}$$

The difference of the first two gives $a(b-a) = c^2$. From the first equation we see that $(a, c) = 1$ so $a = \pm 1$ and $bc = 0$. Then from the second $b = 0$ is impossible and $c = 0$ gives $a = b$ whence $Y = 1$.

Now consider $n = 0$. We obtain

$$1 + 4Y = a^2 - 4bc$$
$$0 = ab - 4bc - c^2$$
$$Y = b^2 + 2ac - 4c^2.$$

From the second of these $(a - 4c)b = c^2$ and so for suitable integers λ, x and y, $a - 4c = \lambda x^2$, $b = \lambda y^2$ and $c = \lambda xy$. Eliminating Y from the first and third then yields

$$\begin{aligned} 1 &= a^2 - 4bc - 4b^2 - 8ac + 16c^2 \\ &= (a - 4c)^2 - 4bc - 4b^2 \\ &= \lambda^2(x^4 - 4xy^3 - 4y^4) \end{aligned}$$

and so $\lambda^2 = 1$ and $x^4 - 4xy^3 - 4y^4 = 1$. We observe that this equation has the solutions $(\pm 1, 0)$ and $\pm(1, -1)$ yielding respectively $Y = 0$ and 3. The remainder of this paper is devoted to showing that the Diophantine equation

$$x^4 - 4xy^3 - 4y^4 = 1,$$

has no other solutions.

We consider the field $Q(\theta)$ where $\theta^4 + 4\theta - 4 = 0$, and then we require $x + y\theta$ to be a unit of norm $+1$. For the integers in this field an internal basis is provided by 1, θ, $\frac{1}{2}\theta^2$ and $\frac{1}{2}\theta^3$. Since two of the roots of the defining equation are real and two complex, there are two fundamental units of infinite order which may be taken to be $\xi = \frac{1}{2}\theta^2$ and $\eta = \theta + \frac{1}{2}\theta^2$ having norms respectively $+1$ and -1, and so we require $\pm(x + y\theta) = \xi^R\eta^{2S}$ for some integers R and S, not necessarily positive. We can absorb the $\pm$ into the values of x and y, and shall assume this has been done. Since $\xi^0 = 1$ and $\xi^2 = 1 - \theta$, we need to show that the only cases that arise are $R = 0$, $S = 0$ and $R = 2$, $S = 0$.

Since $\theta^4 = 4 - 4\theta$ and $1/\theta = 1 + \frac{1}{4}\theta^3$, we may define numbers $A(n)$, $B(n)$, $C(n)$ and $D(n)$ for each integer n by the equation

$$\theta^n = A(n) + B(n)\theta + C(n)\theta^2 + D(n)\theta^3$$

and of course the representation is unique since the defining polynomial of the field is irreducible. It is clear that these numbers are integers for positive n, and are rationals whose denominators are powers of 2 when n is negative. Then

$$\begin{aligned} &A(n+1) + B(n+1)\theta + C(n+1)\theta^2 + D(n+1)\theta^3 \\ &\quad = \theta^{n+1} \\ &\quad = A(n)\theta + B(n)\theta^2 + C(n)\theta^3 + D(n)\theta^4 \\ &\quad = 4D(n) + \{A(n) - 4D(n)\}\theta + B(n)\theta^2 + C(n)\theta^3 \end{aligned}$$

and so

$$A(n+1) = 4D(n)$$
$$B(n+1) = A(n) - 4D(n)$$
$$C(n+1) = B(n)$$
$$D(n+1) = C(n).$$

Thus

$$A(n+4) = 4D(n+3) = 4C(n+2) = 4B(n+1) = 4A(n) - 16D(n)$$

and so

$$A(n+4) = -4A(n+1) + 4A(n),$$

with

$$B(n) = \tfrac{1}{4}A(n+3)$$
$$C(n) = \tfrac{1}{4}A(n+2)$$
$$D(n) = \tfrac{1}{4}A(n+1),$$

and so all the properties of all four sequences can be derived from the sequence $A(n)$. Clearly we have

$$A(0) = 1,\ A(1) = 0,\ A(2) = 0,\ A(3) = 0.$$

It is now convenient to make the substitution

$$\alpha(n) = \begin{cases} A(4m)/2^{2m} & \text{if } n = 4m \\ A(4m+j)/2^{2m+2} & \text{if } n = 4m+j,\ 1 \leqq j \leqq 3. \end{cases}$$

Then the initial and recurrence conditions for the sequence $\alpha(n)$ are

$$\alpha(0) = 1,\ \alpha(1) = 0,\ \alpha(2) = 0,\ \alpha(3) = 0,$$
$$\alpha(n+4) = -\alpha(n+1) + \alpha(n) \text{ if } n \not\equiv 0 \pmod 4$$
$$\alpha(n+4) = -4\alpha(n+1) + \alpha(n) \text{ if } n \equiv 0 \pmod 4,$$

and for these formulae it follows immediately that $\alpha(n)$ is an integer for every integer n, positive or negative, and then by induction on m that

$$\alpha(4m) \equiv 1 \pmod 4.$$

We prove that $\alpha(n) = 0$ if and only if $n = 1, 2, 3, 5, 6$ or 9. Calculation shows that $\alpha(n) = 0$ for these six values, but not for 4, 7 or 8, and that $\alpha(10) = 1$, $\alpha(11) = -2$, $\alpha(12) = 1$, $\alpha(13) = -1$. The recurrence and induction then show

that for $n \geqq 10$, $\alpha(n) > 0$ when n is even and $\alpha(n) < 0$ when n is odd. Similarly $\alpha(0) = \alpha(-1) = \alpha(-2) = \alpha(-3) = 1$, and so by induction on $-n$, $\alpha(n) > 0$ if $n \leqq 0$. In both cases $\alpha(n) \neq 0$. This implies that in the special case $S = 0$, the only solutions arise from $R = 0$ or $R = 2$. For with $S = 0$ we find

$$x + y\theta = (\tfrac{1}{2}\theta^2)^R = \{A(2R) + B(2R)\theta + C(2R)\theta^2 + D(2R)\theta^3\}/2^R,$$

and then successively $C(2R) = D(2R) = 0$, $A(2R+2) = A(2R+1) = 0$ yielding $\alpha(2R+1) = \alpha(2R+2) = 0$. Thus $R = 0$ or 2.

All that remains is to prove that we must have $S = 0$. Consider first $S > 0$. Then irrespective of the sign of R we find

$$\begin{aligned} x + y\theta &= (\tfrac{1}{2}\theta^2)^R(\theta + \tfrac{1}{2}\theta^2)^{2S} \\ &= \sum_{\rho=0}^{2S} \binom{2S}{\rho} \frac{\theta^{2R}}{2^R} \theta^\rho \frac{\theta^{4S-2\rho}}{2^{2S-\rho}}, \end{aligned}$$

and so

$$x = \sum_{\rho=0}^{2S} \binom{2S}{\rho} \frac{A(2R+4S-\rho)}{2^{R+2S-\rho}}.$$

Now if ρ is odd, the binomial coefficient is even. If $\rho \geqq 2$ is even then $A(2R+4S-\rho)/2^{R+2S-\rho}$ is even and so $x \equiv A(2R+4S)/2^{R+2S} \pmod 2$. But now if R were odd it would follow that $A(2R+4S)/2^{R+2S} = 2\alpha(2R+4S)$ and so x would be even which is clearly inconsistent with the Diophantine equation. So R is even, $R = 2r$ say.

The next step is to prove that S must also be even. We observe that $\eta/\xi = 1 + 2/\theta = 3 + \tfrac{1}{2}\theta^3$, and so $x + y\theta = (\tfrac{1}{2}\theta^2)^{2r+2S}(3 + \tfrac{1}{2}\theta^3)^{2S}$ and so if $k = 4r + 10S$

$$x + y\theta \equiv A(k) + \theta B(k) + \theta^2 C(k) + \theta^3 D(k) \pmod 3$$

and it then follows, since x cannot be divisible by 3, that we must have $\alpha(k) \not\equiv 0$, $\alpha(k+1) \equiv 0$, $\alpha(k+2) \equiv 0 \pmod 3$. It is easily calculated from the recurrence relation for α that these imply that $k \equiv 0$ or $4 \pmod{40}$, whence $2 \mid S$. Let $S = 2s$, and then $k = 4r + 20s$. Thus

$$\begin{aligned} x + y\theta &= (\tfrac{1}{2}\theta^2)^{2r+4s}(3 + \tfrac{1}{2}\theta^3)^{4s} \\ &= \sum_{\rho=0}^{4s} \binom{4s}{\rho} 3^\rho \frac{\theta^{k-3\rho}}{2^{2r+8s-\rho}}, \end{aligned}$$

and so we obtain

$$\sum_{\rho=0}^{4s} \binom{4s}{\rho} 6^\rho C(k-3\rho) = \sum_{\rho=0}^{4s} \binom{4s}{\rho} 6^\rho D(k-3\rho) = 0,$$

whence

$$\sum_{\rho=0}^{4s} \binom{4s}{\rho} 6^\rho A(k+1-3\rho) = 0, \tag{1}$$

$$\sum_{\rho=0}^{4s} \binom{4s}{\rho} 6^\rho A(k+2-3\rho) = 0, \tag{2}$$

and then in view of the recurrence relation for A we also have

$$\sum_{\rho=0}^{4s} \binom{4s}{\rho} 6^\rho A(k+5-3\rho) = 0. \tag{3}$$

Then $k \neq 0$, for otherwise since $A(1) = 0$, we should find from (1)

$$\sum_{\rho=1}^{4s} \binom{4s}{\rho} 6^\rho A(1-3\rho) = 0,$$

impossible since $A(n) > 0$ for all $n < 0$. Although we shall not need the fact, the argument proves that k cannot be negative either. The same argument shows that $k \neq 4$, since $A(5) = A(2) = 0$.

Consider first the case $k \equiv 0 \pmod{40}$. Since neither k nor s is zero, we write

$$k = 40 \cdot \lambda \cdot 3^K, \quad s = 3^\sigma \cdot \mu,$$

where $K \geqq 0$, $\sigma \geqq 0$ and neither λ nor μ is divisible by 3. Then

$$\begin{aligned} \theta^{40} &= 2^{20}\{3545 - 5442\,\theta + 2949\,\theta^2 - 1632\,\theta^3\} \\ &\equiv 4\{-1 + 3\theta - 3\theta^2 - 3\theta^3\} \pmod 9 \\ &\equiv -1 + 3\{-1 + \theta - \theta^2 - \theta^3\} \pmod 9, \end{aligned}$$

and so we have

$$A(40 + m) \equiv -A(m) \pmod 3 \tag{4}$$

and so

$$\theta^{40 \cdot 3^K} \equiv -1 + 3^{K+1}\{-1 + \theta - \theta^2 - \theta^3\} \pmod{3^{K+2}},$$

and so

$$A(k+u) \equiv (-1)^\lambda \{A(u) + \lambda \cdot 3^{K+1}[A(u) - A(u+1) + A(u+2) + A(u+3)]\} \pmod{3^{K+2}}.$$

Since $A(2) = 0$ and $A(2) - A(3) + A(4) + A(5) = 4$, we obtain

$$A(k+2) \equiv (-1)^\lambda \cdot \lambda \cdot 3^{K+1} \pmod{3^{K+2}}, \tag{5}$$

and similarly

$$A(k+1) \equiv (-1)^{\lambda} \cdot \lambda \cdot 3^{K+1} \pmod{3^{K+2}}, \tag{6}$$

$$A(k) \equiv (-1)^{\lambda}\{1 + \lambda \cdot 3^{K+1}\} \pmod{3^{K+2}}, \tag{7}$$

$$A(k-1) \equiv (-1)^{\lambda} \pmod{3^{K+2}}, \tag{8}$$

$$A(k-2) \equiv (-1)^{\lambda}\{1 + \lambda \cdot 3^{K+1}\} \pmod{3^{K+2}}, \tag{9}$$

and

$$A(k-4) \equiv (-1)^{\lambda-1} \pmod{3^{K+2}}. \tag{10}$$

We could of course have considered the value of θ^{40} moldulo 27 instead of modulo 9, obtaining more complicated results analogous to those of (5) – (9) but correct to a power of 3 one higher. There is just one result we shall require in this direction, and we state without proof

$$A(k+5) \equiv (-1)^{\lambda-1} \cdot \lambda \cdot 3^{K+2} \pmod{3^{K+3}}. \tag{11}$$

We then find using (2) that $A(k+2) + 24\,sA(k-1) \equiv 0 \pmod{3^{\sigma+2}}$ and so since from (8) $A(k-1)$ is not divisible by 3, it follows immediately from (5) that $K = \sigma$, and that

$$(-1)^{\lambda} \lambda \cdot 3^{\sigma+1} + 24 \cdot 3^{\sigma} \cdot \mu \cdot (-1)^{\lambda} \equiv 0 \pmod{3^{\sigma+2}}$$

and so $\lambda \equiv \mu \pmod 3$.

We now consider equation (3), and distinguish the two cases $K = 0$ and $K \neq 0$. In the first case we find that except for the first three terms of the series, all the terms are divisible by 27, and accordingly $A(k+5) + 24\,sA(k+2) + 72\,s(4s-1)A(k-1) \equiv 0 \pmod{27}$, or in view of the above

$$-(-1)^{\lambda} \cdot 9\lambda + 24\mu \cdot 3\lambda \cdot (-1)^{\lambda} + 72\mu(4\mu - 1) \cdot (-1)^{\lambda} \equiv 0 \pmod{27}$$

whence, cancelling $(-1)^{\lambda-1}9$ we obtain $\lambda + \lambda\mu + 1 - \mu \equiv 0 \pmod 3$, which is impossible as we have already seen that $\lambda \equiv \mu \pmod 3$.

In the second case we find that the first, third and fourth terms are divisible by $3^{\sigma+2}$, and all other terms by higher powers. Thus modulo $3^{\sigma+3}$,

$$(-1)^{\lambda-1} \cdot \lambda \cdot 3^{\sigma+2} + 72 \cdot 3^{\sigma} \cdot \mu \cdot (4s-1)(-1)^{\lambda} + 144 \cdot 3^{\sigma} \cdot \mu \cdot (4s-1)(4s-2)(-1)^{\lambda-1} \equiv 0$$

and cancelling $(-1)^{\lambda-1} \cdot 3^{\sigma+2}$ we obtain $\lambda - \mu - \mu \equiv 0 \pmod 3$, which is also impossible.

Now consider the case $k \equiv 4 \pmod{40}$. Since $k = 4r + 20s$, this implies $r \equiv 1 \pmod 5$, and we shall show that this is impossible, by considering the equation modulo powers of 5. It is found without difficulty that $\xi^6\eta^2 = 5 - 5\theta^2 - 2\theta^3$,

and so

$$x + y\theta = \xi^{2r}\eta^{4s} = \xi^{2r-12s}(5 - 5\theta^2 - 2\theta^3)^{2s}$$
$$= 2^{12s-2r}\theta^{4r-24s}(2\theta^3 + 5\theta^2 - 5)^{2s}.$$

Let $s = 5^\sigma f$, where $5 \nmid f$ and $m = 4r - 18s$. We find easily that

$$A(m+1) + 5s\{A(m) - A(m-2)\} \equiv 0 \pmod{5^{\sigma+2}}, \tag{12}$$

$$A(m+2) + 5s\{A(m+1) - A(m-1)\} \equiv 0 \pmod{5^{\sigma+2}}. \tag{13}$$

It is a matter of routine calculation to show that the period of the sequence $\{A(n)\}$ modulo 5 is 124, and hence that (12)–(13) hold modulo 5 only if $m \equiv 0$ or 1 or 4 (mod 31). We then find modulo 25 that the period is 620 and that (12) and (13) could only hold if $5 \mid s$ and $m \equiv 0 \pmod{31}$ or $m \equiv 1$ or 4 (mod 155). At the next stage we find that $25 \mid s$ and $m \equiv 0 \pmod{155}$ or $m \equiv 1$ or 4 (mod 775). But since $r \equiv 1$, $s \equiv 0 \pmod 5$, we obtain $m = 4r - 18s \equiv 4 \pmod 5$, and so the only possibility is $m \equiv 4 \pmod{775}$. But it is then easily found that $5 \mid \{A(m+1) - A(m-1)\}$ and $5 \nmid \{A(m) - A(m-2)\}$, and so using (12) and (13) we find

$$5^{\sigma+1} \| A(m+1);\ 5^{\sigma+2} \mid A(m+2). \tag{14}$$

It remains to show that (14) is impossible. Certainly $m \neq 4$ and so we let $m - 4 = 31 \cdot 5^\mu \cdot g$ where $5 \nmid g$. Now we find easily that

$$\theta^{31} \equiv 8(1 + 10\theta) \pmod{25}$$

and so $$\theta^m \equiv \theta^{5^\mu g}\theta^4(1 + 2g \cdot 5^{\mu+1}\theta) \pmod{5^{\mu+2}}.$$

Thus $$A(m+1) \equiv 8^{5^\mu g}(A(5) + 2g \cdot 5^{\mu+1}A(6)) \equiv 0 \pmod{5^{\mu+2}},$$

whilst $$A(m+2) \equiv 8^{5^\mu g}(A(6) + 2g \cdot 5^{\mu+1}A(7))$$
$$\equiv -32g \cdot 8^{5^\mu g}5^{\mu+1} \pmod{5^{\mu+2}}$$

and so $A(m+1)$ is divisible by a higher power of 5 than $A(m+2)$. Thus (14) is impossible.

This concludes the proof for the case $S > 0$. To extend the result to negative S, consider the integer congruences as equalities in the ring of 3-adic or 5-adic integers. Then the only differences if S is negative are that (1) and (2) become infinite series, which of course converge as the powers of 3 steadily increase, and similarly modulo 5. The arguments then proceed without change.

REFERENCE

1. L. J. Mordell, *Diophantine Equations*, Academic Press, 1969.

DEPARTMENT OF MATHEMATICS,
RHBNC
UNIVERSITY OF LONDON
EGHAM, SURREY, TW20 OEX
ENGLAND