Internat. J. Math. & Math. Sci.
Vol. 9 No. 2 (1986) 413-415

A DIOPHANTINE SYSTEM

ANDREW BREMNER

Department of Mathematics
Arizona State University
Tempe, Arizona 85287

(Received November 20, 1985)

ABSTRACT: It is shown how to find all integers a,b such that a+b, a^2+b^2 and a^3+b^3 are simultaneously perfect squares.

KEYWORDS AND PHRASES: Diophantine equation, elliptic curve.
1980 AMS SUBJECT CLASSIFICATION CODE. 11B10.

1. INTRODUCTION.

In the Gentleman's Diary of 1795, J. Saul found a solution in integers a,b of the Diophantine system

$$\begin{aligned} a + b &= \text{square} \\ a^2 + b^2 &= \text{square} \\ a^3 + b^3 &= \text{square} . \end{aligned} \tag{1.1}$$

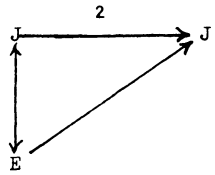
It is the intention of this note to show that recurrence formulae may be developed giving all integral solutions of the system. This amounts to displaying the additive group structure on an elliptic curve, where the curve is given not in standard Weierstrass form, but as the intersection of two quadrics. Such explicit group structure occurs not too frequently in print. For an example, see Cassels [1], or Selmer [2].

2. RESULTS.

First observe that any rational solution of (1.1) gives rise to a rational point (x,y,u,v) = (a,b,u,v) on the elliptic curve

$$E: \begin{cases} x^2 + y^2 = u^2 \\ x^2 - xy + y^2 = v^2 . \end{cases}$$

Conversely, any x,y corresponding to a rational point on E give rise to a solution of the original system (1.1) by multiplying by an appropriate scalar. Thus it suffices to determine all rational points on E. Now E is just a 2-covering of its Jacobian, and indeed we have the commutative diagram



$$J:\ Y^2 = 2X(X+1)(X+3)\ ,$$

the map $J \to J$ is multiplication by 2, and the diagonal map $E \to J$ is given by

$$X = -3u^2/2v^2\ ,\quad Y = 3(y^2-x^2)u/2v^3\ . \tag{2.1}$$

The vertical map $J \to\to E$ is birational (but not, of course, necessarily defined over $\mathbb{Q}$).

Now from (2.1), rational points of E correspond precisely to points of J of which the x-coordinate is -6 modulo squares. It is a straightforward (albeit dull) calculation to show that the group of rational points on J has precisely one generator of infinite order, which may be taken as the point $P = (-3/2,\ 3/2)$. Then any rational point on J is of type $mP + P_0$, $m \in \mathbb{Z}$, where P_0 is one of the four 2-division points of J, namely: (0,0), (-1,0), (-3,0), 0 (the point at infinity, being the zero of the group structure on J).

The addition formula on J is $(X_1,Y_1) + (X_2,Y_2) = (X_3,Y_3)$ with

$$X_3 = \frac{1}{2X_1X_2}\left(\frac{X_1Y_2-X_2Y_1}{X_1-X_2}\right)^2\ ,$$

and so it is readily verified that the first coordinate of $mP + P_0$ is congruent to -6 modulo squares if and only if n is odd, and $P_0 = 0$. Since $2P = (\frac{1}{8}\ ,\ \frac{15}{16})$, it follows on writing $m = 2n + 1$ that the rational points of E are in 1-1 correspondence with the points of J

$$(X_n, Y_n) = n(\tfrac{1}{8}\ ,\ \tfrac{15}{16}) + (-\tfrac{3}{2}\ ,\ \tfrac{3}{2})\ ,\ n \in \mathbb{Z}\ .$$

Using the group structure on J it is easy to deduce a recurrence relation for X_n:

$$X_{n+1} = \frac{1}{X_n}\left[\frac{15X_n-2Y_n}{8X_n-1}\right]^2\ ;$$

and thus

$$\frac{-3u_{n+1}^2}{2v_{n+1}^2} = -\frac{3}{2}\left[\frac{15u_nv_n + 2(y_n^2-x_n^2)}{12u_n^2 + v_n^2}\right]^2\ .$$

Taking

$$u_{n+1} = 15u_nv_n + 2(y_n^2-x_n^2) \tag{2.2}$$

$$v_{n+1} = 12u_n^2 + v_n^2 \tag{2.3}$$

one can now solve for x_{n+1}, y_{n+1} to get

$$x_{n+1} = -4x_n(u_n-v_n) + y_n(v_n+14u_n) \tag{2.4}$$

$$y_{n+1} = x_n(v_n-14u_n) + 4y_n(u_n+v_n) . \tag{2.5}$$

Notice that $(x_{-n}, y_{-n}, u_{-n}, v_{-n}) = (x_{n-1}, y_{n-1}, -u_{n-1}, v_{n-1})$ and so it is only necessary to consider in the recurrences (2.2)-(2.5) non-negative values of n. The initial value n = 0 corresponding to (a,b) = (0,1). Then $(x_1,y_1,u_1,v_1) = (15,8,17,13)$, corresponding to (a,b) = (345,184), $(x_2,y_2,u_2,v_2) = (1768,-2415,2993,3637)$, corresponding to (a,b) = (-1143896,1562505), etc.

REFERENCES

1. CASSELS, J.W.S., Arithmetic on an elliptic curve, Proc. Intern. Congress Math., Stockholm 1962, 234-246.

2. SELMER, E.S., The Diophantine equation $ax^3+by^3+cz^3 = 0$, Acta Math., 85, 1951, 203-362.