A DIOPHANTINE EQUATION

by J. W. S. CASSELS

To Robert Rankin on the occasion of his 70th birthday

0. I was recently challenged to find all the cases when the sum of three consecutive integral cubes is a square; that is to find all integral solutions x, y of

$$\begin{aligned} y^2 &= (x-1)^3 + x^3 + (x+1)^3 \\ &= 3x(x^2+2). \end{aligned} \tag{0.1}$$

This is an example of a curve of genus 1. There is an effective procedure for finding all integral points on a given curve of genus 1 ([**1**, Theorem 4.2], [**2**]): that is, it can be guaranteed to find all the integral points and to show that no others exist with a finite amount of work. Unlike some effective procedures, which have only logical interest, this one can actually be carried out in practice, at least with the aid of a computer ([**3**], [**5**]). There are, however, older methods for dealing with problems of this kind which, while not effective, very often lead more easily to a complete set of solutions (and a proof that it is complete). I solve the problem here by a technique introduced in [**4**]. It requires only the elementary theory of algebraic number-fields. The motivation is p-adic, but it is simpler not to introduce p-adic theory overtly.

There is a discussion of the problem in [**6**].

THEOREM 0.1. *The only solutions of* (0.1) *in integers are* $x = 0, 1, 2, 24$.

We note that the greatest common factor of x and x^2+2 is either 1 or 2. Hence on considering the factorization of x and x^2+2 in (0.1) there are integers u, v such that one of the following holds:

$$x = 3u^2, \qquad x^2+2 = v^2; \tag{0.2}$$

$$x = u^2, \qquad x^2+2 = 3v^2; \tag{0.3}$$

$$x = 2u^2, \qquad x^2+2 = 6v^2; \tag{0.4}$$

$$x = 6u^2, \qquad x^2+2 = 2v^2. \tag{0.5}$$

If (0.2) holds, then

$$9u^4 + 2 = v^2,$$

which is impossible modulo 3. We treat the remaining equations (0.3), (0.4), (0.5) in separate sections.

1. Here we deal with (0.3).

LEMMA 1.1. *The only integral solution of*

$$x = u^2, \qquad x^2+2 = 3v^2 \tag{1.1}$$

is $x = 1$.

Glasgow Math. J. **27** (1985) 11–18.

Clearly $3 \nmid u$ so that $x = 3z - 2$ for some integer z, and

$$z^2 + 2(z-1)^2 = v^2, \tag{1.2}$$

i.e.

$$(v+z)(v-z) = 2(z-1)^2. \tag{1.3}$$

Any common prime divisor p of $v+z$, $v-z$ divides their difference $2z$ and it also divides $z-1$; so $p=2$. As z, v are clearly both odd, there are integers l, m such that one of the two following holds:

$$v+z = 4l^2, \qquad v-z = 2m^2, \qquad z-1 = 2lm; \tag{1.4}$$

$$v+z = 2l^2, \qquad v-z = 4m^2, \qquad z-1 = 2lm. \tag{1.5}$$

If (1.4) holds then

$$1 = 2l^2 - m^2 - 2lm = 3l^2 - (l+m)^2,$$

which is impossible modulo 3. Hence (1.5) holds, and so

$$u^2 = 3z - 2 = l^2 + 4lm - 2m^2 \tag{1.6}$$

and

$$1 = l^2 - 2lm - 2m^2. \tag{1.7}$$

We now introduce γ, where

$$\gamma^2 = -2. \tag{1.8}$$

Then by (1.6), (1.7) we have

$$\begin{aligned} -\gamma &= u^2 - (1+\gamma)(l - \gamma m)^2 \\ &= u^2 - (1+\gamma)\lambda^2, \end{aligned} \tag{1.9}$$

where

$$\lambda = l - \gamma m. \tag{1.10}$$

We now work in the field $\mathbf{Q}(\gamma, \delta)$, where

$$\delta^2 = 1 + \gamma, \tag{1.11}$$

so that (1.9) can be written

$$\mathrm{Norm}(u + \lambda\delta) = -\gamma, \tag{1.12}$$

where the Norm is taken from $\mathbf{Q}(\gamma, \delta)$ to $\mathbf{Q}(\gamma)$.

It is readily verified that 2 is completely ramified in $\mathbf{Q}(\gamma, \delta)$. There is thus a unique extension $|\ |_2$ of the 2-adic valuation to $\mathbf{Q}(\gamma, \delta)$ and

$$|\gamma|_2 = 2^{-1/2}, \qquad |\delta - 1|_2 = 2^{-1/4}. \tag{1.13}$$

It readily follows that $1, \gamma, \delta, \gamma\delta$ is a basis for the integers of $\mathbf{Q}(\gamma, \delta)$.

Solutions of (1.12) are clearly given by $u = \pm 1$, $\lambda = \pm 1$. We must show that these are the only solutions with $u \in \mathbf{Z}$, $\lambda \in \mathbf{Z}[\gamma]$. In any case,

$$u + \lambda\delta = (1+\delta)\mu \tag{1.14}$$

where μ is an integer (because of the complete ramification of 2), and so μ is a unit. [Note that this argument does not require a knowledge of the class-number of $\mathbf{Q}(\gamma, \delta)$.] Further,

$$(1+\delta)^2=\gamma\eta, \tag{1.15}$$

where

$$\eta=1-\gamma-\gamma\delta \tag{1.16}$$

is a unit. Since $\mathrm{Norm}(1+\delta)=1-\delta^2=-\gamma$, it follows that

$$(1+\delta)/(1-\delta)=-\eta. \tag{1.17}$$

It is easy to verify that η is a fundamental unit.

From all this it follows that

$$u+\lambda\delta=\pm(1\pm\delta)\eta^{2n} \tag{1.18}$$

for some $n\in\mathbf{Z}$ and some choices of signs. We have

$$\eta^{\pm 2}=1+\theta, \tag{1.19}$$

where

$$\theta=-4-4\gamma\mp(4+2\gamma)\delta. \tag{1.20}$$

Suppose, if possible, that $n\neq 0$. Let 2^r be the highest power of 2 dividing n and put $N=|n|$. Then

$$\eta^{2n}=(1+\theta)^N=1+N\theta+\sum_2^N T_m, \tag{1.21}$$

where

$$T_m=\frac{N(N-1)\ldots(N-m+1)}{m!}\theta^m. \tag{1.22}$$

Here $2^{[3m/2]}|\theta^m$, $2^r|N$ and $2^m\nmid m!$. Hence

$$T_m\equiv 0 \qquad (2^{r+2}). \tag{1.23}$$

It follows that

$$\begin{aligned}\eta^{2n}&\equiv 1+N\theta \qquad (2^{r+2})\\ &\equiv 1+2^{r+1}\gamma\delta \qquad (2^{r+2}).\end{aligned} \tag{1.24}$$

Hence

$$(1\pm\delta)\eta^{2n}\equiv 1+2^{r+1}\gamma+(\pm 1+2^{r+1}\gamma)\delta \qquad (2^{r+2}). \tag{1.25}$$

In particular, the coefficient of γ is non-zero, which contradicts (1.18).

2. Here we deal with (0.4).

LEMMA 2.1. *The only integral solution of*

$$x=2u^2, \qquad x^2+2=6v^2 \tag{2.1}$$

is $x=2$.

Here

$$x=6z+2$$

https://doi.org/10.1017/S0017089500006030 Published online by Cambridge University Press

for some $z \in \mathbf{Z}$, and so

$$2z^2+(2z+1)^2=v^2, \tag{2.3}$$

that is

$$\{v+(2z+1)\}\{v-(2z+1)\}=2z^2. \tag{2.4}$$

There are thus integers l, m such that one of the two following holds:

$$v+2z+1=4l^2, \qquad v-2z-1=2m^2, \qquad z=2lm; \tag{2.5}$$

$$v+2z+1=2l^2, \qquad v-2z-1=4m^2, \qquad z=2lm. \tag{2.6}$$

If (2.5) holds, we have

$$1=2l^2-4lm-m^2=6l^2-(2l+m)^2,$$

which is impossible modulo 3.

Hence (2.6) holds, and

$$1=l^2-4lm-2m^2, \tag{2.7}$$

$$u^2=l^2+2lm-2m^2. \tag{2.8}$$

As in the preceding section, we define γ by

$$\gamma^2=-2. \tag{2.9}$$

Put

$$\lambda=l-\gamma m, \tag{2.10}$$

so that

$$\begin{aligned}1&=-\gamma u^2+(1+\gamma)\lambda^2\\ &=\{u+(1+\gamma)\mu\}^2+(2-\gamma)\mu^2,\end{aligned} \tag{2.11}$$

where

$$\mu=\lambda-u. \tag{2.12}$$

Clearly, solutions of (2.11) are given by $u=\pm 1$, $\lambda=\pm 1$. We shall show that these are the only solutions with $u \in \mathbf{Z}$, $\lambda \in \mathbf{Z}[\gamma]$.

The argument is similar to that in the previous section. We define δ now by

$$\delta^2=-2+\gamma. \tag{2.13}$$

There is a unique extension $|\ |_2$ of the 2-adic valuation and $|\gamma|_2=2^{-1/2}$, $|\delta|_2=2^{-1/4}$. Hence 1, γ, δ, $\gamma\delta$ is a basis for the integers of $\mathbf{Q}(\gamma, \delta)$.

On putting $u=-1$, $\lambda=1$ in (2.11) we see that

$$\eta=1+2\gamma+2\delta \tag{2.14}$$

is a unit, and it is easy to check that it is fundamental. Then either

$$u+(1+\gamma)\mu+\mu\delta=\pm\eta^{2n} \tag{2.15}$$

or

$$u+(1+\gamma)\mu+\mu\delta=\pm\eta^{1+2n} \tag{2.16}$$

for some $n \in \mathbf{Z}$. The proof now follows much as for Lemma 1.1 on noting that

$$\eta^{\pm 2}=1+\theta \tag{2.17}$$

where

$$\theta = -16 + 8\gamma \pm (4 + 8\gamma)\delta. \tag{2.18}$$

If $2^r \| n$ and $N = |n|$ we have

$$\begin{aligned} \eta^{2n} &\equiv 1 + N\theta \qquad (2^{r+3}) \\ &\equiv 1 + 2^{r+2}\delta \qquad (2^{r+3}). \end{aligned} \tag{2.19}$$

This is incompatible with (2.15). Further,

$$\eta^{1+2n} \equiv 1 + 2\gamma + (2 + 2^{r+2})\delta \qquad (2^{r+3}), \tag{2.20}$$

which similarly contradicts (2.16).

3. We now conclude the proof of Theorem 0.1 by dealing with (0.5).

LEMMA 3.1. *The only solutions in integers of*

$$x = 6u^2, \qquad x^2 + 2 = 2v^2 \tag{3.1}$$

have $x = 0$ *or* $x = 24$.

Clearly v is odd. We have

$$(v+1)(v-1) = \tfrac{1}{2}x^2 = 18u^4 \tag{3.2}$$

and so there are integers l, m such that one of the following holds:

$$v + 1 = 144l^4, \qquad v - 1 = 2m^4; \tag{3.3}$$

$$v + 1 = 16l^4, \qquad v - 1 = 18m^4; \tag{3.4}$$

$$v + 1 = 2l^4, \qquad v - 1 = 144m^4; \tag{3.5}$$

$$v + 1 = 18l^4, \qquad v - 1 = 16m^4. \tag{3.6}$$

On eliminating v, these give respectively:

$$72l^4 - m^4 = 1; \tag{3.7}$$

$$8l^4 - 9m^4 = 1; \tag{3.8}$$

$$l^4 - 72m^4 = 1; \tag{3.9}$$

$$9l^4 - 8m^4 = 1. \tag{3.10}$$

Here (3.7) and (3.8) are both impossible modulo 3. The only solutions of (3.9) have $m = 0$, as follows from the next lemma.

LEMMA 3.2. *All solutions in integers of*

$$l^4 - 2n^2 = 1 \tag{3.11}$$

have $n = 0$.

The proof is simple. First, $(l^2+1)(l^2-1) = 2n^2$. Here l is odd, $l^2 + 1 \equiv 2 \pmod 4$, and so $l^2 + 1 = 2r^2$, $l^2 - 1 = s^2$ for integers r, s. But then $(l+s)(l-s) = 1$, so that $l + s = \pm 1$, $l - s = \pm 1$ and we are done.

We note in passing that Lemma 3.2 implies the theorem of Skolem [**9**] which is reproduced on p. 207 of [**8**].

There remains (3.10). We shall prove the following.

LEMMA 3.3. *All integral solutions of* (3.10) *have* $l^2 = m^2 = 1$.

We have

$$(3l^2+1)(3l^2-1)=8m^4. \tag{3.12}$$

Since

$$3l^2-1\equiv 2 \pmod 4 \tag{3.13}$$

there are integers r, s such that

$$3l^2+1=4r^4; \qquad 3l^2-1=2s^4, \tag{3.14}$$

and so

$$2r^4-s^4=1. \tag{3.15}$$

Here one can invoke the deep theorem of Ljunggren [**7**] that the only positive solutions of $2x^4-y^2=1$ are (1, 1) and (13, 239). Alternatively, we can proceed as follows.

LEMMA 3.4. *All integral solutions of*

$$2t^2-s^4=1 \tag{3.16}$$

have $s^2=t^2=1$.

Without loss of generality $t \geqslant 0$. We have

$$(1+2t+s^2)(1-2t-s^2)=-2(t+s^2)^2$$

where

$$1+2t+s^2>0,$$
$$1-2t-s^2\equiv 2 \pmod 4.$$

Hence there are integers a, b such that

$$1+2t+s^2=4a^2, \tag{3.17}$$
$$1-2t-s^2=-2b^2, \tag{3.18}$$
$$t+s^2=2ab,$$

and so

$$2a^2-b^2=1, \tag{3.19}$$
$$-2a^2+4ab-b^2=s^2. \tag{3.20}$$

We operate now in $\mathbf{Q}(i)$ with $i^2=-1$. It follows that

$$-i=s^2+(1+i)\beta^2, \tag{3.21}$$

where

$$\beta=b-(1-i)a. \tag{3.22}$$

We must show that all solutions of (3.21) have $s^2=1$, $\beta^2=-1$. Following the by now

https://doi.org/10.1017/S0017089500006030 Published online by Cambridge University Press

familiar pattern, we introduce δ with

$$\delta^2 = -1 - i. \tag{3.23}$$

Then 2 ramifies completely in $\mathbf{Q}(i, \delta)$ and $1, i, \delta, i\delta$ is a basis for the integers. Further,

$$\mathrm{Norm}(1 + i\delta) = -i, \tag{3.24}$$

so that

$$\eta = 1 + i\delta \tag{3.25}$$

is a unit, and it is easily checked that it is fundamental.

We have

$$s + \beta\delta = i^f \eta^g \tag{3.26}$$

for some $f, g \in \mathbf{Z}$. By (3.21) and (3.24) g is odd, say $g = \pm 1 + 4n$, and so

$$s + \beta\delta = \pm i(1 \pm i\delta)\eta^{4n} \tag{3.27}$$

or

$$s + \beta\delta = \pm(1 \pm i\delta)\eta^{4n}. \tag{3.28}$$

Now

$$-\eta^{\pm 4} = 1 + \theta \tag{3.29}$$

where

$$\theta = -8 - 8i \pm (4 - 8i)\delta. \tag{3.30}$$

Hence (3.27) leads to a contradiction with (3.26) modulo 2.

Putting $N = |n|$, $2^r \| n$, we have

$$\begin{aligned} \eta^{4n} &= (1+\theta)^N \\ &\equiv 1 + N\theta \qquad (2^{r+3}) \\ &\equiv 1 + 2^{r+2}\delta \qquad (2^{r+3}). \end{aligned} \tag{3.31}$$

Hence

$$(-1)^n(1 \pm i\delta)\eta^{4n} \equiv 1 + 2^{r+2} + 2^{r+2}i + (2^{r+2} \pm i)\delta \qquad (2^{r+3}). \tag{3.32}$$

In particular, the coefficient of i is not zero, in contradiction to (3.26). Hence the only possibility is $n = 0$.

REFERENCES

1. A. Baker, *Transcendental number theory* (Cambridge, 1975).

2. A. Baker and J. Coates, Integer points on curves of genus 1, *Proc. Cambridge Philos. Soc.* **67** (1970), 595–602.

3. A. Baker and H. Davenport, The equations $3x^2 - 2 = y^2$ and $8x^2 - 7 = z^2$, *Quart. J. Math. Oxford Ser.* 2, **20** (1969), 129–37.

4. J. W. S. Cassels, Integral points on certain elliptic curves, *Proc. London Math. Soc.* (3) **14A** (1965), 55–57.

5. F. Ellison, W. J. Ellison, J. Pesek, C. E. Stall and D. S. Stall, The diophantine equation $y^2 + k = x^3$, *J. Number Theory* **4** (1972), 107–117.

https://doi.org/10.1017/S0017089500006030 Published online by Cambridge University Press

6. G. Hoare, Solution and comments on 67.A and 67.B, *Math. Gaz.* **67** (1983), 228–230.

7. W. Ljunggren, Zur Theorie der Gleichung $x^2+1=Dy^4$, *Avh. Norske Vid.-Akad. Oslo*, 1942 No. 5, 1.

8. L. J. Mordell, *Diophantine equations* (Academic Press, 1969).

9. T. Skolem, The use of p-adic methods in the theory of diophantine equations, *Bull. Soc. Math. Belg.* **7** (1955), 83–95.

D.P.M.M.S.
University of Cambridge
16 Mill Lane
Cambridge
CB2 1SB