ROCKY MOUNTAIN
JOURNAL OF MATHEMATICS
Volmue 6, Number 1, 1976

THE DIOPHANTINE EQUATION $Y^4 = X^3 + X^2 + 1$

W. J. LEAHEY AND D. F. HSU

The object of this paper is to show that the only solutions to the Diophantine equation of the title are $(X, Y) = (0, \pm 1), (-1, \pm 1)$, and $(4, \pm 3)$. It is, of course, sufficient to show that the only solutions to $Y^2 = X^3 + X^2 + 1$ are $(X, Y) = (0, \pm 1), (-1, \pm 1)$, and $(4, \pm 9)$. We will show that this is in fact the case. Our methods are standard, viz., we introduce a root to the equation on the right-hand side and then investigate the possibility of the linear factor, which arises, being a square or certain multiples of a square. Of the various cases which occur, most can be dealt with by elementary means. One case, however, seems to be more difficult. In fact for this case we need to know that the only solutions to the Diophantine equation $s^4 - 2s^2t^2 - 8st^3 + t^4 = 1$ are $s = 0, t = \pm 1$ and $s = \pm 1, t = 0$. Thus we divide the paper into two parts. In the first part we reduce the solution of the equation of the title to a knowledge of the solutions of this fourth degree equation. In the second part we show that the only solutions of this fourth degree equation are as stated.

PART 1. Let $f(X) = X^3 + X^2 + 1$ and let θ be the real root of f. Set $F = Q(\theta)$, where Q denotes the rationals. We begin by investigating the arithmetic of F.

1. Since the norm of $f'(\theta) = 3\theta^2 + 2\theta$ is -31, it follows that $1, \theta, \theta^2$ form an integral basis for F and that the discriminant of F is -31. On the other hand the Minkowski bound for F, $((4/\pi)^{r^2} (n!/n^n) \sqrt{|D|})$, is less than 2 and hence the class number of F is 1. Finally, according to a table published by Delone and Faddeev in [1], θ is a fundamental unit for F.

2. In F we have

$$X^3 + X^2 + 1 = (X - \theta)(X^2 + (1 + \theta)X + \theta(1 + \theta)).$$

Suppose now x is a rational integer and let d be the greatest common divisor of $x - \theta$ and $x^2 + (1 + \theta)x + \theta(1 + \theta)$. Then d divides

$$x^2 + (1 + \theta)x + \theta(1 + \theta) - (x + 1 + 2\theta)(x - \theta) = \theta(2 + 3\theta).$$

Now θ is a unit and since the norm of $2 + 3\theta$ is 31, $2 + 3\theta$ is prime. It follows that d is either 1 or $2 + 3\theta$.

Thus if there are rational integers x and y such that $y^2 = x^3 + x^2 + 1$, then there exists an algebraic integer α in F which satisfies one of the following four equations:

1. $x - \theta = \pm\alpha^2$
2. $x - \theta = \pm\,\theta \cdot \alpha^2$
3. $x - \theta = \pm(2 + 3\theta)\alpha^2$
4. $x - \theta = \pm\,\theta(2 + 3\theta)\alpha^2.$

We have assumed that θ is real. It is easy to check that θ satisfies $-3/2 < \theta < -2/3$. In particular then $2 + 3\theta < 0$. On the other hand there is no loss in generality if we assume $x \geqq 2$ and hence $x - \theta > 0$. Since α^2 is positive we have then only the following possibilities:

1′. $x - \theta = \alpha^2$

2′. $x - \theta = -\,\theta \cdot \alpha^2$

3′. $x - \theta = -(2 + 3\theta) \cdot \alpha^2$

4′. $x - \theta = \theta(2 + 3\theta) \cdot \alpha^2.$

We will treat each of these cases in turn (not in the order listed, however).

Case 1. $x - \theta = \alpha^2$. Write $\alpha = a + b\theta + c\theta^2$ with a, b, and c rational integers. Expanding $(a + b\theta + c\theta^2)^2$ and equating the coefficients of 1, θ, and θ^2 we obtain the equations

$$\text{(i)}\quad x = a^2 + c^2 - 2bc$$

$$\text{(ii)}\quad -1 = -c^2 + 2ab$$

$$\text{(iii)}\quad 0 = b^2 + c^2 + 2ac - 2bc.$$

From (ii) b and c must be relatively prime. Writing (iii) in the form $b^2 = c(2b - 2a - c)$ and using the fact that $(b, c) = 1$ we see that $c = \pm 1$. It follows from (iii) that $b \equiv c(2)$ and hence b is odd. In particular $b \neq 0$. Equation (ii) then implies that $a = 0$. If $c = 1$, (iii) becomes $0 = b^2 + 1 - 2b = (b - 1)^2$, and hence $b = 1$. This implies $x = -1$. Similarly, the choice $c = -1$ leads to the solution $x = -1$.

Case 2. $x - \theta = -(2 + 3\theta)\alpha^2$. As in Case 1, we write $\alpha = a + b\theta + c\theta^2$, expand $-(2 + 3\theta)\alpha^2$, and equate coefficients to obtain the system of equations

$$\begin{aligned}
&\text{(i)} \quad -x = 2a^2 - 3b^2 - c^2 - 6ac + 2bc\\
&\text{(ii)} \quad 1 = 3a^2 + c^2 + 4ab - 6bc\\
&\text{(iii)} \quad 0 = -b^2 - 4c^2 + 6ab - 2ac + 2bc.
\end{aligned}$$

Equation (iii) implies $b \equiv 0$ (2). Viewing equation (ii) mod 4, then, we see that a must be even and c odd. From equation (i) $x \equiv 1$ (4). But then from $y^2 = x^3 + x^2 + 1$ we would obtain $y^2 \equiv 3$ (4) which is not possible. Hence there is no solution in this case.

CASE 3. $x - \theta = \theta(2 + 3\theta)\alpha^2$. Here we are led to the equations

$$\begin{aligned}
&\text{(i)} \quad x = b^2 + 4c^2 - 6ab + 2ac - 2bc\\
&\text{(ii)} \quad -1 = 2a^2 - 3b^2 - c^2 - 6ac + 2bc\\
&\text{(iii)} \quad 0 = 3a^2 + b^2 + 5c^2 - 2ab + 2ac - 8bc.
\end{aligned}$$

Adding (ii) and (iii) we see that $a \equiv 1$ (2). From equation (ii) b and c must be of opposite parity.

If $b \equiv 1$ (2), then $c \equiv 0$ (2) and mod 4 equation (iii) becomes

$$\begin{aligned}
0 &\equiv 3a^2 + b^2 - 2ab\\
&\equiv 3 + 1 - 2\\
&\equiv 2\ (4)
\end{aligned}$$

which is a contradiction. On the other hand if $b \equiv 0$ (2) then $c \equiv 1$ (2). From equation (i) we would have $x \equiv 0$ (2). The equation $y^2 = x^3 + x^2 + 1$ implies y is odd. Rewriting this equation in the form $(y - 1)(y + 1) = x^2(x + 1)$ and noticing that the left-hand side is divisible by 8, we see that x must be divisible by 4. But then equation (i) becomes $0 \equiv 2ac$ (4) which is not possible since $a \equiv 1 \equiv c$ (2). Thus there is no solution in this case.

CASE 4. $x - \theta = -\theta \cdot \alpha^2$. Here we have

$$\begin{aligned}
&\text{(i)}\ x = b^2 + c^2 + 2ac - 2bc\\
&\text{(ii)}\ 1 = a^2 + c^2 - 2bc\\
&\text{(iii)}\ 0 = b^2 + 2c^2 - 2ab + 2ac - 2bc.
\end{aligned}$$

Equation (iii) is equivalent to (iii)$'$ $a^2 = c^2 + (a + c - b)^2$. From (ii) a and c must be relatively prime. Hence from (iii)$'$ a, c, and $a + c - b$ represent a primitive Pythagorean triple. From (iii) $b \equiv 0$ (2). From (ii) a and c have opposite parity. It follows that $a + c - b$ is odd and c is even. By the well-known parametric representation of Pythagorean triples then there exist integers s and t such that

$$a = \pm(s^2 + t^2)$$
$$c = \pm 2st$$
$$a + c - b = \pm(s^2 - t^2).$$

Since we are seeking solutions to $x - \theta = -\theta(a + b\theta + c\theta^2)^2$, we may assume that a is non-negative. Then by suitably choosing s and t we may write

$$a = s^2 + t^2$$
$$c = 2st$$
$$a + c - b = s^2 - t^2.$$

Solving for b we have $b = 2t(s + t)$. Substituting these expressions for $a, b,$ and c in (ii) we are led to the equation $1 = s^4 - 2s^2t^2 - 8st^3 + t^4$.

Now we will show in Part 2 that the only solutions to this last equation are $s = 0$, $t = \pm 1$ and $s = \pm 1$, $t = 0$. These lead to the values $a = 1$, $b = 0$, $c = 0$ and $a = 1$, $b = 2$, $c = 0$ for a, b, c. From equation (i) the corresponding values of x are $x = 0$ and $x = 4$.

Assuming then the results of Part 2 we have the following

THEOREM. *The only solutions to the equation*

$$Y^2 = X^3 + X^2 + 1$$

in rational integers are $(X, Y) = (0, \pm 1), (-1, \pm 1)$, *and* $(4, \pm 9)$.

PART 2. We now show that the only solutions to the Diophantine equation

$$F(X, Y) = X^4 - 2X^2Y^2 - 8XY^3 + Y^4 = 1$$

are $X = 0$, $Y = \pm 1$ and $X = \pm 1$, $Y = 0$. The methods we use are those developed by Th. Skolem in [2].

1. Let $f(X) = F(X, 1)$ and let θ be a root of f. Suppose that (x, y) is a solution to $F(X, Y) = 1$. Since

$$f(X) = (X - \theta)(X^3 + \theta X^2 + (\theta^2 - 2)X + (\theta^3 - 2\theta - 8))$$

and

$$F(X, Y) = Y^4 \cdot f(X/Y)$$

it follows that

$$1 = (x - y\theta)(x^3 + \theta x^2y + (\theta^2 - 2)xy^2 + (\theta^3 - 2\theta - 8)y^3)$$

and hence that $x - y\theta$ is a unit in the number field $E = Q(\theta)$, where

Q denotes the field of rational numbers. Since $F(x, y)$ is the norm from E to Q of $x - y\theta$, we wish to show that the only units of the form $x - y\theta$ which are of positive norm are ± 1 and $\pm\ \theta$.

2. Denote by α the element

$$\alpha = 1/4(-5 - \theta + \theta^2 + \theta^3)$$

of E. It is not difficult to check that α is a root of the polynomial

$$g(X) = X^4 - 2X^3 - 2X^2 + 2X - 1.$$

The polynomial $g(X + 1)$ satisfies Eisenstein's irreducibility criterion relative to the prime 2, and hence $g(X)$ is irreducible. It follows that $E = Q(\alpha)$ and that E is of degree 4 over Q. Using standard methods now, one can show that $1, \alpha, \alpha^2, \alpha^3$ form an integral basis for E. The discriminant D of E is then the discriminant of α which turns out to be $-2^6 \cdot 31$.

3. We turn now to the question of determining a set of fundamental units for E. A sketch of the curve $Y = g(X)$ indicates that g has 2 real roots and hence 2 complex roots. If α_1 and α_2 are the real roots with α_1 the smaller of the two, then after some calculation we see that

$$-\ 1.28 \leqq \alpha_1 \leqq -1.27$$

$$2.53 \leqq \alpha_2 \leqq 2.54.$$

On the other hand if α_3 is one of the complex roots, then

$$0.307 \leqq \alpha_3\bar{\alpha}_3 \leqq 0.312$$

where the bar indicates the complex conjugate.

Let us agree that we have chosen θ such that $\alpha = \alpha_1$. Since E is real then, the only roots of unity in E are ± 1. Since there are two real conjugate fields of E and one complex conjugate field there will be two fundamental units.

Let $\beta = 1 - \alpha + \alpha^3$. Then β is a root of the polynomial $X^4 - 16X^3 + 18X^2 - 8X + 1$ and hence a unit. We will show that α and β form a pair of fundamental units for E. To do this we will use a theorem of Berwick [3] and a method discussed by Ljunggren in [4].

For $i = 1, 2, 3$ we define values v_i on E by

$$v_i\left(\sum_{j=0}^{3} x_j\alpha^j\right) = \left|\sum_{j=0}^{3} x_j\alpha_i^j\right| \quad \text{for } i = 1, 2, \text{ and}$$

$$v_3\left(\sum_{j=0}^{3} x_j\alpha^j\right) = \left|\sum_{j=0}^{3} x_j\alpha_3^j\right|^2.$$

The theorem of Berwick to which we refer is the following

THEOREM 1. *Let ϵ_i $i = 1, 2, 3$ be units of E with the following properties*:

1. $v_j(\epsilon_i) < 1$ *for* $j \neq i$;
2. $v_i(\epsilon_i) > 1$ *and is minimal among the units which satisfy* 1.

Then any two of the ϵ_i form a pair of fundamental units for E.

In order to show that α and β form a pair of fundamental units it is sufficient, by Berwick's Theorem, to show that

$$\text{A. } v_1(\beta) <_{.} 1, v_3(\beta) < 1 \text{ and for no unit } \gamma \text{ is it the case that}$$
$$v_1(\gamma) < 1, v_3(\gamma) < 1 \text{ and } v_2(\gamma) < v_2(\beta)$$

and that

$$\text{B. } v_1(\alpha) > 1, v_2(\alpha) > 1 \text{ and for no unit } \gamma \text{ is it the case that}$$
$$v_1(\gamma) > 1, v_2(\gamma) > 1 \text{ and } v_3(\gamma) > v_3(\alpha).$$

We begin with statement A. It is easy to check that $v_1(\beta) < 1$, $v_3(\beta) < 1$ and $v_2(\beta) < 14.85$. For $\gamma = \sum_{i=0}^{3} x_i\alpha^i \in E$, denote by γ_j the numbers $\gamma_j = \sum_{i=0}^{3} x_i\alpha_j^i$ for $j = 1, 2, 3$. Suppose now that γ is an element of E which satisfies

$$v_1(\gamma) < 1, \gamma_3(\gamma) < 1 \text{ and } \gamma_2(\gamma) < 14.85.$$

We have the equations

$$\begin{aligned}
\gamma_1 &= x_0 + x_1\alpha_1 + x_2\alpha_1^2 + x_3\alpha_1^3 \\
\gamma_2 &= x_0 + x_1\alpha_2 + x_2\alpha_2^2 + x_3\alpha_2^3 \\
\gamma_3 &= x_0 + x_1\alpha_3 + x_2\alpha_3^2 + x_3\alpha_3^3 \\
\bar{\gamma}_3 &= x_0 + x_1\bar{\alpha}_3 + x_2\bar{\alpha}_3^2 + x_3\bar{\alpha}_3^3.
\end{aligned}$$

Let M be the coefficient matrix of this system and denote by M_{ij} the (i, j)th cofactor of M. After some simple, but lengthy, calculations we obtain

$$\begin{array}{lll}
|M_{11}| \leqq 7.27 & |M_{21}| \leqq 1.20 & |M_{31}| = |M_{41}| \leqq 32.97 \\
|M_{12}| \leqq 12.61 & |M_{22}| \leqq 2.00 & |M_{32}| = |M_{42}| \leqq 47.57 \\
|M_{13}| \leqq 19.41 & |M_{23}| \leqq 2.99 & |M_{33}| = |M_{43}| \leqq 37.31 \\
|M_{14}| \leqq 9.15 & |M_{24}| \leqq 2.99 & |M_{34}| = |M_{44}| \leqq 18.14 .
\end{array}$$

If, for example, we solve the above system for x_0 we have

$$x_0 = (1/\sqrt{D})(\gamma_1 M_{11} + \gamma_2 M_{21} + \gamma_3 M_{31} + \bar{\gamma}_3 M_{41}).$$

Using the fact that $|1/\sqrt{D}| \leqq 0.0226$ and the above bounds for $|\gamma_i| = v_i(\gamma)$ and the $|M_{ij}|$'s, we see that $|x_0| \leqq 2$. Similarly, we obtain $|x_1| \leqq 3$, $|x_2| \leqq 3$, and $|x_3| \leqq 2$.

Now among the $5^2 \cdot 7^2$ integers $\sum_{i=0}^{3} x_i\alpha^i$ which satisfy $|x_0|$, $|x_3| \leqq 2$ and $|x_1|$, $|x_2| \leqq 3$ there are exactly 32 which are units. We present these 32 units along with their values in a table in the Appendix. These units were obtained with the aid of a simple program run on a CDC 1130 computer. From the table we see that β satisfies condition (A) above.

In the same way we find that if there is a unit γ such that $v_1(\gamma) > 1$, $v_2(\gamma) > 1$ and $v_3(\gamma) > v_3(\alpha)$, then it must be among the 32 units listed in the Appendix. Again we see from the table that α satisfies condition (B).

4. We recall that we are investigating units in E of the form $a + b\theta$ with a, b integral and which are of positive norm. Since $\theta = -3\alpha - \alpha^2 + \alpha^3$, we are thus interested in units of the form $a - 3b\alpha - b\alpha^2 + b\alpha^3$. We will make constant use of a theorem of Th. Skolem (see [2]). For convenience we state here a version of the theorem which is appropriate for our applications.

THEOREM 2. *Let p be a rational prime, and let*

$$P(X, Y) = \sum_{i=0}^{\infty} P_i(X, Y)p^i$$

$$Q(X, Y) = \sum_{i=0}^{\infty} Q_i(X, Y)p^i$$

be series where the P_i and Q_i are polynomials in X and Y with rational coefficients which are integral at p. Suppose there exist polynomials $A(X, Y)$, $B(X, Y)$, $C(X, Y)$, and $D(X, Y)$ with integral coefficients such that

$$A(X, Y)P_0(X, Y) + B(X, Y)Q_0(X, Y)$$
$$\equiv \textit{non-zero polynomial in } X \pmod p$$

and

$$C(X, Y)P_0(X, Y) + D(X, Y)Q_0(X, Y)$$
$$\equiv \textit{non-zero polynomial in } Y \pmod p.$$

Then there exist at most $\deg P_0(X, Y) \cdot \deg Q_0(X, Y)$ *pairs of rational integers x, y which satisfy the equations*

$$P(x, y) = 0$$

$$Q(x, y) = 0$$

in the field of p-adic numbers.

REMARK. Suppose that $P_0(X, Y)$ is a polynomial in X only and that P_0 has exactly s linear factors mod p. Similarly, suppose that $Q_0(X, Y)$ is a polynomial in Y only and that it has exactly t linear factors mod p. Then it is not difficult to see from the proof of Skolem's theorem that the equations $P(X, Y) = 0$ and $Q(X, Y) = 0$ have no more than $s \cdot t$ solutions.

In our applications we will take $p = 3$.

5. Since α and β form a pair of fundamental units, so do $\alpha^4\beta$ and α. Now it turns out that for certain integral ζ and η

$$\alpha^4\beta = 1 + 3\zeta, \text{ with } \zeta \equiv 1 + 2\alpha + 2\alpha^3 \ (3), \text{ and}$$

$$\alpha^{80} = 1 + 3\eta, \text{ with } \eta \equiv 1 + \alpha^3 \ (3).$$

Any unit can be written in the form $\pm (\alpha^4\beta)^x(\alpha^{80})^y\alpha^i$ where $0 \leqq i \leqq 79$. In our case we are looking for integers x, y, and i such that $(\alpha^4\beta)^x(\alpha^{80})^y\alpha^i$ is of the form $a - 3b\alpha - b\alpha^2 + b\alpha^3$. Since $(\alpha^4\beta)^x(\alpha^{80})^y \equiv 1 \ (3)$, i must be such that α^i is of the form $a - b\alpha^2 + b\alpha^3$ (3). There are exactly 8 values of i for which this is the case. It is not difficult to check that they are $i = 0, 8, 9, 34, 40, 48, 49$, and 74. We will treat each of these cases in turn.

CASE 1. $i = 0$. We have

$$\begin{aligned}(\alpha^4\beta)^x(\alpha^{80})^y &= (1 + 3\zeta)^x(1 + 3\eta)^y \\ &= 1 + (x\zeta + y\eta)3 + (\cdots)3^2 + \cdots \\ &= 1 + [x(1 + 2\alpha + 2\alpha^3) + y(1 + \alpha^3)]3 + (\cdots)3^2 + \cdots \\ &= (1 + x3 + (\cdots)3^2 + \cdots) \\ &\quad + ((2x)3 + (\cdots)3^2 + \cdots)\alpha \\ &\quad + (0 \cdot 3 + (\cdots)3^2 + \cdots)\alpha^2 \\ &\quad + ((2x + y)3 + (\cdots)3^2 + \cdots)\alpha^3.\end{aligned}$$

We are assuming that $(\alpha^4\beta)^x(\alpha^{80})^y$ is a unit of the form $a - 3b\alpha - b\alpha^2 + b\alpha^3$. Equating the coefficients of α, α^2, and α^3, we obtain then the system of equations

$$-3b = (2x)3 + (\cdots)3^2 + \cdots$$
$$-b = 0\cdot 3 + (\cdots)3^2 + \cdots$$
$$b = (2x + y)3 + (\cdots)3^2 + \cdots.$$

Adding 3 times the last equation to the first, and adding the last to the second, we obtain

$$0 = (2x)3 + (\cdots)3^2 + \cdots$$
$$0 = (2x + y)3 + (\cdots)3^2 + \cdots.$$

This system is clearly equivalent to

$$0 = 2x + (\cdots)3 + \cdots$$
$$0 = 2x + y + (\cdots)3 + \cdots.$$

Now since $(\alpha^4\beta)^0(\alpha^{80})^0 = 1$ is of the proper form, $x = 0 = y$ is a solution to this system. On the other hand this system satisfies the conditions of Theorem 2, and hence $x = 0 = y$ is the only solution.

Case 2. $i = 8$ and $i = 48$. It is easy to check that $\alpha^8 = 1 + \alpha^2 + 2\alpha^3 + 3\xi$, where $\xi \equiv \alpha + 2\alpha^2$ (3). We have then

$$(\alpha^4\beta)^x(\alpha^{80})^y\alpha^8 = (1 + 3\zeta)^x(1 + 3\eta)^y(1 + \alpha^2 + 2\alpha^3 + 3\xi).$$

Expanding the right-hand side, equating it to $a - 3b\alpha - b\alpha^2 + b\alpha^3$, and looking at the constant and α^3 terms, we obtain equations of the form

$$a = 1 + (\cdots)3 + \cdots$$
$$b = 2 + (\cdots)3 + \cdots.$$

In particular then if a solution exists we would have $a \equiv 1$ (3) and $b \equiv 2$ (3). But we are seeking solutions to the diophantine equation $F(a, b) = a^4 - 2a^2b^2 - 8ab^3 + b^4 = 1$, and if $a \equiv 1$ (3) and $b \equiv 2$ (3), then $F(a, b) \equiv 2$ (3). Hence there is no possible solution in this case.

The same situation occurs when $i = 48$.

Case 3. $i = 9$ and $i = 49$. Since α is a root of $g(X) = X^4 - 2X^3 - 2X^2 + 2X - 1$, we have $\alpha^4 = 1 - 2\alpha + 2\alpha^2 + 2\alpha^3$, and hence $\alpha^4 \equiv 1$ (2). On the other hand it is easy to check that $\beta^2 = 1 + 2(2 - 4\alpha + 3\alpha^2 + 6\alpha^3)$, and therefore $\beta^2 \equiv 1$ (2). Now any unit can be written in the form $\pm\alpha^{4s}\beta^{2t}\alpha^i\beta^j$ with $0 \leqq i \leqq 3$ and $0 \leqq j \leqq 1$. Since $\alpha^{4s}\beta^{2t} \equiv 1$ (2) and we are seeking units of the form $a - 3b\alpha - b\alpha^2 + b\alpha^3 \equiv a + b\alpha + b\alpha^2 + b\alpha^3$ (2), i and j must have the property that $\alpha^i\beta^j$

is of the form $a + b\alpha + b\alpha^2 + b\alpha^3 \bmod 2$. It is not hard to verify that the only values of i and j which have this property are $i = 0 = j$ and $i = 2, j = 1$. Thus we are looking for units of one of the two forms $\alpha^{4s}\beta^{2t}$ and $\alpha^{4s+2}\beta^{2t+1}$. Suppose now there were a solution of the form $(\alpha^4\beta)^x(\alpha^{80})^y\alpha^9$. We would then have $4x + 80y + 9 = 4s$ or $4s + 2$. But this is clearly not possible.

The same argument holds for $i = 49$.

Case 4. $i = 40$. Suppose there exists a solution to the equation

$$(\alpha^4\beta)^x(\alpha^{80})^y\alpha^{40} = a - 3b\alpha - b\alpha^2 + b\alpha^3.$$

We can rewrite the left-hand side as $(\alpha^4\beta)^x(\alpha^{40})^{2y+1}$. Thus we would have a solution to the equation

$$(\alpha^4\beta)^x(\alpha^{40})^y = a - 3b\alpha - b\alpha^2 + b\alpha^3$$

with y odd. Since y is odd we may multiply through by -1 to obtain $(\alpha^4\beta)^x(-\alpha^{40})^y$ on the left-hand side. We consider now the equation

$$(\alpha^4\beta)^x(-\alpha^{40})^y = a - 3b\alpha - b\alpha^2 + b\alpha^3.$$

One calculates that $-\alpha^{40} \equiv 1 + (2 + 2\alpha^3)3\ (3^2)$. Thus

$$\begin{aligned}(\alpha^4\beta)^x(-\alpha^{40})^y &= [1 + (1 + 2\alpha + 2\alpha^3)3 + (\cdots)3^2 \\ &\quad + \cdots]^x[1 + (2 + 2\alpha^3)3 + (\cdots)3^2 + \cdots]^y \\ &= 1 + [x(1 + 2\alpha + 2\alpha^3) + y(2 + 2\alpha^3)]3 \\ &\quad + (\cdots)3^2 + \cdots.\end{aligned}$$

Equating the α, α^2, and α^3 coefficients we obtain the system

$$\begin{aligned}-3b &= (2x)3 + (\cdots)3^2 + \cdots \\ -b &= 0\cdot 3 + (\cdots)3^2 + \cdots \\ b &= (2x + 2y)3 + (\cdots)3^2 + \cdots.\end{aligned}$$

These equations imply the equations

$$\begin{aligned}0 &= 2x + (\cdots)3 + \cdots \\ 0 &= 2x + 2y + (\cdots)3 + \cdots.\end{aligned}$$

As in Case 1 we conclude that the solution $x = 0 = y$ is unique. In particular then, there is no solution with y odd.

Case 5. $i = 74$. Here we are looking for solutions to the equation

$$(\alpha^4\beta)^x(\alpha^{80})^y\alpha^{74} = a - 3b\alpha - b\alpha^2 + b\alpha^3.$$

Now

$$(\alpha^4\beta)(\alpha^{80})^{-1}\alpha^{74} = \alpha^{-2}\beta = -3\alpha - \alpha^2 + \alpha^3,$$

and thus $x = 1$, $y = -1$ is a solution. We wish to show that this is the only solution.

The left-hand side of the above equation can be written as

$$(\alpha^4\beta)^x(\alpha^{80})^y\alpha^{74} = (\alpha^{-2}\beta)(\alpha^4\beta)^{x-1}(\alpha^{80})^{y+1}.$$

A rountine calculation shows that $(\alpha^2\beta^{-1})(a - 3b\alpha - b\alpha^2 + b\alpha^3)$ is of the form $A - B\alpha + 3B\alpha^2 - B\alpha^3$. Thus we want to show that the only solution to the equation

$$(\alpha^4\beta)^x(\alpha^{80})^y = A - B\alpha + 3B\alpha^2 - B\alpha^3$$

is $x = 0 = y$. This is more difficult than the previous cases. In fact we must compute things mod 3^3.

To begin with one must check that

$$\zeta \equiv 1 + 2\alpha + 2\alpha^3 + (1 + 2\alpha^2)3\ (3^2)$$

$$\eta \equiv 1 + \alpha^3 + (\alpha + 2\alpha^2 + \alpha^3)3(3^2).$$

Then after a long calculation one obtains

$$\begin{aligned}(\alpha^4\beta)^x(\alpha^{80})^y &= 1 + (x\zeta + y\eta)3 + \left[xy\zeta\eta + \tbinom{x}{2}\zeta^2 + \tbinom{y}{2}\eta^2\right.\\ &\quad \left.+ 3\tbinom{x}{3}\zeta^3 + 3\tbinom{y}{3}\eta^3\right]3^2 + (\cdots)3^3 + \cdots\\ &= 1 + [x(1 + 2\alpha + 2\alpha^2) + y(1 + \alpha^3)]\,3\\ &\quad + [x(1 + 2\alpha^2) + y(\alpha + 2\alpha^2 + \alpha^3)\\ &\quad + xy(2\alpha + \alpha^2 + 2\alpha^3) + \tbinom{x}{2}(2\alpha + 2\alpha^2 + \alpha^3)\\ &\quad + \tbinom{y}{2}(1 + 2\alpha + \alpha^3) + 3\tbinom{x}{3}(2 + 2\alpha^2)\\ &\quad + 3\tbinom{y}{3}(\alpha^2 + 2\alpha^3)]\,3^2 + (\cdots)3^3 + \cdots.\end{aligned}$$

Equating the α, α^2, and α^3 coefficients we obtain the system

$$\begin{aligned}-B &= (2x)3 + (\cdots)3^2 + \cdots\\ 3B &= 0\cdot 3 + (2x + 2y + xy + 2\tbinom{x}{2} + 2\cdot 3\tbinom{x}{3}\\ &\quad + 3\tbinom{y}{3})3^2 + (\cdots)3^3 + \cdots\\ -B &= (2x + y)3 + (\cdots)3^2 + \cdots.\end{aligned}$$

From these equations we extract

$$\begin{aligned}0 &= y + (\cdots)3 + \cdots\\ 0 &= 2x + x^2 + x^3 + xy + 2y^3 + (\cdots)3 + \cdots.\end{aligned}$$

Solutions to these equations are easily seen to be the same as solutions to a set of equations of the form

$$\begin{aligned} 0 &= y + (\cdots)3 + \cdots \\ 0 &= x(x^2 + x + 2) + (\cdots)3 + \cdots. \end{aligned}$$

By the Remark following Theorem 2, there is only one solution, viz., $x = 0 = y$.

Case 6. $i = 34$. As in the case of $i = 74$, we write the term $(\alpha^4\beta)^x(\alpha^{80})^y\alpha^{34}$ in the form $(\alpha^{-2}\beta)(\alpha^4\beta)^{x-1}(\alpha^{80})^y\alpha^{40}$ and then multiply through by $\alpha^2\beta^{-1}$ to obtain an equation of the form

$$(\alpha^4\beta)^x(\alpha^{80})^y\alpha^{40} = A - B\alpha + 3B\alpha^2 - B\alpha^3.$$

Now, as in the $i = 40$ case, we can rewrite the left-hand side as $(\alpha^4\beta)^x(\alpha^{40})^{2y+1}$, then multiply through by -1, and we are thus looking for solutions to

$$(\alpha^4\beta)^x(-\alpha^{40})^y = A - B\alpha + 3B\alpha^2 - B\alpha^3$$

with y odd. Now $-\alpha^{40} = 1 + 3\xi$ where $\xi \equiv (2 + 2\alpha^3) + (2 + \alpha + \alpha^2 + \alpha^3)3\ (3^2)$. Using this fact and expanding the left-hand side we obtain after lengthy calculations the equations

$$\begin{aligned} B &= (2x)3 + (\cdots)3^2 + \cdots \\ -3B &= 0\cdot 3 + (x^2 + 2xy + x^3 + y^3)3^2 + (\cdots)3^3 + \cdots \\ B &= (2x + 2y)3 + (\cdots)3^2 + \cdots. \end{aligned}$$

These imply

$$\begin{aligned} 0 &= 2y + (\cdots)3 + \cdots \\ 0 &= 2x + 2y + x^2 + 2xy + x^3 + y^3 + (\cdots)3 + \cdots \end{aligned}$$

which in turn is equivalent to a system of the form

$$\begin{aligned} 0 &= y + (\cdots)3 + \cdots \\ 0 &= x(x^2 + x + 2) + (\cdots)3 + \cdots. \end{aligned}$$

Now we know that $x = 0 = y$ is a solution to this system. But, by the Remark following Theorem 2, this is the only solution. There is then no solution with y odd.

We summarize our results in the following

Theorem 3. *The only solutions to*

$$X^4 - 2X^2Y^2 - 8XY^3 + Y^4 = 1$$

in rational integers are $X = 0, Y = \pm 1$ *and* $X = \pm 1, Y = 0$.

Appendix

We present here a list of units $\gamma = x_0 + x_1\alpha + x_2\alpha^2 + x_3\alpha^3$ which satisfy $|x_0|$, $|x_3| \leqq 2$ and $|x_1|$, $|x_2| \leqq 3$. If γ appears we do not list $-\gamma$. We also exclude $\gamma = \pm 1$.

We also present for each γ the values $v_i(\gamma)$ for $i = 1, 2, 3$. The entry (a, b) under $v_i(\gamma)$ indicates that $v_i(\gamma)$ lies in the interval (a, b). If there is no entry under $v_i(\gamma)$, it means that γ was excluded from consideration as a possible fundamental unit because of values of $v_j(\gamma)$ for $j \neq i$.

γ	$v_1(\gamma)$	$v_2(\gamma)$	$v_3(\gamma)$
α	(1.27, 1.28)	(2.53, 2.54)	(0.30, 0.32)
α^2	(1.00, ∞)	(1.00, ∞)	(0.00, 0.10)
α^3	(1.00, ∞)	(1.00, ∞)	(0.00, 0.10)
$\alpha - 3\alpha^2 + \alpha^3$	(4.01, 4.15)	(0.42, 0.48)	—
$2\alpha - \alpha^2 - 2\alpha^3$	(0.00, 0.06)	(15.0, ∞)	(0.00, 0.10)
$3\alpha + \alpha^2 - \alpha^3$	(0.10, 0.15)	(2.19, 2.32)	(2.85, 4.55)
$1 - 3\alpha + \alpha^2$	(6.42, 6.48)	(0.16, 0.19)	—
$1 - 2\alpha - \alpha^2 + \alpha^3$	(0.12, 0.18)	(5.73, 5.86)	(1.08, 1.23)
$1 - 2\alpha + 2\alpha^2 + 2\alpha^3$	(1.00, ∞)	(41.1, 41.6)	(0.00, 0.03)
$1 - 2\alpha + 3\alpha^2 - \alpha^3$	(10.4, 10.6)	(1.05, 1.12)	(0.00, 0.10)
$1 - \alpha + \alpha^3$	(0.18, 0.23)	(14.6, 14.9)	(0.30, 0.39)
$1 - \alpha + \alpha^2 + 2\alpha^3$	(0.21, 0.28)	(15.0, ∞)	—
$1 + \alpha + 2\alpha^2 - \alpha^3$	(5.00, 5.10)	(0.00, 1.00)	—
$2 - 2\alpha - 2\alpha^2 + \alpha^3$	(0.73, 0.82)	(0.33, 0.41)	—
$2 - \alpha - 2\alpha^2$	(0.00, 0.05)	(13.3, 13.5)	(1.00, ∞)

References

1. B. N. Delone and D. K. Faddeev, *The Theory of Irrationalities of the Third Degree,* AMS Translations of Mathematical Monographs, Vol. 10 (1964).

2. Th. Skolem, *Ein Verfahren zur Behandlung gewisser exponentialer Gleichungen und diophantischer Gleichungen,* 8^{de} Skand. Mat. Kongress, Stockholm 1934, 163-188.

3. W. E. H. Berwick, *Algebraic number-fields with two independent units,* Proc. London Math. Soc. 34 (1932), 360-378.

4. W. Ljunggren, *On the diophantine equation $y^2 - k = x^3$,* Acta Arithmetica VIII (1963), 451-463.

University of Texas at El Paso, Texas 79968