PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 69, Number 2, May 1978

THE SOLUTION OF $3y^2 \pm 2^n = x^3$

STANLEY RABINOWITZ[1]

ABSTRACT. The diophantine equation

(*) $\qquad 3y^2 + 2^n\gamma = x^3, \quad \text{with } \gamma = \pm 1$

is solved.

Let $\theta = 2^{1/3}$, where $\theta \in$ Reals. Then $\Omega = \{a + b\theta + c\theta^2 | a, b, c \in Z\}$ is the ring of integers of $Q(\theta)$, $-1 + \theta$ is the fundamental unit of Ω and Ω is a unique factorization domain (U.F.D.) (see e.g. [3]).

All English letters (except Z, Q and N) will represent elements of Z and all lower case Greek letters elements of Ω.

$\alpha|_\Omega \beta$ and $(\alpha, \beta)_\Omega$ are read (respectively) as "α divides β in Ω" and "the greatest common divisor of α and β in Ω".

Table I is taken from [1].

TABLE I

The solution of $y^2 + v = x^3$ for some values of v.

v: Solutions $\langle x, \lvert y\rvert\rangle$	$-v$: Solutions $\langle x, \lvert y\rvert\rangle$
3: no solutions	3: $\langle 1, 2\rangle$
24: no solutions	24: $\langle -2, 4\rangle$, $\langle 1, 5\rangle$, $\langle 10, 32\rangle$, $\langle 8158, 736844\rangle$
27: $\langle 3, 0\rangle$	27: $\langle -3, 0\rangle$
54: $\langle 7, 17\rangle$	54: $\langle 3, 9\rangle$
108: no solutions	108: $\langle -3, 9\rangle$, $\langle -2, 10\rangle$, $\langle 6, 18\rangle$, $\langle 366, 7002\rangle$
216: $\langle 6, 0\rangle$, $\langle 10, 28\rangle$, $\langle 33, 189\rangle$	216: $\langle -6, 0\rangle$
432: $\langle 12, 36\rangle$	432: no solutions

Note that if (*) holds, then $n \geqslant 0$, since $2^n = \gamma(x^3 - 3y^2)$.

PROPOSITION 1. *If* (*) *holds with* $n = 3k$ *and* xy *odd, then* $\langle \gamma, n, x, |y| \rangle = \langle 1, 3, 11, 21\rangle$.

PROOF. Since $n = 3k$, $(9y)^2 + 27 \cdot 2^{3k}\gamma = (3x)^3$. Using Table I we may assume that $k > 1$. By (*), $3y^2 = ab$, where $a = x - 2^k\gamma$ and $b = x^2 + 2^k\gamma x + 2^{2k}$. Since x is odd, b is odd. $b > 0$ [3, Lemma 1] and therefore $a > 0$.

Received by the editors October 18, 1976.

AMS (MOS) subject classifications (1970). Primary 10B10.

Key words and phrases. Ring of integers, norm.

[1]This material forms a part of the author's doctoral dissertation ("On Mordell's equation $y^2 + k = x^3$, with $k = \pm 2^n 3^m$") completed in 1971 at the City University of New York/Graduate Center.

$$a = x - 2^k\gamma \equiv x^3 - 2^{3k}\gamma = 3y^2 \equiv 0 \text{ (Mod 3)}.$$

Hence $x \equiv 2^k\gamma$ (Mod 3), which implies that

$$b = x^2 + 2^k\gamma x + 2^{2k} \equiv 2^{2k} + 2^{2k} + 2^{2k} \equiv 0 \text{ (Mod 3)}.$$

Thus $9|ab = 3y^2$, implying that $3|y$. Also $(a, b)|3 \cdot 2^{2k}$ [3, Lemma 2]. Since b is odd, $(a, b) = 3$. Since $3(y/3)^2 = (a/3)(b/3)$, [3, Lemma 3] proves that

$$\langle a/3, b/3\rangle = \langle r^2, 3s^2\rangle \quad \text{or} \quad \langle 3r^2, s^2\rangle.$$

If $\langle a/3, b/3\rangle = \langle r^2, 3s^2\rangle$, then $x = 3r^2 + 2^k\gamma$ and we obtain

$$3(s^2 - 2^k\gamma r^2 - r^4) = 2^{2k},$$

which cannot hold. Therefore $\langle a/3, b/3\rangle = \langle 3r^2, s^2\rangle$. Hence s is odd, $x = 9r^2 + 2^k\gamma$, and

$$27r^4 + 9 \cdot 2^k\gamma r^2 + (2^{2k} - s^2) = 0.$$

$108s^2 - 27 \cdot 2^{2k} = d^2$ [3, Lemma 4]. Consequently $3^3 2^2 | d^2$, since $k > 1$. Thus $d = 18D$ and $s^2 - 3D^2 = 2^{2k-2}$. Therefore D is odd and it follows that $s^2 - 3D^2 \equiv -2$(Mod 8). But $4|2^{2k-2}$.

PROPOSITION 2. *If* (*) *holds with* $n = 3k + 1$ *and* xy *odd, then*

$$\langle \gamma, n, x, |y|\rangle = \langle -1, 1, 1, 1\rangle, \langle -1, 7, -5, 1\rangle \quad \textit{or} \quad \langle -1, 13, 1915, 48383\rangle.$$

PROOF. If $k = 0$, then $(9y)^2 + 54\gamma = (3x)^3$. We may assume that $k > 0$ by using Table I.

$(x, 3) = 1$, for otherwise $3|2^n$. Thus by [3, Lemma 5],

$$3y^2 = x^3 - 2^{3k+1}\gamma \equiv \pm 1 \pm 2 \quad \text{(Mod 9)}.$$

Hence $(y, 3) = 1$. By (*), $3y^2 = \alpha\beta$, where $\alpha = x - 2^k\gamma\theta$ and $\beta = x^2 + 2^k\gamma\theta x + (2^k\theta)^2$. $\beta > 0$ [3, Lemma 1] and thus $\alpha > 0$. $(\alpha, \beta)_\Omega | _\Omega 3(2^k\theta)^2$ [3, Lemma 2]. Since $(\alpha\beta, 2)_\Omega = 1$ [3, Lemma 6], $(\alpha, \beta)_\Omega | _\Omega 3 = (1 + \theta)^3(-1 + \theta)$.

By [4, (13), p. 132] and [2, Theorem 2-11, p. 48] the norm N of Ω (over Z) is

$$N(a + b\theta + c\theta^2) = a^3 + 2b^3 + 4c^3 - 6abc.$$

Now $N(1 + \theta) = 3$. Thus $1 + \theta$ is a prime of Ω [2, Theorem 2-12, 2-15, pp. 49, 53]. Also

$$x + 2^k\gamma \equiv x^3 + 2^{3k}\gamma \equiv x^3 - 2^{3k+1}\gamma = 3y^2 \equiv 0 \quad \text{(Mod 3)}.$$

Let $w = (x + 2^k\gamma)/3$. Then $\alpha = (1 + \theta)(w - 2^k\gamma - w\theta + w\theta^2)$. Therefore $1 + \theta | _\Omega \alpha$. If $(1 + \theta)^2 | _\Omega \alpha$, then $9 = N((1 + \theta)^2) | N(\alpha) = 3y^2$, contradicting $(y, 3) = 1$. Since Ω is a U.F.D. and $-1 + \theta$ is a unit of Ω, $(\alpha/(1 + \theta), \beta)_\Omega = 1$. Also

$$((1 + \theta)y)^2 = (\alpha/(1 + \theta))(\beta/(-1 + \theta)).$$

$\alpha/(1 + \theta) = \mu(a + b\theta + c\theta^2)^2$, where $\mu = 1$ or $-1 + \theta$ [3, Lemma 3]. We may assume that $a - b \geqslant 0$, since $(a + b\theta + c\theta^2)^2 = (-a - b\theta - c\theta^2)^2$.

If $\mu = 1$, then since 1, θ and θ^2 are linearly independent over Q,

$$x = a^2 + 4bc + 2b^2 + 4ac \quad \text{and} \quad -2^k\gamma = a^2 + 4bc + 2c^2 + 2ab.$$

The first equation implies that a is odd and the second that a is even (since $k > 0$). Thus $\mu = -1 + \theta$ and we have the following:

$$x = -a^2 - 4bc + 4c^2 + 4ab, \tag{1}$$

$$-2^{k-1}\gamma = -c^2 - ab + b^2 + 2ac, \tag{2}$$

and

$$0 = a^2 + 4bc - b^2 - 2ac. \tag{3}$$

By (1), a is odd. From (3) it follows that b is odd and

$$2c(a - 2b) = a^2 - b^2. \tag{4}$$

Multiplying (2) by $4(a - 2b)^2$ and using (4) we have

$$-2^{k+1}\gamma(a - 2b)^2 = 3(a - b)(a^3 - 3a^2b + 3ab^2 - 5b^3). \tag{5}$$

Let $g = (a, b) > 0$, $A = a/g$ and $B = b/g$. Thus gB is odd, $A - B \geqslant 0$ and $(A, B) = 1$. $(A - 2B, A - B) = 1$, since $2(A - B) - (A - 2B) = A$, and $(A - B) - (A - 2B) = B$. (5) yields

$$-2^{k+1}\gamma(A - 2B)^2 = 3g^2(A - B)(A^3 - 3A^2B + 3AB^2 - 5B^3). \tag{6}$$

Hence $3g^2 | (A - 2B)^2$. Thus $3g | A - 2B$. Therefore $(A - B, 3) = 1$ and $A + B \equiv A - 2B \equiv 0$ (Mod 3). Consequently $(A - 2B, A + B) = 3$, since $(A - 2B) + 2(A + B) = 3A$ and $(A + B) - (A - 2B) = 3B$. It follows from (4) that

$$2c \cdot (A - 2B)/3g = (A - B) \cdot (A + B)/3.$$

Hence $A - 2B = \pm 3g$. By (6),

$$-3 \cdot 2^{k+1}\gamma = (A - B)(A^3 - 3A^2B + 3AB^2 - 5B^3). \tag{7}$$

Therefore $A - B = 2^r$, where $0 \leqslant r \leqslant k + 1$. (7) implies that

$$-3 \cdot 2^{k+1-r}\gamma = (A - B)^3 - 4B^3 = 2^{3r} - 4B^3.$$

Thus $r \neq 0$. Therefore $3r > 2$. Hence $k + 1 - r = 2$ [3, Lemma 7] and we have

$$2^{3r-2} + 3\gamma = B^3. \tag{8}$$

If $r = 2t$, then $(2^{3t-1})^2 + 3\gamma = B^3$. There are no solutions in this case by Table I. Thus $r = 2t + 1$ and by (8),

$$(2^{3t+2})^2 + 24\gamma = (2B)^3.$$

Using Table I, $\gamma = -1$ and $\langle 2B, 2^{3t+2} \rangle = \langle -2, 4 \rangle$ or $\langle 10, 32 \rangle$.

If $\langle 2B, 2^{3t+2} \rangle = \langle -2, 4 \rangle$, then $B = -1$, $t = 0$, $r = 2t + 1 = 1$, $A = B + 2^r = 1$, $k = 1 + r = 2$ and $n = 3k + 1 = 7$. Since $\pm 3g = A - 2B = 3$ and $g > 0$, $g = 1$, $a = gA = 1$ and $b = gB = -1$. By (4), (1) and (*), $c = 0$, $x = -5$ and $|y| = 1$.

If $\langle 2B, 2^{3t+2} \rangle = \langle 10, 32 \rangle$ we obtain similarly, $k = 4$, $x = 1915$ and $|y| = 48383$.

PROPOSITION 3. *If* (*) *holds with* $n = 3k + 2$ *and* xy *odd, then* $\langle \gamma, n, x, |y| \rangle = \langle -1, 2, -1, 1 \rangle$ *or* $\langle -1, 8, 11, 23 \rangle$.

PROOF. If $k = 0$, then $(9y)^2 + 108\gamma = (3x)^3$. The solution of this equation is given in Table I. Thus we may assume that $k > 0$.

$(x, 3) = 1$. By [3, Lemma 5], $3y^2 = x^3 - 2^{3k+2}\gamma \equiv \pm 1 \pm 4 \pmod 9$. Thus $(y, 3) = 1$. By (*), $3y^2 = \alpha\beta$, where

$$\alpha = x - 2^k\gamma\theta^2 \quad \text{and} \quad \beta = x^2 + 2^k\gamma\theta^2 x + (2^k\theta^2)^2.$$

As in Proposition 2, $\alpha > 0$ and $(\alpha, \beta)_{\Omega|\Omega}3 = (1 + \theta)^3(-1 + \theta)$. Also

$$x - 2^k\gamma \equiv x^3 - 2^{3k}\gamma \equiv x - 2^{3k+2}\gamma = 3y^2 \equiv 0 \pmod 3.$$

Let $u = (x - 2^k\gamma)/3$. Then $\alpha = (1 + \theta)(x - 2u + (2u - x)\theta + u\theta^2)$. Following the argument of Proposition 2 we see that since $N(\alpha) = 3y^2$, $\alpha/(1 + \theta) = \mu(a + b\theta + c\theta^2)^2$, where $\mu = 1$ or $-1 + \theta$, and $c \geqslant 0$.

If $\mu = 1$, then

$$x = a^2 + 4bc + 2b^2 + 4ac \quad \text{and} \quad 0 = a^2 + 4bc + 2c^2 + 2ab.$$

The first equation implies that a is odd and the second that a is even. Hence $\mu = -1 + \theta$. Consequently

$$x = -a^2 - 4bc + 4c^2 + 4ab, \tag{9}$$

$$0 = -c^2 - ab + b^2 + 2ac, \tag{10}$$

and

$$-2^k\gamma = a^2 + 4bc - b^2 - 2ac. \tag{11}$$

a is odd by (9). Therefore since $k > 0$, b is odd by (11). (10) implies

$$a(b - 2c) = b^2 - c^2. \tag{12}$$

Multiplying (11) by $-(b - 2c)^2$ and applying (12) yields

$$2^k\gamma(b - 2c)^2 = 3c(c^3 - 6bc^2 + 6b^2c - 2b^3). \tag{13}$$

Let $g = (b, c) > 0$, $B = b/g$ and $C = c/g$. Therefore gB is odd, $C \geqslant 0$, $(B, C) = 1$ and by (13),

$$2^k\gamma(B - 2C)^2 = 3g^2C(C^3 - 6BC^2 + 6B^2C - 2B^3). \tag{14}$$

As in Proposition 2, $(B - 2C, B - C) = 1$, $3g|B - 2C$, and $(B - 2C, B + C) = 3$. Thus $(C, 3) = 1$. It follows from (12) that

$$a \cdot (B - 2C)/3g = (B - C) \cdot (B + C)/3.$$

Therefore $B - 2C = \pm 3g$. By (14),

$$3 \cdot 2^k\gamma = C(C^3 - 6BC^2 + 6B^2C - 2B^3).$$

Hence $C = 2^r$, where $0 \leqslant r \leqslant k$. Thus

$$3 \cdot 2^{k-r}\gamma = 2^{3r} - 3 \cdot 2^{2r+1}B + 3 \cdot 2^{r+1}B^2 - 2B^3. \tag{15}$$

$r \neq 0$, since $k > 0$. Therefore $3r \geqslant 2r + 1 > r + 1 \geqslant 2$. By (15), $k - r = 1$ and

$$2^{3r-1} + 3\gamma = (2^r - B)^3. \tag{16}$$

If $r = 2t$, then $(2^{3t+1})^2 + 24\gamma = (2(2^r - B))^3$. There are no solutions of this equation by Table I. Thus $r = 2t + 1$ and (16) becomes

$$(2^{3t+1})^2 + 3\gamma = (2^r - B)^3.$$

Using Table I we find that $\gamma = -1$, $2^{3t+1} = 2$, and $2^r - B = 1$. Therefore $t = 0$, $r = 2t + 1 = 1$, $B = 2^r - 1 = 1$, $C = 2^r = 2$, $k = r + 1 = 2$, and $\pm 3g = B - 2C = -3$. Hence $g = 1$, $b = gB = 1$, $c = gC = 2$, and by (10), $a = 1$. By (9), $x = 11$ and finally $3y^2 = x^3 - 2^{3k+2}\gamma = 3(23)^2$.

THEOREM. *All the solutions of* (*) *are given in Table* II, *where* $x = 2^g e$ *and* $y = \pm 2^h f$.

EXPLANATION OF TABLE II. n is given modulo 6 and is nonnegative. If $f = 0$, the value of h is irrelevant. The solutions are numbered for reference in the proof.

TABLE II

γ	n (modulo 6)		$3g$	e	$2h$	f	Solution number
1	0		n	1	–	0	1
1	3		n	1	–	0	2
1	3		$n-3$	11	$n-3$	21	3
1	4		$n+2$	1	n	1	4
−1	0		n	−1	–	0	5
−1	1		$n-1$	1	$n-1$	1	6
−1	1	$(n \geqslant 7)$	$n-7$	−5	$n-7$	1	7
−1	1	$(n \geqslant 13)$	$n-13$	1915	$n-13$	48383	8
−1	2		$n-2$	−1	$n-2$	1	9
−1	2	$(n \geqslant 8)$	$n-8$	11	$n-8$	23	10
−1	2		$n+1$	1	n	1	11
−1	2		$n+1$	61	n	389	12
−1	3		n	−1	–	0	13

PROOF. By direct calculation the above can be shown to be solutions of (*).

Suppose now that (*) holds. Obviously $x \neq 0$. If $y = 0$, then $x^3 = 2^n\gamma$ and therefore $3|n$. Thus solution 1, 2, 5 or 13 holds.

Assume that $y \neq 0$. Therefore $x = 2^g e$ and $y = 2^h f$, where ef is odd. By (*),

$$3 \cdot 2^{2h} f^2 + 2^n\gamma = 2^{3g} e^3. \tag{17}$$

It follows from [3, Lemma 7] that

$$2h = 3g < n, \tag{18}$$

$$2h = n < 3g, \tag{19}$$

or

$$3g = n < 2h. \tag{20}$$

If (18), then $2h = 3g = 6w$. By (17), $3f^2 + 2^{n-6w}\gamma = e^3$. Propositions 1, 2 and 3 imply that solution 3, 6, 7, 8, 9 or 10 must hold.

If (19), then $n = 6w + 2i$, where $i = 0$, 1 or 2. By (17), $(9 \cdot 2^i f)^2 + 27 \cdot 2^{2i}\gamma = (3 \cdot 2^{g-2w} e)^3$. By Table I, solution 4, 11 or 12 holds.

If (20), then $n = 6w + 3j$, where $j = 0$ or 1. By (17),

$$(9 \cdot 2^{h-3w}f)^2 + 27 \cdot 2^{3j}\gamma = (3 \cdot 2^j e)^3.$$

There are no solutions by Table I.

NOTE ADDED IN PROOF. I wish to thank Professor N. M. Stephens for informing me that the results of my doctoral dissertation, from which this paper and [3] are taken, were also determined by Professor F. B. Coghlan in his doctoral dissertation "*Elliptic curves with conductor* $N = 2^m3^n$" completed in 1967 at Manchester.

REFERENCES

1. O. Hemer, *On the Diophantine equation* $y^2 - k = x^3$, Thesis, Univ. of Uppsala, Almqvist & Wiksells, Uppsala, 1952. MR **14**, 354.

2. W. J. LeVeque, *Topics in number theory*, Vol. II, Addison-Wesley, Reading, Mass., 1961.

3. S. Rabinowitz, *The solution of* $y^2 \pm 2^n = x^3$, Proc. Amer. Math. Soc. **62** (1977), 1–6.

4. B. L. van der Waerden, *Modern algebra*, Vol. I, Ungar, New York, 1949.

DEPARTMENT OF MATHEMATICS AND COMPUTER SCIENCE, KINGSBOROUGH COMMUNITY COLLEGE/CUNY, BROOKLYN, NEW YORK 11235