PROCEEDINGS OF THE
AMERICAN MATHEMATICAL SOCIETY
Volume 62, Number 1, January 1977

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

STANLEY RABINOWITZ[1]

ABSTRACT. All solutions to the diophantine equation

$$(*) \qquad y^2 + \gamma 2^n = x^3; \qquad \gamma = \pm 1,$$

are found.

The solution of $(*)$, with $n = \gamma = 1$, is due to Euler [4], [6, p. 103]. His was the first solution of a diophantine equation of the form $y^2 - k = x^3$, where the given value of k is neither the square nor the cube of an integer. Table I is from [5].

TABLE I. The solution of $(*)$ in some special cases

	$\gamma = 1$		$\gamma = -1$
n	$\langle x, \|y\|\rangle$	n	$\langle x, \|y\|\rangle$
0	$\langle 1, 0\rangle$	0	$\langle -1, 0\rangle, \langle 0, 1\rangle, \langle 2, 3\rangle$
1	$\langle 3, 5\rangle$	1	$\langle -1, 1\rangle$
2	$\langle 2, 2\rangle, \langle 5, 11\rangle$	2	$\langle 0, 2\rangle$
3	$\langle 2, 0\rangle$	3	$\langle -2, 0\rangle, \langle 1, 3\rangle, \langle 2, 4\rangle, \langle 46, 312\rangle$
4	no solutions	4	$\langle 0, 4\rangle$

DEFINITIONS: Let $\theta = 2^{1/3}$; θ real. Then by [6, p. 105], $\Omega = \{a + b\theta + c\theta^2 | a, b, c \in Z\}$ is the ring of integers of $Q(\theta)$. The class number of Ω is 1 [1, p. 427] and therefore Ω is a unique factorization domain (U.F.D.).

Λ will be either Z or Ω. Hence Λ is real.

All Latin letters (except Z and Q) will represent elements of Z and all lower case Greek letters elements of Λ.

The units of Λ are $\pm\varepsilon^r$ $(r \in Z)$; $\varepsilon = 1$ for $\Lambda = Z$ and $\varepsilon = -1 + \theta$ for $\Lambda = \Omega$ [6, p. 112], [3, p. 304]. Note that $\varepsilon > 0$. Let $\gamma = \pm 1$.

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

LEMMA 1. *If $\alpha \neq 0$ or $\beta \neq 0$, then $\alpha^2 + \alpha\beta + \beta^2 > 0$.*

PROOF. $4(\alpha^2 + \alpha\beta + \beta^2) = (2\alpha + \beta)^2 + 3\beta^2$.

Received by the editors February 10, 1976.

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

Key words and phrases. Diophantine equation, ring of integers, class number, unique factorization domain, greatest common divisor.

[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.

LEMMA 2. $(\alpha + \beta, \alpha^2 - \alpha\beta + \beta^2)_\Lambda |_\Lambda 3\beta^2$.

PROOF. $(2\beta - \alpha)(\alpha + \beta) + (\alpha^2 - \alpha\beta + \beta^2) = 3\beta^2$.

LEMMA 3. *If* $\varphi^2 = \alpha\beta$, $(\alpha, \beta)_\Lambda = 1$ *and* $\alpha > 0$, *then* $\alpha = \mu\xi^2$; $\mu = 1$ *or* ε.

PROOF. Since Λ is a U.F.D. and $\alpha > 0$, $\alpha = \varepsilon^r\psi^2$. If $r = 2t$, let $\mu = 1$, $\xi = \varepsilon^t\psi$. If $r = 2t + 1$, let $\mu = \varepsilon$, $\xi = \varepsilon^t\psi$.

LEMMA 4. *If* $as^2 + bs + c = 0$, *then* $b^2 - 4ac = d^2$.

PROOF. Let $d = 2as + b$.

LEMMA 5. *If* $(x, 3) = 1$, *then* $x^3 \equiv \pm 1 \pmod 9$.

PROOF. $x = \pm 1 + 3k$. Thus $x^3 = (\pm 1 + 3k)^3 \equiv (\pm 1)^3 = \pm 1 \pmod 9$.

LEMMA 6. *If* $(a, b) = 1$, *then* $(a, b)_\Omega = 1$.

PROOF. There exist integers e and f such that $ea + fb = 1$.

LEMMA 7. *If* $2^x a + 2^y b + 2^z c = 0$, *where* $(abc, 2) = 1$, *and* $0 \leqslant x \leqslant y \leqslant z$, *then* $x = y < z$.

PROOF. $2^y | 2^x a$. Thus $x \geqslant y$.
If $y = z$, then $a + b + c = 0$. But $a + b + c$ is odd.
Note that if $(*)$ holds, then, since $2^n = \gamma(x^3 - y^2)$, $n \geqslant 0$.

PROPOSITION 1.

$y^2 + 2^{3k} = x^3$; x *odd* $\Rightarrow \langle k, x, |y|\rangle = \langle 0, 1, 0\rangle$.

$y^2 - 2^{3k} = x^3$; x *odd* $\Rightarrow \langle k, x, |y|\rangle = \langle 0, -1, 0\rangle, \langle 1, 1, 3\rangle$ *or* $\langle 3, -7, 13\rangle$.

PROOF. Using Table I, we may assume that $k > 1$. Now

$$y^2 = ab; \qquad a = x - \gamma 2^k, \;\; b = x^2 + \gamma 2^k x + 2^{2k}.$$

Hence $(ab, 2) = 1$. By Lemma 1, $b > 0$. Therefore $a > 0$. By Lemma 2, $(a, b) | 3 \cdot 2^{2k}$. Thus $(a, b) = 1$ or 3.

Suppose first that $(a, b) = 3$. Then $3 | y$ and $(y/3)^2 = (a/3)(b/3)$. By Lemma 3, $a = 3u^2$ and $b = 3v^2$. Hence v is odd. Eliminating x from the latter two equations,

$$3u^4 + \gamma 3 \cdot 2^k u^2 + (2^{2k} - v^2) = 0.$$

Thus by Lemma 4, $12v^2 - 3 \cdot 2^{2k} = d^2$. Therefore $d = 2D$ and since $k > 1$, $3v^2 - D^2 = 3 \cdot 2^{2k-2} \equiv 0 \pmod 4$. But since v is odd, D is odd and, hence, $3v^2 - D^2 \equiv 2 \pmod 4$.

Thus $(a, b) = 1$. Therefore $a = u^2$ and $b = v^2$, implying $(uv, 2) = 1$. Eliminating x,

$$u^4 + 3 \cdot 2^k \gamma u^2 + (3 \cdot 2^{2k} - v^2) = 0. \tag{1}$$

By Lemma 4, $4v^2 - 3 \cdot 2^{2k} = d^2$. Thus $d = 2D$ and

$$v^2 - D^2 = 3 \cdot 2^{2k-2}. \tag{2}$$

Since $k \geqslant 2$ and v is odd, D is odd. Also $3|(v - D)(v + D)$. Let $V = \pm v$ where $3|V - D$. By (2), $V - D = 3 \cdot 2^s\delta$ and $V + D = 2^t\delta$; $s + t = 2k - 2$ and $\delta = \pm 1$. Since $(DV, 2) = 1$, $s \geqslant 1$ and $t \geqslant 1$. Hence

$$D = \delta(2^{t-1} - 3 \cdot 2^{s-1}). \tag{3}$$

Thus either ($t > 1$ and $s = 1$) or ($t = 1$ and $s > 1$). Solving (1) for u^2,

$$u^2 = -\gamma 3 \cdot 2^{k-1} \pm D. \tag{4}$$

Suppose first that $t > 1$ and $s = 1$. Hence $t = 2k - 3$ and by (3), $D = \delta(2^{2k-4} - 3)$. Thus $k > 2$ and by (4),

$$u^2 = -\gamma 3 \cdot 2^{k-1} \pm (2^{2k-4} - 3).$$

If $k > 3$, $u^2 \equiv \pm 3 \pmod 8$. Therefore $k = 3$ and $u^2 = \pm 12 \pm 1$, which is impossible.

Thus $t = 1$ and $s > 1$. Hence $s = 2k - 3$ and by (3), $D = \delta(1 - 3 \cdot 2^{2k-4})$. Thus $k > 2$ and by (4),

$$u^2 = \pm(1 - 3 \cdot 2^{2k-4}) - \gamma 3 \cdot 2^{k-1}. \tag{5}$$

The first minus sign cannot hold modulo 3.

If $\gamma = 1$, then $u^2 < 0$. Hence $\gamma = -1$. By (5), $u^2 = 3(2^{k-1} - 2^{2k-4}) + 1$.

If $k > 3$, then $2k - 4 > k - 1$ and thus $u^2 < 0$. Hence $k = 3$ and $u^2 = 1$. Since $a = u^2$, $x = u^2 - 2^k = -7$. Therefore $y^2 = x^3 + 2^{3k} = 169$.

PROPOSITION 2.

$$y^2 + 2^{3k+1} = x^3; \quad x \textit{ odd} \Rightarrow \langle k, x, |y| \rangle = \langle 0, 3, 5 \rangle.$$

$$y^2 - 2^{3k+1} = x^3; \quad x \textit{ odd} \Rightarrow \langle k, x, |y| \rangle = \langle 0, -1, 1 \rangle \textit{ or } \langle 2, 17, 71 \rangle.$$

PROOF. Suppose $3|y$. Then $(x, 3) = 1$ and by Lemma 5,

$$0 \equiv y^2 = x^3 \pm 2 \cdot 8^k \equiv \pm 1 \pm 2 \pmod 9.$$

This contradiction shows that $(y, 3) = 1$. Obviously y is odd and so by Lemma 6, $(y, 6)_\Omega = 1$. By Table I we may assume that $k > 0$. Now

$$y^2 = \alpha\beta; \qquad \alpha = x - \gamma 2^k\theta, \quad \beta = x^2 + \gamma 2^k\theta x + (2^k\theta)^2.$$

By Lemma 1, $\beta > 0$ and thus $\alpha > 0$. By Lemma 2, $(\alpha, \beta)_\Omega|_\Omega 3(2^k\theta)^2$. But $(\alpha\beta, 6)_\Omega = 1$. Hence $(\alpha, \beta)_\Omega = 1$. By Lemma 3,

$$\alpha = \mu(a + b\theta + c\theta^2)^2; \qquad \mu = 1 \quad \text{or} \quad -1 + \theta.$$

We may assume that $c \geqslant 0$ since $\alpha = \mu(-a - b\theta - c\theta^2)^2$.

If $\mu = -1 + \theta$, we obtain

$$x = -a^2 - 4bc + 2b^2 + 4ac \quad (\Rightarrow a \text{ is odd})$$

and

$$-\gamma 2^k = -2c^2 - 2ab + a^2 + 4bc \quad (\Rightarrow a \text{ is even, since } k > 0).$$

Hence $\mu = 1$. Therefore

$$x = a^2 + 4bc \quad (\Rightarrow a \text{ is odd}), \tag{6}$$

(7) $$-\gamma 2^{k-1} = c^2 + ab,$$

and

(8) $$0 = b^2 + 2ac \quad (\Rightarrow b \text{ is even}).$$

If $b = 0$, then by (8), $c = 0$. This contradicts (7). Thus $b = 2^s B$; $s \geqslant 1$ and B is odd. From (8), $c = 2^{2s-1}C$; C odd. $C > 0$, since $c \geqslant 0$. By (8) and (7),

(9) $$0 = B^2 + aC$$

and

(10) $$-\gamma 2^{k-1} = 2^{4s-2}C^2 + 2^s aB.$$

Let p be a prime of Z. If $p|C$, then by (9), $p|B$ and by (10), $p|2^{k-1}$. Therefore $C = 1$. Hence $a = -B^2$ and $-\gamma 2^{k-1} = 2^{4s-2} - 2^s B^3$. Since $s \geqslant 1$, $4s - 2 > s$. By Lemma 7, $k - 1 = s$. Hence $(-\gamma)^3 + B^3 = 2(2^{s-1})^3$. [2, pp. 70–72] gives $B = -\gamma = 2^{s-1}$. Thus $\gamma = -1$, $B = 1$, $s = 1$, $k = 2$, $a = -1$, $c = 2$ and $b = 2$. By (6), $x = 17$ and therefore $|y| = 71$.

PROPOSITION 3.

$$y^2 + 2^{3k+2} = x^3; \quad x \textit{ odd} \Rightarrow \langle k, x, |y| \rangle = \langle 0, 5, 11 \rangle.$$

$$y^2 - 2^{3k+2} = x^3; \quad x \textit{ odd, has no solutions.}$$

PROOF. Assume $k > 0$ (see Table I).

$$y^2 = \alpha\beta; \qquad \alpha = x - \gamma 2^k \theta^2, \quad \beta = x^2 + \gamma 2^k \theta^2 x + (2^k \theta^2)^2.$$

As in Proposition 2, $\alpha = \mu(a + b\theta + c\theta^2)^2$; $\mu = 1$ or $-1 + \theta$ and $b \geqslant 0$.

If $\mu = -1 + \theta$, then

$$x = -a^2 - 4bc + 2b^2 + 4ac \quad (\Rightarrow a \text{ is odd})$$

and

$$0 = -2c^2 - 2ab + a^2 + 4bc \quad (\Rightarrow a \text{ is even}).$$

Thus $\mu = 1$ and

(11) $$x = a^2 + 4bc \quad (\Rightarrow a \text{ is odd}),$$

(12) $$0 = c^2 + ab,$$

and

(13) $$-\gamma 2^k = b^2 + 2ac \quad (\Rightarrow b \text{ is even}).$$

By (12), c is even.

If $c = 0$, then by (12), $b = 0$. But this contradicts (13). Thus $c = 2^s C$; $s \geqslant 1$ and C odd. By (12), $b = 2^{2s}B$; B odd. Therefore $B > 0$. By (12) and (13), $0 = C^2 + aB$ and

$$-\gamma 2^k = 2^{4s}B^2 + 2^{s+1}aC.$$

As in Proposition 2, $B = 1$. Hence $a = -C^2$ and $-\gamma 2^k = 2^{4s} - 2^{s+1}C^3$. Since $4s > s + 1$, $k = s + 1$ and $(-\gamma)^3 + C^3 = 4(2^{s-1})^3$. This equation has no solutions by [2, pp. 70–72].

THEOREM. *All the solutions of* (∗) *are given in the following table with* $x = 2^g e$ *and* $y = \pm 2^h f$.

EXPLANATION OF TABLE II. If $e = 0$ (respectively $f = 0$), then the value of g (respectively h) is irrelevant. n is given modulo 6 and is nonnegative.

The solutions are numbered for reference in the proof.

TABLE II

$\gamma = 1$

n (modulo 6)	$3g$	e	$2h$	f	Solution Number
0	n	1	–	0	1
1	$n-1$	3	$n-1$	5	2
2	$n+1$	1	n	1	3
2	$n-2$	5	$n-2$	11	4
3	n	1	–	0	5

$\gamma = -1$

n (modulo 6)	$3g$	e	$2h$	f	Solution Number
0	n	-1	–	0	6
0	–	0	n	1	7
0	$n+3$	1	n	3	8
1	$n-1$	-1	$n-1$	1	9
1 ($n > 7$)	$n-7$	17	$n-7$	71	10
2	–	0	n	1	11
3 ($n > 9$)	$n-9$	-7	$n-9$	13	12
3	n	-1	–	0	13
3	$n-3$	1	$n-3$	3	14
3	n	1	$n+1$	1	15
3	n	23	$n+3$	39	16
4	–	0	n	1	17

PROOF. By direct calculation the above can be shown to be solutions. Suppose now that (∗) holds.

If $x = 0$, then $\gamma = -1$ and $y^2 = 2^n$. Therefore n is even implying solution 7, 11 or 17.

If $y = 0$, then $3 | n$ yielding solution 1, 5, 6 or 13.

Suppose now that $xy \neq 0$. Therefore $x = 2^g e$ and $|y| = 2^h f$; ef odd. By (∗),

$$2^{2h} f^2 + \gamma 2^n = 2^{3g} e^3. \tag{14}$$

By Lemma 7,

$$2h = 3g < n, \tag{15}$$

$$2h = n < 3g, \tag{16}$$

or

$$3g = n < 2h. \tag{17}$$

If (15), then $2h = 3g = 6q$ and by (14), $f^2 + \gamma 2^{n-6q} = e^3$. Propositions 1, 2 and 3 imply solution 2, 4, 14, 12, 9 or 10.

If (16), then $n = 6w + 2i$; $i = 0$, 1 or 2. So $(2^i f)^2 + \gamma 2^{2i} = (2^{g-2w}e)^3$. Table I gives solution 3 or 8.

If (17), then $n = 6w + 3j$; $j = 0$ or 1. So $(2^{h-3w}f)^2 + \gamma 2^{3j} = (2^j e)^3$. Table I yields solution 15 or 16.

References

1. Z. I. Borevich and I. R. Shafarevich, *Number theory*, Academic Press, New York, 1966. MR **33** #4001.

2. R. D. Carmichael, *The theory of numbers and Diophantine analysis*, Dover, New York, 1959. MR **21** #4123.

3. B. N. Delone and D. K. Faddeev, *The theory of irrationailities of the third degree*, Transl. Math. Monographs, vol. 10, Amer. Math. Soc., Providence, R. I., 1964. MR **28** #3955.

4. L. Euler, Comm. Acad. Petrop. **10** (1738), 145; Comm. Arith. Coll. I, 33–34; Opera Omnia, (1), II, 56–58.

5. O. Hemer, *On the diophantine equation* $y^2 - k = x^3$, Doctoral dissertation, Uppsala, 1952.

6. W. J. Le Veque, *Topics in number theory*, Vol. II, Addison-Wesley, Reading, Mass., 1961.

Current address: Department of Mathematics and Computer Science, Kingsborough Community College (CUNY), Brooklyn, New York 11235.