JOURNAL OF NUMBER THEORY 50, 286–298 (1995)

On the Equation $x^4 + mx^2y^2 + y^4 = z^2$

ANDREW BREMNER AND JOHN W. JONES*

Department of Mathematics, Arizona State University, Tempe, Arizona 85287-1804

Submitted by A. C. Woods

Received October 27, 1992; revised January 25, 1993

By relating the title equation to an elliptic curve E and performing calculations with the L-series of E, we are able (subject to the standard conjectures) to determine solvability in rationals of the title equation for all m in the range $|m| \leqslant 3000$. A wild assertion of Euler is corrected, a table of solutions given for $|m| \leqslant 200$, and statistical information tabulated concerning the distribution of Mordell–Weil ranks and conjectural orders of Shafarevich–Tate groups.

1

The equation

$$a^4 + ma^2b^2 + b^4 = c^2, \qquad (a, b) = 1,\ a, b > 0, \tag{1}$$

has been studied by several mathematicians since the 17th century. A solution of (1) is said to be trivial if either $ab = 0$ or $a = b = 1$, which can occur only when m is of the form $k^2 - 2$. Fermat, around 1637, showed there are no nontrivial solutions of (1) for $m = 0$. Euler [5] showed that, for $m = 14$, there are only trivial solutions of (1); he also found nontrivial solutions for 47 values of m between 2 and 200, and for 73 values of $-m$ between 2 and 200. Pocklington [7], Sinha [9], and Zhang [12] produced classes of m for which (1) has no nontrivial solutions; and Brown [1] completed the determination of solvability of (1) in the range $0 \leqslant m \leqslant 100$. (Euler had missed precisely one solvable instance, namely $m = 85$.) By relating (1) to the elliptic curve

$$E: Y^2 = X(X^2 + mX + 1) \tag{2}$$

and performing calculations with the L-series of E, we are able, subject to all the standard conjectures, to determine solvability of (1) for all m in the range $|m| \leqslant 3000$. We correct a wild assertion of Euler and actually give a

* This author is partially supported by NSF Grant DMS-9100238.

0022-314X/95 $6.00

table of solutions of (1) (which has been lacking to date) for the solvable cases in the range $|m| \leqslant 200$. Some statistical information is tabulated concerning the distribution of Mordell–Weil ranks and (conjectural) orders of Shafarevich–Tate groups. A surprisingly high proportion of nonzero ranks is found, cf. Brumer and McGuinness [2] and Zagier and Kramarz [11]. Finally, we draw attention to a curious property of some sums expected to be transcendental, which appear to be rational.

2

Equation (2) defines an elliptic curve E for $m \neq \pm 2$, which restriction on m we henceforth assume. The rational points on E form a finitely generated Abelian group known as the Mordell–Weil group of E; the study of these groups and their associated rank is one of the fundamental topics in the theory of elliptic curves. Integers a, b, c satisfying (1) imply the existence of a rational point $(a^2/b^2, ac/b^3)$ on the curve (2); and it is easy to verify that this point is of infinite order on E precisely when the solution (a, b, c) is nontrivial. Conversely, a rational point P of infinite order on (2) is necessarily of type $(\alpha^2, \alpha\gamma)$ or $(-\alpha^2, \alpha\gamma)$ for rational numbers α, γ, with $\alpha \neq 0, 1, \infty$ (and the latter type can only occur when $m > 0$). If $P = (\alpha^2, \alpha\gamma)$ then we immediately obtain a nontrivial solution of (1), and if $P = (-\alpha^2, \alpha\gamma)$, then $2P$ provides a nontrivial solution of (1) with $(a, b) = (\alpha^4 - 1, 2\alpha\gamma)$.

So nontrivial solutions of (1) occur precisely when the Mordell–Weil rank of (2) is strictly positive.

We estimate the rank r of the curve E by the following formula concerning the L-series $L_E(s)$ of E. We assume the Taniyama–Weil conjecture that in particular E is modular (for any fixed m, it is a finite calculation to verify this), and take on faith the Birch and Swinnerton–Dyer conjectures, which then imply (see, for instance, Tate [10])

$$\lim_{s \to 1} \frac{L_E(s)}{(s-1)^r} = \omega \cdot c \cdot \frac{|Ш| \cdot \det \langle P_i, P_j \rangle}{|\mathrm{Tor}\,(E)|^2}, \tag{3}$$

where ω is the real period of E, c is a constant depending on the primes p of bad reduction of E (the "fudge-factor"), Ш is the Shafarevich–Tate group, conjecturally of finite order, $\langle P_i, P_j \rangle$ is the canonical height pairing on a system of generators $\{P_i\}$ for the Mordell–Weil group $E(\mathbf{Q})$, and $\mathrm{Tor}(E)$ is the torsion group of E (the reader is referred to Silverman [8] for a full definition and description of the foregoing arithmetic invariants of the elliptic curve E). In particular, $L_E(s)$ has a zero of order r at $s = 1$ (the "weak" Birch and Swinnerton–Dyer conjecture).

Put $\Lambda(s) = N^{s/2}(2\pi)^{-s}\Gamma(s)L_E(s)$, where N is the conductor of E. The curve E being modular says that its L-series is the L-function of a modular form of weight 2, so is entire and has a functional equation which may be written

$$\Lambda(s) = \varepsilon\Lambda(2-s), \tag{4}$$

where $\varepsilon = \pm 1$ is known as the sign of the functional equation. There are standard rapidly convergent series that allow estimation of $L_E(1)$ and the derivatives $L_E^{(k)}(1)$ for $k \geqslant 1$; see, for example, Buhler and Gross [3], and Buhler *et al.* [4]. Namely, put

$$L_E(s) = \sum_{n \geqslant 1} \frac{a_n}{n^s}; \tag{5}$$

then

$$L_E(1) = \sum_{n \geqslant 1} \frac{a_n}{n}\left(e^{-2\pi nx/\sqrt{N}} + \varepsilon e^{-2\pi n/x\sqrt{N}}\right), \tag{6}$$

where x is any positive real number (note that this formula allows a simple means of computing the sign ε). Further,

$$L_E^{(k)}(1) = 2k! \sum_{n=1}^{\infty} \frac{a_n}{n} G_k\left(\frac{2\pi n}{\sqrt{N}}\right),$$

where

$$G_k(t) = \frac{1}{(k-1)!}\int_1^{\infty} e^{-ty}(\log y)^{k-1}\frac{dy}{y} \qquad (k \geqslant 1),$$

from which can be obtained (see [3])

$$L_E'(1) = \sum_{n \geqslant 1} \frac{a_n}{n}\left(G\left(\frac{2\pi nx}{\sqrt{N}}\right) - \varepsilon G\left(\frac{2\pi n}{x\sqrt{N}}\right)\right) \tag{7}$$

where $G(t)$ is the exponential integral function

$$G(t) = \int_1^{\infty} \frac{e^{-tu}}{u}\,du,$$

and again x is any positive real number.

Our procedure for performing the calculations was as follows. For a given m, first compute the sign ε, using (6). First, if $\varepsilon = +1$, then (6) with $x = 1$ collapses to

$$L_E(1) = 2\sum_{n \geqslant 1} \frac{a_n}{n} e^{-2\pi n/\sqrt{N}} \tag{8}$$

and so $L_E(1)$ can be computed to any desired degree of accuracy. If $L(1) \neq 0$, then the rank is zero, and the conjectural order of $|Ш|$ can be calculated from (3). If $L_E(1) = 0$, then the rank, which is even, is thus at least 2. Over the range of computations, there are no instances of rank 4 or greater, which was verified by calculating $L_E^{(2)}(1)$.

Second, if $\varepsilon = -1$, then necessarily the rank, which is odd, is at least 1. From (7) with $x = 1$, we have

$$L'_E(1) = 2 \sum_{n \geq 1} \frac{a_n}{n} G\left(\frac{2\pi n}{\sqrt{N}}\right); \tag{9}$$

if $L'_E(1) \neq 0$, then the rank is precisely one, and if $L'_E(1) = 0$, then the rank is at least 3. Over the range of the computations, there are no instances of rank 5 or greater, verified by calculating $L_E^{(3)}(1)$.

Pari-GP was used for the programming, and the calculations were performed on a DEC 5000 work station. Accuracy was such that values of the sums either were quite far from zero (nearly always larger than 1, for instance), or else equal to zero to about six decimal places; we have confidence that the sums equal to zero are identified correctly.

3

Much information is available that we do not actually list here, for instance, a specific list of values of m in the range $|m| \leqslant 3000$ for which (1) is solvable. We content ourselves with mentioning those m in the range for which (2) has rank 3, namely $m = -2916, -1115, -676, 716, 863, 1024, 1311, 1448, 1492, 1584, 1724, 2208, 2506, 2714$.

Table I lists the distribution of ranks of the curve (2) in the range $1 \leqslant m \leqslant 3000$, $m \neq 2$; about 20.95% of curves where the sign of the functional equation is $+1$ have rank 2. Table II gives the distribution of $|Ш|$ amongst the rank 0 curves of Table I. Table III lists the distribution of ranks of (2) in the range $-3000 \leqslant m \leqslant -1$, $m \neq -2$; about 11.22% of curves where the sign of the functional equation is $+1$ have rank 2. Table IV gives the distribution of $|Ш|$ amongst the rank 0 curves of Table III. In accordance with these rank calculations, Table V lists precisely those m in the range considered by Euler (namely $-200 \leqslant m \leqslant 200$) for which there exists a nontrivial solution of (1), and gives a single solution in the case $r = 1$, and a pair of solutions in the case $r = 2$. These solutions in fact correspond to generators for the respective Mordell–Weil group of (2), with the exception of the three instances $m = 99, 155, 195$, where the listed solution corresponds to twice a generator (having a negative value of x).

TABLE I

$(m > 0)$

Rank	Curves (2) with this rank
0	1204 (40.15%)
1	1465 (48.85%)
2	319 (10.64%)
3	11 (0.37%)

TABLE II

Distribution of |Ш| Among Rank 0 Curves of Table I

|Ш|	No.	|Ш|	No.
1	246	25	4
4	664	36	18
9	40	49	0
16	228	64	4

TABLE III

$(m < 0)$

Rank	Curves (2) with this rank
0	1322 (44.08%)
1	1507 (50.25%)
2	167 (5.57%)
3	3 (0.10%)

TABLE IV

Distribution of |Ш| Among Rank 0 Curves of Table 2

|Ш|	No.	|Ш|	No.
1	35	81	1
4	324	100	19
9	15	144	37
16	531	256	25
25	3	324	1
36	99	400	2
49	0	576	1
64	229		

TABLE V

m	a	b	c
8	2	1	7
12	3	2	23
13	4	3	47
16	2	1	9
17	4	1	23
23	3	1	17
24	3	2	31
26	2	1	11
27	4	3	65
31	3	1	19
33	21	8	1063
36	12	1	161
38	2	1	13
41	4	3	79
42	6	1	53
44	4	1	31
	3	2	41
48	6	1	55
49	56	9	4721
52	2	1	15
55	15	1	251
56	5	2	79
57	55	12	5831
60	273	10	77471
61	5	4	159
63	4	3	97
64	3	2	49
	12	7	689
66	3	1	26
67	21	4	817
68	2	1	17
71	5	1	49
73	8	3	215
77	8	1	95
78	3	1	28
79	4	1	39
83	8	1	97
84	12	5	569
85	4340	1287	54858119
86	2	1	19
87	8	3	233
89	4	1	41
	5	4	191
90	35	6	2339
92	7	2	143
94	3	2	59
95	15	7	1049
96	4	3	119
99	312	215	676081
100	15	4	641
104	6	1	71
	7	2	151
106	2	1	21
107	5	4	209
109	1596	869	14721631
112	6	1	73

TABLE V—*Continued*

m	a	b	c
118	10	3	341
120	2091	1550	35852719
122	4	1	47
	3	2	67
125	1480	949	15880601
127	3	1	35
128	2	1	23
	4	3	137
131	12	1	199
132	10	3	359
	12	7	977
133	7	4	327
134	4	1	49
135	39	5	2729
137	377	28	188327
140	5	2	121
	15	8	1439
141	60	7	6151
143	3	1	37
	7	1	97
144	427	132	700729
151	7	1	99
152	2	1	25
153	4635	1672	98276359
155	104	95	123809
156	4	3	151
	9	2	239
159	5	3	191
160	5	2	129
161	7	4	359
162	3	2	77
166	6	5	389
168	9	2	247
	55	6	5239
169	56	11	8601
171	33	4	2041
172	21	10	2791
173	4	1	55
175	891	425	5075131
177	12	1	215
178	2	1	27
181	780	31	689911
183	12	1	217
184	6	1	89
186	252	221	763751
187	4	1	57
188	8	1	127
189	432	65	428801
191	5	3	209
194	5	1	74
195	1412568	474985	9582059430001
196	8	1	129
	4	3	169
197	8	3	343
	56	1	3233
198	3	2	85

TABLE V—*Continued*

m	a	b	c
199	15	7	1499
200	70	1	4999
-4	2	1	1
-9	3	1	1
-11	4	1	9
-13	4	1	7
-15	95	24	1951
-16	4	1	1
-25	5	1	1
-26	6	1	19
-27	21	4	65
-28	6	1	17
-32	12	1	127
-36	6	1	1
	39	4	1199
-39	155	24	6151
-40	15	2	121
-42	21	2	347
-43	55	8	911
-44	20	3	41
-47	8	1	33
-49	7	1	1
	8	1	31
-51	88	3	7511
-64	8	1	1
-67	33	4	137
-70	35	4	359
-72	104	3	10487
-74	10	1	51
-76	10	1	49
-77	72	7	2705
-78	55	6	811
-79	48	5	871
-80	4560	469	8155961
-81	9	1	1
-85	39284	3055	1075823719
-86	28	3	89
-89	12	1	89
-90	1290	133	346811
-92	20	1	351
-96	408	23	138769
-99	693505	47424	352465113601
-100	10	1	1
-101	287	8	79071
-103	55	4	2041
-104	105	4	10159
-105	130515	12319	4330566239
-106	33	2	851
-107	12	1	73
-108	3950	147	14388391
-109	12	1	71
-111	26546303927	2267574960	307287992933073391278
-113	63	5	2131
-115	332755	30912	9676740631
-116	69	4	3719
-118	55	2	2779
-119	56	5	711

TABLE V—*Continued*

m	a	b	c
-121	11	1	1
-123	12	1	55
-125	10301109	819640	48470941790119
-126	35	3	334
-129	90513	4879	6477768001
-131	644	39	298951
-132	657	56	87457
-133	6068	517	6846703
-134	145	12	6031
-136	209	14	27271
-140	271908	10165	66307815911
-141	67124	4845	2321283551
-142	12	1	17
-144	12	1	1
	2580	77	6214871
-146	14	1	99
-148	14	1	97
-149	592	45	130711
-151	689	40	332671
-156	152	3	22391
-160	21320	1519	196995361
-166	35	2	829
-167	56	3	2263
-168	689	24	423583
-169	13	1	1
-171	150017	8772	14503826441
-176	67452	5083	109317209
-179	335	24	31999
	780	29	527791
-180	70	3	4009
-181	184428	13585	4557781991
-182	28	1	687
-185	2403	175	793159
-186	204	11	28201
-187	301	12	75953
-189	4721145	208544	17708744652239
-190	35	1	1126
-191	16	1	129
	56	1	3039
-192	154908	3241	22965971473
-193	16	1	127
-195	3677683140865	239483286336	5628067524800453986859521
-196	14	1	1
	70	1	4801
-197	72	5	1159
	399	8	152767
-200	145	4	19359

This table allows correction of a wild assertion by Euler [5, Sect. 28] that he had found all m in the range $-200 \leqslant m \leqslant -2$ for which there exist nontrivial solutions of (1)—he was missing 22 values, including the cases $m = -80, -85, -99$. The editors of Euler's collected works do, however, remark in a footnote that a proof of the assertion is missing!

We do not provide a proof that Table V is complete either, although we have every belief that it is so. What is missing is to verify the Taniyama–Weil conjecture for the values of m where $L(1)$ was calculated to be nonzero. Then we could invoke the results of Kolyvagin [6], which prove the weak Birch and Swinnerton–Dyer conjecture for modular elliptic curves over $\mathbf{Q}$ whose L-functions vanish to order at most 1.

The tables allow other errors to be corrected. Euler [5, Section 19] lists a solution $m = 145$, $(a, b) = (159, 40)$; but $m = 145$ has no nontrivial solutions, and $(a, b) = (159, 40)$ "belongs" to $m = 303$. Further, in addition to the omissions for negative values of m mentioned above, he lists $m = 188$ as possessing nontrivial solutions, which is not the case. Pocklington [7, Sect. 9] states that [1] has no solutions for $m = -27$, but see Table V. Brown [1, Sect. 1] has the equation solvable for $m = 39$; a misprint for $m = 38$.

We remark that there is a striking difference between the curves with $m > 0$ and $m < 0$. As the tables show, curves with $m < 0$ seem less likely to have rank 2 or 3, and have significantly larger values for the order of Ш than the curves with $m > 0$. Furthermore, for the rank 1 curves with $m < 0$, the height of a generator tends to be larger than for rank 1 curves with $m > 0$.

The only explanation we offer is the trivial observation that if m is negative, Eq. (2) has no solutions with $x < 0$; hence it is less likely to have nontorsion points. (Note that curves with $m < 0$ have roughly half as many rank 2 curves as those with $m > 0$.) However, a precise statement and proof for these differences seems to be currently out of reach.

At the suggestion of the referee, however, we give illustrative details for one of the entries in Table V (namely, $m = -195$) where a solution was previously unknown.

Without loss of generality we can suppose from $a^4 - 195a^2b^2 + b^4 = c^2$ that $a \equiv 1 \bmod 2$, $b \equiv 0 \bmod 2$. By parametrizing the underlying quadratic form, it follows that there exist integers h, p, q, $(p, q) = 1$, satisfying

$$\begin{aligned} ha^2 &= 197p^2 + 390pq + 193q^2 \\ hb^2 &= 4pq, \end{aligned} \tag{10}$$

and then $h \mid 2.193.197$.

Since $h \equiv p^2 - 2pq + q^2 \equiv (p - q)^2 \bmod 4$, then $h \not\equiv 2 \bmod 4$, so $h \mid 193.197$. Taking $h = 1$, then

$$\begin{aligned} (197p + 193q)(p + q) &= a^2 \\ pq &= (b/2)^2. \end{aligned} \tag{11}$$

We can assume without loss of generality that p, q are positive, and then coprimality of the factors on the left-hand side of (11) implies that there exist integers r, s, t, u satisfying

$$197p + 193q = r^2; \qquad p + q = s^2; p = t^2; q = u^2,$$

with $r \equiv s \equiv u \equiv 1 \bmod 2$, $t \equiv 0 \bmod 2$. Then

$$r^2 = 197s^2 - 4u^2 \tag{12}$$

$$t^2 = s^2 - u^2. \tag{13}$$

From (12),

$$(r + 2iu)(r - 2iu) = 197s^2$$

and it follows that there exist coprime integers g, h with

$$r \pm 2iu = (\text{unit})(-1 + 14i)(g + ih)^2 \tag{14}$$

with the unit equal to 1 or i.

From (14) mod 2,

$$1 \equiv (\text{unit})(g + ih)^2$$

which forces the unit to equal 1.

Expanding (14),

$$\begin{aligned} r &= -g^2 - 28gh + h^2 \\ \pm u &= 7g^2 - gh - 7h^2 \end{aligned} \tag{15}$$

with

$$s = g^2 + h^2.$$

Further, from (13), there exist integers j, k with

$$\begin{aligned} t &= 2jk \\ u &= j^2 - k^2 \\ s &= j^2 + k^2 \end{aligned} \tag{16}$$

so that, from (15) and (16),

$$\begin{aligned} g^2 + h^2 &= j^2 + k^2 \\ 7g^2 - gh - 7h^2 &= \pm(j^2 - k^2). \end{aligned} \tag{17}$$

A small computer search reveals the solution $(g, h, j, k) = (456, -553, 688, 201)$, leading to the solution of Table V.

4

In the case of a curve (2) of rank 0, the sign of the functional equation is $+1$, and (3) and (8) may be combined to give

$$\frac{1}{\omega} \sum_{n \geq 1} \frac{a_n}{n} e^{-2\pi n/\sqrt{N}} = \frac{c\,|Ш|}{2\,|\mathrm{Tor}(\varepsilon)|^2}. \tag{18}$$

In particular, the sum on the left-hand side of (18) delivers a rational number.

Now if the sign of the functional equation is -1, then the right-hand side of (8) is no longer equal to $L_E(1)$, and there seems no reason why the left-hand side of (18) should still deliver a rational number. This indeed appears to be borne out in practice, with values appearing decently transcendental, though there are a few curious exceptions. Within the range of computation of this paper ($|m| \leqslant 3000$), there are precisely five values of m where the sign in the functional equation for E is -1, yet

$$S_E = \frac{1}{\omega} \sum_{n \geq 1} \frac{a_n}{n} e^{-2\pi n/\sqrt{N}} \tag{19}$$

appears to be *rational* (with calculations to 28 decimal places). These values are given in Table VI.

Here E' is the 2-isogenous curve to E, given by

$$y^2 = x(x^2 - 2mx + m^2 - 4). \tag{20}$$

We have observed this phenomenon on just two other elliptic curves, namely the 3-isogenous pair $E: y^2 = x^3 - 4$ and $E': y^2 = x^3 + 108$, for which $s_E = 1/3$, $s_{E'} = 1/3$. We are not able to give a satisfactory explanation of this rationality.

TABLE VI

m	s_E	$s_{E'}$
-222	4	2
-70	2	1
13	1/2	1
178	1	1
418	2	2

REFERENCES

1. E. BROWN, $x^4 + dx^2y^2 + y^4 = z^2$: Some cases with only trivial solutions—and a solution Euler missed, *Glasgow Math. J.* **31** (1989), 297–307.
2. A. BRUMER AND O. MCGUINNESS, The behaviour of the Mordell–Weil group of elliptic curves, *Bull. Amer. Mat. Soc (N.S.)* **23** No. 2 (1990), 375–382.
3. J. P. BUHLER AND B. H. GROSS, Arithmetic on elliptic curves with complex multiplication, II, *Invent. Math.* **79** (1985), 11–29.
4. J. P. BUHLER, B. H. GROSS, AND D. B. ZAGIER, On the conjecture of Birch and Swinnerton-Dyer for an elliptic curve of rank 3, *Math. Comp.* **44** (1985), 473–481.
5. L. EULER, De casibus quibus formulam $x^4 + mxxyy + y^4$ ad quadratum reducere licet, *Mém. Acad. Sci. St.-Pétersbourg* **7** (1815/1816, 1820), 10–22; *Opera Omnia, Ser. I* **5** (1944), 35–47.
6. A. KOLYVAGIN, On the Mordell–Weil group and the Shafarevich–Tate group of modular elliptic curves, *in* "Proceedings of the International Congress of Mathematicians, Kyoto, Japan, 1990," pp. 429–436.
7. H. C. POCKLINGTON, Some Diophantine impossibilities, *Proc. Cambridge Philos. Soc.* **17** (1914), 108–121.
8. J. H. SILVERMAN, The Arithmetic of Elliptic Curves, Springer Verlag, New York/Berlin, 1986.
9. T. N. SINHA, A class of quartic diophantine equations with only trivial solutions, *Amer. J. Math.* **100** (1978), 585–590.
10. J. TATE, The arithmetic of elliptic curves, *Invent. Math.* **23** (1974), 179–206.
11. D. ZAGIER AND G. KRAMARZ, Numerical investigations related to the L-series of certain elliptic curves, *J. Indian Math. Soc.* **52** (1987), 51–69.
12. M. Z. ZHANG, On the diophantine equation $x^4 + kx^2y^2 + y^4 = z^2$, *Sichuan Daxue Xuebao* **2** (1983), 24–31.