MATHEMATICS OF COMPUTATION
VOLUME 42, NUMBER 165
JANUARY 1984, PAGES 257-264

On the Equation $Y^2 = X(X^2 + p)$

By A. Bremner and J. W. S. Cassels

Abstract. Generators are found for the group of rational points on the title curve for all primes $p \equiv 5 \pmod 8$ less than 1,000. The rank is always 1 in accordance with conjectures of Selmer and Mordell. Some of the generators are rather large.

1. Let p be a positive prime,

$$p \equiv 5 \pmod 8. \tag{1}$$

It is easy to see that the Mordell-Weil rank of

$$Y^2 = X(X^2 + p) \tag{2}$$

is at most 1 (e.g. Section 5 of Birch and Swinnerton-Dyer [1]); and the Selmer conjecture [5] predicts rank exactly 1. As we shall note below, this is equivalent to a conjecture of Mordell [3], [4].

We shall verify this conjecture for all $p < 1{,}000$. Table 1 gives for each p a point P_0 which, together with the point $(0,0)$ of order 2, generates the entire Mordell-Weil group. Some of the generators P_0 are rather large, the most startling being that for $p = 877$, namely

$$\begin{aligned} X &= \frac{37\,5494\,5281\,2716\,2193\,1055\,0406\,9942\,0927\,9234\,6201}{6215\,9877\,7687\,1505\,4254\,6322\,0780\,6972\,3804\,4100}, \\ Y &= \frac{256\,2562\,6798\,8926\,8093\,8877\,6834\,0455\,1308\,9648\,6691\,5320\,4356\,6034\,6478\,6949}{4900\,7802\,3219\,7875\,8895\,9802\,9339\,9592\,8925\,0960\,6161\,6470\,7799\,7926\,1000}. \end{aligned} \tag{3}$$

A rational point (X, Y) on (3) is of the shape

$$X = R/S^2, \qquad Y = T/S^3 \tag{4}$$

for integers R, S, T with

$$R \geqslant 0, \qquad (R,S) = 1. \tag{5}$$

The height $H(X, Y)$ is by definition

$$H(X,Y) = \max(R,S^2), \tag{6}$$

so that the height of (3) is $\sim 3.75 \times 10^{41}$. It is of interest to compare this with the discriminant $|\Delta| = 4p^3$ of (2), which for $p = 877$ is $\sim 2.70 \times 10^9$. Hence $H(P_0) \sim |\Delta|^{4.41}$. Lang observed to us that in tables of elliptic curves and generators published to date the heights of generators are never much greater than $|\Delta|^2$. This, in our view, is almost certainly because these tables cover only curves with relatively small

Received December 28, 1982.
1980 *Mathematics Subject Classification*. Primary 10B10, 14K07.

discriminant. Further, unless one has strong reason to believe that a rational point exists, there is a marked reluctance to persevere in a search once the numbers cease to be small.

2. In (2) clearly either X or pX is square. Since

$$(X, Y) + (0,0) = (p/X, -pY/X^2), \tag{7}$$

we may suppose that X is a square. Then

$$X = r^2/s^2, \qquad Y = rt/s^3 \tag{8}$$

for integers r, s, t with r, s coprime and

$$r^4 + ps^4 = t^2. \tag{9}$$

It was for this equation that Mordell made his conjecture mentioned above.

Clearly

$$r \not\equiv 0, \qquad t \not\equiv 0 \pmod{p}, \tag{10}$$

and (1) implies that

$$r \equiv t \equiv 1, \qquad s \equiv 0 \pmod{2}. \tag{11}$$

We choose the sign of t so that $t \equiv 1 \pmod{4}$, and then

$$t \equiv 1 \pmod{8} \tag{12}$$

by (9) and (11). Since (9) can be written as

$$(t + r^2)(t - r^2) = ps^4, \tag{13}$$

we have $t + r^2 = 2a^4$ or $2pa^4$ for some odd a. The first alternative leads to a point Q on (2) with $(X, Y) = 2Q$. Hence by the "infinite descent" argument we may suppose that there is a coprime pair of integers a, b with

$$r^2 = pa^4 - 4b^4, \qquad a \equiv b \equiv 1 \pmod{2} \tag{14}$$

and

$$s = 2ab, \qquad t = pa^4 + 4b^4. \tag{15}$$

We can write (14) in the shape

$$(r + 2ib^2)(r - 2ib^2) = pa^4 \tag{16}$$

and consider factorization in $\mathbf{Z}[i]$. By (1)

$$p = u^2 + 4v^2, \tag{17}$$

where u, v are odd and without loss of generality

$$v \equiv 1 \pmod{4}. \tag{18}$$

The sign of r may be chosen so that $r + 2ib^2$ is divisible by $u + 2iv$, and then (16) implies

$$r + 2ib^2 = (u + 2iv) \cdot \text{unit} \cdot (c + id)^4 \tag{19}$$

for some c, d with

$$c^2 + d^2 = a. \tag{20}$$

On considering (19) modulo 8 and using (18), we find that the unit is necessarily 1. Hence on equating real and imaginary parts,

$$b^2 = v(l^2 - m^2) + ulm, \tag{21}$$

with

$$l = c^2 - d^2, \qquad m = 2cd. \tag{22}$$

If there are solutions of (2), then (21) must have rational solutions. This turns out to be the case for all the p under consideration, and so every solution of (21) is given by one of a finite number of parametrizations

$$l = q_1(\theta,\psi), \quad m = q_2(\theta,\psi), \quad b = q_3(\theta,\psi). \tag{23}$$

Here q_1, q_2, q_3 are known quadratic forms with rational integer coefficients and θ, ψ are integers to be found. It turns out that only one parametrization is compatible with the other conditions.

We have now

$$q_1(\theta,\psi) + iq_2(\theta,\psi) = (c + id)^2. \tag{24}$$

Arguing as before, but in $\mathbf{Z}[i]$, we have

$$\theta = Q_1(\lambda,\mu), \quad \psi = Q_2(\lambda,\mu), \quad c + id = Q_3(\lambda,\mu), \tag{25}$$

where Q_1, Q_2, Q_3 are known quadratic forms with coefficients in $\mathbf{Z}[i]$ and where λ, μ are elements of $\mathbf{Z}[i]$ to be found. Again, only one parametrization turns out to be compatible with the other conditions. The condition that θ, ψ are real leads to a pair of simultaneous homogeneous quadratic equations in the four variables $\mathrm{Re}\lambda$, $\mathrm{Im}\lambda$, $\mathrm{Re}\mu$, $\mathrm{Im}\mu$. These were the equations searched for solutions, though most of the entries in Table 1 could be spotted at an earlier stage in the process. The primes 317, 797, 877, 997 required an HP67, but the other solutions were found by hand.

At the suggestion of the referee we illustrate the last part of the argument and take

$$p = 877, \quad u = 29, \quad v = -3. \tag{26}$$

Then (21) is

$$b^2 + 3l^2 - 3m^2 - 29lm = 0. \tag{27}$$

The left-hand side vanishes for $(b,l,m) = (7,2,1)$ and so, by a standard algorithm, (27) is equivalent to

$$-LM + 877N^2 = 0, \tag{28}$$

where the forms

$$L = 14b - 17l - 64m, \tag{29$_1$}$$

$$M = 5074b - 6242l - 23035m, \tag{29$_2$}$$

$$N = 9b - 11l - 41m \tag{29$_3$}$$

are unimodular. On taking $-b$ for b if need be, we have $877 \nmid M$, so (28) implies

$$\pm L = 877\theta^2, \quad \pm M = \phi^2, \quad \pm N = \theta\phi \tag{30}$$

for some integers θ, ϕ and some choice of sign.

On solving for b, l, m and putting

$$\phi = -\psi + 563\theta, \tag{31}$$

we obtain

$$\pm b = -7\psi^2 - 11\psi\theta + 27\theta^2, \tag{32_1}$$

$$\pm l = -2\psi^2 + 6\psi\theta - 3\theta^2, \tag{32_2}$$

$$\pm m = -\psi^2 - 4\psi\theta - 7\theta^2. \tag{32_3}$$

The lower sign is incompatible 2-adically with (22), so we must take the upper sign.

By (22) we have

$$l + im = (c + id)^2 = \gamma^2 \text{ (say)}; \tag{33}$$

and so

$$\gamma^2 + (2 + i)\psi^2 + (-6 + 4i)\psi\theta + (3 + 7i)\theta^2 = 0 \tag{34}$$

by (32_2), (32_3). This is equivalent to

$$(6 - 29i)S^2 + RT = 0, \tag{35}$$

where

$$S = (1 + i)\gamma + (-4 + i)\theta - i\psi, \tag{36_1}$$

$$R = (3 + 2i)\gamma + (-10 + 5i)\theta - 2i\psi, \tag{36_2}$$

$$T = (-15 + 6i)\gamma + (8 - 45i)\theta + (14 + 4i)\psi. \tag{36_3}$$

Hence

$$2\theta = (-4 - 3i)R + (22 + 10i)S + iT, \tag{37_1}$$

$$2\psi = (-1 + 2i)R + (6 - 16i)S + T, \tag{37_2}$$

$$2\gamma = (-15 + 6i)R + (70 - 46i)S + (3 + 2i)T. \tag{37_3}$$

By (35), on taking $-\gamma$ for γ if need be, there are Gaussian integers λ, μ such that

$$R = (1 \pm i)\lambda^2, \quad T = (6 - 29i)(1 \pm i)\mu^2, \quad S = (1 \mp i)\lambda\mu, \tag{38}$$

for either the upper or the lower signs. Put

$$\lambda = x + iy, \qquad \mu = u + iv, \tag{39}$$

where x, y, u, v are rational integers. On substituting (38), (39) in (37_1), (37_2) we get

$$2\theta = F_1(x,y,u,v) + iF_2(x,y,u,v), \tag{40_1}$$

$$2\psi = G_1(x,y,u,v) + iG_2(x,y,u,v), \tag{40_2}$$

where F_1, F_2, G_1, G_2 are quadratic forms with rational integer coefficients. [There is a set of forms for each choice of sign in (38).] Hence

$$F_2(x,y,u,v) = G_2(x,y,u,v) = 0. \tag{41}$$

If the lower signs hold in (39), the simultaneous equations (41) turn out to be 2-adically incompatible, so we must take the upper signs. A search yields

$$\lambda = 324 - 385i, \qquad \mu = 136 + 145i. \tag{42}$$

It may be noted that (41) implies congruence conditions on x, y, u, v to various small moduli, and these greatly facilitate the search.

3. Having indicated how the rational points P_0 were obtained, we must now show that they are generators. This requires consideration of heights.

Let (4) be a rational point P on (2). The X-coordinate of $2P$ is

$$X_1 = \frac{(R^2 - pS^4)^2}{4S^2T^2} = \frac{(R^2 - pS^4)^2}{4RS^2(R^2 + pS^4)}. \tag{43}$$

We consider only points of the type (8), (9), so $p \nmid R$. It is then easy to see that the numerator and denominator in (43) are coprime. Hence

$$H(2P) = \max\{(R^2 - pS^4)^2,\ 4RS^2(R^2 + pS^4)\}. \tag{44}$$

We distinguish three cases:

(i) $0 \leqslant S^2/R \leqslant 1/2p^{1/2}$. Then

$$H(2P) \geqslant (R^2 - pS^4)^2 \geqslant (9/16)R^4 = (9/16)H(P)^4.$$

(ii) $1/2p^{1/2} \leqslant S^2/R \leqslant 1$. Then

$$H(2P) \geqslant 4RS^2(R^2 + pS^4) \geqslant (2/p^{1/2})R^4 = (2/p^{1/2})H(P)^4.$$

(iii) $1 \leqslant S^2/R$. Then

$$H(2P) \geqslant (R^2 - pS^4)^2 \geqslant (p-1)^2S^8 = (p-1)^2H(P)^4.$$

Hence in any case

$$H(2P) \geqslant (2/p^{1/2})H(P)^4. \tag{45}$$

Similarly, but more simply,

$$H(2P) \leqslant p^2H(P)^4. \tag{46}$$

With the usual notation $h(P) = \log H(P)$ it follows that

$$4h(P) - \tfrac{1}{2}\log(p/4) \leqslant h(2P) \leqslant 4h(P) + 2\log p. \tag{47}$$

Now (43) is a perfect square, so the argument applies to $2P$ instead of P. By induction

$$4^nh(P) - (1/6)(4^n - 1)\log(p/4) \leqslant h(2^nP) \leqslant 4^nh(P) + (2/3)(4^n - 1)\log p$$

for every $n \geqslant 1$. The Tate height is

$$\hat{h}(P) = \lim_{n\to\infty} 4^{-n}h(2^nP), \tag{48}$$

so

$$h(P) - (1/6)\log(p/4) \leqslant \hat{h}(P) \leqslant h(P) + (2/3)\log p. \tag{49}$$

Let P_0 be one of the points on (2) listed in Table 1. The descent argument shows that neither P_0 nor $P_0 + (0,0)$ is divisible by 2. Suppose that P_0 is divisible by 3, say $P_0 = 3Q$. Let q be a prime distinct from 2, p. Then (2) has good reduction modulo q and the reduced points $\overline{P}_0$, $\overline{Q} \bmod q$ would satisfy $\overline{P}_0 = 3\overline{Q}$. For each P_0 Table 1 gives a prime q such that $\overline{P}_0$ is not divisible by 3 in the group of points on (2) over the finite field $\mathbf{F}_q$. Hence if P_0 is not a generator we have $P_0 = kQ$ for some odd

TABLE 1

For each prime p the table lists a, b, r, s, t satisfying (14) and (15). A point P_0 on (2) is given by (8). The second column gives a prime q such that P_0 is not divisible by 3 when considered on (2) modulo q.

p	q	a	b	r	s	t
5	11	1	1	1	2	9
13	11	1	1	3	2	17
29	47	1	1	5	2	33
37	11	5	3	151	30	23449
53	11	1	1	7	2	57
61	11	5	9	109	90	64369
101	23	29	25	8359	1450	72997881
109	11	5	1	261	10	68129
149	47	5	7	289	70	102729
157	11	85	93	88861	15810	8494718929
173	11	1	1	13	2	177
181	23	461	715	2670111	659230	9220300757321
197	11	4505	9541	219078991	85964410	114288283364168169
229	11	1	1	15	2	233
269	23	5	11	331	110	226689
277	11	2105	3901	67173561	16423210	6364939035625529
293	13	1	1	17	2	297
317	11	73265	48869	95450823979	7160774570	9156486995910318703809
349	11	1	3	5	6	673

TABLE 1 (*continued*)

p	q	a	b	r	s	t
373	11	1	3	7	6	697
389	11	5	13	359	130	357369
397	11	34205	76227	20208571931	5214689070	678486823935140827489
421	11	185	587	135009	217190	968049796169
461	11	6341	18985	475038539	240767770	1264941190283659521
509	23	61	187	46435	22814	11938856913
541	11	29	95	7539	5510	708441521
557	11	185	59	807709	21830	652490767569
613	11	1	3	17	6	937
653	11	13	23	4187	598	19769697
661	47	85	219	159071	37230	43705643209
677	47	85	251	139511	42670	51216327129
701	11	33085	53407	28414544861	3533941190	872471631054132766929
709	11	13	47	855	1222	39768473
733	47	1	1	27	2	737
757	11	8725	20521	1917696399	358091450	5096238244666339049
773	11	13	17	4663	442	22411737
797	47	2731885	1773371	210600981540301	9689291268670	4443189381141835355436425649
821	11	185	667	412279	246790	1753383752409
829	23	5	17	429	170	852209
853	13	1	3	23	6	1177
877	11	4612160965	8547136197	612776083187947368101	78841535860683900210	418189082471629807342957247493327168750049
941	11	93029	199915	253160835589	37195785070	76868662544190706581921
997	11	52589605	202793163	29340760454551241	21329624677741230	14391049283467552993254253873806169

$k \geqslant 5$ and some rational point Q. By the quadratic property of heights

$$\hat{h}(P_0) = k^2 \hat{h}(Q) \tag{50}$$

(e.g. Cassels [2, p. 262]). From this and (49) it follows that

$$\begin{aligned} h(Q) &\leqslant (1/k^2)h(P_0) + (2/3k^2)\log p + (1/6)\log(p/4) \\ &\leqslant (1/25)h(P_0) + (2/75)\log p + (1/6)\log(p/4). \end{aligned}$$

Even in the extreme case $p = 877$ this implies $H(Q) < 136$, which in turn implies a solution of (9) with $0 < r, s < 12$; a contradiction.

Department of Pure Mathematics
and Mathematical Statistics
University of Cambridge
Cambridge CB2 1SB, England

1. B. J. BIRCH & H. P. F. SWINNERTON - DYER, "Notes on elliptic curves II," *J. Reine Angew. Math.*, v. 218, 1965, pp. 79–108.

2. J. W. S. CASSELS, "Diophantine equations with special reference to elliptic curves," *J. London Math. Soc.*, v. 41, 1966, pp. 193–291.

3. L. J. MORDELL, "The diophantine equation $x^4 + my^4 = z^2$," *Quart. J. Math.* (2), v. 18, 1967, pp. 1–6.

4. L. J. MORDELL, $y^2 = Dx^4 + 1$, Number Theory Colloquium, János Bolyai Math. Soc., Debrecen, 1968, pp. 141–145 (North-Holland, Amsterdam, 1970).

5. E. SELMER, "A conjecture concerning rational points on cubic curves," *Math. Scand.*, v. 2, 1954, pp. 49–54.