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 \( p = 5 \mod 8 \) 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,

\[ p = 5 \mod 8. \]

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

\[ Y^2 = X(X^2 + p) \]

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

\[
\begin{align*}
X &= 375494528127162193105504069942092792346201 \\
&
6215987776871505425463220780697238044100
\end{align*}
\]

\[ \ldots \]

\[
\begin{align*}
y &= 256256267988926809388776834045513089648669153204356603464786949 \\
&
490078023219787588959802933995928925096061616470779979261000
\end{align*}
\]

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

\[ X = R/S^2, \quad Y = T/S^3 \]

for integers \( R, S, T \) with

\[ R \geq 0, \quad (R,S) = 1. \]

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

\[ H(X,Y) = \max(R,S^2), \]

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.
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

\[ (X, Y) + (0, 0) = \left( \frac{p}{X}, -\frac{pY}{X^2} \right), \]

we may suppose that $X$ is a square. Then

\[ X = \frac{r^2}{s^2}, \quad Y = \frac{rt}{s^3} \]

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

\[ r^4 + ps^4 = t^2. \]

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

Clearly

\[ r \not\equiv 0, \quad t \not\equiv 0 \pmod{p}, \]

and (1) implies that

\[ r \equiv t \equiv 1, \quad s \equiv 0 \pmod{2}. \]

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

\[ t \equiv 1 \pmod{8} \]

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

\[ (t + r^2)(t - r^2) = ps^4, \]

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

\[ r^2 = pa^4 - 4b^4, \quad a \equiv b \equiv 1 \pmod{2} \]

and

\[ s = 2ab, \quad t = pa^4 + 4b^4. \]

We can write (14) in the shape

\[ (r + 2ib^2)(r - 2ib^2) = pa^4 \]

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

\[ p = u^2 + 4v^2, \]

where $u, v$ are odd and without loss of generality

\[ v \equiv 1 \pmod{4}. \]

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

\[ r + 2ib^2 = (u + 2iv) \cdot \text{unit} \cdot (c + id)^4 \]

for some $c, d$ with

\[ c^2 + d^2 = a. \]
On considering (19) modulo 8 and using (18), we find that the unit is necessarily 1. Hence on equating real and imaginary parts,

\[(21) \quad b^2 = v(t^2 - m^2) + ulm,\]

with

\[(22) \quad l = c^2 - d^2, \quad m = 2cd.\]

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

\[(23) \quad l = q_1(\theta, \psi), \quad m = q_2(\theta, \psi), \quad b = q_3(\theta, \psi).\]

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

We have now

\[(24) \quad q_1(\theta, \psi) + iq_2(\theta, \psi) = (c + id)^2.\]

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

\[(25) \quad \theta = Q_1(\lambda, \mu), \quad \psi = Q_2(\lambda, \mu), \quad c + id = Q_3(\lambda, \mu),\]

where $Q_1, Q_2, Q_3$ are known quadratic forms with coefficients in $\mathbb{Z}[i]$ and where $\lambda, \mu$ are elements of $\mathbb{Z}[i]$ to be found. Again, only one parametrization turns out to be compatible with the other conditions. The condition that $\theta, \psi$ are real leads to a pair of simultaneous homogeneous quadratic equations in the four variables $\text{Re}\lambda, \text{Im}\lambda, \text{Re}\mu, \text{Im}\mu$. 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

\[(26) \quad p = 877, \quad u = 29, \quad v = -3.\]

Then (21) is

\[(27) \quad b^2 + 3l^2 - 3m^2 - 29lm = 0.\]

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

\[(28) \quad -LM + 877N^2 = 0,\]

where the forms

\[(29_1) \quad L = 14b - 17l - 64m,\]
\[(29_2) \quad M = 5074b - 6242l - 23035m,\]
\[(29_3) \quad N = 9b - 11l - 41m\]

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

\[(30) \quad \pm L = 877\theta^2, \quad \pm M = \phi^2, \quad \pm N = \theta\phi\]

for some integers $\theta, \phi$ and some choice of sign.
On solving for $b$, $l$, $m$ and putting

\[(31) \quad \phi = -\psi + 563\theta,\]

we obtain

\[(32_1) \quad \pm b = -7\psi^2 - 11\psi\theta + 27\theta^2,\]
\[(32_2) \quad \pm l = -2\psi^2 + 6\psi\theta - 3\theta^2,\]
\[(32_3) \quad \pm m = -\psi^2 - 4\psi\theta - 7\theta^2.\]

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

By (22) we have

\[(33) \quad l + im = (c + id)^2 = \gamma^2\text{ (say)};\]

and so

\[(34) \quad \gamma^2 + (2 + i)\psi^2 + (-6 + 4i)\psi\theta + (3 + 7i)\theta^2 = 0\]

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

\[(35) \quad (6 - 29i)S^2 + RT = 0,\]

where

\[(36_1) \quad S = (1 + i)\gamma + (-4 + i)\theta - i\psi,\]
\[(36_2) \quad R = (3 + 2i)\gamma + (-10 + 5i)\theta - 2i\psi,\]
\[(36_3) \quad T = (-15 + 6i)\gamma + (8 - 45i)\theta + (14 + 4i)\psi.\]

Hence

\[(37_1) \quad 2\theta = (-4 - 3i)R + (22 + 10i)S + iT,\]
\[(37_2) \quad 2\psi = (-1 + 2i)R + (6 - 16i)S + T,\]
\[(37_3) \quad 2\gamma = (-15 + 6i)R + (70 - 46i)S + (3 + 2i)T.\]

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

\[(38) \quad R = (1 \pm i)\lambda^2, \quad T = (6 - 29i)(1 \pm i)\mu^2, \quad S = (1 \mp i)\lambda\mu,\]

for either the upper or the lower signs. Put

\[(39) \quad \lambda = x + iy, \quad \mu = u + iv,\]

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

\[(40_1) \quad 2\theta = F_1(x,y,u,v) + iF_2(x,y,u,v),\]
\[(40_2) \quad 2\psi = G_1(x,y,u,v) + iG_2(x,y,u,v),\]

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

\[(41) \quad F_2(x,y,u,v) = G_2(x,y,u,v) = 0.\]

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

\[(42) \quad \lambda = 324 - 385i, \quad \mu = 136 + 145i.\]

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

\[
X_1 = \frac{(R^2 - pS^4)^2}{4S^2T^2} = \frac{(R^2 - pS^4)^2}{4RS^2(R^2 + pS^4)}.
\]

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

\[
H(2P) = \max\{(R^2 - pS^4)^2, 4RS^2(R^2 + pS^4)\}.
\]

We distinguish three cases:

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

\[
H(2P) \geq (R^2 - pS^4)^2 \geq (9/16)R^4 = (9/16)H(P)^4.
\]

(ii) \( 1/2p^{1/2} < S^2/R \leq 1 \). Then

\[
H(2P) \geq 4RS^2(R^2 + pS^4) \geq (2/p^{1/2})R^4 = (2/p^{1/2})H(P)^4.
\]

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

\[
H(2P) \geq (R^2 - pS^4)^2 \geq (p - 1)^2S^8 = (p - 1)^2H(P)^4.
\]

Hence in any case

\[
H(2P) \geq (2/p^{1/2})H(P)^4.
\]

Similarly, but more simply,

\[
H(2P) \leq p^2H(P)^4.
\]

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

\[
4h(P) - \frac{1}{2} \log(p/4) \leq h(2P) \leq 4h(P) + 2 \log p.
\]

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

\[
4^n h(P) - (1/6)(4^n - 1) \log(p/4) \leq h(2^n P) \leq 4^n h(P) + (2/3)(4^n - 1) \log p
\]

for every \( n \geq 1 \). The Tate height is

\[
\hat{h}(P) = \lim_{n \to \infty} 4^{-n} h(2^n P),
\]

so

\[
h(P) - (1/6) \log(p/4) \leq \hat{h}(P) \leq h(P) + (2/3) \log p.
\]

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 \( \overline{P}_0, \overline{Q} \) mod \( q \) would satisfy \( \overline{P}_0 = 3 \overline{Q} \). For each \( P_0 \) Table 1 gives a prime \( q \) such that \( P_0 \) is not divisible by 3 in the group of points on (2) over the finite field \( F_q \). 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 $q$.

<table>
<thead>
<tr>
<th>$p$</th>
<th>$q$</th>
<th>$a$</th>
<th>$b$</th>
<th>$r$</th>
<th>$s$</th>
<th>$t$</th>
</tr>
</thead>
<tbody>
<tr>
<td>5</td>
<td>11</td>
<td>1</td>
<td>1</td>
<td>1</td>
<td>2</td>
<td>9</td>
</tr>
<tr>
<td>13</td>
<td>11</td>
<td>1</td>
<td>1</td>
<td>3</td>
<td>2</td>
<td>17</td>
</tr>
<tr>
<td>29</td>
<td>47</td>
<td>1</td>
<td>1</td>
<td>5</td>
<td>2</td>
<td>33</td>
</tr>
<tr>
<td>37</td>
<td>11</td>
<td>5</td>
<td>3</td>
<td>151</td>
<td>30</td>
<td>23449</td>
</tr>
<tr>
<td>53</td>
<td>11</td>
<td>1</td>
<td>1</td>
<td>7</td>
<td>2</td>
<td>57</td>
</tr>
<tr>
<td>61</td>
<td>11</td>
<td>5</td>
<td>9</td>
<td>109</td>
<td>90</td>
<td>64369</td>
</tr>
<tr>
<td>101</td>
<td>23</td>
<td>29</td>
<td>25</td>
<td>8359</td>
<td>1450</td>
<td>72997881</td>
</tr>
<tr>
<td>109</td>
<td>11</td>
<td>5</td>
<td>1</td>
<td>261</td>
<td>10</td>
<td>68129</td>
</tr>
<tr>
<td>149</td>
<td>47</td>
<td>5</td>
<td>7</td>
<td>289</td>
<td>70</td>
<td>102729</td>
</tr>
<tr>
<td>157</td>
<td>11</td>
<td>85</td>
<td>93</td>
<td>88861</td>
<td>15810</td>
<td>8494718929</td>
</tr>
<tr>
<td>173</td>
<td>11</td>
<td>1</td>
<td>1</td>
<td>13</td>
<td>2</td>
<td>177</td>
</tr>
<tr>
<td>181</td>
<td>23</td>
<td>461</td>
<td>715</td>
<td>2670111</td>
<td>659230</td>
<td>9220300757321</td>
</tr>
<tr>
<td>197</td>
<td>11</td>
<td>4505</td>
<td>9541</td>
<td>21907899</td>
<td>85964410</td>
<td>114288283364168169</td>
</tr>
<tr>
<td>229</td>
<td>11</td>
<td>1</td>
<td>1</td>
<td>15</td>
<td>2</td>
<td>233</td>
</tr>
<tr>
<td>269</td>
<td>23</td>
<td>5</td>
<td>11</td>
<td>331</td>
<td>110</td>
<td>226689</td>
</tr>
<tr>
<td>277</td>
<td>11</td>
<td>2105</td>
<td>3901</td>
<td>67173561</td>
<td>16423210</td>
<td>6364939035625529</td>
</tr>
<tr>
<td>293</td>
<td>13</td>
<td>1</td>
<td>1</td>
<td>17</td>
<td>2</td>
<td>297</td>
</tr>
<tr>
<td>317</td>
<td>11</td>
<td>73265</td>
<td>48869</td>
<td>95450823979</td>
<td>7160774570</td>
<td>9156486995910318703809</td>
</tr>
<tr>
<td>349</td>
<td>11</td>
<td>1</td>
<td>3</td>
<td>5</td>
<td>6</td>
<td>673</td>
</tr>
<tr>
<td>p</td>
<td>q</td>
<td>a</td>
<td>b</td>
<td>r</td>
<td>s</td>
<td>t</td>
</tr>
<tr>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>----</td>
<td>-----</td>
<td>-----</td>
</tr>
<tr>
<td>373</td>
<td>11</td>
<td>1</td>
<td>3</td>
<td>7</td>
<td>6</td>
<td></td>
</tr>
<tr>
<td>389</td>
<td>11</td>
<td>5</td>
<td>13</td>
<td>359</td>
<td>130</td>
<td>357369</td>
</tr>
<tr>
<td>397</td>
<td>11</td>
<td>34205</td>
<td>76227</td>
<td>20208571931</td>
<td>5214689070</td>
<td>678486823935140827489</td>
</tr>
<tr>
<td>421</td>
<td>11</td>
<td>185</td>
<td>587</td>
<td>135009</td>
<td>217190</td>
<td>968049796169</td>
</tr>
<tr>
<td>461</td>
<td>11</td>
<td>6341</td>
<td>18985</td>
<td>475038539</td>
<td>240767770</td>
<td>1264941190283659521</td>
</tr>
<tr>
<td>509</td>
<td>23</td>
<td>61</td>
<td>187</td>
<td>46435</td>
<td>22814</td>
<td>11938856913</td>
</tr>
<tr>
<td>541</td>
<td>11</td>
<td>29</td>
<td>95</td>
<td>7539</td>
<td>5510</td>
<td>708441521</td>
</tr>
<tr>
<td>557</td>
<td>11</td>
<td>185</td>
<td>59</td>
<td>807709</td>
<td>21830</td>
<td>652490767569</td>
</tr>
<tr>
<td>613</td>
<td>11</td>
<td>1</td>
<td>3</td>
<td>17</td>
<td>6</td>
<td>937</td>
</tr>
<tr>
<td>653</td>
<td>11</td>
<td>13</td>
<td>23</td>
<td>4187</td>
<td>598</td>
<td>19769697</td>
</tr>
<tr>
<td>661</td>
<td>47</td>
<td>85</td>
<td>219</td>
<td>159071</td>
<td>37230</td>
<td>43705643209</td>
</tr>
<tr>
<td>677</td>
<td>47</td>
<td>85</td>
<td>251</td>
<td>139511</td>
<td>42670</td>
<td>51216327129</td>
</tr>
<tr>
<td>701</td>
<td>11</td>
<td>33085</td>
<td>53407</td>
<td>28414544861</td>
<td>3533941190</td>
<td>872471631054132766929</td>
</tr>
<tr>
<td>709</td>
<td>11</td>
<td>13</td>
<td>47</td>
<td>855</td>
<td>1222</td>
<td>39768473</td>
</tr>
<tr>
<td>733</td>
<td>47</td>
<td>1</td>
<td>1</td>
<td>27</td>
<td>2</td>
<td>737</td>
</tr>
<tr>
<td>757</td>
<td>11</td>
<td>8725</td>
<td>20521</td>
<td>1917696399</td>
<td>358091450</td>
<td>5096238244666339049</td>
</tr>
<tr>
<td>773</td>
<td>11</td>
<td>13</td>
<td>17</td>
<td>4663</td>
<td>442</td>
<td>22411737</td>
</tr>
<tr>
<td>797</td>
<td>47</td>
<td>2731885</td>
<td>1773371</td>
<td>210600981540301</td>
<td>9689291268670</td>
<td>4443189381141835335436425649</td>
</tr>
<tr>
<td>821</td>
<td>11</td>
<td>185</td>
<td>667</td>
<td>412279</td>
<td>246790</td>
<td>1753383752409</td>
</tr>
<tr>
<td>821</td>
<td>23</td>
<td>5</td>
<td>17</td>
<td>429</td>
<td>170</td>
<td>852209</td>
</tr>
<tr>
<td>853</td>
<td>13</td>
<td>1</td>
<td>3</td>
<td>23</td>
<td>6</td>
<td>1177</td>
</tr>
<tr>
<td>877</td>
<td>11</td>
<td>4612160965</td>
<td>8547136197</td>
<td>612776083187947368101</td>
<td>78841535860683900210</td>
<td>418189082471629807342957247493327168750049</td>
</tr>
<tr>
<td>941</td>
<td>11</td>
<td>93029</td>
<td>199915</td>
<td>253160835589</td>
<td>37195785070</td>
<td>768686254419076581921</td>
</tr>
<tr>
<td>997</td>
<td>11</td>
<td>52589605</td>
<td>202793163</td>
<td>29340760454551241</td>
<td>21329624677741230</td>
<td>14391049283467552993254253873806169</td>
</tr>
</tbody>
</table>
$k \geq 5$ and some rational point $Q$. By the quadratic property of heights

\begin{equation}
\hat{h}(P_0) = k^2 \hat{h}(Q)
\end{equation}

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

\[ h(Q) \leq (1/k^2) h(P_0) + (2/3k^2) \log p + (1/6) \log (p/4) \]

\[ \leq (1/25) A(P_0) + (2/75) \log p + (1/6) \log (p/4). \]

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.