On the Equation $Y^2 = X^5 + k$

Andrew Bremner

CONTENTS

2000 AMS Subject Classification: Primary 11D41; Secondary 11D25, 11G05, 11G30

Keywords: Fifth powers, genus two curve, elliptic curve

We show that there are infinitely many nonisomorphic curves $Y^2 = X^5 + k$, $k \in \mathbb{Z}$, possessing at least twelve finite points for $k > 0$, and at least six finite points for $k < 0$. We also determine all rational points on the curve $Y^2 = X^5 - 7$.

1. INTRODUCTION

We are interested in rational solutions to the title equation

$$C_k : Y^2 = X^5 + k,$$

where we may assume without loss of generality that k is tenth-power-free. The equation defines a curve of genus 2, so has only finitely many points (with precisely one point at infinity). When the Jacobian variety of C_k (which is irreducible) has rank at most 1, then there exist "Chabauty" techniques for determining the set of rational points on C_k. Michael Stoll [Stoll 06] has proved the interesting and elegant theorem that when the Jacobian variety of C_k does have rank at most 1, then the number of rational points on C_k is bounded above by 7; further, the bound of 7 is achieved only for $k = 324$.

We were motivated to see what can be said about the number of points on curves of this type when we allow the Jacobian to have rank greater than 1.

The smallest value of $|k|$ for which we found 9 points on the curve is $k = 257$; with 11 points, $k = 153124$. No k with 13 points has yet been found for $|k| < 10^7$.

Stoll gives the example of

$$k = 25344958401 = 3^4 7^4 19^4$$

when there are at least 15 points; we found several other such examples (all with larger k), and just one case in which there are at least 17 points: $k = 2^6 3^4 5^4 7^4 13^4 17^4 19^4 37^4$, when C_k has points with x-coordinates equal to $2 \cdot 3 \cdot 5 \cdot 7 \cdot 13 \cdot 17 \cdot 19 \cdot 37 \cdot a$, for

$$a = 0,\ 4,\ \frac{1}{6},\ \frac{2}{17},\ -\frac{1}{26},\ \frac{2}{35},\ \frac{2}{39},\ -\frac{8}{259}.$$

1058-6458/2008 $0.50 per page
Experimental Mathematics **17**:3, page 371

When $k<0$, then C_k seems to possess far fewer points, and in the range $0<-k<10^7$, we found only 12 values of k such that C_k possesses at least 6 finite points (we searched for points with height less than 10^6): namely, $-k$ equal to 21303, 114143, 148507, 204732, 1044976, 1541468, 3369375, 3926151, 7019351, 7907868, 7942460, and 9055625. (For these k, the point of largest height occurred for $k=-148507$ with $x=17299/169$.)

We shall prove below that there do, however, exist infinitely many nonisomorphic curves C_k, $k<0$, that possess at least 6 finite points. We know of only two examples for $k<0$ where C_k has at least 8 finite points, namely $k=-11331151$, with points at $x=35$, 40, 56, 386, and $k=-16410368$, with the 10 points at $x=48$, 153, 464, $\frac{568}{9}$, $\frac{1752}{49}$.

For positive k, we note that the curve

$$y^2=x^5+\left(2^{10r-2}+1\right)$$

contains one point at infinity and the 8 finite points

$$(x,\pm y)=\left(-1,2^{5r-1}\right),\quad \left(-2^r,2^{5r-1}-1\right),\quad \left(2^r,2^{5r-1}+1\right),\quad \left(\frac{1}{2^r},\frac{1}{2^{5r}}+2^{5r-1}\right).$$

But we can do better, and shall show by parameterization that there exist infinitely many nonisomorphic curves C_k, $k>0$, that possess at least 12 finite points.

In analogy with Mordell's equation $y^2=x^3+k$, it is of interest to describe all the rational solutions of $y^2=x^5+k$. For any given value of k such that the Jacobian of C_k has rank at least 2, it is not at all straightforward to determine explicitly all rational points on C_k.

We conclude this note with an example in which we find all rational points on $y^2=x^5-7$ whose Jacobian is of rank 2. The methods are not intrinsically new, but they do show that (working over a fifth-degree number field) a certain amount of luck is required in order that computer routines finish in a reasonable amount of time.

2. THE CASE $k<0$

Theorem 2.1. *There exist infinitely many nonisomorphic curves $y^2=x^5+k$, $k<0$, containing six finite points.*

Proof: Put $-k=m^4$, where $m=u^2+1$. Then the curve contains the two points $(x,\pm y)=(m,m^2u)$. Demanding that there be points with $x=rm$, $x=sm$, necessitates

$$r^5u^2+(r^5-1)=\square,\qquad s^5u^2+(s^5-1)=\square.$$

Choosing r,s essentially at random can lead to some thorny elliptic-curve computations, so we set $(r,s)=(\frac14,\frac25)$, values chosen by observation of numerical data. Then

$$u^2-1023=v^2,\quad 160u^2-15465=w^2. \tag{2–1}$$

The intersection of these two quadrics represents a curve of genus 1, which is a rational elliptic curve given that there exists a rational point at $u=\frac{137}{4}$. The routine `GenusOneModel` of Magma [Bosma et al. 97] establishes an isomorphism of this curve with the cubic model

$$E: Y^2Z=(X-103965Z)(X+44250Z)(X+59715Z),$$

which Magma tells us is of rank 2, with generators $(127975,-27858950)$, $(-46710,-2195550)$. These latter correspond to $u=-137/4$ and $u=-24884803/278396$, respectively.

Accordingly, we can find infinitely many points u satisfying equations (2–1), and with $-k=m^4=(u^2+1)^4$, the corresponding curve $y^2=x^5+k$ has six points at $x=m,\frac14m,\frac25m$.

The curves arising from u_1 and u_2 are isomorphic if and only if the ratio of u_2^2+1 to u_1^2+1 is a fifth power. Suppose we have constructed as above u_i, $i=1,\dots,n$, corresponding to nonisomorphic quintic curves C_i. Then the n curves $x^2+1=(u_i^2+1)y^5$, $i=1,\dots,n$, are all curves of genus 2 with accordingly only finitely many rational points lying on their union.

By constructing u_{n+1} as above, and avoiding a finite set of values, we thus construct an $(n+1)$th curve C_{n+1} not isomorphic to any C_i, $i=1,\dots,n$. Inductively, we obtain infinitely many nonisomorphic curves with six finite rational points. □

3. THE CASE $k>0$

Theorem 3.1. *There exist infinitely many nonisomorphic curves $y^2=x^5+k$, $k>0$, containing twelve finite points.*

Proof: Put $k=m^4$ with $m=u^2-1$. This ensures points at $x=0,m$. We demand points at $x=am$ for further values of a, equivalent to demanding

$$f(a)=ma^5+1=(u^2-1)a^5+1=\square.$$

Taking $u=(n^2+2nr+2r^2)/n^2$ (a parameterization suggested by tables of numerical data) yields

$$m=\frac{4r(n+r)(n^2+nr+r^2)}{n^4},$$

and we obtain the following points $(x, \pm y)$ on C_k, an extra pair corresponding to $a = n/r$, $-n/(n+r)$:

$$\left(0, m^2\right), \ \left(m, m^2 u\right), \ \left(mn/r, m^2\left(2n^2 + 2nr + r^2\right)/r^2\right), \\ \left(-mn/\left(n+r\right), m^2\left(n^2 + r^2\right)/\left(n+r\right)^2\right).$$

To get additional points, set $(n, r) = (2t^5, 1 - t^5 - t^{10})$. Then

$$m = \frac{1 - 2t^{10} - t^{20} - 2t^{30} + t^{40}}{4t^{20}}, \tag{3–1}$$

with

$$f\left(t^2\right) = mt^{10} + 1 = \left(\frac{-1 - t^{10} + t^{20}}{2t^5}\right)^2$$

and

$$f\left(\frac{1}{t^2}\right) = \frac{m}{t^{10}} + 1 = \left(\frac{-1 + t^{10} + t^{20}}{2t^{15}}\right)^2,$$

in addition to the points already known, given by

$$f\left(0\right) = 1, \quad f\left(1\right) = u^2,$$
$$f\left(\frac{n}{r}\right) = \frac{\left(2n^2 + 2nr + r^2\right)^2}{r^4},$$
$$f\left(-\frac{n}{n+r}\right) = \frac{\left(n^2 + r^2\right)^2}{\left(n+r\right)^4}.$$

Accordingly, the curve C_k with $k = m^4$, where m is given by (3–1), has at least twelve finite points. Similar arguments as in Theorem 2.1 show that infinitely many non-isomorphic curves arise. □

4. AN EXAMPLE: $k = -7$

While there exist in the literature examples in which all integer points are found on curves of type $y^2 = x^5 + k$ (see, for example, [Blass 74, Blass 76, Mignotte and de Weger 96, Wren 73]), the methods will not determine the full set of rational points. When the rank of the Jacobian variety is at least 2, standard Chabauty arguments (see, for example, the exposition in [Cassels and Flynn 96]) are inapplicable, and it is difficult to determine explicitly all rational points. It seems that the best approach is the elliptic-curve Chabauty method developed by Bruin; for a good overview, see [Bruin 06].

We do not know of any example in the literature that finds all the rational points on a curve C_k whose Jacobian is at least of rank 2, though Bremner and Tzanakis consider the similar family of genus 2 curves $y^2 = x^6 + k$ [Bremner and Tzanakis 06]. Here, we take a specific curve and find all rational points corresponding to $k = -7$.

Theorem 4.1. *The finite points on*

$$Y^2 = X^5 - 7 \tag{4–1}$$

are given by $(X, \pm Y) = (2, 5), (8, 181)$.

Proof: We work in the algebraic number field $K = \mathbb{Q}(\theta)$, where $\theta^5 = 7$. The ring of integers is

$$\mathcal{O}_K = \mathbb{Z}\left[1, \theta, \theta^2, \theta^3, \frac{1}{5}(\theta^4 + 2\theta^3 + 4\theta^2 + 3\theta + 1)\right],$$

the class number of $\mathcal{O}_K$ is 1, the ideal $\langle 5 \rangle$ factors as $\langle 5 \rangle = \mathcal{P}_1\mathcal{P}_2^4$, and the real fifth root of 7 is given by $\theta_0 \approx 1.475773161594552$. There are two fundamental units ϵ_1, ϵ_2 in K, which we normalize to satisfy $\epsilon_i(\theta_0) > 0$, $i = 1, 2$.

In (4–1), put

$$X = x/z^2, \quad Y = y/z^5, \quad x, y, z \in \mathbb{Z}, \quad (x, z) = 1.$$

The equation takes the form

$$(x - \theta z^2)(x^4 + \theta x^3 z^2 + \theta^2 x^2 z^4 + \theta^3 x z^6 + \theta^4 z^8) = y^2.$$

A prime ideal dividing the two factors on the left divides both $\langle x - \theta z^2 \rangle$ and $\langle 5\theta^4 \rangle$, and since clearly $(x, 7) = 1$, the greatest common divisor is $\langle 1 \rangle$ for $x \not\equiv 2z^2 \bmod 5$, and is $\mathcal{P}_1\mathcal{P}_2 = \langle 2 - \theta \rangle$ in the case $x \equiv 2z^2 \bmod 5$.

Thus we have the element equations

$$x - \theta z^2 = g \cdot u \cdot \alpha^2, \tag{4–2}$$
$$x^4 + \theta x^3 z^2 + \theta^2 x^2 z^4 + \theta^3 x z^6 + \theta^4 z^8 = g \cdot u^{-1} \cdot \beta^2,$$

for the greatest common divisor g equal to 1 or $2 - \theta$, unit u, and elements $\alpha, \beta \in \mathcal{O}_\mathcal{K}$, with $g\alpha\beta = y$.

Without loss of generality, $u = \pm\epsilon_1^{i_1}\epsilon_2^{i_2}$, where $i_1, i_2 = 0, 1$, and by specializing the second equation in (4–2) to θ_0, only the positive sign can hold. Eliminating x in (4–2) results in

$$g^4u^4\alpha^8 + 5\theta g^3u^3\alpha^6 z^2 + 10\theta^2 g^2u^2\alpha^4 z^4 + 10\theta^3 gu\alpha^2 z^6 \\ + 5\theta^4 z^8 = u^{-1}\beta^2. \tag{4–3}$$

We consider two cases:

Case 1: $g = 1$. The cases $u = \epsilon_2$, $\epsilon_1\epsilon_2$, render (4–3) locally unsolvable at $\mathcal{P}_2$, so only $u = 1$, ϵ_1, must be considered.

When $u = 1$, we have

$$x^4 + \theta x^3 z^2 + \theta^2 x^2 z^4 + \theta^3 x z^6 + \theta^4 z^8 = \beta^2,$$

defining an elliptic curve E_1 over K with $\mathbb{Z}/2\mathbb{Z}$ torsion. The routine `PseudoMordellWeilGroup` in MAGMA tells us that the K-rank of E_1 is equal to 2; and the routine `Chabauty`, which works p-adically in this instance with $p = 3$, tells us that the only K-points on E_1 satisfying $x/z^2 \in \mathbb{Q}$ are given by

$$\left(x, z^2, \beta\right) = (1, 0, 1), \quad \left(0, 1, \theta^2\right),$$

and

$$\left(8, 1, \frac{1}{5}\left(42\theta^4 - 26\theta^3 - 27\theta^2 + 146\theta + 82\right)\right).$$

Only the latter returns a finite point on the original curve, namely at $X = 8$.

When $u = \epsilon_1$, then

$$\epsilon_1\left(x^4 + \theta x^3 z^2 + \theta^2 x^2 z^4 + \theta^3 x z^6 + \theta^4 z^8\right) = \beta^2,$$

defining an elliptic curve (again with $\mathbb{Z}/2\mathbb{Z}$ torsion) of K-rank 2 (this computation was laborious, taking two weeks on a desktop PC, in contrast to at most a couple of minutes for the computation of the other ranks in this paper). Using MAGMA with `Chabauty` working 11-adically, we discover that there are no points on the curve satisfying $x/z^2 \in \mathbb{Q}$. (This ran for four days, compared to the one or two seconds for the corresponding calculations in the other cases).

Case 2: $g = 2 - \theta$**.** At $u = \epsilon_1$, $\epsilon_1\epsilon_2$, the curve (4–3) is locally unsolvable at the prime $\langle 2, 3 + \theta\rangle$; and at $u = \epsilon_2$, we have unsolvability at the prime $\langle 2, \theta^4+\theta^3+\theta^2+\theta+1\rangle$. So only $u = 1$ remains to be considered, giving the curve

$$x^4 + \theta x^3 z^2 + \theta^2 x^2 z^4 + \theta^3 x z^6 + \theta^4 z^8 = (2 - \theta)\beta^2,$$

defining an elliptic curve of K-rank 2 with $\mathbb{Z}/2\mathbb{Z}$ torsion.

Working 3-adically, `Chabauty` shows that the only K-point with $x/z^2 \in \mathbb{Q}$ is given by

$$\left(x, z^2, \beta\right) = \left(2, 1, \frac{1}{5}\left(\theta^4 + 2\theta^3 + 4\theta^2 + 8\theta + 16\right)\right),$$

returning $X = 2$ on the original curve. □

REFERENCES

[Blass 74] J. Blass. "On the Diophantine Equation $Y^2 + K = X^5$." *Bull. Amer. Math. Soc.* 80 (1974), 329.

[Blass 76] J. Blass. "A Note on Diophantine Equation $Y^2 + k = X^5$." *Math. Comp.* 30:135 (1976), 638–640.

[Bosma et al. 97] W. Bosma, J. Cannon, and C. Playoust. "The Magma Algebra System. I. The User Language." *J. Symbolic Comput* 24:3–4 (1997), 235–265.

[Bremner and Tzanakis 06] A. Bremner and N. Tzanakis. "On the Equation $Y^2 = X^6 + k$." Preprint, 2006.

[Bruin 06] N. Bruin. "Some Ternary Diophantine Equations of Signature $(n, n, 2)$." In *Discovering Mathematics with Magma*, pp. 63–91, Algorithms Comput. Math. 19. Berlin: Springer 2006.

[Cassels and Flynn 96] J. W. S. Cassels and V. E. Flynn. *Prolegomena to a Middlebrow Arithmetic of Curves of Genus* 2, London Math. Soc. Lect. Notes 230. Cambridge: Cambridge University Press, 1996.

[Mignotte and de Weger 96] M. Mignotte and B. M. M. de Weger. "On the Diophantine Equations $x^2 + 74 = y^5$ and $x^2 + 86 = y^5$." *Glasgow Math. J.* 38:1 (1996), 77–85.

[Stoll 06] M. Stoll. "On the Number of Rational Squares at Fixed Distance from a Fifth Power." *Acta Arith.* 125:1 (2006), 79–88.

[Wren 73] B. M. E. Wren. "$y^2 + D = x^5$." *Eureka* 36 (1973), 37–38.

Andrew Bremner, Department of Mathematics and Statistics, Arizona State University, Tempe AZ 85287-1804
(bremner@asu.edu)

Received April 18, 2007; accepted January 9, 2008.