Notes on Number Theory and Discrete Mathematics
Print ISSN 1310–5132, Online ISSN 2367–8275
Vol. 26, 2020, No. 1, 40–44
DOI: 10.7546/nntdm.2020.26.1.40-44

A parametrised family of Mordell curves with a rational point of order 3

Ajai Choudhry[1] and Arman Shamsi Zargar[2]

[1] 13/4 A Clay Square, Lucknow - 226001, India
e-mail: ajaic203@yahoo.com

[2] Department of Mathematics and Applications, Faculty of Science
University of Mohaghegh Ardabili
Ardabil 56199-11367, Iran
e-mail: zargar@uma.ac.ir

Received: 1 April 2019 **Revised:** 30 December 2019 **Accepted:** 8 January 2020

Abstract: An elliptic curve defined by an equation of the type $y^2 = x^3 + d$ is called a Mordell curve. This paper is concerned with Mordell curves for which $d = k^2,\ k \in \mathbb{Z},\ k \neq 1$. The point $(0,\, k)$ on such curves is of order 3 and the torsion subgroup of the group of rational points on such Mordell curves is necessarily $\mathbb{Z}/3\mathbb{Z}$. We obtain a parametrised family of Mordell curves $y^2 = x^3 + k^2$ such that the rank of each member of the family is at least three. Some elliptic curves of the family have ranks 4 and 5.

Keywords: Mordell curves, Rank of elliptic curves.
2010 Mathematics Subject Classification: 11D25, 11G05.

1 Introduction

Ever since Fermat's assertion that the only solution in positive integers of the equation $y^2 = x^3 - 2$ is $(x,\, y) = (3,\, 5)$ [10], the Diophantine equation,

$$y^2 = x^3 + d, \tag{1}$$

has been subjected to extensive investigations (see [1, 3–5, 7–11], [12, Chapter 26, pp. 238–254], [13, 17]). Eq. (1) has now been solved for all integer values of d with $|d| \leq 10^7$ [1].

The elliptic curve represented by Eq. (1) is known as a Mordell curve. Despite the vast literature on Mordell curves, it seems that the family of Mordell curves defined by the equation,

$$y^2 = x^3 + k^2, \quad k \in Z, \ \ k \neq 1, \tag{2}$$

has not been specifically studied. It has, however, been shown that the point $(0,\ k)$ on such curves is of order 3 and the torsion subgroup of the group of rational points on such Mordell curves is necessarily $\mathbb{Z}/3\mathbb{Z}$ [6, Theorem 5.3, p. 134]. While numerical examples of such curves with ranks 8, 9 and 10 have been found using computational methods [2, pp. 191–192], a parametrised family of such curves has not yet been obtained.

2 A parametrised family of Mordell curves

We will construct, in this paper, a parametrised family of curves defined by an equation of type (2) such that the rank of the elliptic curves belonging to this family is, in general, at least three.

We will first solve the system of Diophantine equations,

$$v_1^2 = u_1^3 + k^2, \tag{3}$$

$$v_2^2 = u_2^3 + k^2, \tag{4}$$

$$v_3^2 = u_3^3 + k^2. \tag{5}$$

On writing,

$$u_1 = am, \quad u_2 = bm, \quad u_3 = cm, \tag{6}$$

and eliminating m first between Eq. (3) and Eq. (4), and then between Eq. (3) and Eq. (5), we get the following two equations:

$$b^3(v_1^2 - k^2) = a^3(v_2^2 - k^2), \tag{7}$$

$$c^3(v_1^2 - k^2) = a^3(v_3^2 - k^2). \tag{8}$$

To solve equations (7) and (8), we write,

$$v_1 = w_1t + k, \quad v_2 = w_2t + k, \quad v_3 = w_3t + k,$$

when each of the two equations (7) and (8) can be readily solved to get a nonzero solution for t. Equating these two values of t, we get the condition,

$$(b^3w_1 - a^3w_2)(c^3w_1^2 - a^3w_3^2) = (c^3w_1 - a^3w_3)(b^3w_1^2 - a^3w_2^2). \tag{9}$$

Now Eq. (9) is a homogeneous cubic equation in the variables w_1, w_2 and w_3 and it represents a cubic curve in the projective plane. Further, a rational point on this curve is easily seen to be $(w_1,\ w_2,\ w_3) = (a^3,\ b^3,\ c^3)$. The tangent to the cubic curve (9) at the aforementioned rational point necessarily intersects the curve (9) at another rational point which is thus easily found, and is given by,

$$w_1 = a^3(b^3 + c^3 - a^3), \ \ w_2 = b^3(c^3 + a^3 - b^3), \ \ w_3 = c^3(a^3 + b^3 - c^3).$$

With these values of w_1, w_2, w_3, we obtain the following solution of the simultaneous equations (7) and (8):

$$\begin{aligned} v_1 &= -(3a^6 - 2a^3b^3 - 2a^3c^3 - b^6 + 2b^3c^3 - c^6)r,\\ v_2 &= (a^6 + 2a^3b^3 - 2a^3c^3 - 3b^6 + 2b^3c^3 + c^6)r,\\ v_3 &= (a^6 - 2a^3b^3 + 2a^3c^3 + b^6 + 2b^3c^3 - 3c^6)r,\\ k &= (a^6 - 2a^3b^3 - 2a^3c^3 + b^6 - 2b^3c^3 + c^6)r, \end{aligned} \tag{10}$$

where a, b, c and r are arbitrary parameters. Substituting the values of v_1, v_2, v_3 and k given by (10) and the value of u_1 given by (6) in (3), we get,

$$a^3m^3 = -8a^3r^2(a^3 + b^3 - c^3)(b^3 + c^3 - a^3)(c^3 + a^3 - b^3). \tag{11}$$

Now Eq. (11) is readily solved by taking $m = -2r$, when we get,

$$r = (a^3 + b^3 - c^3)(b^3 + c^3 - a^3)(c^3 + a^3 - b^3).$$

We thus obtain a solution of the system of equations (3), (4) and (5) which is given by

$$k = (a^3 + b^3 - c^3)(b^3 + c^3 - a^3)(c^3 + a^3 - b^3)(a^6 - 2a^3b^3 - 2a^3c^3 + b^6 - 2b^3c^3 + c^6), \tag{12}$$

and

$$\begin{aligned} u_1 &= -2a(a^3 + b^3 - c^3)(b^3 + c^3 - a^3)(c^3 + a^3 - b^3),\\ u_2 &= -2b(a^3 + b^3 - c^3)(b^3 + c^3 - a^3)(c^3 + a^3 - b^3),\\ u_3 &= -2c(a^3 + b^3 - c^3)(b^3 + c^3 - a^3)(c^3 + a^3 - b^3),\\ v_1 &= (a^3 + b^3 - c^3)(b^3 + c^3 - a^3)(c^3 + a^3 - b^3)\\ &\qquad \times (3a^6 - 2a^3b^3 - 2a^3c^3 - b^6 + 2b^3c^3 - c^6),\\ v_2 &= (a^3 + b^3 - c^3)(b^3 + c^3 - a^3)(c^3 + a^3 - b^3)\\ &\qquad \times (a^6 + 2a^3b^3 - 2a^3c^3 - 3b^6 + 2b^3c^3 + c^6),\\ v_3 &= (a^3 + b^3 - c^3)(b^3 + c^3 - a^3)(c^3 + a^3 - b^3)\\ &\qquad \times (a^6 - 2a^3b^3 + 2a^3c^3 + b^6 + 2b^3c^3 - 3c^6), \end{aligned} \tag{13}$$

where a, b, c are arbitrary parameters.

It follows that when k is given by (12), there are three rational points $P_1(a,\, b,\, c)$, $P_2(a,\, b,\, c)$ and $P_3(a,\, b,\, c)$ on the elliptic curve (2) with co-ordinates $(u_i,\, v_i)$, $i = 1,\, 2,\, 3$, where the values of u_i, $v_i, i = 1,\, 2,\, 3$, are given by (13).

We will now apply a theorem of Silverman [16, Theorem 11.4, p. 271] to show that these points are linearly independent. For this, we must find a specialisation $(a, b, c) = (a_0, b_0, c_0)$ such that the points $P_1(a_0, b_0, c_0)$, $P_2(a_0, b_0, c_0)$, and $P_3(a_0, b_0, c_0)$ are linearly independent on the specialised curve over $\mathbb{Q}$.

We take $(a, b, c) = (1, 2, 3)$, when we get the elliptic curve,

$$y^2 = x^3 + 3574080^2, \tag{14}$$

on which we get the three points,

$$\begin{aligned}P_1(1,2,3) &= (24480, 5238720),\\ P_2(1,2,3) &= (48960, 11407680),\\ P_3(1,2,3) &= (73440, 20220480),\end{aligned}$$

each of which is of infinite order. The regulator of these three points, as determined by the software SAGE [14] is 33.9574760167017. As this is nonzero, it follows from a well-known theorem [15, Theorem 8.1, p. 242] that these three points are linearly independent. Hence, the rank of the Mordell curve (14) is at least 3.

It now follows from the aforementioned theorem of Silverman that, in general, the rank of the elliptic curves of the parametrised family of Mordell curves (2), where k is given by (12), is at least 3.

3 Mordell curves of rank greater than 3

For specific numerical values of the parameters $a,\ b,\ c$, the parametrised family of Mordell curves, obtained in Section 2, yields Mordell curves of rank greater than 3.

In fact, we note that the rank of the Mordell curve (14), as determined by the software SAGE, is 4 with four generators of the Mordell–Weil group being given by $(-23360,\ 163520)$, $(-19856,\ 2223872)$, $(-10880,\ 3389120)$, $(7200,\ 3625920)$.

We found two more curves of rank 4 obtained by taking $(a,\ b,\ c) = (1,\ 2,\ -2)$ and $(a,\ b,\ c) = (1,\ 2,\ -3)$. We thus get the elliptic curve

$$y^2 = x^3 + 4294836225,$$

whose four generators are $(-1190,\ 51085)$, $(-1020,\ 56865)$, $(-510,\ 64515)$, and $(64,\ 65537)$, and the curve

$$y^2 = x^3 + 957451920998400$$

whose four generators are $(-97920,\ 4308480)$, $(-70784,\ 24551936)$, $(-48960,\ 28984320)$, and $(29440,\ 31352320)$.

Finally, when $(a,\ b,\ c) = (1,\ -3,\ -4)$, we get the following elliptic curve of rank 5:

$$y^2 = x^3 + 38153227600134144.$$

The five generators of this curve are as $(-335232,\ 21901824)$, $(-23408/9,\ 5273868608/27)$, $(109440,\ 198655488)$, $(120960,\ 199807488)$, and $(61682688,\ 484445551104)$.

Acknowledgements

The first author thanks the Harish-Chandra Research Institute, Allahabad for providing him with all necessary facilities that have helped him to pursue his research work in mathematics.

References

[1] Bennett, M., & Ghadermarzi, A. (2015). Mordell's equation: a classical approach, *LMS J. Comput. Math.*, 18 (1), 633–646.

[2] Elkies, N. D., & Rogers, N. F. (2004). Elliptic curves $x^3 + y^3 = k$ of high rank, in Algorithmic number theory (ANTS-VI), ed. D. Buell, *Lecture Notes in Comput. Sci.*, 3076, Springer, Berlin, 184–193.

[3] Ellison, W. J., Ellison, F., Pesek, J., Stahl, C. E., & Stall, D. S. (1972). The Diophantine equation $y^2 + k = x^3$, *J. Number Theory*, 4 (2), 107–117.

[4] Gebel, J., Pethö, A., & Zimmer, H. G. (1998). On Mordell's equation, *Compos. Math.*, 110 (3), 335–367.

[5] Hall, Jr., M. (1953). Some equations $y^2 = x^3 - k$ without integer solutions, *J. Lond. Math. Soc. (1)*, 28 (3), 379–383.

[6] Knapp, A. (1992). *Elliptic Curves*, Princeton University Press, Princeton.

[7] Lal, M., Jones, M. F., & Blundon, W. J. (1966). Numerical solutions of the Diophantine equation $y^3 - x^2 = k$, *Math. Comp.*, 20 (94), 322–325.

[8] Ljunggren, W. (1963). On the Diophantine equation $y^2 - k = x^3$, *Acta Arith.*, 8 (4), 451–463.

[9] Mordell, L. J. (1914). The Diophantine equation $y^2 + k = x^3$, *Proc. Lond. Math. Soc. (2)*, 13 (1), 60–80.

[10] Mordell, L. J. (1920). A statement by Fermat, *Proc. Lond. Math. Soc. (2)*, 18 (1).

[11] Mordell, L. J. (1966). The infinity of rational solutions of $y^2 = x^3 + k$, *J. Lond. Math. Soc. (1)*, 41 (1), 523-525.

[12] Mordell, L. J. (1969). *Diophantine Equations*, Academic Press, London.

[13] Poulakis, D. (1999). The number of solutions of the Mordell equation, *Acta Arith.*, 88 (2), 173–179.

[14] SAGE software, Available online at: `http://www.sagemath.org`.

[15] Schmitt, S., & Zimmer, H. G. (2003). *Elliptic Curves: A Computational Approach*, Walter de Gruyter, Berlin.

[16] Silverman, J. H. (1994). *Advanced Topics in the Arithmetic of Elliptic Curves*, Springer, New York.

[17] Young, M. P. (2015). The number of solutions to Mordell's equation in constrained ranges, *Mathematika*, 61 (3), 708–718.