A family of elliptic curves with the rank of at least three arising from quartic curves

Seiji Tomita

Abstract

We will construct a new family of elliptic curves with the rank of at least three arising from quartic curves.

1. Introduction

The equation $Y^2 = aX^4 + bX^2 + c$ has been studied by many mathematicians. Euler[2] found many solutions of $x^4+mx^2y^2+y^4 = z^2$ for $|m| < 200$. Pocklington[3] and Zhang[6] proved that $x^4+mx^2y^2+y^4 = z^2$ has only trivial solutions for the restricted m. Bremner[1] and Jones determined the solvability of the equation $x^4 + mx^2y^2 + y^4 = z^2$ for $|m| < 3000$ by perfoming calculations with L-series of elliptic curve.

In this paper, we present a new family of elliptic curves with the rank of at least three arising from quartic curves.

$$E : y^2 = x^3 - a^2x^2 + b^2x \tag{1}$$

$$Q : Y^2 = aX^4 + bX^2 + c$$

We often come across this type of quartic curve, $Y^2 = aX^4 + bX^2 + c$, when studying diophantine equations. This quartic curve can be transformed into an elliptic curve if we know a rational point. However, if the height of the rational point is very large, we cannot transform it into an elliptic curve. Thus, a method of conversion without rational points is effective. In particular, we consider the quartic curve $Y^2 = X^4 - a^2X^2 + b^2$. Taking $U = X^2$ and $V = XY$, then we get an elliptic curve

$$E : V^2 = U^3 - a^2U^2 + b^2U.$$

If a rational point $P(U,\ V)$ on E is known, computing $2P(U,\ V)$ is possible using the group structure. Since x-coordinate of $2P(U,\ V)$ is a perfect square number by the duplication formula of $P(U,\ V)$, we obtain a rational point $X = \sqrt{U}$ on the quartic curve. Thus, the information of rational points(e.g.,rank, generators) on an elliptic curve can be pulled back to quartic curve. Therefore, we can know the solubility of the quartic curve from the elliptic curve.

2. Main result

We shall construct a parametrized family with the rank of at least three. Forcing a^2 to be x-coordinates of the point on E. Thus we get a first point $P_1 = (a^2,\ ab)$ on the elliptic curve. Now, we try to increase the rank by forcing the x-coordinates of the second point P_2 to be $x = b^2$. This holds when $b^2 - a^2 + 1 = u^2$ for some rational number u.

A simple calculation shows that $(a,\ b) = \Big(\dfrac{k^2-2k-4}{k^2},\ -\dfrac{k^2+2k+4}{k^2}\Big)$.

Hence, the second point

$$P_2 = \Big(\frac{(k^2+2k+4)^2}{k^4},\ \frac{(k^2+2k+4)^2(k+4)}{k^5}\Big)$$

is a rational point on

$$y^2 = x^3 - \frac{(k^2-2k-4)^2}{k^4}x^2 + \frac{(k^2+2k+4)^2}{k^4}x.$$

We try to increase the rank by forcing the x-coordinates of the 3rd point P_3 to be $x = a^2 - b^2$. This holds when $k + 2 = -2m^2$ for some rational number m.

A simple calculation shows that

$$x = \frac{4m^2}{(m^2+1)^2}.$$

Hence, the point

$$P_3 = \Big(\frac{4m^2}{(m^2+1)^2},\ \frac{2m(m-1)(m+1)(m^2-m+1)(m^2+m+1)}{(m^2+1)^4}\Big)$$

is a rational point on

$$y^2 = x^3 - \frac{(m^4+3m^2+1)^2}{(m^2+1)^4}x^2 + \frac{(m^2-m+1)^2(m^2+m+1)^2}{(m^2+1)^4}x, \tag{2}$$

which contains the points,

$$P_1 = \Big(\ \frac{(m^4+3m^2+1)^2}{(m^2+1)^4},\ \frac{(m^2-m+1)(m^2+m+1)(m^4+3m^2+1)}{(m^2+1)^4}\ \Big),$$

$$P_2 = \Big(\ \frac{(m^2-m+1)^2(m^2+m+1)^2}{(m^2+1)^4},\ \frac{(m^2-m+1)^2(m^2+m+1)^2(m-1)(m+1)}{(m^2+1)^5}\ \Big),$$

$$P_3 = \Big(\ \frac{4m^2}{(m^2+1)^2},\ \frac{2m(m-1)(m+1)(m^2-m+1)(m^2+m+1)}{(m^2+1)^4}\ \Big).$$

Specialization to $m = 3$ yields the elliptic curve

$$y^2 = x^3 - \frac{11881}{10000}x^2 + \frac{8281}{10000}x.$$

The points

$$P_1 = \Big(\frac{11881}{10000},\ \frac{9919}{10000}\Big),\ P_2 = \Big(\frac{8281}{10000},\ \frac{8281}{12500}\Big),\ P_3 = \Big(\frac{9}{25},\ \frac{273}{625}\Big)$$

have regulator 67.8487922570794 by Sage[4], then the three points are independent, and Silverman's specialization theorem[5] shows the rank of the family of elliptic curves given by the parametric solution of (2) is at least three.

3. High rank examples

We calculated (2) for $m < 100$ and found several elliptic curves of the rank $4, 5, 6$, and 7.

Table 1: High rank examples

rank	m					
4	1/2,	1/4,	1/6,	1/8,	5/2,	5/7, $\cdots$
5	1/5,	3/5,	5/8,	3/10,	4/11,	3/16, $\cdots$
6	1/7,	1/10,	3/11,	4/19,	7/19,	8/25, $\cdots$
7	74/57, $\cdots$					

References

[1] A. Bremner and John W. Jones, On the Equation $x^4 + mx^2y^2 + y^4 = z^2$, February 1995,Journal of Number Theory 50(2):268-298

[2] Euler, L., De casibus quibus formulam $x^4 + mxxyy + y^4$ ad quadratum reducere licet, Mem. acad. sci. St. Petersbourg 7 (1815/1816, 1820), 10?22; Opera Omnia, ser. I, V, 365?47, Geneva, 1944

[3] H. C. Pocklington, Some diophantine impossibilities, Proc. Cambridge Phil. Soc. 17 (1914), 108-121.

[4] SAGE software, Available at `http://sagemath.org`.

[5] J. H. Silverman, Advanced topics in the arithmetic of elliptic curves, Springer, New York, 1994.

[6] Zhang, M. Z., On the diophantine equation $x^4 + kx^2y^2 + y^4 = z^2$, Sichuan Daxue Xuebao 2, (1983), 24?31.