International Journal of Algebra, Vol. 13, 2019, no. 4, 161 – 166
HIKARI Ltd, www.m-hikari.com
https://doi.org/10.12988/ija.2019.9314

Rational Points on the Elliptic Curve

$y^2 = x^3 - p^2x$

Baraah Maya

Faculty of Mathematics, Tishreen University, Syria

Hasan Sankari

Faculty of Mathematics, Tishreen University, Syria

Abstract

We consider the problem of finding a nontrivial rational points on the elliptic curve $y^2 = x^3 - p^2x$. We give a relationship between rational points on this curve and integer solutions to a system of two homogeneous equations of degree 2. Namely, every solution to this set corresponds to different eight rational points on the elliptic curve $y^2 = x^3 - p^2x$.

Keywords: elliptic curves, congruent, rational points, prime.

1 Introduction

Let E be a nonsingular cubic curve with rational coefficients, then the group $E(\mathbb{Q})$of rational points on E is finitely generated. We write:

$$E(\mathbb{Q}) \cong E(Q)_{tor} \oplus \mathbb{Z}^r$$

where $E(\mathbb{Q})_{tor}$ is a finite group and r is a non-negative integer called the rank Mordell-Weil of E.

In this paper we study a special case of curves which have three rational points of order 2. Namely, elliptic curves of the form:

$$y^2 = x^3 - p^2x \tag{1}$$

For an odd prime p. These curves have dram a lot of attention because of its connection to the congruent number problem. A positive integer n is a *congruent* if it is the area of a right triangle with all rational side lengths. It is well-known that the positive integer n is a congruent if there is a rational point $P(x, y)$ on the curve $y^2 = x^3 - n^2x$ with $y \neq 0$.
The equation (1) can be written as follows:

$$y^2 = x(x-p)(x+p) \tag{2}$$

So the factors on the right-hand side can be written:

$$\begin{cases} x = au^2 \\ x - p = bv^2 \\ x + p = cw^2 \end{cases} \tag{3}$$

Here $u, v, w \in \mathbb{Q}$, a, b, c are square-free integers, and the product abc is a perfect square.
Let $\mathbb{Q}^{*2}$ be the group of non-zero rational squares, and let $\mathbb{Q}^{\star}/\mathbb{Q}^{\star 2}$ be the group of the co-sets $m\mathbb{Q}^{\star 2}$, where m is a non-zero rational number. Let α be the map:

$$\alpha\colon\ E(\mathbb{Q}) \to \mathbb{Q}^{\star}/\mathbb{Q}^{\star 2} \oplus \mathbb{Q}^{\star}/\mathbb{Q}^{\star 2} \oplus \mathbb{Q}^{\star}/\mathbb{Q}^{\star 2}$$

Which is defined for every rational point $P \in E(\mathbb{Q})$ as follows:

- If order of P doesn't equal 2, then:
$$\alpha(P) = (x, x-p, x+p)$$
- If order of P equals 2, then:
$$\alpha(0,0) = (-1, -p, p)$$
$$\alpha(p, 0) = (p, 2, 2p)$$
$$\alpha(-p, 0) = (-p, -2p, 2)$$
- Finally, we have:
$$\alpha(\infty) = (1,1,1)$$

The map α which defined above is a group homomorphism (by proposition 5,[6]), and $im\alpha$ is a finite set of triples (a, b, c) which satisfy (1) (by proposition4,[6]), and the prime factors for the product abc divide $2p^3$(by proposition4,[6]).
Since a, b, c are square-free integer numbers, we find:

$$a, b, c \in \{\pm 1, \pm 2, \pm p, \pm 2p\}$$

We notice that a, b are either negative together or positive together, we also notice that a can't be even. So the triples (a, b, c) which could belong to $im\alpha$ are the triples which belong to the set S, where:

S $= \{(1,1,1), (1,2,2), (1,p,p), (1,2p,2p), (p,1,p), (p,2,2p), (p,p,1), (p,2p,2), (-1,-2p,2p), (-1,-p,p), (-1,-2,2), (-1,-1,1), (-p,-2p,2), (-p,-p,1), (-p,-2,2p), (-p,-1,p)\}$

Hence $im\alpha \subseteq$ S.

According to the definition of α we find that for any prime p, the triples:

$$(1,1,1), (p,2,2p), (-1,-p,p), (-p,-2p,2)$$

belong to $im\alpha$.

By using certain calculative operations, we can get the following corollary.

2 Corollary

(1) If the triples:

$$(1,2,2), (-1,-2p,2p), (p,1,p), (-p,-p,1)$$

belong to $im\alpha$, *then* $p \equiv 1$ *or* $7 \pmod 8$.

(2) If the triples:

$$(1,p,p), (-1,-1,1), (p,2p,2), (-p,-2,2p)$$

belong to $im\alpha$, *then* $p \equiv 1$ or $5 \pmod 8$.

(3) If the triples:

$$(1,2p,2p), (-1,-2,2), (p,p,1), (-p,-1,p)$$

belong to $im\alpha$, *then* $p \equiv 1 \pmod 8$.

Let's define S_0 as follows:

$$S_0 = \{(1,1,1), (-1,-p,p), (p,2,2p), (-p,-2p,2)\}$$

We notice that $S_0 \subseteq im\alpha$ for any odd prime.

Now let's define S_1, S_2, S_3 as follows:

$$S_1 = \{(1,2,2), (-1,-2p,2p), (p,1,p), (-p,-p,1)\} \cup S_0$$
$$S_2 = \{(1,p,p), (-1,-1,1), (p,2p,2), (-p,-2,2p)\} \cup S_0$$
$$S_3 = \{(1,2p,2p), (-1,-2,2), (p,p,1), (-p,-1,p)\} \cup S_2 \cup S_1 = S$$

3 Theorem

Let p is an odd prime, then there is a nontrivial rational point on the elliptic curve $y^2 = x^3 - p^2x$ if the system of two equations:

$$\begin{cases} X^2 - (-1)^{\frac{p-i}{2}} Y^2 = 2^{\varepsilon} Z^2 \\ X^2 - (-1)^{\frac{p+i}{2}} Y^2 = 2^{\varepsilon} p W^2 \end{cases} \qquad (I)$$

has an integer solution (X, Y, Z, W) *with* $XYZW \neq 0$, *where:*

$$(i,\varepsilon)=\begin{cases}(1,0) & if\ p\equiv 7(mod\ 8)\\ (1,1) & if\ p\equiv 5(mod\ 8)\\ (-1,0),(1,0),or\ (1,1) & if\ p\ \equiv 1(mod\ 8)\end{cases}$$

Moreover, If this condition is satisfied, then for every solution to *(I)* we get a set of different eight rational points on the curve $y^2=x^3-p^2x$, which are:

$$P_1=\left(\frac{(-1)^{\frac{p+i}{2}}Z^2}{W^2},\frac{2^{1-\varepsilon}ZYX}{W^3}\right)\quad,\quad -P_1=\left(\frac{(-1)^{\frac{p+i}{2}}Z^2}{W^2},-\frac{2^{1-\varepsilon}ZYX}{W^3}\right)$$

$$P_2=\left(\frac{pX^2}{Y^2},\frac{2^{\varepsilon}p^2XWZ}{Y^3}\right)\quad,\quad -P_2=\left(\frac{pX^2}{Y^2},-\frac{2^{\varepsilon}p^2XWZ}{Y^3}\right)$$

$$P_3=\left(\frac{(-1)^{\frac{p-i}{2}}p^2W^2}{Z^2},\frac{2^{1-\varepsilon}p^2XWY}{Z^3}\right)\quad,\quad -P_3=\left(-\frac{(-1)^{\frac{p-i}{2}}p^2W^2}{Z^2},-\frac{2^{1-\varepsilon}p^2XWY}{Z^3}\right)$$

$$P_4=\left(-\frac{pY^2}{X^2},\frac{2^{\varepsilon}p^2WYZ}{X^3}\right)\quad,\quad -P_4=\left(-\frac{pY^2}{X^2},-\frac{2^{\varepsilon}p^2WYZ}{X^3}\right)$$

Proof: Suppose that p is congruent, and let's proof that (I) is solvable.
First suppose that $p\equiv 7(mod\ 8)$. In this case, there is a rational point $P=(x,y)$ on the curve $y^2=x^3-p^2x$ where $y\neq 0$, so $\alpha(P)\in S_1\backslash S_0$. Without loss of generalizing we can assume that $\alpha(P)$ = (1,2,2), hence:

$$\begin{cases}x=u^2\\ x-p=2v^2\\ x+p=2w^2\end{cases}\tag{4}$$

Here $u=\frac{n}{e}$, $v=\frac{m}{e}$, $w=\frac{s}{e}$ are non-zero rational numbers written in lowest terms, then by substituting in (4) we find:

$$x=\frac{n^2}{e^2}\tag{5}$$
$$n^2-pe^2=2m^2\tag{6}$$
$$n^2+pe^2=2s^2\tag{7}$$

By adding (6) to (7), then subtracting (6) from (7) we find:

$$s^2+m^2=n^2$$
$$s^2-m^2=pe^2$$

Hence (X,Y,Z,W) = (s,m,n,e) is a solution for (I) when (i,ε) = (1,0) with $XYZW\neq 0$ because $u,v,w$are non-zero rational numbers.

By similar way we can proof that if $p\equiv 5(\text{mod } 8)$ is a congruent, (I) is solvable.

Now suppose that $p\equiv 1 (\text{mod } 8)$, and $P = (x, y)$ is a rational point on the curve $y^2 = x^3 - p^2x$ with $y\neq 0$, then $\alpha(P) \in S_3 \backslash S_0$ where:

$$S_3 = \{(1,2p,2p), (-1,-2,2), (p,p,1), (-p,-1,p)\} \cup S_2 \cup S_1$$

So we distinguish between three cases:

- $\alpha(P) \in S_1 \backslash S_0$: In this case, the proof is exactly as the proof when $p \equiv 7 (mod\ 8)$, and (I) is solvable when $(i,\varepsilon) = (1,0)$.
- $\alpha(P) \in S_2 \backslash S_0$: In this case, the proof is exactly as the proof when $p \equiv 5 (mod\ 8)$, and (I) is solvable when $(i,\varepsilon) = (1,1)$.
- $\alpha(P) \in S_3 \backslash (S_1 \cup S_2)$: We can assume that $\alpha(P) = (1,2p,2p)$, and continue by similar way to the first case.

Conversely, suppose that (I) is solvable, and (X,Y,Z,W) is a solution with $XYZW\neq 0$.

We notice that:

$$Z^2 - pW^2 = (-1)^{\frac{p+i}{2}} 2^{1-\varepsilon} Y^2$$
$$Z^2 + pW^2 = 2^{1-\varepsilon} X^2$$

We will proof that $\pm P_1$ are points on the curve $y^2 = x^3 - p^2x$:

$$\left[\frac{(-1)^{\frac{p+i}{2}} Z^2}{W^2}\right]^3 - p^2\left[\frac{(-1)^{\frac{p+i}{2}} Z^2}{W^2}\right] = \frac{(-1)^{\frac{p+i}{2}} Z^2}{W^2}\left[\frac{(-1)^{p+i} Z^4}{W^4} - p^2\right] = \frac{(-1)^{\frac{p+i}{2}} Z^2}{W^2}\left[\frac{Z^4 - p^2W^4}{W^4}\right] = \frac{(-1)^{\frac{p+i}{2}} Z^2}{W^6}(Z^2 - pW^2)(Z^2 + pW^2) = \frac{(-1)^{\frac{p+i}{2}} Z^2}{W^6} . (-1)^{\frac{p+i}{2}} 2^{1-\varepsilon} Y^2 . 2^{1-\varepsilon} X^2 = \left(\pm\frac{2^{1-\varepsilon} XYZ}{W^3}\right)^2$$

So the points $\pm P_1$ satisfy the equation $y^2 = x^3 - p^2x$. By the same way, we find that the rest of the points $\pm P_2$, $\pm P_3$, $\pm P_4$ also satisfy the equation $y^2 = x^3 - p^2x$.

4 Example

$p = 41$ is congruent because (I) is solvable. Now We want to find a set of rational points on the elliptic curve $y^2 = x^3 - 1681x$.
First we solve (I) for $(i,\varepsilon) = (1,0)$. One of the solution is $(X,Y,Z,W) =$ (21,20,29,1), and so we find the rational points:

$$(841, \pm 24360), \left(\frac{18081}{400}, \pm\frac{1023729}{8000}\right), \left(-\frac{1681}{841}, \pm\frac{1412040}{24389}\right), \left(-\frac{16400}{441}, \pm\frac{974980}{9261}\right)$$

Now we solve (I) for $(i,\varepsilon) = (1,1)$. We find the solution $(X,Y,Z,W) =$ (99,93,24,15) and the rational points:

$$\left(\frac{378225}{576}, \pm\frac{232154505}{13824}\right), \left(\frac{401841}{8649}, \pm\frac{119821680}{804357}\right), \left(-\frac{576}{225}, \pm\frac{220968}{3375}\right), \left(-\frac{354609}{9801}, \pm\frac{112559760}{970299}\right)$$

Finally, let's solve (I) for (i, ε) = (-1,0).We find the solution (X, Y, Z, W) = (5,4,3,1), and so the following rational points:

$$\left(\frac{1681}{9}, \pm\frac{67240}{27}\right), \left(\frac{1025}{16}, \pm\frac{25215}{64}\right), \left(-\frac{656}{25}, \pm\frac{20172}{125}\right), (-9, \pm 120)$$

References

[1] E. Bach, and N. Ryan, Efficient verification of Tunnell's criterion, *Japan J. Indust. Appl. Math.*, **24**, no. 3 (2007), 229-239. https://doi.org/10.1007/bf03167537

[2] D. M. Burton, *Elementary Number Theory*, 6th ed., McGraw-Hill, New York, 2007.

[3] A. Gica, *Rational Points on Elliptic curves*, Institute of Mathematics of the Romanian Academy (IMAR), University of Bucharest, Romania, 2006.

[4] A. Knapp, *Elliptic Curves*, Princeton Univ., Princeton, 1992. https://doi.org/10.2307/j.ctv346st5

[5] F. Lemmermeyer, *Lecture 20, Monday 18. 04. 04*, Bilkent University, Ankara, Turkey, 2004.

[6] Danielle Li, *Proving Mordell-Weil: A Descent in Three Parts,* Cambridge, MA, Harvard University, 2005.

[7] N. M. Stephens, Congruence properties of congruent numbers, *Bulletin of the London Math. Society*, **7** (1975), 182-184. https://doi.org/10.1112/blms/7.2.182

Received: March 19, 2019; Published: April 23, 2019