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:

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

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:

\[ y^2 = x^3 - p^2x \] (1)
For an odd prime $p$. These curves have drawn 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:

$$y^2 = x(x - p)(x + p) \quad (2)$$

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

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

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 $\mathbb{Q}^* / \mathbb{Q}^2$ be the group of the co-sets $m \mathbb{Q}^2$, where $m$ is a non-zero rational number. Let $\alpha$ be the map:

$$\alpha: E(\mathbb{Q}) \to \mathbb{Q}^*/\mathbb{Q}^2 \oplus \mathbb{Q}^*/\mathbb{Q}^2 \oplus \mathbb{Q}^*/\mathbb{Q}^2$$

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 $\alpha$ which defined above is a group homomorphism (by proposition 5,[6]), and $\text{ima} \alpha$ is a finite set of triples $(a, b, c)$ which satisfy (1) (by proposition 4,[6]), and the prime factors for the product $abc$ divide $2p^3$(by proposition 4,[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 $\text{ima} \alpha$ are the triples which belong to the set $S$, where:
Rational points on the elliptic curve $y^2 = x^3 - p^2x$

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

Hence $ima \subseteq S$.

According to the definition of $\alpha$ we find that for any prime $p$, the triples:

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

belong to $ima$.

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 $ima$, then $p \equiv 1$ or $7$(mod 8).

(2) If the triples:

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

belong to $ima$, then $p \equiv 1$ or $5$(mod 8).

(3) If the triples:

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

belong to $ima$, then $p \equiv 1$(mod 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 $S_0 \subseteq ima$ for any odd prime.

Now let’s define $S_1, S_2, S_3$ as follows:

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

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

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

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:

\[
\begin{align*}
X^2 - (-1) \frac{p-i}{i} Y^2 &= 2^6 Z^2 \\
X^2 - (-1) \frac{p+i}{i} Y^2 &= 2^6 p W^2
\end{align*}
\]

has an integer solution $(X, Y, Z, W)$ with $XYZW \neq 0$, where:
Baraah Maya and Hasan Sankari

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

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:

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

\[P_2 = \left(\frac{pX^2}{y^3}, \frac{2^{i}p^2XZW}{y^3}\right), \quad P_2 = \left(\frac{pX^2}{y^3}, -\frac{2^{i}p^2XZW}{y^3}\right)\]

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

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

**Proof:** Suppose that \(p\) is congruent, and let’s proof that (I) is solvable. First suppose that \(p \equiv 7(\text{mod } 8)\). 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:

\[
\begin{cases} 
\frac{x = u^2}{x - p = 2v^2} \\
x + p = 2w^2
\end{cases}
\]

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

\[
x = \frac{n^2}{e^2}
\]

\[
n^2 - pe^2 = 2m^2
\]

\[
n^2 + pe^2 = 2s^2
\]

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 \((i,\varepsilon) = (1,0)\) 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 \( p \equiv 1 \pmod{8} \), and \( P = (x, y) \) is a rational point on the curve \( y^2 = x^3 - p^2x \) with \( y \neq 0 \), then \( \alpha(P) \in S_3 \setminus S_0 \) where:

\[
S_3 = \{(1,2p,2p),(1,1),(1,0)\} \cup S_2 \cup S_1
\]

So we distinguish between three cases:
- \( \alpha(P) \in S_3 \setminus S_0 \): In this case, the proof is exactly as the proof when \( p \equiv 7 \pmod{8} \), and (I) is solvable when \( (i, \varepsilon) = (1,0) \).
- \( \alpha(P) \in S_2 \setminus S_0 \): In this case, the proof is exactly as the proof when \( p \equiv 5 \pmod{8} \), and (I) is solvable when \( (i, \varepsilon) = (1,1) \).
- \( \alpha(P) \in S_3 \setminus (S_3 \cup S_2) \): 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:

\[
\begin{align*}
Z^2 - pW^2 &= (-1)^{\frac{p+i}{2}} 2^{1-\varepsilon}Y^2 \\
Z^2 + pW^2 &= 2^{1-\varepsilon}X^2
\end{align*}
\]

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

\[
\begin{align*}
\left[\frac{-p+i}{W^2}\right]^2 Z^2 - p^2 \left[\frac{-p+i}{W^2}\right] Z^2 &= \left[\frac{-p+i}{W^2}\right] Z^2 \left[\frac{-p+i}{W^2}\right] Z^2 - p^2 \\
&= \left[\frac{-p+i}{W^2}\right]^2 Z^2 - p^2 \left[\frac{-p+i}{W^2}\right] Z^2 + p^2 - p^2 \\
&= \left[\frac{-p+i}{W^2}\right]^2 \left( Z^2 - pW^2 \right) \left( Z^2 + pW^2 \right) \\
&= \left(\frac{-p+i}{W^2}\right)^2 \left( Z^2 - pW^2 \right) \left( Z^2 + pW^2 \right)
\end{align*}
\]

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

\[
\left(\frac{378225}{576}, \pm \frac{232154505}{13824}\right), \left(\frac{401841}{8649}, \pm \frac{119821680}{804357}\right), \left(-\frac{576}{225}, \pm \frac{220968}{3375}\right), \left(-\frac{303}{656}, \pm \frac{20172}{25}\right), \left(-\frac{9}{25}, \pm \frac{120}{64}\right), \left(-9, \pm 120\right)
\]

References


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