A Note About The Determination of Integer Coordinates of Elliptic Curves
- Part II, v1 -

Abdelmajid Ben Hadj Salem*

November 11, 2022

Abstract

In this paper, we give an elliptic curve \((E)\) given by the equation:

\[ y^2 = \varphi(x) = x^3 + px + q \]  

with \(p, q \in \mathbb{Z}\) not null simultaneous. We study the conditions verified by \((p, q)\) so that \(\exists (x, y) \in \mathbb{Z}^2\) the coordinates of a point of the elliptic curve \((E)\) given by the equation (1).

Key words: elliptic curves, integer points, solutions of degree three polynomial equations, solutions of Diophantine equations.

Contents

1 Introduction 1

2 Proof 2

2.1 Case \(\Delta = 0\) ................................................................. 2

2.1.1 Case \(u^3 = v^3 = p^2\) ............................................... 3

2.1.2 Case \(u^3 = v^3 = -p^2\) ............................................... 3

2.2 Case \(\Delta > 0\) ................................................................. 4

2.2.1 We suppose that \(3 | p\) ............................................... 4

2.2.2 We suppose that \(3 \nmid p\) ............................................... 8

*Résidence Bousten 8, Bloc B, Mosquée Raoudha, 1181 Soukra Raoudha, Tunisia.
; Email: abenhadj Salem@gmail.com
1 Introduction

Elliptic curves are related to number theory, geometry, cryptography, string theory, data transmission,... We consider an elliptic curve \((E)\) given by the equation:

\[
y^2 = \varphi(x) = x^3 + px + q
\]

where \(p\) and \(q\) are two integers and we assume in this article that \(p, q\) are not simultaneous equal to zero. For our proof, we consider the equation:

\[
\varphi(x) - y^2 = x^3 + px + q - y^2 = 0
\]

of the unknown the parameter \(x\), and \(p, q, y\) given with the condition that \(y \in \mathbb{Z}^+\). We resolve the equation \((3)\) and we discuss so that \(x\) is an integer.

2 Proof

We suppose that \(y > 0\) is an integer, to resolve \((3)\), let:

\[
x = u + v
\]

where \(u, v\) are two complexes numbers. Equation \((3)\) becomes:

\[
u^3 + v^3 + q - y^2 + (u + v)(3uv + p) = 0
\]

With the choose of:

\[
3uv + p = 0 \implies uv = -\frac{p}{3}
\]

then, we obtain the two conditions:

\[
uv = -\frac{p}{3}
\]

\[
u^3 + v^3 = y^2 - q
\]

Hence, \(u^3, v^3\) are solutions of the equation of second order:

\[
X^2 - (y^2 - q)X - \frac{p^3}{27} = 0
\]

Let \(\Delta\) the discriminant of \((9)\) given by:

\[
\Delta = (y^2 - q)^2 + \frac{4p^3}{27}
\]
2.1 Case $\Delta = 0$

In this case, the equation has one double root:

$$X_1 = X_2 = \frac{y^2 - q}{2} \quad (11)$$

As $\Delta = 0 \implies \frac{4p^3}{27} = -(y^2 - q)^2 \implies p < 0$. $y, q$ are integers then $3|p \implies p = 3p_1$ and $4p_1^3 = -(y^2 - q)^2 \implies p_1 = -p_2 \implies y^2 - q = \pm 2p_2^3$ and $p = -3p_2^3$.

As $y^2 = q \pm 2p_2^3$, it exists solutions if:

$q \pm 2p_2^3$ is a square \( (12) \)

We suppose that $q \pm 2p_2^3$ is a square. The solution $X = X_1 = X_2 = \pm p_2^2$.

Using the unknowns $u, v$, we have two cases:

1. $u^3 = v^3 = p_2^3$;
2. $u^3 = v^3 = -p_2^3$.

2.1.1 Case $u^3 = v^3 = p_2^3$

The solutions of $u^3 = p_2^3$ are:

- a - $u_1 = p_2$;
- b - $u_2 = j.p_2$ with $j = \frac{-1 + i\sqrt{3}}{2}$ is the unitary cubic complex root;
- c - $u_3 = j^2.p_2$.

Case a - $u_1 = v_1 = p_2 \implies x = 2p_2$. The condition $u_1.v_1 = -p/3$ is verified. The integers coordinates of the elliptic curve $(E)$ are:

$$\begin{align*}
(2p_2, +\alpha) \\
(2p_2, -\alpha) \\
\alpha = \sqrt{\varphi(2p_2)}
\end{align*} \quad (13, 14, 15)$$

Case b - $u_2 = p_2.j, v_2 = p_2.j^2 = p_2.j \implies x = u_2 + v_2 = p_2(j + j) = p_2$, in this case, the integers coordinates of the elliptic curve $(E)$ are:

$$\begin{align*}
(p_2, +\alpha) \\
(p_2, -\alpha) \\
\alpha = \sqrt{\varphi(p_2)}
\end{align*} \quad (16, 17, 18)$$

Case c - $u_2 = p_2.j, v_2 = p_2.j^2 = p_2.j$, it is the same as case b above.
2.1.2 Case $u^3 = v^3 = -p_2^3$

The solutions of $u^3 = -p_2^3$ are:
- d - $u_1 = -p_2$;
- e - $u_2 = -j \cdot p_2$;
- f - $u_3 = -j^2 \cdot p_2 = -\bar{j}p_2$.

Case d - $u_1 = v_1 = -p_2 = -p_2 \Rightarrow x = -2p_2$. The condition $u_1v_1 = -p_3$ is verified. The integers coordinates of the elliptic curve $(E)$ are:

$$(2p_2, +\alpha) \quad (2p_2, -\alpha) \quad \alpha = \varphi(2p_2) \quad (19)$$

Case e - $u_2 = -p_2j, v_2 = -p_2j^2 = -p_2\bar{j} \Rightarrow x = u_2 + v_2 = -p_2(j + \bar{j}) = -p_2$, in this case, the integers coordinates of the elliptic curve $(E)$ are:

$$( -p_2, +\alpha) \quad (-p_2, -\alpha) \quad \alpha = \varphi(p_2) \quad (20)$$

Case f - $u_2 = -p_2j, v_2 = -p_2j^2 = p_2\bar{j}$ it is the same of case e above.

2.2 Case $\Delta > 0$

We suppose that $\Delta > 0$ and $\Delta = m^2$ where $m \in \mathbb{R}$ is a positive real number.

$$\Delta = (y^2 - q)^2 + \frac{4p_3}{27} = \frac{27(y^2 - q)^2 + 4p_3}{27} = m^2 \quad (21)$$

$$27(y^2 - q)^2 + 4p_3 = 27m^2 \Rightarrow 27(m^2 - (y^2 - q)^2) = 4p_3 \quad (22)$$

2.2.1 We suppose that $3|p$

We suppose that $3|p \Rightarrow p = 3p_1$. We consider firstly that $|p_1| = 1$.

Case $p_1 = 1$: the equation (22) is written as:

$$m^2 - (y^2 - q)^2 = 4 \Rightarrow (m + y^2 - q)(m - y^2 + q) = 2 \times 2 \quad (23)$$

That gives the system of equations(with $m > 0$):

$$\begin{cases} m + y^2 - q = 1 \\ m - y^2 + q = 4 \end{cases} \Rightarrow m = 5/2 \text{ not an integer} \quad (24)$$

$$\begin{cases} m + y^2 - q = 2 \\ m - y^2 + q = 2 \end{cases} \Rightarrow m = 2 \text{ and } y^2 - q = 0 \quad (25)$$

$$\begin{cases} m + y^2 - q = 4 \\ m - y^2 + q = 1 \end{cases} \Rightarrow m = 5/2 \text{ not an integer} \quad (26)$$
We obtain:

\[ X_1 = u^3 = 1 \implies u_1 = 1; u_2 = j; u_3 = j^2 = -\bar{j} \] (27)
\[ X_2 = v^3 = -1 \implies v_1 = -1; v_2 = -j; v_3 = -j^2 = -\bar{j} \] (28)
\[ x_1 = u_1 + v_1 = 0 \] (29)
\[ x_2 = u_2 + v_3 = j - j^2 = i\sqrt{3} \text{ not an integer} \] (30)
\[ x_3 = u_3 + v_2 = j^2 - j = -i\sqrt{3} \text{ not an integer} \] (31)

As \( y^2 - q = 0 \), if \( q = q'^2 \) with \( q' \) a positive integer, we obtain the integer coordinates of the elliptic curve \((E)\):

\[ y^2 = x^3 + 3x + q^2 \] (32)
\[ (0, q'); (0, -q') \] (33)

**Case** \( p_1 = -1 \): using the same method as above, we arrive to the acceptable value \( m = 0 \), then \( y^2 = q \pm 2 \implies q \pm 2 \) must be a square to obtain the integer coordinates of the elliptic curve \((E)\).

If \( y^2 = q + 2 \), a square \( \implies (X - 1)^2 = 0 \implies u^3 = v^3 = 1 \), then \( x_1 = 2,x_2 = 1 \).

The integer coordinates of the elliptic curve \((E)\) are:

\[ y^2 = x^3 - 3x + q \] (34)
\[ (1, \sqrt{q + 2}); (1, -\sqrt{q + 2}); (2, \sqrt{q + 2}); (2, -\sqrt{q + 2}) \] (35)

If \( y^2 = q - 2 \), a square \( \implies (X + 1)^2 = 0 \implies u^3 = v^3 = -1 \), then \( x_1 = -2,x_2 = -1 \). The integer coordinates of the elliptic curve \((E)\) are:

\[ y^2 = x^3 - 3x + q \] (36)
\[ (-1, \sqrt{q - 2}); (-1, -\sqrt{q - 2}); (-2, \sqrt{q - 2}); (-2, -\sqrt{q - 2}) \] (37)

For the trivial case \( q = 2 \implies y^2 = x^3 - 3x + 2 \) and \( q - 2, q + 2 \) are squares, the integer coordinates of the elliptic curve are:

\[ y^2 = x^3 - 3x + 2 \] (38)
\[ (1, 0); (-2, 0); (2, 2); (2, -2); (-1, 2); (-1, -2) \] (39)

For \( q > 2, q - 2 \) and \( q + 2 \) can not be simultaneous square numbers.

Now, we consider that \( |p_1| > 1 \).
We suppose that \( p_1 > 1 \) The equation (22) is written as:

\[
m^2 - (y^2 - q)^2 = 4p_1^3 \implies m^2 - (y^2 - q)^2 = 4p_1^3
\] (40)

From the last equation (40), \((m, y^2 - q)\) (respectively in the case \(y^2 - q \leq 0\), \((m, q - y^2))\) are solutions of the Diophantine equation:

\[
X^2 - Y^2 = N \quad X > 0, Y > 0
\] (41)

where \(N\) is a positive integer equal to \(4p_1^3\).

For the general solutions of the equation (41), let \(Q(N)\) the number of solutions of (41) and \(\tau(N)\) the number of factorization of \(N\), then we give the following result concerning the solutions of (41) (see theorem 27.3 of [1]):

- if \(N \equiv 2(\text{mod} \ 4)\), then \(Q(N) = 0\);
- if \(N \equiv 1\) or \(N \equiv 3(\text{mod} \ 4)\), then \(Q(N) = \lceil \tau(N)/2 \rceil\);
- if \(N \equiv 0(\text{mod} \ 4)\), then \(Q(N) = \lceil \tau(N/4)/2 \rceil\).

As \(N = 4p_1^3 \implies N \equiv 0(\text{mod} \ 4)\), then \(Q(N) = \lceil \tau(N/4) \rceil = \lceil \tau(p_1^3)/2 \rceil > 1\). A solution \((X', Y')\) of (41) is used if \(Y' = y^2 - q \implies q + Y'\) is a square (respectively if \(Y' = q - y^2 \implies q - Y'\) is a square), then \(X' = m > 0\) and \(\pm y = \pm \sqrt{q + Y'}\) (respectively \(\pm y = \pm \sqrt{q - Y'}\). The roots of (9) are:

\[
X_1 = \frac{y^2 - q + m}{2} = \frac{Y' + m}{2} > 0
\] (42)
\[
X_2 = \frac{y^2 + q - m}{2} = \frac{Y' - m}{2} < 0
\] (43)

(Respectively, the roots of (9) are:

\[
X_1 = \frac{y^2 - q + m}{2} = \frac{-Y' + m}{2} > 0
\] (44)
\[
X_2 = \frac{y^2 + q - m}{2} = \frac{-Y' - m}{2} < 0
\] (45)

). From \(X'^2 - Y'^2 = 4p_1^3 = N\), \(2|(Y' - m)\) and \(2|(Y' - m + 2m) \implies 2|(Y' + m) \implies X_1, X_2 \in \mathbb{Z}\), and we obtain the equations:

\[
u^3 = X_2 \implies v_1 = \sqrt[3]{X_2}; v_2 = j \sqrt[3]{X_2}; v_3 = j^2 \sqrt[3]{X_2}
\] (47)

\[1[x] is the largest integer less or equal to x.\]
A real $x$ is obtained if $x = u_1 + v_1 = \sqrt[3]{X_1} + \sqrt[3]{X_2}$. If $X_1, X_2$ are cubic integers: $X_1 = t_1^3, X_2 = t_2^3$, then we obtain an integer solution:

$$x = t_1 + t_2, \quad \pm y = \pm \sqrt[3]{Y' + q} \quad \text{respectively} \quad \pm y = \pm \sqrt[3]{q - Y'} \quad (48)$$

If not, there are no integer coordinates of the elliptic curve $(E)$.

**We suppose that** $p < 0 \implies p_1 < -1$ : in this case, $(y^2 - q, m)$ (respectively $(q - y^2, m)$) is a solution of the Diophantine equation:

$$X^2 - Y^2 = N' \quad X > 0, Y > 0 \quad (49)$$

and $N'$ is a positive integer equal to $-4p^3_1 > 0$. As seen above, a solution $(X', Y')$ of (49) is used if $X' = y^2 - q \implies q + X'$ is a square (respectively $X' = q - y^2 \implies q - X'$ is a square), then $\pm y' = \pm \sqrt[3]{q + X'}$ (respectively $\pm y' = \pm \sqrt[3]{q - X'}$) and $Y' = m > 0$. The roots of (49) are:

$$X'_1 = \frac{y^2 - q + m}{2} = \frac{X' + m}{2} \quad (50)$$

$$X'_2 = \frac{y^2 + q - m}{2} = \frac{X' - m}{2} \quad (51)$$

(Respectively the roots of (49) are:

$$X'_1 = \frac{y^2 - q + m}{2} = \frac{-X' + m}{2} > 0 \quad (52)$$

$$X'_2 = \frac{y^2 + q - m}{2} = \frac{-X' - m}{2} < 0 \quad (53)$$

From $X'^2 - Y'^2 = -4p^3_1 = N'$, $2|(X' - m)$ and $2|(X' + m) \implies X'_1, X'_2 \in \mathbb{Z}$, and we obtain the equations:

$$u'^3 = X'_1 \implies \quad u'_1 = \sqrt[3]{X'_1}; u'_2 = j \sqrt[3]{X'_1}; u'_3 = j^2 \sqrt[3]{X'_1} \quad (54)$$

$$v'^3 = X'_2 \implies \quad v'_1 = \sqrt[3]{X'_2}; v'_2 = j \sqrt[3]{X'_2}; v'_3 = j^2 \sqrt[3]{X'_2} \quad (55)$$

A real $x'$ is obtained if $x' = u'_1 + v'_1 = \sqrt[3]{X'_1} + \sqrt[3]{X'_2}$. If $X'_1, X'_2$ are cubic integers: $X'_1 = t'_1^3, X'_2 = t'_2^3$ then we obtain an integer solution:

$$x' = t'_1 + t'_2, \quad \pm y' = \pm \sqrt[3]{X' + q} \quad \text{respectively} \quad \pm y' = \pm \sqrt[3]{q - X'} \quad (56)$$

If not, there are no integer coordinates of the elliptic curve $(E)$. 7
2.2.2 We suppose that $3 \nmid p$

We rewrite the equations (9) and (22):

$$X^2 - (y^2 - q)X - \frac{p^3}{27} = 0$$

$$\Delta = (y^2 - q)^2 + \frac{4p^3}{27} = \frac{27(y^2 - q)^2 + 4p^3}{27} = m^2$$

with $m > 0$ a real scalar. As seen above, we find the same results, there are no integer coordinates of the elliptic curve $(E)$.

2.3 Case $\Delta < 0$

The expression of $\Delta$ is given by (84):

$$\Delta = (y^2 - q)^2 + \frac{4p^3}{27}$$

We suppose that $\Delta < 0 \implies (y^2 - q)^2 + \frac{4p^3}{27} < 0 \implies (y^2 - q)^2 < -\frac{4p^3}{27}$, then $p < 0$. Let $p' = -p > 0 \implies \Delta = (y^2 - q)^2 - \frac{4p'^3}{27}$.

2.3.1 We suppose $3|p'$:

We suppose that $3|p' \implies p' = 3p_1$. $\Delta$ becomes:

$$\Delta = (y^2 - q)^2 - 4p_1^3$$  (57)

**Case** $p_1 = 1$. We obtain $\Delta = (y^2 - q)^2 - 4$. $\Delta = -m^2$ with $m$ integer, then $m^2 = 4 - (y^2 - q)^2 \implies m^2 + (y^2 - q)^2 = 2^2$, the solutions are:

** m$^2 = 4, y^2 - q = 0 \implies y^2 = q$. If $q$ is a square, let $q = q_1^2$, then $y = \pm q_1$.

We have also $x^3 - 3x = 0$. The only integer coordinates of the elliptic curve are:

$$(0, q_1), \ (0, -q_1)$$  (58)

** m$^2 = 1, \ y^2 - q = \sqrt{3} or y^2 - q = -\sqrt{3}$$

**-1- $y^2 - q = \sqrt{3}$, If $q = \sqrt{3}$, we have the equation $y^2 = x^3 - 3x + \sqrt{3}$ and $X^2 - \sqrt{3}X + 1 = 0$ and :

$$X_1 = \frac{\sqrt{3} + i}{2} = e^{i \frac{\pi}{6}}$$  (59)

$$X_2 = \frac{\sqrt{3} - i}{2} = e^{i \frac{\pi}{6}}$$  (60)

8
\( u, v \) verify \( u^3 = e^{\frac{i\pi}{6}}; v^3 = e^{-\frac{i\pi}{6}} \implies |u_i| = 1 \) and \( |v_j| = 1 \), \( |x_k| = |u_i + v_k| = |2\cos \frac{\pi}{18}| < 2 \implies \text{no integer coordinates if } q = \sqrt{3}.

**2.** \( y^2 - q = -\sqrt{3} \), we suppose that \( q = -\sqrt{3} \) then \( X^2 + \sqrt{3}X + 1 = 0 \). We obtain:

\[
X_1 = \frac{-\sqrt{3} + i}{2} = e^{\frac{i5\pi}{6}} \tag{61}
\]

\[
X_2 = \frac{-\sqrt{3} - i}{2} = e^{-\frac{i5\pi}{6}} \tag{62}
\]

Using the same remark as above, we arrive to \( |x_k| < 2 \), with \( |x_k| \neq 1 \), then there are no integer coordinates when \( q = -\sqrt{3} \).

**Case** \( p_1 > 1 \). We obtain \( m^2 = 4p_1^3 - (y^2 - q)^2 \implies m^2 + (y^2 - q)^2 = 4p_1^3 \), then \( \pm m, \pm (y^2 - q) \) are solutions of the Diophantine equation:

\[
A^2 + B^2 = N \tag{63}
\]

with \( N = 4p_1^3 \). The following theorem (theorem 36.3, [2]) gives the conditions to be verified by \( N \):

**Theorem 2.1.** *The Diophantine equation:*

\[
A^2 + B^2 = N \tag{64}
\]

*has a solution if and only if:*

\[
N = 2^\alpha p_1^{h_1} \cdots p_k^{h_k} q_1^{2\beta_1} \cdots q_n^{2\beta_n} \tag{65}
\]

where the \( p_i \) are primes congruent to 1 modulo 4, and the \( q_j \) are prime congruent to 3 modulo 4. When \( N \) is of this form, equation (64) has:

\[
N_S = \left\lfloor \frac{(h_1 + 1) \cdots (h_k + 1) + 1}{2} \right\rfloor \tag{66}
\]

*inequivalent solutions[^2]*

[^2]: \( [x] \) is the largest integer less or equal to \( x \).
From the conditions given by the theorem above, \(2 \nmid p_1\) and \(p_1\) must be written as:
\[
p_1 = p_1^a_1 \cdots p_k^a_k \cdot q_1^{b_1} \cdots q_n^{b_n}
\]
and \(p_1 \equiv 1 \pmod{4}\).

We suppose in the following, that equation \((67)\) is true. We obtain:
\[
\begin{aligned}
X_1 &= \frac{y_l^2 - q + im_l}{2} \quad l = 1, 2, \ldots, N_S \\
X_2 &= \frac{y_l^2 - q - im_l}{2}
\end{aligned}
\]
We have to resolve:
\[
\begin{aligned}
u^3 &= X_1 = \frac{y_l^2 - q + im_l}{2} \\
v^3 &= X_2 = \bar{X}_1 = \frac{y_l^2 - q - im_l}{2}
\end{aligned}
\]
We write \(X_1\) as \(X_1 = \rho e^{i\theta}\) with:
\[
\rho = \sqrt{\frac{(y^2 - q)^2 + m^2}{4}} = p_1 \sqrt{p_1}; \quad \sin \theta = \frac{\sqrt{\Delta}}{2\rho} = \frac{m_1}{2\rho} > 0; \quad \cos \theta = \frac{y^2 - q}{2\rho}
\]
If \(y^2 - q > 0 \implies \cos \theta > 0 \implies 0 < \theta < \frac{\pi}{2}[2\pi] \implies \frac{1}{4} < \cos^2 \theta < 1\).

If \(y^2 - q < 0 \implies \cos \theta < 0\), then:
\[
\frac{\pi}{2} < \theta < \pi[2\pi] \implies \frac{1}{4} < \cos^2 \theta < \frac{3}{4}
\]
A. We suppose that \(y^2 - q > 0 \implies 0 < \frac{\theta}{3} < \frac{\pi}{6}[2\pi] \implies \frac{1}{4} < \cos^2 \theta < 1\).

Then the expression of \(X_2\): \(X_2 = \rho e^{-i\theta}\). Let :
\[
u = re^{i\psi}; \quad \text{and} \quad j = \frac{-1 + i\sqrt{3}}{2} = e^{\frac{2\pi}{3}}
\]
The parameters \(u\) and \(v\) are:
\[
\begin{aligned}
u_1 &= re^{i\psi_1} = \sqrt{\rho}e^{i\frac{\theta}{3}} \\
u_2 &= re^{i\psi_2} = \sqrt{\rho}e^{i\frac{\theta + 2\pi}{3}} \\
u_3 &= re^{i\psi_3} = \sqrt{\rho}e^{i\frac{\theta + 4\pi}{3}}
\end{aligned}
\]
\[
\begin{align*}
v_1 &= re^{-i\psi_1} = \sqrt[3]{pe^{-i\frac{\theta}{3}}} \\
v_2 &= re^{-i\psi_2} = \sqrt[3]{p_1^2 e^{-i\frac{\theta}{3}}} = \sqrt[3]{pe^{i\frac{4\pi}{3} - i\frac{\theta}{3}}} = \sqrt[3]{pe^{i\frac{4\pi - \theta}{3}}}
\end{align*}
\]

We choose \( u_k \) and \( v_h \) so that \( u_k + v_h \) is real. In this case, we have necessary:

\[
v_1 = u_1; \quad v_2 = u_2; \quad v_3 = u_3
\]

Then, the real solutions of the equation (3):

\[
\begin{align*}
x_1 &= u_1 + v_1 = 2\sqrt[3]{p} \cos \frac{\theta}{3} \\
x_2 &= u_2 + v_2 = 2\sqrt[3]{p} \cos \left( \frac{\theta + 2\pi}{3} \right) = -\sqrt[3]{p} \left( \cos \frac{\theta}{3} + \sqrt[3]{3} \sin \frac{\theta}{3} \right) \\
x_3 &= u_3 + v_3 = 2\sqrt[3]{p} \cos \left( \frac{\theta + 4\pi}{3} \right) = \sqrt[3]{p} \left( -\cos \frac{\theta}{3} + \sqrt[3]{3} \sin \frac{\theta}{3} \right)
\end{align*}
\]

**The discussion of the integrity of \( x_1, x_2, x_3 \):** We suppose that \( x_1 \) is an integer, then \( x_1^2 \) is an integer. We obtain:

\[
x_1^2 = 4\sqrt[3]{p^2 \cos^2 \frac{\theta}{3}} = 4p_1 \cos^2 \frac{\theta}{3} \tag{72}
\]

We write \( \cos^2 \frac{\theta}{3} \) as:

\[
\cos^2 \frac{\theta}{3} = \frac{1}{a} \quad \text{or} \quad \frac{a}{b} \tag{73}
\]

where \( a, b \) are relatively coprime integers.

**\( \cos^2 \frac{\theta}{3} = \frac{1}{a} \).** In this case, \( \frac{1}{4} < \frac{1}{a} < 1 \Longrightarrow 1 < a < 4 \Longrightarrow a = 2 \) or \( a = 3 \).

Case \( a = 2 \), we obtain \( x_1^2 = 4\sqrt[3]{p^2 \cos^2 \frac{\theta}{3}} = 2p_1 \Longrightarrow 2\mid p_1 \), but \( 2 \nmid p_1 \), then the contradiction. We verify easily that \( x_2 \) and \( x_3 \) are irrationals.

Case \( a = 4 \), we obtain \( x_1^2 = 4\sqrt[3]{p^2 \cos^2 \frac{\theta}{3}} = 4p_1 \cdot \frac{1}{3} \). If \( 3 \nmid p_1 \) \( \Longrightarrow \) \( x_1^2 \) is a rational. We suppose that \( 3\mid p_1 \), then \( p_1 \) must be written as \( p_1 = 3\omega^2 \). From the equation (67), \( p_1 \equiv 1 \pmod{4} \). We deduce that \( \omega^2 \equiv 3 \pmod{4} \), as \( \omega^2 \) is a square, \( \omega^2 \equiv 0 \pmod{4} \) or \( \omega^2 \equiv 1 \pmod{4} \). Then \( x_1 \) can not be an integer. We verify easily that \( x_2, x_3 \) are also not integers.
\[ \cos^2 \frac{\theta}{3} = \frac{a}{b}, \quad a, b \text{ coprime with } a > 1. \]

We obtain:

\[ x_1^2 = 4p_1 \cos^2 \frac{\theta}{3} = \frac{4p_1 a}{b} \]

where \( b \) verifies the condition:

\[ b \mid 4p_1 \] \hspace{1cm} (74)

and using the \((70)\), we obtain a second condition:

\[ b < 4a < 3b \] \hspace{1cm} (75)

A-1- \( b = 2 \implies a = 1 \implies x_1^2 = 2p_1 \implies 2 \mid p_1 \), then case to reject.

A-2- \( b = 4 \implies a = 2, a, b \) no coprime. Case to reject.

A-3- \( b = 2' \) avec \( 2 \nmid b' \), then we obtain:

\[ x_1^2 = \frac{4p_1 a}{b} = \frac{2p_1 a}{b'} \implies b' \mid p_1 \] \hspace{1cm} (76)

then \( p_1 = b'^a p_2 \) with \( a \geq 1 \) and \( b' \nmid p_2 \), we obtain \( x_1^2 = 2b'^{a-1}.p_2.a \implies 2 \mid (p_2.a) \),

but from \((67)\) \( 2 \mid p_1 \implies 2 \nmid p_2 \) and \( 2 \nmid a \), if not \( a, b \) are not coprime. Then \( x_1^2 \)
cannot be an square integer, the case \( b = 2' \) is to reject.

A-4- \( b = 4' \) avec \( 4 \nmid b' \), then we obtain:

\[ x_1^2 = \frac{4p_1 a}{b} = \frac{p_1 a}{b'} \implies b' \mid p_1 \] \hspace{1cm} (77)

then \( p_1 = b'^a p_2 \) with \( a \geq 1 \) and \( b' \nmid p_2 \), we obtain \( x_1^2 = b'^{a-1}.p_2.a \).

* if \( b'^{a-1}.p_2.a = f^2 \) a square then \( x_1 = \pm f \), if not \( x_1 \) is not an integer.

We consider that \( x_1 = \epsilon f \) is an integer with \( \epsilon = \pm 1 \). As \( x_1 + x_2 + x_3 = 0 \implies x_2 + x_3 = -x_1 \). The product \( x_2.x_3 = f^2 - 3p_1 \), then \( x_2, x_3 \) are solutions of the equation:

\[ \lambda^2 - \epsilon f \lambda + f^2 - 3p_1 = 0 \] \hspace{1cm} (78)

The discriminant of \((78)\) is:

\[ \delta = f^2 - 4(f^2 - 3p_1) = 12p_1 - 3f^2 = 3(4p_1 - f^2) = 3p_2 b'^{a-1}(b - a) > 0 \]

If \( \delta \) is not a square, then \( x_2, x_3 \) are not integers. We suppose that \( \delta = g^2 \) a square. The real roots of \((78)\) are:

\[ \lambda_1 = \frac{\epsilon f + g}{2} \] \hspace{1cm} (79)

\[ \lambda_2 = \frac{\epsilon f - g}{2} \] \hspace{1cm} (80)
From the expressions of $f$ and $g$, we deduce that $2|f$ and $2|g$, then $\lambda_1, \lambda_2$ are integers.

We recall that $y^2 - q$ is supposed $> 0$ and are determined by the equations \([63, 64, 66]\), we obtain the integer coordinates $\in$ to the elliptic curve $(E)$:

For $l = 1, 2, \ldots, N_S$

$(f, y_l), (-f, y_l), (f, -y_l), (-f, -y_l),$

$(\lambda_1, y_l), (\lambda_2, y_l), (\lambda_1, -y_l), (\lambda_2, -y_l),$

$(-\lambda_1, y_l), (-\lambda_2, y_l), (-\lambda_1, -y_l), (-\lambda_2, -y_l)$ \hspace{1cm} (81)

**B. We suppose that $y^2 - q < 0 \implies \frac{\pi}{6} < \frac{\theta}{3} < \frac{\pi}{3} \left[\frac{2\pi}{a}\right]$**

that gives:

\[
\frac{1}{2} < \cos \frac{\theta}{3} < \frac{\sqrt{3}}{2} \implies \frac{1}{4} < \cos^2 \frac{\theta}{3} < \frac{3}{4}
\]

\[
\cos^2 \frac{\theta}{3} = \frac{1}{a}. \quad \text{In this case,} \quad \frac{3}{4} < \frac{1}{a} < 1 \implies 3a < 4 \text{ which is impossible case to reject.}
\]

\[
\cos^2 \frac{\theta}{3} = \frac{a}{b}. \quad \text{In this case,} \quad \frac{3}{4} < \frac{a}{b} < 1 \implies 3b < 4a. \text{ Then we obtain:}
\]

\[
x_1^2 = 4\sqrt{\rho^2 \cos^2 \frac{\theta}{3}} = 4p_1 \cos^2 \frac{\theta}{3} = \frac{4p_1 a}{b} \Rightarrow b | (4p_1)
\]

\hspace{1cm} (82)

B-1- $b = 2 \implies a = 1 \implies 8 < 4$ case to reject.

B-2- $b = 4 \implies 3 < a < 4$ case to reject.

B-3- $b = 2b'$ avec $2 \nmid b'$, then we obtain:

\[
x_1^2 = \frac{4p_1 a}{b'} = \frac{2p_1 a}{b'} \Rightarrow b' | p_1
\]

\hspace{1cm} (83)

then $p_1 = b'\alpha p_2$ with $\alpha \geq 1$ and $b' \nmid p_2$, we obtain $x_1^2 = 2b'\alpha - 1, p_2, a$.

* if $2b'\alpha - 1, p_2, a = f^2$ a square then $x_1 = \pm f$, if not $x_1$ is not an integer. We consider that $x_1 = \epsilon f$ is an integer with $\epsilon = \pm 1$. As $x_1 + x_2 + x_3 = 0 \implies x_2 + x_3 = -x_1$. The product $x_2 x_3 = f^2 - 3p_1$, then $x_2, x_3$ are solutions of the equation:

\[
\lambda^2 - \epsilon f \lambda + f^2 - 3p_1 = 0
\]

\hspace{1cm} (84)
The discriminant of \(84\) is:

\[
\delta = f^2 - 4(f^2 - 3p_1) = 12p_1 - 3f^2 = 3(4p_1 - f^2) = 2p_2b'^{\alpha-1}(b-a) > 0
\]

If \(\delta\) is not a square, then \(x_2, x_3\) are not integers. We suppose that \(\delta = g^2\) a square. The real roots of \(84\) are:

\[
\lambda_1 = \frac{\epsilon f + g}{2} \quad (85)
\]

\[
\lambda_2 = \frac{\epsilon f - g}{2} \quad (86)
\]

From the expressions of \(f\) and \(g\), we deduce that \(2|f\) and \(2|g\), then \(\lambda_1, \lambda_2\) are integers.

B-4- \(b = 4b'\) avec \(4 \nmid b'\), then we obtain:

\[
x_1^2 = \frac{4p_1a}{b} = \frac{p_1a}{b'} \Rightarrow b'|p_1 \quad (87)
\]

then \(p_1 = b'^\alpha p_2\) with \(\alpha \geq 1\) and \(b' \nmid p_2\), we obtain \(x_1^2 = b'^{\alpha-1}.p_2.a.\)

* if \(b'^{\alpha-1}.p_2.a = f^2\) a square then \(x_1 = \pm f\), if not \(x_1\) is not an integer.

We consider that \(x_1 = \epsilon f\) is an integer with \(\epsilon = \pm 1\). As \(x_1 + x_2 + x_3 = 0 \Rightarrow x_2 + x_3 = -x_1\). The product \(x_2.x_3 = f^2 - 3p_1\), then \(x_2, x_3\) are solutions of the equation:

\[
\lambda^2 - \epsilon f \lambda + f^2 - 3p_1 = 0 \quad (88)
\]

The discriminant of \(88\) is:

\[
\delta = f^2 - 4(f^2 - 3p_1) = 12p_1 - 3f^2 = 3(4p_1 - f^2) = 2p_2b'^{\alpha-1}(b-a) > 0
\]

If \(\delta\) is not a square, then \(x_2, x_3\) are not integers. We suppose that \(\delta = g^2\) a square. The real roots of \(88\) are:

\[
\lambda_1 = \frac{\epsilon f + g}{2} \quad (89)
\]

\[
\lambda_2 = \frac{\epsilon f - g}{2} \quad (90)
\]

From the expressions of \(f\) and \(g\), we deduce that \(2|f\) and \(2|g\), then \(\lambda_1, \lambda_2\) are integers.
We recall that $y^2 - q$ is supposed < 0 and are determined by the equations (63, 64, 66), we obtain the integer coordinates $\in$ to the elliptic curve $(E)$:

$$\begin{align*}
\text{For } l = 1, 2, ..., N_s \\
(f, y_l), (-f, y_l), (f, -y_l), (-f, -y_l), \\
(\lambda_1, y_l), (\lambda_2, y_l), (\lambda_1, -y_l), (\lambda_2, -y_l), \\
(-\lambda_1, y_l), (-\lambda_2, y_l), (-\lambda_1, -y_l), (-\lambda_2, -y_l)
\end{align*}$$

(91)

2.3.2 We suppose $3 \nmid p'$:

Then $\Delta = (y^2 - q)^2 - \frac{4p'^3}{27} = -m^2$ where $m > 0$ is a real. As in paragraph 2.2.2 above, we find the same results there are no integers coordinates of the elliptic curve $(E)$.

References


