A Note About the Determination of The Integer Coordinates of An Elliptic Curve: Part I

Abdelmajid Ben Hadj Salem

December 6, 2018

Abstract

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

$$y^2 = x^3 + px + q \tag{1}$$

with $p, q \in \mathbb{Z}$ not null simultaneous. We study a part of 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.

1 Introduction

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

$$y^2 = x^3 + px + q \tag{2}$$

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 :

$$x^3 + px + q - y^2 = 0 \tag{3}$$

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:

$$x = u + v \tag{4}$$

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

$$u^3 + v^3 + q - y^2 + (u + v)(3uv + p) = 0 \tag{5}$$

With the choose of:

$$3uv + p = 0 \Longrightarrow uv = -\frac{p}{3} \tag{6}$$

then, we obtain the two conditions:

$$uv = -\frac{p}{3} \tag{7}$$

$$u^3 + v^3 = y^2 - q \tag{8}$$

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

$$X^2 - (y^2 - q)X - \frac{p^3}{27} = 0 \tag{9}$$

Let Δ the discriminant of (9) given by:

$$\Delta = (y^2 - q)^2 + \frac{4p^3}{27} \tag{10}$$

2.1 Case $\Delta = 0$

In this case, the (9) has one double root :

$$X_1 = X_2 = \frac{y^2 - q}{2} \tag{11}$$

As $\Delta = 0 \Longrightarrow \dfrac{4p^3}{27} = -(y^2 - q)^2 \Longrightarrow p < 0$. y, q are integers then $3|p \Longrightarrow p = 3p_1$ and $4p_1^3 = -(y^2 - q)^2 \Longrightarrow p_1 = -p_2^2 \Longrightarrow y^2 - q = \pm 2p_2^3$ and $p = -3p_2^3$. As $y^2 = q \pm 2p_2^3$, it exists solutions if:

$$\boxed{q \pm 2p_2^3 \text{ is a square}} \tag{12}$$

We suppose that $q \pm 2p_2^3$ is a square. The solution $X = X_1 = X_2 = \pm p_2^3$. 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 $j = \dfrac{1+i\sqrt{3}}{2}$ is the unitary cubic complex root;

c - $u_3 = j^2.p_2$.

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

$$(2p_2, +\alpha) \tag{13}$$

$$(2p_2, -\alpha) \tag{14}$$

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

$$(p_2, +\alpha) \tag{15}$$

$$(p_2, -\alpha) \tag{16}$$

Case c - $u_2 = p_2.j, v_2 = p_2.j^2 = p_2.\bar{j}$, 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 - $u_2 = -j.p_2$;

f - $u_3 = -j^2.p_2 = -\bar{j}p_2$.

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

$$(2p_2, +\alpha) \quad (2p_2, -\alpha) \tag{17}$$

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

$$(-p_2, +\alpha) \quad (-p_2, -\alpha) \tag{18}$$

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

2.2 Case $\Delta > 0$

We suppose that $\Delta > 0$ and $\Delta = m^2$ where m is a positive rational.

$$\Delta = (y^2 - q)^2 + \frac{4p^3}{27} = \frac{27(y^2-q)^2 + 4p^3}{27} = m^2 \tag{19}$$

$$27(y^2-q)^2 + 4p^3 = 27m^2 \Longrightarrow 27(m^2 - (y^2-q)^2) = 4p^3 \tag{20}$$

2.2.1 We suppose that $3|p$

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

Case $p_1 = 1$**:** the equation (20) is written as:

$$m^2 - (y^2-q)^2 = 4 \Longrightarrow (m + y^2 - q)(m - y^2 + q) = 2 \times 2 \tag{21}$$

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

$$\left\{\begin{array}{l} m + y^2 - q = 1 \\ m - y^2 + q = 4 \end{array}\right. \Longrightarrow m = 5/2 \text{ not an integer} \tag{22}$$

$$\left\{\begin{array}{l} m + y^2 - q = 2 \\ m - y^2 + q = 2 \end{array}\right. \Longrightarrow m = 2 \text{ and } y^2 - q = 0 \tag{23}$$

$$\left\{\begin{array}{l} m + y^2 - q = 4 \\ m - y^2 + q = 1 \end{array}\right. \Longrightarrow m = 5/2 \text{ not an integer} \tag{24}$$

We obtain:

$$X_1 = u^3 = 1 \Longrightarrow u_1 = 1; u_2 = j; u_3 = j^2 = \bar{j} \tag{25}$$

$$X_2 = v^3 = -1 \Longrightarrow v_1 = -1; v_2 = -j; v_3 = -j^2 = -\bar{j} \tag{26}$$

$$x_1 = u_1 + v_1 = 0 \tag{27}$$

$$x_2 = u_2 + v_3 = j - j^2 = i\sqrt{3}\,\text{not an integer} \tag{28}$$

$$x_3 = u_3 + v_2 = j^2 - j = -i\sqrt{3}\,\text{not an integer} \tag{29}$$

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

$$y^2 = x^3 + 3x + q'^2 \tag{30}$$

$$(0, q'); (0, -q') \tag{31}$$

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

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

$$y^2 = x^3 - 3x + q \tag{32}$$

$$(1, \sqrt{q+2}); (1, -\sqrt{q+2}); (2, \sqrt{q+2}); (2, -\sqrt{q+2}) \tag{33}$$

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

$$y^2 = x^3 - 3x + q \tag{34}$$

$$(-1, \sqrt{q-2}); (-1, -\sqrt{q-2}); (-2, \sqrt{q-2}); (-2, -\sqrt{q-2}) \tag{35}$$

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

$$y^2 = x^3 - 3x + 2 \tag{36}$$

$$(1,0); (-2,0); (2,2); (2,-2); (-1,2); (-1,-2) \tag{37}$$

For $q > 2$, $q-2$ and $q+2$ can not be simultaneous square numbers.

Now, we consider that $|p_1| > 1$, the equation (20) is written as:

$$m^2 - (y^2-q)^2 = 4p_1^3 \Longrightarrow m^2 - (y^2-q)^2 = 4p_1^3 \tag{38}$$

From the last equation (38), $(\pm m, \pm(y^2-q))$ are solutions of the Diophantine equation :

$$X^2 - Y^2 = N \tag{39}$$

where N is a positive integer equal to $4p_1^3$. A solution (X', Y') of (39) is used if $Y' = y^2 - q \Longrightarrow q + Y'$ is a square, then $X' = m > 0$ and $\pm y = \pm\sqrt{q+Y'}$.

We return to the general solutions of the equation (39). Let $Q(N)$ the number of solutions of (39) and $\tau(N)$ the number of factorization of N, then we give the following result concerning the solutions of (39) (see theorem 27.3 of [S]):

- if $N \equiv 2 \pmod 4$, then $Q(N) = 0$;
- if $N \equiv 1$ or $N \equiv 3 \pmod 4$, then $Q(N) = [\tau(N)/2]$;
- if $N \equiv 0 \pmod 4$, then $Q(N) = [\tau(N/4)/2]$[1].

As $N = 4p_1^3 \Longrightarrow N \equiv 0 \pmod 4$, then $Q(N) = [\tau(N/4)/2] = [\tau(p_1^3)/2] > 1$, but $Q(N) = 1$, there is one solution $X' > 0, Y' > 0$ so that $Y' + q$ is a square. Hence the contradiction, the hypothesis that $3|p,\ |p| > 3$ is impossible in the case $\Delta > 0$.

[1] $[x]$ is the largest integer less or equal to x.

2.2.2 We suppose that $3 \nmid p$

We rewrite the equations (9-20):

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

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

We call:

$$r = 27(y^2 - q)^2 + 4p^3 \Longrightarrow m^2 = \frac{r}{27} = \Delta \tag{40}$$

r can be written as:

$$l^2 - 3(3y^2 - 3q)^2 = 4p^3 \tag{41}$$

or $l, 3(y^2 - q)$ are solutions of the Diophantine equation :

$$A^2 - 3B^2 = N \tag{42}$$

where N is the $4p^3$. As we consider the last equation with A, B integers and the coefficient of B is 3 does not verify $\equiv 1(\mod 4)$, then equation (42) has a solution if N can be written as:

$$N = \pm p_1^{h_1} ... p_k^{h_k} . q_1^{2\beta_1} ... q_n^{\beta_n} \tag{43}$$

where p_j, q_i are prime integers (see chapter 6 of [B]). Having A, B we calculate y^2:

$$y^2 = q + \frac{B}{3} \Longrightarrow q + \frac{B}{3} \text{ a square} \tag{44}$$

Then:

$$y = \pm\sqrt{q + \frac{B}{3}} \tag{45}$$

We return to x. $m^2 = \dfrac{r}{27} = \dfrac{l^2}{27} \Longrightarrow m = \dfrac{l}{3\sqrt{3}} = \dfrac{l\sqrt{3}}{9}$. As $3 \nmid p \Longrightarrow 3 \nmid r \Longrightarrow 3 \nmid l^2 \Longrightarrow 3 \nmid l$, then m is an irrational number. The roots of (9) are:

$$X_1 = \frac{y^2 - q + m}{2} = \frac{9(y^2 - q) + l\sqrt{3}}{18} \tag{46}$$

$$X_2 = \frac{y^2 - q - m}{2} = \frac{9(y^2 - q) - l\sqrt{3}}{18} \tag{47}$$

From the expressions of X_1, X_2, we conclude that X_1 and X_2 are irrational numbers $\in \mathbb{R}\backslash\mathbb{Q}$. For the unknowns u, v, we obtain :

$$u_1 = \sqrt[3]{X_1}, \;\; u_2 = j\sqrt[3]{X_1}, \;\; u_3 = j^2\sqrt[3]{X_1} \tag{48}$$

$$v_1 = \sqrt[3]{X_2}, \;\; v_2 = j\sqrt[3]{X_2}, \;\; v_3 = j^2\sqrt[3]{X_2} \tag{49}$$

As we choose x a real number, then $x = u_1 + v_1 = \sqrt[3]{X_1} + \sqrt[3]{X_2}$. We search x, y to be integer numbers. We suppose that $x = \sqrt[3]{X_1} + \sqrt[3]{X_2}$ is an integer:

$$x = \sqrt[3]{X_1} + \sqrt[3]{X_2}$$
$$x.(\sqrt[3]{X_1^2} - \sqrt[3]{X_1.X_2} + \sqrt[3]{X_2^2}) = X_1 + X_2 = y^2 - q$$
$$x.(\sqrt[3]{X_1^2} + \sqrt[3]{X_2^2} + \frac{p}{3}) = y^2 - q$$

$$\sqrt[3]{X_1^2} + \sqrt[3]{X_2^2} = +\frac{3(y^2-q) - px}{3x} = t \in \mathbb{Q}^* \tag{50}$$

with $x \neq 0$. As $x = \sqrt[3]{X_1} + \sqrt[3]{X_2} \Longrightarrow \sqrt[3]{X_2^2} = (x - \sqrt[3]{X_1})^2 \Longrightarrow x^2 - 2x\sqrt[3]{X_1} + \sqrt[3]{X_1^2} = \sqrt[3]{X_2^2}$. Adding to the two members of the last equation $\sqrt[3]{X_1}$, we obtain:

$$\sqrt[3]{X_1^2} - x\sqrt[3]{X_1} + \frac{x^2 - t}{2} = 0 \tag{51}$$

then $\sqrt[3]{X_1}$ is a root of the equation:

$$\alpha^2 - x\alpha + \frac{x^2 - t}{2} = 0 \tag{52}$$

The expression of the roots is:

$$\alpha = \frac{x \pm \sqrt{\delta}}{2} \tag{53}$$

$$\delta = 2t - x^2 > 0 \tag{54}$$

δ is > 0 because $2t - x^2 = 2\sqrt[3]{X_1^2} + 2\sqrt[3]{X_2^2} - \sqrt[3]{X_1^2} - \sqrt[3]{X_2^2} - 2\sqrt[3]{X_1X_2} = (\sqrt[3]{X_1^2} - \sqrt[3]{X_2^2})^2 > 0$ as $X_1 \neq X_2$. Then δ is a square. We conclude that α is a rational number. It follows that $\sqrt[3]{X_1}$ is a rational number that we note by s, then $X_1 = s^3$ is also a rational number which is in contradiction with the precedent result above that X_1 is irrational. The hypothesis that x is an integer is false, it follows that x is a irrational number. Then, no integer coordinates exist when r is a square.

Case r is not a square: we write :

$$r = 27(y^2 - q)^2 + 4p^3 \Longrightarrow m^2 = \frac{r}{27} = \Delta \Longrightarrow m = \frac{\sqrt{3r}}{9}$$

As $3 \nmid r \Longrightarrow 3r$ is not a square, then m is irrational number. The roots of (9) are:

$$X_1 = \frac{y^2 - q + m}{2} = \frac{9(y^2 - q) + \sqrt{3r}}{18} \tag{55}$$

$$X_2 = \frac{y^2 - q - m}{2} = \frac{9(y^2 - q) - \sqrt{3r}}{18} \tag{56}$$

Using the same reasoning as for the case r is a square, there is no integer coordinates for (E) when r is not a square.

In the second part of the paper, we will study the case $\Delta < 0$.

References

[S] B.M. Stewart : Theory of numbers. 2sd ed. The Macmillan Company, New-York (1964).

[B] E.D. Bolker : Elementary number theory: an algebraic approach. W.A. Benjamin, Inc., New-York (1970).