ECC, problem 02.***08

Roman

November 26, 2023

Problem

Let $E(\mathbb{Q}) : y^2 = f(x) = x^3 + Ax + B$. Prove that

$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)} = \frac{\psi_3(x)}{4yf(x)}$$

where $\psi_3(x) = 3x^4 + 6Ax^2 + 12Bx - A^2$ is the **third division polynomial** of E.[1]

Use this to deduce that a point $P = (x, y) \in E$ (not equal to ∞) is a point of order three if and only if $P \neq \infty$ and P is a point of inflection on the curve E.

[1] It is a polynomial whose roots are the x-coordinates of the 3-torsion points of E. In general, there is an m-th division polynomial $\psi_m(x)$ whose roots give the x-coordinates of the m-torsion points of E. See this link for information.

Solution

Proof. First, we compute the second derivative of y with respect to x. For the first derivative, we have

$$2yy' = f'(x) \tag{1}$$

Differentiating both sides with respect to x gives

$$2y'^2 + 2yy'' = f''(x) \tag{2}$$

Solving equation (1) for y' and substituting into the above equation gives

$$2y\left(\frac{f'(x)}{2y}\right)^2 + 2yy'' = f''(x) \tag{3}$$

Now we can simplify the left-hand side to get the desired result:

$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)} \tag{4}$$

That holds for any implicit function $y^2 = f(x)$. For our curve $E(\mathbb{Q})$ that is

$$y^2 = x^3 + Ax + B \tag{5}$$

we have

$$\frac{d^2y}{dx^2} = \frac{2f''(x)f(x) - f'(x)^2}{4yf(x)} \overset{\text{[some laborious algebra]}}{=} \frac{3x^4 + 6Ax^2 + 12Bx - A^2}{4yf(x)} = \frac{\psi_3(x)}{4yf(x)} \tag{6}$$

To find the point of inflection, we need the roots of the third division polynomial $\psi_3(x)$. With a help of a computer, we find that [2]

$$x_1 = \frac{\sqrt{\sqrt[3]{8A^3+54B^2} - 2A} - \sqrt{-\sqrt[3]{8A^3+54B^2} - \frac{6\sqrt{6}B}{\sqrt{\sqrt[3]{8A^3+54B^2}-2A}} - 4A}}{\sqrt{6}} \tag{7}$$

$$x_2 = \frac{\sqrt{\sqrt[3]{8A^3+54B^2} - 2A} + \sqrt{-\sqrt[3]{8A^3+54B^2} - \frac{6\sqrt{6}B}{\sqrt{\sqrt[3]{8A^3+54B^2}-2A}} - 4A}}{\sqrt{6}} \tag{8}$$

$$x_3 = \frac{-\sqrt{\sqrt[3]{8A^3+54B^2} - 2A} - \sqrt{-\sqrt[3]{8A^3+54B^2} + \frac{6\sqrt{6}B}{\sqrt{\sqrt[3]{8A^3+54B^2}-2A}} - 4A}}{\sqrt{6}} \tag{9}$$

$$x_4 = \frac{-\sqrt{\sqrt[3]{8A^3+54B^2} - 2A} + \sqrt{-\sqrt[3]{8A^3+54B^2} + \frac{6\sqrt{6}B}{\sqrt{\sqrt[3]{8A^3+54B^2}-2A}} - 4A}}{\sqrt{6}} \tag{10}$$

[2] A curious property of the roots is $\sum_i x_i^2 = -4A$. Interesting, like a norm of some vector (it's ≤ 0 due to the complex roots)! Computed $\sum_i x_i^2$ for ψ_2: $-2A$, $\psi_4 : -10A$, $\psi_5 : -124/5A$ (can multiply by m?), $\psi_6 : -50A$, $\psi_7 : -88A$, $\psi_8 : -148A$. That last one is a polynomial of the 33rd power and takes 266 KiB, sure I was leaning on Sage Math for getting the explicit form for ψ_m and Wolfram Mathematica for manipulating with roots. Can't compute more it appears. The question is what is that sequence, known or even useful perhaps?

Using the discriminant $\Delta = 4A^3 + 27B^2$ of the cubic polynomial $f(x)$, we can simplify the above expressions to

$$x_1 = \frac{\sqrt{\sqrt[3]{2\Delta} - 2A} - \sqrt{-\sqrt[3]{2\Delta} - \frac{6\sqrt{6}B}{\sqrt{\sqrt[3]{2\Delta}-2A}} - 4A}}{\sqrt{6}} \tag{11}$$

$$x_2 = \frac{\sqrt{\sqrt[3]{2\Delta} - 2A} + \sqrt{-\sqrt[3]{2\Delta} - \frac{6\sqrt{6}B}{\sqrt{\sqrt[3]{2\Delta}-2A}} - 4A}}{\sqrt{6}} \tag{12}$$

$$x_3 = \frac{-\sqrt{\sqrt[3]{2\Delta} - 2A} - \sqrt{-\sqrt[3]{2\Delta} + \frac{6\sqrt{6}B}{\sqrt{\sqrt[3]{2\Delta}-2A}} - 4A}}{\sqrt{6}} \tag{13}$$

$$x_4 = \frac{-\sqrt{\sqrt[3]{2\Delta} - 2A} + \sqrt{-\sqrt[3]{2\Delta} + \frac{6\sqrt{6}B}{\sqrt{\sqrt[3]{2\Delta}-2A}} - 4A}}{\sqrt{6}} \tag{14}$$

Introducing

$$M = \sqrt[3]{2\Delta} - 2A \tag{15}$$

$$N = \frac{6\sqrt{6}B}{\sqrt{M}} - 6A \tag{16}$$

we further simplify the expressions for the roots to

$$x_1 = \frac{\sqrt{M} - \sqrt{-M-N}}{\sqrt{6}} \tag{17}$$

$$x_2 = \frac{\sqrt{M} + \sqrt{-M-N}}{\sqrt{6}} \tag{18}$$

$$x_3 = \frac{-\sqrt{M} - \sqrt{-M+N}}{\sqrt{6}} \tag{19}$$

$$x_4 = \frac{-\sqrt{M} + \sqrt{-M+N}}{\sqrt{6}} \tag{20}$$

In the case of $B = 0$, the roots are:

$$x_1 = -\sqrt{\frac{2}{\sqrt{3}} + 1} \quad \sqrt{-A} \tag{21}$$

$$x_2 = \sqrt{\frac{2}{\sqrt{3}} + 1} \quad \sqrt{-A} \tag{22}$$

$$x_3 = -\sqrt{\frac{2}{\sqrt{3}} - 1} \quad \sqrt{A} \tag{23}$$

$$x_4 = \sqrt{\frac{2}{\sqrt{3}} - 1} \quad \sqrt{A} \tag{24}$$

In the case of $A = 0$, the roots are:

$$x_1 = 0 \tag{25}$$

$$x_2, x_3, x_4 = -\sqrt[3]{4B} \tag{26}$$

Sufficient condition.

Necessary condition.

Conclusion.

□