Topics: Elliptic curves.

7.1. Consider the curves given by the equations

$$C_1 : \ y^2 = x^3 \qquad \text{and} \qquad C_2 : \ y^2 = x^3 - 2x^2 + x.$$

Using calculus methods, find all the singular points of C_1 and C_2.

Solution. Let $F_1(x, y) = y^2 - x^3$, then

$$\frac{\partial F_1}{\partial x} = -3x^2, \qquad \frac{\partial F_1}{\partial y} = 2y.$$

For a point (x_0, y_0) to be singular we need therefore $-3x_0^2 = 0$ and $2y_0 = 0$, so $(x_0, y_0) = (0, 0)$. This point does lie on the curve, since $F_1(0, 0) = 0$. So $(0, 0)$ is the only singular point of the curve C_1.

Let $F_2(x, y) = y^2 - x^3 + 2x^2 - x$, then

$$\frac{\partial F_2}{\partial x} = -3x^2 + 4x - 1, \qquad \frac{\partial F_2}{\partial y} = 2y.$$

Suppose (x_0, y_0) is singular, then $y_0 = 0$, so x_0 must satisfy the two equations

$$-x_0^3 + 2x_0^2 - x_0 = x_0(-x_0^2 + 2x_0 - 1) = 0 \qquad \text{and} \qquad -3x_0^2 + 4x_0 - 1 = 0.$$

Since $x_0 = 0$ does not satisfy the second equation, we are reduced to two quadratic equations. Eliminating the x_0^2 term leaves us with $2x_0 - 2 = 0$, so $x_0 = 1$. So $(1, 0)$ is the only singular point of the curve C_2. □

7.2. In this question we work out how to turn a more general type of Weierstrass equation into one of the type we have been working with: $y^2 = x^3 + ax + b$.

(a) Consider the equation

$$y^2 + a_1xy + a_3y = x^3 + a_2x^2 + a_4x + a_6, \qquad a_i \in \mathbf{F}. \tag{1}$$

Apply the change of variables

$$y = u - \frac{a_1x}{2} - \frac{a_3}{2}$$

and simplify to an equation of the form

$$u^2 = x^3 + b_2x^2 + b_4x + b_6 \tag{2}$$

for appropriate $b_i \in \mathbf{F}$.

(Here is where we have to assume that $2 \neq 0$ in $\mathbf{F}$.)

(b) In (2), apply the change of variables

$$x = v - \frac{b_2}{3}$$

and simplify to a short Weierstrass equation of the form

$$u^2 = v^3 + c_4v + c_6$$

for appropriate $c_i \in \mathbf{F}$.

(Here is where we have to assume that $3 \neq 0$ in $\mathbf{F}$.)

Solution.

(a) Plugging in the change of variables for y in (1), the left hand side becomes

$$u^2 - \frac{a_1^2 x^2}{4} - \frac{a_1 a_3 x}{2} - \frac{a_3^2}{4},$$

so that the entire equation (1) becomes

$$u^2 = x^3 + \left(a_2 + \frac{a_1^2}{4}\right) x^2 + \left(a_4 + \frac{a_1 a_3}{2}\right) x + \left(a_6 + \frac{a_3^2}{4}\right)$$

and it is clear what b_2, b_4, b_6 are.

(b) We now plug in the change of variables for x in (2) and get

$$u^2 = v^3 + \left(b_4 - \frac{b_2^2}{3}\right) v + \left(b_6 - \frac{b_2 b_4}{3} + \frac{2b_2^3}{27}\right). \qquad \square$$

7.3. Fix a parameter c and let $P = (x_0, y_0)$ be a point on the elliptic curve

$$E_c : \; y^2 = x^3 + c.$$

Use the duplication formula to compute the coordinates of $[2]P$.

Compare your answer to Bachet's recipe for producing a new point (x_1, y_1) from an existing point (x_0, y_0) on E_c.

Solution. Let $(x_2, y_2) = [2]P$, then

$$x_2 = \frac{x_0^4 - 8cx_0}{(2y_0)^2} = x_1,$$

$$y_2 = \frac{x_0^6 + 20cx_0^3 - 8c^2}{(2y_0)^3} = -y_1,$$

where (x_1, y_1) is the point from Bachet's formula.

We conclude that Bachet's formula takes P to $[-2]P$. $\square$

7.4. Consider an elliptic curve

$$E : \; y^2 = f(x) = x^3 + ax + b \qquad \text{with } a, b \in \mathbf{Z}$$

and a point $P = (x_1, y_1) \in E(\mathbf{Q})$ with $y_1 \neq 0$.

Recall that the x-coordinate of the point $[2]P$ is given by

$$x_2 = \frac{x_1^4 - 2ax_1^2 - 8bx_1 + a^2}{(2y_1)^2}.$$

Let $g(x) = x^4 - 2ax^2 - 8bx + a^2$ be the polynomial appearing in the numerator.

(a) Find polynomials of the form

$$r(x) = c_2 x^2 + c_0, \qquad s(x) = d_3 x^3 + d_1 x + d_0$$

with integer coefficients depending on a and b, such that

$$r(x) g(x) - s(x) f(x) = 4a^3 + 27b^2.$$

[**Hint**: Start by figuring out how d_3 and c_2 are related, then by looking at the overall constant term and making an educated guess for what c_0 and d_0 should be.]

(b) Use part (a) and the approach in Proposition 3.14 to show that if P and $[2]P$ both have integer coordinates, then either $y_1 = 0$ or $y_1^2 \mid 4a^3 + 27b^2$.

Solution.

(a) Looking at the desired identity, we see that everything except for the constant term on the left hand side must cancel out. In particular, from the degree 6 term we see that $d_3 = c_2$.

The constant term is $a^2c_0 - bd_0 = 4a^3 + 27b^2$, so the only reasonable choice is $c_0 = 4a$ and $d_0 = -27b$.

We plug all of this in and expand

$$\begin{aligned}&(c_2x^2 + 4a)(x^4 - 2ax^2 - 8bx + a^2) - (c_2x^3 + d_1x - 27b)(x^3 + ax + b) \\ &= (4a-3ac_2-d_1)x^4+9b(3-c_2)x^3+a(ac_2-d_1-8a)x^2-b(d_1+5a)x+(4a^3+27b^2),\end{aligned}$$

from which we find that $c_2 = 3$ and $d_1 = -5a$.

So the two polynomials are

$$r(x) = 3x^2 + 4a \qquad \text{and} \qquad s(x) = 3x^3 - 5ax - 27b.$$

(b) We follow the proof of Proposition 3.14 and suppose $y_1 \neq 0$. Then $[2]P = (x_2, y_2)$ with $x_2 = \dfrac{g(x_1)}{4y_1^2}$. Since $x_2 \in \mathbf{Z}$ we see that $y_1^2 \mid g(x_1)$. But $y_1^2 = f(x_1)$, so from the identity

$$r(x_1)g(x_1) - s(x_1)f(x_1) = 4a^3 + 27b^2$$

we can conclude that $y_1^2 \mid 4a^3 + 27b^2$. $\square$

7.5. Consider an elliptic curve given by a Weierstrass equation

$$E: \ y^2 = f(x) = x^3 + ax + b, \qquad a, b \in \mathbf{R}.$$

(a) Let $P = (x_1, y_1)$ be a point of order three. Use the formulas for $[2]P$ and $-P$ to find a polynomial ψ of degree 4 such that $\psi(x_1) = 0$.

(b) Show that $\psi(x) = 2f(x)f''(x) - f'(x)^2$ and $\psi'(x) = 12f(x)$.

(c) Use part (b) to show that ψ and ψ' have no common roots; conclude that ψ has simple roots.

(d) Show that

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

(e) Use part (d) to show that if P is a point of order three then it is an inflection point on the curve (a point where the second derivative changes sign).

(f) Prove that ψ has exactly two real roots, say $\alpha_1 < \alpha_2$. Prove that $f(\alpha_1) < 0$ and $f(\alpha_2) > 0$.

[**Hint**: Use the formulas in part (b) to think about the stationary points and the roots of ψ. Maybe draw some pictures of what the degree 4 polynomial ψ can look like.]

(g) How many points of order three are there in $E(\mathbf{R})$?

Solution.

(a) We have $-P = (x_1, -y_1)$ so using the x-coordinate of $[2]P$ we get

$$\frac{x_1^4 - 2ax_1^2 - 8bx_1 + a^2}{4(x_1^3 + ax_1 + b)} = x_1,$$

so

$$\psi(x_1) = 0 \quad \text{where} \quad \psi(x) = 3x^4 + 6ax^2 + 12bx - a^2.$$

(b) Since $f'(x) = 3x^2 + a$, $f''(x) = 6x$, we have

$$2f(x)f''(x) - f'(x)^2 = 2(x^3 + ax + b)(6x) - (3x^2 + a)^2 = 3x^4 + 6ax^2 + 12bx - a^2 = \psi(x).$$

Differentiating and using $f'''(x) = 6$:

$$\psi'(x) = 2f(x)f'''(x) = 12f(x).$$

(c) From the last part we see that any common root of $\psi(x)$ and $\psi'(x)$ would be a common root of $2f(x)f''(x) - f'(x)^2$ and $12f(x)$, hence a common root of $f(x)$ and $f'(x)$. But there are no common roots of $f(x)$ and $f'(x)$, since E is an elliptic curve.

(d) Differentiate implicitly the relation $y^2 = f(x)$ to get

$$2y\,\frac{dy}{dx} = f'(x).$$

Differentiating implicitly a second time:

$$2\left(\frac{dy}{dx}\right)^2 + 2y\,\frac{d^2y}{dx^2} = f''(x),$$

so

$$\frac{d^2y}{dx^2} = \frac{1}{2y}\left(f''(x) - \frac{f'(x)^2}{2f(x)}\right) = \frac{2f(x)f''(x) - f'(x)^2}{4yf(x)} = \frac{\psi(x)}{4yf(x)}.$$

(e) If $P = (x_1, y_1)$ is a point of order 3 then $\psi(x_1) = 0$ so ψ changes sign at P by part (c). Note that $f(x_1) \neq 0$ since, from our work in part (c), a common root of ψ and f would be a common root of ψ and ψ'.

Therefore the second derivative d^2y/dx^2 changes sign at P, so P is an inflection point.

(f) Since $\psi'(x) = 12f(x)$, the stationary points of ψ are precisely the roots of f.

Moreover, if x_0 is such a stationary point then

$$\psi(x_0) = 2f(x_0)f''(x_0) - f'(x_0)^2 = -f'(x_0)^2 < 0,$$

since we know that f has simple roots.

The last observation is that ψ is a degree 4 polynomial with positive leading coefficient, so it tends to $+\infty$ as $x \longrightarrow \pm\infty$.

Now we consider the two possibilities for f:

- If f has a single real root x_0, then ψ has the single stationary point x_0. Since $\psi(x_0) < 0$, there must be precisely one root $\alpha_1 < x_0$ and one root $\alpha_2 > x_0$. Moreover, ψ is decreasing at α_1 so $f(\alpha_1) = \psi'(\alpha_1)/12 < 0$, and is increasing at α_2 so $f(\alpha_2) > 0$.

- If f has three real roots $x_0 < x_1 < x_2$, then ψ has three stationary points $x_0 < x_1 < x_2$. Then x_0 and x_2 are local minima, and x_1 is a local maximum. But $\psi(x_1) < 0$, so ψ remains negative between x_0 and x_2, so that it has precisely one root $\alpha_1 < x_0$ and one root $\alpha_2 > x_2$. As before we see that $f(\alpha_1) < 0$ and $f(\alpha_2) > 0$.

(g) Let $P \in E(\mathbf{R})$ be a point of order 3. Its x-coordinate must be a real root of ψ, so it is either α_1 or α_2. However, $y^2 = f(\alpha_1) < 0$ has no real solutions. Therefore there are exactly two points of order 3, given by $P = (\alpha_2, \sqrt{f(\alpha_2)})$ and $-P = (\alpha_2, -\sqrt{f(\alpha_2)})$. $\square$