**Topics: Automorphisms; more elliptic curves.**

**8.1.** Recall that a (group) homomorphism $\varphi: G \longrightarrow H$ from one abelian group to another is a map such that $\varphi(x+y) = \varphi(x) + \varphi(y)$ for all $x, y \in G$.

(a) Let $G = \langle g \rangle$ be a cyclic group. Let $H$ be an arbitrary abelian group.

For a group homomorphism $\varphi: G \longrightarrow H$, what property must $\varphi(g)$ satisfy?

(b) Find all the group homomorphisms from $\mathbf{Z}/6\mathbf{Z}$ to $\mathbf{Z}/9\mathbf{Z}$.

(c) Find all the group homomorphisms from $\mathbf{Z}/9\mathbf{Z}$ to $\mathbf{Z}/6\mathbf{Z}$.

(d) Find all the group homomorphisms from $\mathbf{Z}/6\mathbf{Z}$ to $\mathbf{Z}/6\mathbf{Z}$.

(e) An *automorphism* of a group $G$ is a bijective homomorphism $G \longrightarrow G$.

Prove that for a cyclic group $G = \langle g \rangle$, a homomorphism $\varphi: G \longrightarrow G$ is an automorphism if and only if $\varphi(g)$ is a generator of $G$.

(f) Find all the automorphisms of $\mathbf{Z}$.

(g) Find all the automorphisms of $\mathbf{Z}/n\mathbf{Z}$, where $n \in \mathbf{Z}_{\geqslant 1}$.

(h) Find all the automorphisms of $(\mathbf{Z}/p\mathbf{Z})^\times$, where $p$ is prime.

**8.2.** Consider an elliptic curve over the complex numbers $\mathbf{C}$ given by

$$E: \ y^2 = x^3 + ax + b.$$

Let $j$ be the $j$-invariant of $E$, that is

$$j = -1728\,\frac{(4a)^3}{\Delta} = 1728\,\frac{4a^3}{4a^3 + 27b^2}.$$

An *automorphism of $E$* is an isomorphism from $E$ to itself.

(a) Prove that if $j \neq 0, 1728$ then there are exactly 2 automorphisms of $E$ (given by multiplication by $u = \pm 1$).

(b) Prove that if $j = 1728$ then there are exactly 4 automorphisms of $E$.

(c) Prove that if $j = 0$ then there are exactly 6 automorphisms of $E$.

**8.3.** Let $p > 3$ be a prime number and consider the elliptic curve over $\mathbf{Q}$ defined by

$$E_p: \ y^2 = f(x), \qquad \text{where } f(x) = x^3 + px.$$

We (more precisely: you) will determine all the points of finite order of $E_p(\mathbf{Q})$.

(a) How many real roots does the function $f(x)$ have?

(b) That was too easy. Given a constant $C \in \mathbf{R}$, how many real roots does the function $g(x) = f(x) + C$ have?

[**Hint**: Think about the derivative.]

(c) What are the points of order 2 of $E_p(\mathbf{Q})$?

(d) Use the Lutz–Nagell Theorem to find a complete set of possibilities for $y^2$, given that $P = (x, y)$ is a point of finite order $> 2$.

(e) Rule out all the possibilities from part (d) one by one, keeping in mind that $p > 3$.

[**Hint**: Use part (b) in each of the cases.]

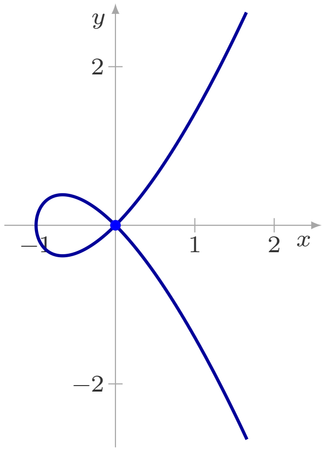
(f) What happens if $p = 3$ or $p = 2$?

**8.4.** [Singularities, revisited] Consider the curves over $\mathbf{R}$ given by the equations

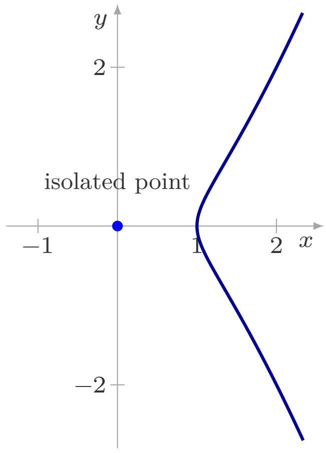
$$C_1 : \; y^2 = x^3 + x^2 = x^2(x+1) \qquad \text{and} \qquad C_2 : \; y^2 = x^3 - x^2 = x^2(x-1).$$

(a) Using calculus methods, find all the singular points of $C_1$ and $C_2$.

Judging by the equations of $C_1$ and $C_2$, we may expect the curves to look somewhat similar. The reality (or perhaps $\mathbf{R}$-ity?) is that they look very different:




$C_1 : \; y^2 = x^3 + x^2$




$C_2 : \; y^2 = x^3 - x^2$

Can we detect this difference algebraically?

Given a curve $C : \; F(x, y) = 0$ that passes through the point $(0, 0)$, the *tangent cone to $C$ at $(0, 0)$* is obtained as follows: write

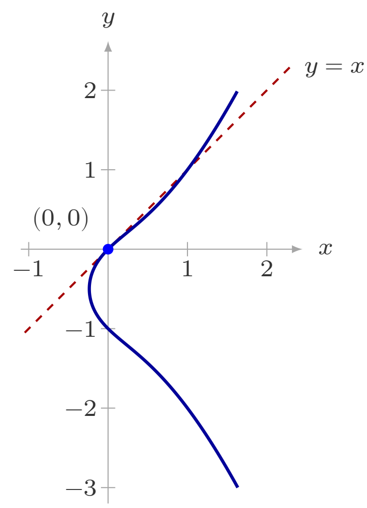
$$F(x, y) = F_m(x, y) + F_{m+1}(x, y) + \cdots + F_d(x, y),$$

where for each $m \leqslant j \leqslant d$, $F_j(x, y)$ contains all the terms of total degree $j$ in $F(x, y)$ and we ask that $F_m(x, y) \neq 0$.
Then the tangent cone is defined by the equation $F_m(x, y) = 0$.

For example, if $F(x, y) = y^2 + y - x^3 - x$, then

$$F_m(x, y) = F_1(x, y) = y - x,$$

so the tangent cone has equation $y - x = 0$ (so it is the line $y = x$).
We can visualise this as in the graph on the right.




$C : \; y^2 + y = x^3 + x$

(b) Compute the equations of the tangent cones of the above two curves $C_1$ and $C_2$, and draw them on the same graphs as the curves themselves.

Can you tell from the equations that something is very different (at least if we are working over $\mathbf{R}$) between the two curves?

What if we work over $\mathbf{C}$ instead?