Instructions: Problems 4 and 6 are to be handed in by next Friday (as always, theoretical part on Moodle, SAGE exercises via CoCalc).

1. Find examples of elliptic curves $E/\mathbb{Q}$ with rational 2-torsion group $E(\mathbb{Q})[2]$ isomorphic to O, $\mathbb{Z}/2\mathbb{Z}$ and $(\mathbb{Z}/2\mathbb{Z})^2$ (explain why these isomorphisms hold).

2. (a) Code a function `avgfivetorsion(p,B)` which computes the proportion over all elliptic curves E over $\mathbb{F}_p$ for $p > 3$ prime with non-trivial $\mathbb{F}_q$-rational five-torsion $E[5](\mathbb{F}_q)$ for each $q = p^r$ with r varying between one and B. *(Hint: you can deduce non-trivial five-torsion from a computation of the order of $E(\mathbb{F}_q)$, for which you may use a SAGE function)*

   (b) Set $B = 30$ and run your code for $p = 7$ and then $p = 5$. What do you observe and how would you explain it? Make a conjecture from the data you see and check if further varying the prime p confirms it.

3. Prove that the q-th power Frobenius map on $E/\mathbb{F}_q$ is actually an endomorphism by showing
$$\varphi(P) \in E(\overline{\mathbb{F}}_q) \text{ and } \varphi(P+Q) = \varphi(P) + \varphi(Q)$$
for points $P, Q \in E(\overline{\mathbb{F}}_q)$ (for simplicity assume $p > 3$). *(Hint: use the fact that the Frobenius $\sigma : x \mapsto x^q$ on $\overline{\mathbb{F}}_q$ is a field automorphism.)*

4. Prove that if two elliptic curves E, E' over $\mathbb{F}_p$ are $\mathbb{F}_p$-isogenous (so there exists an isogeny $f : E \to E'$ given by rational functions with $\mathbb{F}_p$-coefficients, in particular f preserves $\mathbb{F}_p$-rational points), then $|E(\mathbb{F}_p)| = |E'(\mathbb{F}_p)|$.

   (Hint : consider the p-th power Frobenius maps $\varphi_p : E \to E$ and $\varphi'_p : E' \to E'$, and compare $(\mathrm{Id} - \varphi'_p) \circ f$ and $f \circ (\mathrm{Id} - \varphi_p)$ as well as the degrees of these morphisms.)

5. The *zeta function* of an elliptic curve $E/\mathbb{F}_q$ is defined as the power series in $\mathbb{Q}[[T]]$ given by
$$Z(T, E/\mathbb{F}_q) := e^{\sum_{r \geq 1} N_r T^r / r},$$
where $N_r = \sharp E(\mathbb{F}_{q^r})$. Weil proved that in fact the zeta function is a rational function
$$Z(T, E/\mathbb{F}_q) = \frac{1 - a_q T + qT^2}{(1-T)(1-qT)},$$
where $a_q = N_1 - q - 1$ satisfies the Hasse bound.

   (a) Deduce that the zeroes of the zeta function are complex conjugate of absolute value q^{-s} with $s = \frac{1}{2}$. (you should think of this as a Riemann Hypothesis in this setting !).

   (b) The zeta function encodes data about all the cardinalities N_r. Writing the numerator of $Z(T, E/\mathbb{F}_q)$ as $(1 - \alpha T)(1 - \beta T)$, show that:
$$N_r = q^r + 1 - \alpha^r - \beta^r.$$
   (Hint: take log derivatives of the two formulas for zeta)

(c) Compute N_r for the so-called *Koblitz curves* defined over $\mathbb{F}_2$ by

$$y^2 + xy = x^3 + ax^2 + 1 \text{ for } a \in \mathbb{F}_2$$

.

6. (a) Prove that for an elliptic curve $E/\mathbb{F}_p$ defined by $E : y^2 = f(x)$, if the cubic satisfies $f(-x) = -f(x)$, then $|E(\mathbb{F}_p)| = p + 1$ for all primes $p \equiv 3 \mod 4$.
   (b) Find the group structure of $E(\mathbb{F}_{107})$ for $E : y^2 = x^3 - x$.

7. A number n is called a *congruent number* if n can be realized as the area of a right-angled triangle with rational sides (this goes back to the Greeks!). So iff there exist rational a, b, c with $a^2 + b^2 = c^2$ and $ab = 2n$.

   (a) Check that there is a bijection between the two sets:

$$\{(a, b, c) \in \mathbb{Q}^3 : a^2 + b^2 = c^2, 2n = ab\} \leftrightarrow \{(x, y) \in \mathbb{Q}^2 : y^2 = x^3 - n^2x, y \neq 0\}$$

   given by the maps

$$(a, b, c) \mapsto \left(\frac{nb}{c-a}, \frac{2n^2}{c-a}\right) \text{ and } (x, y) \mapsto \left(\frac{x^2 - n^2}{y}, \frac{2nx}{y}, \frac{x^2 + n^2}{y}\right).$$

   (b) Use this to produce 20 rational points on $E_6 : y^2 = x^3 - 36x$ (you may use SAGE). Given that Mazur proved that the torsion part of $E(\mathbb{Q})$ has size ≤ 16 what do you deduce about the rank of E_6?

   (c) Show that the only rational torsion on the elliptic curve $E_n : y^2 = x^3 - n^2x$ is $E_n(\mathbb{Q})[2]$ and deduce a relationship between congruent numbers and the rank of the elliptic curves E_n. *(Hint: you can use that for $p \nmid \Delta(E_n)$ the rational torsion injects into $E(\mathbb{F}_p)$ and argue $\sharp E(\mathbb{F}_p) = p + 1$ for $p \equiv 3 \mod 4$. Then conclude by using Dirichlet's theorem on infinitely many primes in arithmetic progressions.)*