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

1. Given points $P = (x_1, y_1), Q = (x_2, y_2)$ on an elliptic curve $E : y^2 = x^3 + ax + b$ with $x_1 \neq x_2$, establish the coordinates of $P - Q$ (without using the formulas from class).

2. Suppose the cubic $x^3 + ax + b = (x - \lambda_1)(x - \lambda_2)(x - \lambda_3)$ factors. Show that the discriminant $\Delta = 0$ if and only if the λ_i are not all distinct.

3. Prove that there are $q + 1$ points in $E(\mathbb{F}_q)$ for $E : y^2 = x^3 - 1$ when $q \equiv 2 \mod 3$ is a power of an odd prime.

4. Let $E : y^2 = x^3 - x + 2$. Compute (by hand!) the number of points in $E(\mathbb{F}_q)$ for $q = 3, 5, 9$.

5. First read up on how to work with elliptic curves in SAGE.

   (a) Consider the elliptic curve $E : y^2 = x^3 + x + 2$. Write code that does the following: for primes p that do not divide the discriminant $\Delta(E)$ and running up to some bound B, compute (using SAGE's functions)

   $$a_p = p + 1 - \sharp E(\mathbb{F}_p)$$

   and, dividing $[-1, 1]$ into 21 intervals of equal length, count for each interval I the number of primes p such that $a_p/2\sqrt{p} \in I$. Take B reasonably large (around $B = 7 \cdot 10^4$) and plot the counts for each interval against its starting point.

   (b) Now do the same for $E : y^2 = x^3 - 15x + 22$. Do you notice any difference?

6. In SAGE, code a function `randompoint(a,b,p)` which for $p \geq 5$ returns a random point on $E(\mathbb{F}_p)$ for the elliptic curve $E : y^2 = x^3 + ax + b$. *(You may use a SAGE function in order to generate a random integer or to take square roots in $\mathbb{F}_p$ but should code the rest yourself.)*

7. (a) Projective space of dimension n, denoted $\mathbb{P}^n$, is the set of equivalence classes $(X_0 : \cdots : X_n)$ of triples $(X_0, \ldots X_n)$, not all zero, where we identify scalar multiples: $(X_0, \ldots X_n) \sim (\lambda X_0, \ldots, \lambda X_n)$. Such an equivalence class with coordinates in a field K is called a projective point in $\mathbb{P}^n(K)$. Show that as sets $\mathbb{P}^n(K) = K^n \bigsqcup \mathbb{P}^{n-1}(K)$. *(Hint: the two pieces can be obtained as $X_n \neq 0$ by taking new coordinates $x_j = X_j/X_n$ and as $X_n = 0$.)*

   (b) Use this to show that the solutions in the projective plane $\mathbb{P}^2(K)$ of the homogeneous cubic

   $$Y^2Z = X^3 + aXZ^2 + bZ^3$$

   correspond to solutions $(x, y) \in K^2$ of the equation $E : y^2 = x^3 + ax + b$ together with a point at infinity O which represents the point $(0 : 1 : 0) \in \mathbb{P}^2(K)$. (N.B.: This is where the point at infinity comes from and why elliptic curves are projective)

(c) Working in projective space has some advantages as many geometric properties behave better. As an example, we have that for 3 cubic curves C_1, C_2, C_3, if C_3 passes through 8 of the 9 intersection points of C_1, C_2 (with multiplicities, but you can ignore this for now), then C_3 passes through the ninth as well. Use this result to prove associativity of the group law on an elliptic curve!

8. (optional)

(a) Make a list of $a_p = p+1-\sharp E(\mathbb{F}_p)$ for primes $p < 20$ for the curve $E : y^2-y = x^3-x^2$ (you may use SAGE).

(b) Consider the function on the complex upper half plane which maps $\tau \in \mathbb{H}$ to

$$f(q) = q\prod_{n=1}^{\infty}(1-q^n)^2(1-q^{11n})^2,$$

using the notation $q = e^{2\pi i\tau}$. Compute the first 20 coefficients in the Fourier expansion $\sum_{k\geq 1} b_k q^k$ of $f(q)$. Compare the b_p and a_p for p prime.

(c) The function f above is what is called a *modular form* of weight **2** and level **11**: this means that for matrices $\begin{pmatrix} a & b \\ c & d \end{pmatrix} \in M_2(\mathbb{Z})$ with determinant $ad - bc = 1$ acting via fractional linear transformations on the upper half plane f is almost invariant under that transformation, namely we have the identity:

$$f\left(\frac{a\tau + b}{c\tau + b}\right) = (c\tau + d)^{\mathbf{2}} f(\tau) \text{ provided } c \equiv 0 \mod \mathbf{11}.$$

and f is holomorphic (feel free to check these identities!). Where does the level 11 of f appear for E?

(d) The phenomenon you just observed is an instance of what is called *modularity of elliptic curves* $E/\mathbb{Q}$: the numbers a_p are encoded by Fourier coefficients of a normalized modular form f_E associated to E. The biggest step in proving modularity of elliptic curves was achieved by Andrew Wiles and Richard Taylor, and this in particular implied a proof of Fermat's Last Theorem!

Very briefly, Fermat's Last Theorem was deduced roughly as follows: if there is a non-trivial solution

$$a^l + b^l = c^l \text{ for some prime } l \geq 5$$

then one considers the elliptic curve $E : y^2 = x(x - a^l)(x + b^l)$ (called the Frey curve) of discriminant $\Delta = 2^{-8}(abc)^{2l}$. By modularity, E corresponds to a modular form f_E of weight 2 and level $N_E = \prod_{p|abc} p$. The last ingredient is a "level-lowering result" of Ken Ribet, which tells us that given the properties we know f_E must have by modularity, we can strip away all odd prime divisors of N_E and f_E must secretly already exist at level 2. But there are actually no such modular forms, a contradiction!