Instructions: Problems 1 and 3: (b)-(c) are to be handed in by next Friday (as always, theoretical part on Moodle, SAGE exercises via CoCalc).

1. Using SAGE and results from class/homework, come up with a triple (E, q, P) such that E is an elliptic curve defined over $\mathbb{F}_q$ and $P \in E(\mathbb{F}_q)$ is a safe base point for discrete log-based cryptographic schemes (or rather, prove it avoids the pitfalls from class). The larger the order of P, the better! *(Hint: there are various ways to go about it, you could search for prime $\sharp E(\mathbb{F}_p)$ or take $q = p^r$ with r large and use the formula from the exercise on zeta functions for $\sharp E(\mathbb{F}_q)$ etc.)*

2. Code a function `LenstraEC(N)` which finds a non-trivial factor of N using Lenstra's elliptic curve factorization method. Can you factor the numbers from the quadratic sieve exercise in homework 8?

3. In this exercise we study the use of so-called *Schreier graphs* for key exchange protocols. Let G be a group acting freely on a set X, meaning that any $g \in G$ sends $x \in X$ to some element $g \cdot x \in X$ so that the induced map

$$\begin{aligned} G &\to \mathrm{Aut}(X) \\ g &\mapsto (x \mapsto g \cdot x) \end{aligned}$$

is a group homomorphism and $g \cdot x \neq x$ holds $\forall g \neq 1_G, \forall x \in X$. Let $S \subset g$ be a symmetric subset, namely stable under inversion and not containing 1_G. The *Schreier graph* of (S, X) is the graph whose vertices are elements of X and where x, x' are connected by an edge iff $\exists g \in S$ with $g \cdot x = x'$.

(a) We consider the following setup: let $X = (\mathbb{Z}/p\mathbb{Z})^*$ for prime p and let $D \subset G = (\mathbb{Z}/p\mathbb{Z})^*$ be a generating set satisfying $g \in D \Rightarrow g^{-1} \notin D$. Here $g \in G$ acts on X via $x \mapsto x^g$. Finally we set $S = D \cup D^{-1}$, writing $D^{-1} = \{g^{-1} | g \in D\}$. Plot the Schreier graph of (S, X) for $p = 13$ and $D = \{2, 3, 5\}$ in this setup.

(b) Prove that a k-regular graph is a one-sided ε-expander for some $\varepsilon > 0$ if and only if it is connected. Deduce that the Schreier graphs (S, X) from the previous point are one-sided ε-expanders. *(Hint: for the connected implies expander direction, show that the $\lambda_1 = k$-eigenspace of the adjacency matrix is one-dimensional: the span of $v = (1, \ldots, 1)$.)*

(c) Aurélie and Beat decide to use the setup from the previous points to exchange a secret key as follows:

   i. They publicly pick X a large cyclic group of prime order and D and S as above, together with a fixed generator g of X.
   ii. They both pick secret random walks ρ_A and ρ_B in the Schreier graph of (S, X) starting at g and publicly share their respective arrival points/vertices, which we denote by $\rho_A(g)$ and $\rho_B(g)$.
   iii. They can then each compute their shared secret $\rho_A(\rho_B(g)) = \rho_B(\rho_A(g))$.

Explain why this has a chance of working and being secure by relating it to a known hard problem/key exchange protocol. Find one additional necessary requirement for Aurélie and Beat's setup without which their setup is easier to crack than the key exchange protocol you related it to.

4. Let l, p be distinct primes and consider the graph $G = (V, E)$ of l-isogenies of supersingular curves over $\mathbb{F}_{p^2}$. Fix a constant $C > 2$. Give an estimate (in l, C) of a lower bound for the length of a random walk so that one lands in a subset $F \subset V$ of size $|V|/C$ with probability $\geq 1/2C$.

5. The goal of this exercise is to be able to compute supersingular isogeny graphs. There are a couple notions/subtleties you may find useful which we include here:

   - The vertices of the graph are isomorphism classes of supersingular ellitpic curves over $\overline{\mathbb{F}_p}$. One way to keep track of iso. classes of elliptic curves is by what is called the *j-invariant* of $E : y^2 = x^3 + ax + b$. It is defined by:

     $$j(E) = 1728 \cdot \frac{4a^3}{4a^3 + 27b^2}$$

     and each isomorphism class has a unique j-invariant. For supersingular curves $j(E) \in \mathbb{F}_{p^2}$ and each iso. class has a representative defined over $\mathbb{F}_{p^2}$, so often people label the vertices by j-invariants.

   - Automorphisms (isomorphisms: $E \to E$) which are not the identity exist. For $p \neq 2, 3$ they are given by changes of variable

     $$x = u^2 x' \text{ and } y = u^3 y' \text{ for some } u \in \overline{\mathbb{F}_p^*}$$

     in the Weierstrass equation $y^2 = x^3 + ax + b$ which have to satisfy $u^{-4}a = a$ and $u^{-6}b = b$. One then checks there are exactly two automorphisms unless $j(E) = 0$ when $|\operatorname{Aut}(E)| = 6$ and $j(E) = 1728$ when $|\operatorname{Aut}(E)| = 4$.

   - The edges of the graph between two curves E and E' are equivalence classes of isogenies of degree l, where we identify isogenies which have the same kernel as a subgroup of E or differ by an automorphism of E'. This leads via the previous remark to the exceptional situation for $j(E') \in \{0, 1728\}$ that one may identify isogenies and not their duals-in this case the graph needs to be considered as directed.

   - In general, though the graph is $l + 1$-regular, beware there may be self-loops or multiple edges between two vertices.

   Find the graph of 2-isognies of supersingular elliptic curves in $\overline{\mathbb{F}_{53}}$ (equivalently $\mathbb{F}_{53^2}$) and draw it, labeling each vertex with the equation of the corresponding curve. *(Hint: you may use SAGE or any other resource you like.)*