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

1. (a) Code a function `doubleandadd(E,p,P,n)` that for an elliptic curve $E/\mathbb{F}_p$ outputs the coordinates of $[n]P$ for points $P \in E(\mathbb{F}_p)$.

   (b) Write out the elliptic curve version of the Diffie Hellman key exchange (as was done in Lecture 4 for $\mathbb{F}_p^*$).

   (c) Use this with $E/\mathbb{F}_{3851}$ given by $E : y^2 = x^3 + 324x + 1287$ and the point $P = (920, 303) \in E(\mathbb{F}_{3851})$ to share a secret key (just a secret point on $E(\mathbb{F}_{3851})$) with someone! *(Ideally, find a partner in the class to do this with.)*

2. (a) Code a function `annShanks(E,P,p)` that takes as input $E/\mathbb{F}_p$ and a point $P \in E(\mathbb{F}_p)$ and outputs an integer m in the interval $(p+1-2\sqrt{p}, p+1+2\sqrt{p})$ such that $mP = O$ via Shanks babystep-giantstep method. *(Hint: In this setting, take $s \approx p^{1/4}$ and the babysteps compute $O, \pm P \pm 2P, \ldots, \pm sP$. Then compute $Q = (2s+1)P$ and $R = (p+1)P$ and the giantsteps are $R \pm Q, R \pm 2Q, \ldots, R \pm tQ$ for $t = \lfloor 2\sqrt{p}/(2s+1) \rfloor$. Show a collision between these lists has to happen and produces m with $mP = O$.)*

   (b) If there is a unique such integer m in that range, then the above function has computed the order of $E(\mathbb{F}_p)$. This is quite likely to happen, but what could go wrong? Write a function `orderShanks(E,p)` which samples `annShanks(E,P,p)` for a bunch of random points P in $E(\mathbb{F}_p)$ and outputs the deduced likely size $\sharp E(\mathbb{F}_p)$. How often does your code get it right?

3. For various practical purposes, it can be beneficial to work with elliptic curves over $\mathbb{F}_{2^r}$ (though there are some additional security concerns e.g. if r is composite). We consider elliptic curves $E/\mathbb{F}_2$ which we may then also view over larger fields:

   (a) Show that for cryptographic purposes using the elliptic curve over $\mathbb{F}_2$ given by

   $$E : y^2 + y = x^3$$

   and $E(\mathbb{F}_{2^r})$ is a bad idea even for fairly large primes r. *(Hint: deduce this from a computation of $a_p(E)$.)*

   (b) Instead one can use the Koblitz curves

   $$E_a : y^2 + xy = x^3 + ax^2 + 1 \text{ for } a \in \{0, 1\}.$$

   The Frobenius (which here simply squares coordinates) satisfies (as an endomorphism) $\varphi^2 + (-1)^a \varphi + 2 = 0$. Deduce that every integer N has a "φ-adic" expansion, that is, the multiplication-by-N map can be written as

   $$N = n_0 + n_1\varphi + \cdots + n_r\varphi^r \text{ for } n_i \in \{-1, 0, 1\}$$

   with $r \approx 2\log_2(N)$. (N.B.: This makes cumputing multiples of points more efficient on such curves.)

4. Let $E/\mathbb{F}_q$ an elliptic curve and let $l \nmid q$ be a prime. Let k large enough so that $E[l] \subset E(\mathbb{F}_{q^k})$. Prove that if P, Q form a basis of $E[l] \cong (\mathbb{Z}/l\mathbb{Z})^2$, then the Weil pairing $e_l(P, Q)$ is a primitive l-th root of unity in $\mathbb{F}_{q^k}$. For a fixed P of order l, how likely is it that a random $Q \in E[l]$ does not make P, Q into a basis of $E[l]$?

5. Given a basis (P, Q) of $E[N]$ for $N \geq 1$, prove that for arbitrary N-torsion points P_1, P_2, which can be written as $P_1 = a_1P + b_1Q$ and $P_2 = a_2P + b_2Q$, the Weil pairing satisfies:
$$e_N(P_1, P_2) = e_N(P, Q)^{a_1b_2 - a_2b_1} = e_N(P, Q)^{\det \begin{pmatrix} a_1 & a_2 \\ b_1 & b_2 \end{pmatrix}}.$$

6. Create on SAGE a function `MOV(E,P,Q,nbtry)` that implements the MOV attack on an elliptic curve E over $\mathbb{F}_p$ in order to solve the discrete logarithm $kP = Q$, with `nbtry` trials of a random point T as in the algorithm given in class. *(You may use the implemented SAGE functions for the Weil pairing and for solving discrete logarithms over finite fields, but* not *solve DLP over elliptic curves directly in SAGE!).* Then try to use your function to solve the following DLP:

$$\begin{aligned} p &= 18446744073709555927 \\ E &: y^2 = x^3 - x \quad \text{over } \mathbb{F}_p \\ P &= (8492951324596411969, 7618631852165291801) \in E(\mathbb{F}_p) \\ Q &= (10878994278098623565, 9310007525395656987) = kP \in E(\mathbb{F}_p) \end{aligned}$$

(Hint:You may want to define E directly over $\mathbb{F}_{p^2}$ on SAGE to make taking Weil pairings easier).

Even if you don't succeed breaking this DLP, explain why the MOV attack can work on this curve E.