Homework 9

Due **Wednesday**, November 24

Implementation Part

The implementation part sets up the basics of elliptic curve arithmetic.

1. Let's start by setting up and testing the basic data structures for our objects. For our purposes we will save an elliptic curve as a pair of integers: `E = [A,B]`, corresponding to the equation $y^2 = x^3 + Ax + B$. For this assignment, all elliptic curves will be over a finite field $\mathbb{F}_p$. A point of an elliptic curve will either be an ordered pair $(x, y) \in \mathbb{F}_p^2$, or else the point $\mathcal{O}$ at infinity. We will save a point in $\mathbb{F}_p^2$ as a ordered pair `P = [x,y]`, and the point at infinity as a character `'O'`.

   (a) Recall that an equation $y^2 = x^3 + Ax + B$ gives an elliptic curve precisely when the discrimant $\Delta = 4A^3 + 27B^2$ is nonzero. Write a function `isElliptic(E,p)` which takes the equation of a (potential) elliptic curve and a prime p, and returns `True` if it is in fact an elliptic curve (mod p), and `False` otherwise.

   (b) Recall that $E(\mathbb{F}_p)$ is the set of points $(x, y) \in \mathbb{F}_p^2$ satisfying the equation for E, together with a point $\mathcal{O}$ at infinity. Write a function `onCurve(P,E,p)` which takes as input a point P, an elliptic curve E, and a prime p, returning `True` if $P \in E(\mathbb{F}_p)$ and `False` otherwise. (Be sure to include the possibility that $P = \mathcal{O}$).

   (c) Consider the elliptic curve E given by $y^2 = x^3 + 3x + 2$ and the point $P = (3, 5)$. Using the algorithms above: for the first 7 odd primes $(3, 5, 7, 11, 13, 17, 19)$ print the answer the following questions.

      i. Is E an elliptic curve over $\mathbb{F}_p$?
      ii. Is $P \in E(\mathbb{F}_p)$?
      iii. Is $\mathcal{O} \in E(\mathbb{F}_p)$?

   (d) Print the list of points for $y^2 = x^3 + 3x + 2$ over $\mathbb{F}_7$.

2. Now let's throw some arithmetic into the mix.

   (a) Write a function `addPoints(P,Q,E,p)`. It should take as input an elliptic curve E and a prime p, together with two points $P, Q \in E(\mathbb{F}_p)$, and should return the sum $P + Q \in E(\mathbb{F}_p)$. Use the elliptic curve addition algorithm described in class. (Be sure to allow for P, Q, or $P + Q$ to be $\mathcal{O}$).

   (b) Let's do some testing:

      i. Let E be $y^2 = x^3 + 3x + 8$, over $\mathbb{F}_{13}$, $P = (9, 7)$ and $Q = (1, 8)$. Compute $P + Q$, $2P$ and $\mathcal{O} + Q$. (Note: the entire multiplication table for this curve is worked out in [HPS] Table 6.1, so it would be a good example to troubleshoot with).
      ii. Let E be $y^2 = x^3 + 3x + 2$ over $\mathbb{F}_7$. Print the entire multiplication table for E. (You can avoid adding a new line at the end of a print command as follows: `print(stuffToPrint,end='')`, and print $\mathcal{O}$ as `[OOOO]` to keep rows even).
      iii. Let E be $y^2 = x^3 + 231x + 473$ over $p = 17389$. Let $P = (11259, 11278)$ and $Q = (11017, 14637)$. Compute $P + Q$, $2Q$ and $3P$.

Written Part

3. Graph the following curves over $\mathbb{R}$ in the following steps. Since each is of the form $y^2 = f(x)$ first draw a graph of $y = f(x)$ by finding its roots and critical points. Then deduce the shape of $y^2 = f(x)$ by taking square roots of the y coordinates (when you can). Which of them are elliptic curves?

   (a) $y^2 = x^3 - 2x + 4$

   (b) $y^2 = x^3 - 7x + 6$

   (c) $y^2 = x^3 - 12x + 16$

4. Consider the elliptic curve E over $\mathbb{R}$ given by the equation $y^2 = x^3 - 2x + 4$. Let $P = (0, 2)$ and $Q = (3, -5)$. Compute the following *by hand*, explaining the geometry behind each step.

   (a) Show $P, Q \in E$.

   (b) Compute $P \oplus Q$.

   (c) Compute $P \oplus P$.

   (d) Compute $P \oplus P \oplus P$.

Recall that a curve given by an equation $y^2 = x^3 + ax + b$ is an elliptic curve if and only if the value $\Delta_E = 4a^3 + 27b^2 = 0$. This has to do with the right side of the equation having double roots, leading to nonuniqueness of tangent lines after taking square roots (cf. the graphs in question 3). Let's make this more precise.

5. Let $f(x) = x^3 + ax + b$ be a cubic equation, which factors over $\mathbb{C}$ as $(x - e_1)(x - e_2)(x - e_3)$. Show that $4a^3 + 27b^2 = 0$ if and only if the e_i are all distinct.