Exercises on Elliptic Curves

You do not need to do all of these, but at least try problem 1. You might want to work in groups.

1. Consider the elliptic curve $y^2 = x^3 + x + 3$ over the field $F = F_7$.

(a) For which values of $x \in F_7$ is $x^3 + x + 3$ equal to a perfect square in F_7?

(b) List $E(F_7)$. (There should be six points.)

(c) Find the line through the two points $(4, 1)$ and $(6, 1)$. Find the third point of E which this line passes through. Find $(4, 1) + (6, 1)$.

(d) This question may be answered with the help of Magma. Show that $E(F)$ is cyclic and find a generator.

Useful Magma commands:

```
F := GF(7);
E := EllipticCurve([F!1,3]);
P := E![F!4,1];
```

(e) Find the Discrete Logarithm of $(6, 1)$ to the base $(4, 1)$. That is, find k such that $(6, 1) = k(4, 1)$.

(f) Find a point on $E(F)$ of order 3. Find a point of order 2.

2. This exercise explains how to attack the discrete log on a cyclic group of composite order.

Let G be a cyclic group of order N. Let P be a generator of G. Let Q be an unknown multiple of P, say $Q = aP$. The goal is to find $a \pmod N$.

(a) Show if $N = nm$, then nP has order m, and nQ is a multiple of nP. Show that solving the discrete log problem for nP, nQ will give some useful information about a. What information does it give?

(b) If $N = pq$, explain how to find a by doing one discrete log problem of size p and one of size q, and then using the Chinese Remainder Theorem.

(c) The elliptic curve $E : y^2 = x^3 + x + 7$ over the field F_{29} has exactly 35 elements. On this curve, find a such that $a * (8, 11) = (24, 14)$, by using the method of part (b).

(d) If $N = p^2$, explain how to find a by doing two discrete log problems of size p.

(e) The curve $E : y^2 = x^3 + x + 24$ over F_{541} has 539 points. Solve the discrete log problem: $(423, 398) = a(111, 58)$. (Break this down into three smaller discrete log problems.)

3. This exercise explains how to attack the discrete log problem on a group using the baby-step-giant-step attack:

(a) Suppose a group G has prime order r. Let $m = \lceil \sqrt{r} \rceil$. Show that any $a \in Z/rZ$ can be written as $a_1 m + a_2$, where $0 \leq a_1, a_2 < m$.

(b) If P generates G and Q is some multiple of P, show there exist integers a_1 and a_2 with $0 \leq a_i < \sqrt{r}$ such that $a_1 * (mP) = Q - a_2P$. The baby-step-giant-step attack consists of listing all $a_1 * (mP)$ and all $Q - a_2P$ and looking for a match between the two lists.

(c) Apply the baby-step-giant-step attack to find the log of $Q = (285, 1043)$ with respect to the base point $P = (1070, 200)$ on the elliptic curve $E : y^2 = x^3 + x + 33$ over the field $F = F_{1319}$. This curve has order 1373.

Hint: Here is code to create the list of all pairs $\langle Q - a_2P, a_2 \rangle$, sorted on the x-coordinate of $Q - a_2P$:

```
F := GF(1319);
E := EllipticCurve([F!1,33]);
P := E![F!1070,200];
Q := E![F!285,1043];
list1 := [Q];
for i in [2..38] do list1[i] := list1[i-1]-P; end for;
L1 := [ [list1[i,1], list1[i,2], i ] : i in [1..38] ];
Sort(~L1);
```

4. Let $E_1 : y^2 = x^3 + 2$ over the field $F = F_7$. Let $E_2 : y^2 = x^3 + 3x + 2$ over F.

Find the number of points in $E_1(F)$ and in $E_2(F)$. Try this by hand, or by using a Magma command. Is $E_1(F)$ a cyclic group? Is $E_2(F)$ a cyclic group?

Useful magma commands:

Order(E); // the number of rational points in E

Random(E); // creates a random point on $E(F)$

IsIdentity(P); // tests whether the point P equals the identity element.