CS 259C/Math 250: Elliptic Curves in Cryptography
Homework #1

Due October 10

Answers must be handed in in class or to Mark (494 Gates) by 4pm on the due date. Use of SAGE is allowed on any problem; however, if you do use SAGE you must show your work by printing out your computations and attaching it to the homework you turn in. Use of LaTeX is encouraged but **not** required.

1. (2 points, due Monday, October 3, 11.59 pm.) Go to http://www.surveymonkey.com/s/JKPS8MY and fill out the survey there.

2. (2 points[1]) Sign up for a SAGE account at http://www.sagenb.org. Click "Help" and then "Tutorial" and work through the sections "Introduction," "A guided tour," and "Programming." Work through any further sections you feel would be helpful for your use of SAGE.

3. (5 points) Practice computing on elliptic curves. For all of the following, let E be the elliptic curve $y^2 = x^3 - 4x$. Use of SAGE is highly recommended!

   (a) Plot (on separate graphs) $E(\mathbb{R})$ and $E(\mathbb{F}_{31})$.

   (b) List all of the points of $E(\mathbb{F}_{31})$. (You can use projective coordinates if that happens to be more convenient.)

   (c) What is the group structure of $E(\mathbb{F}_{31})$? (Specifically, determine k and $r_1, \ldots, r_k > 1$ such that $E(\mathbb{F}_{31})$ is isomorphic to $\mathbb{Z}_{r_1} \times \cdots \times \mathbb{Z}_{r_k}$.)

   (d) Let $P = (1, 11)$ and $Q = (25, 5)$ on $E(\mathbb{F}_{31})$. Find an integer a such that $Q = [a]P$.

   (e) Let p be the smallest prime larger than 2^{259}. Compute $\#E(\mathbb{F}_p)$ (i.e., the order of the group $E(\mathbb{F}_p)$). Do you notice anything surprising about the group order?

4. (3 points) Let $E : y^2 = x^3 + Ax + B$ be an elliptic curve over a field K.

   (a) Show that any point on E with y-coordinate equal to zero has order 2.

   (b) Suppose $A = 0$. Show that any point on E with x-coordinate equal to zero has order 3.

5. (6 points) In this exercise we show that it is not so easy to define a group law on an elliptic curve. Let E be a curve of the form $y^2 = x^3 + Ax + B$ defined over a field K. Let O be the point at infinity on E.

[1] Since there's no way to check that you did this problem, you will get these points no matter what. However, the things you learn in the tutorial will probably come in handy later.

Consider the operation $\boxplus$ defined on $E(K)$ as follows: given points P and Q in $E(K)$, neither equal to O, let L be the line through P and Q (or the tangent line to E at P if $P = Q$). Define $P \boxplus Q$ to be the third point of $L \cap E$, or O if the line L is vertical. Define $P \boxplus O$ to be P for all points P.

(a) Assume (for now) that $\boxplus$ does define a group law on $E(K)$. By considering a line that intersects E at P, Q, and R, show that every point P in $E(K)$ has order at most 2.

(b) Use the previous fact to show that the operation $\boxplus$ does not (in general) have a unique identity element. (What happens when you try to compute $P \boxplus P$ for different values of P?)

(c) Use the associativity of the real group law on E to show that $\boxplus$ is not (in general) associative.

(d) (Bonus, 2 points) Give an example of an elliptic curve E over a finite field $\mathbb{F}_q$ such that $\boxplus$ **does** define a group law on $E(\mathbb{F}_q)$.

6. (3 points) Washington exercise 2.9.

7. (3 points) Washington exercise 2.16. (You may assume that $d \neq 0$.)

8. (3 points) Washington exercise 2.17.

9. (4 points) Let $E_1 : y^2 + y = x^3$, $E_2 : y^2 + y = x^3 + 1$ and $E_3 : y^2 + y = x^3 + x$ be elliptic curves over $\mathbb{F}_2$. Since $j(E_1) = j(E_2) = j(E_3) = 0$ it follows that there are isomorphisms over $\overline{\mathbb{F}}_2$ from E_1 to E_2 and from E_1 to E_3. Write down such isomorphisms.

10. (8 points) Consider $E : y^2 + y = x^3$ over $\mathbb{F}_2$. Let $u \in \overline{\mathbb{F}}_2$ satisfy $u^3 = 1$, $s \in \overline{\mathbb{F}}_2$ satisfy $s^4 + s = 0$ and $t \in \overline{\mathbb{F}}_2$ satisfy $t^2 + t = s^6$.

(a) Show that
$$\phi(x, y) = (u^2 x + s^2, y + u^2 s x + t)$$
is an automorphism of E.

(b) Show that every automorphism arises this way and so $\#\mathrm{Aut}(E) = 24$.[2]

(c) Show that if $\phi \in \mathrm{Aut}(E)$ then either $\phi^2 = \pm 1$ or $\phi^3 = \pm 1$.

(d) Show that $\mathrm{Aut}(E)$ is non-abelian.

[2] If the powers of u and s come out differently in your calculations, you may need to replace u with u^2 and/or s with s^2, which you can do because squaring permutes the solutions to the defining equations for u and s.