18.783 Elliptic Curves **Spring 2015**
Problem Set #1 **Due: 02/13/2015**

Description

For this first problem set, choose one of Problems 1 and 2, do both Problems 3 and 4. Be sure also to complete Problem 5, which is a required survey whose results will help shape future problem sets and lectures. You can use the latex source for this problem set as a template for writing up your solutions – SageMathCloud includes a latex editor, but feel free to use the latex environment of your choice.

Be sure to put your name on your solution (you can replace the due date in the header with your name). If you should discover a typo/error in the problem set or lecture notes, please let me know as soon as possible – the first person to find each error will receive 1–3 points of extra credit.

Problem 1. Edwards curves (20 points)

(a) Show that $(c, 0)$ is a point of order 4 on the Edwards curve $x^2 + y^2 = c^2(1 + dx^2y^2)$.

(b) Modify the group law so that $(c, 0)$ is the identity and $(0, c)$ is a point of order 4. This defines a new group on the same set of elements (rational points on the curve). Show that this group is isomorphic to the standard one.

(c) Let n be the integer formed by the last 2 digits of your student ID, and let

$$x_3 = \frac{n^2 - 1}{n^2 + 1}, \qquad y_3 = -\frac{(n-1)^2}{n^2 + 1}, \qquad d = \frac{(n^2 + 1)^3(n^2 - 4n + 1)}{(n-1)^6(n+1)^2}.$$

Show that $P = (x_3, y_3)$ is a point of order 3 on the curve $x^2 + y^2 = 1 + dx^2y^2$ over $\mathbb{Q}$.

(d) Find a point of order 12 on the curve in part (c).

Problem 2. Automorphisms (20 points)

Recall that an *endomorphism* is a homomorphism from a group to itself, and an *automorphism* is an endomorphism that is also an isomorphism. The automorphisms of a group G form a group $\mathrm{Aut}(G)$ under composition, and the endomorphisms of an additive abelian group G form a ring $\mathrm{End}(G)$ in which multiplication is composition (so the product of $\alpha, \beta \in \mathrm{End}(G)$ is defined by $(\alpha\beta)(g) = \alpha(\beta(g))$), and addition is addition in the group (so the sum of $\alpha, \beta \in \mathrm{End}(G)$ is defined by $(\alpha + \beta)(g) = \alpha(g) + \beta(g)$).

Let $E\colon y^2 = x^3 + Ax + B$ be an elliptic curve defined over an algebraically closed field k whose characteristic is not 2 or 3. In each of the problems below, assume that the specified map sends the identity element $(0 : 1 : 0)$ of $E(k)$ to itself (a necessary requirement of any endomorphism).

(a) Show that the map $(x, y) \mapsto (x, -y)$ is an automorphism of order 2.

(b) Assume $B = 0$ and suppose $i \in k$ satisfies $i^2 = -1$. Show that $\alpha\colon (x, y) \mapsto (-x, iy)$ is an automorphism of order 4, and that the equation $\alpha^2 + 1 = 0$ holds in $\mathrm{End}(E(k))$.

(c) Assume $A = 0$ and suppose $\zeta \in k$ satisfies $\zeta^3 = 1$ and $\zeta \neq 1$. Show that the map $\beta\colon (x, y) \to (\zeta x, -y)$ is an automorphism of order 6 and that the equation $\beta^2 - \beta + 1 = 0$ holds in $\mathrm{End}(E(k))$.

Problem 3. Quadratic twists (40 points)

Let E/k be an elliptic curve in short Weierstrass form

$$E\colon \qquad y^2 = x^3 + Ax + B.$$

The *quadratic twist* of E by $c \in k^*$ is the elliptic curve over k defined by the equation

$$E_c\colon \qquad cy^2 = x^3 + Ax + B.$$

(a) Using a linear change of variables, show that E_c is isomorphic to an elliptic curve in standard Weierstrass form $y^2 = x^3 + A'x + B'$, and express A' and B' in terms of A and B and c. Verify that E_c is not singular.

(b) For any group G and positive integer n, we use $G[n]$ to denote the n-torsion subgroup of G, consisting of all elements whose order divides n. Prove that $E(k)[2] = E_c(k)[2]$.

(c) Prove that if c is a square in k^*, then E and E_c are isomorphic over k (via a linear change of variables with coefficients in k). Conclude that E and E_c are always isomorphic over $k(\sqrt{c})$, whether c is a square in k^* or not (in general, curves defined over k are said to be *twists* if they are isomorphic over some extension of k).

(d) Now assume that k is a finite field $\mathbb{F}_p \simeq \mathbb{Z}/p\mathbb{Z}$, for some odd prime p, and let t be the unique integer for which

$$\#E(\mathbb{F}_p) = p + 1 - t,$$

where $\#E(\mathbb{F}_p)$ is the cardinality of the group of $\mathbb{F}_p$-rational points of E. Prove that

$$\#E_c(\mathbb{F}_p) = p + 1 - \left(\frac{c}{p}\right) t,$$

where $\left(\frac{c}{p}\right)$ is the Legendre symbol, which is equal to $+1$ when c is a square modulo p and -1 when it is not (note that $c \in \mathbb{F}_p^*$ is never zero modulo p).

(e) Continuing with $k = \mathbb{F}_p$, show that if $t \neq 0$ then E_c and $E_{c'}$ are isomorphic if and only if $\left(\frac{c}{p}\right) = \left(\frac{c'}{p}\right)$ (this is also true when $t = 0$ but you need not consider this case).

Problem 4. Sato-Tate for elliptic curves with complex multiplication (40 points)

Recall from Lecture 1 that the elliptic curve $E/\mathbb{Q}$ defined by $y^2 = x^3 + Ax + B$ has *good reduction* at a prime p whenever p does not divide $\Delta(E) = -16(4A^3 + 27B^2)$. For each prime p of good reduction, let

$$a_p = p + 1 - \#E_p(\mathbb{F}_p) \qquad \text{and} \qquad x_p = a_p/\sqrt{p},$$

where E_p denotes the reduction of E modulo p.

To create an elliptic curve defined by a short Weierstrass equation in Sage, you can type `E=EllipticCurve([A,B])`. To check whether the elliptic curve E has good reduction at p, use `E.has_good_reduction(p)`, and to compute a_p, use `E.ap(p)`.

In this problem you will investigate the distribution of x_p for some elliptic curves over $\mathbb{Q}$ to which the Sato-Tate conjecture does not apply. These are elliptic curves with *complex multiplication* (CM for short), a term we will define later in the course. In Sage you can check for CM using `E.has_cm()`.

(a) Let $E/\mathbb{Q}$ be the curve defined by $y^2 = x^3 + 1$. Compute a list of a_p values for the primes $p \leq 200$ where E has good reduction (all but 2 and 3). The following block of Sage code does this.

```
E=EllipticCurve([0,1])
for p in primes(0,200):
    if E.has_good_reduction(p): print p, E.ap(p)
```

You will notice that many of the a_p values are zero. Give a conjectural criterion for the primes p for which $a_p = 0$. Verify your conjecture for all primes $p \leq 2^{10}$ where E has good reduction.

(b) Given a bound B, the nth *moment statistic* M_n of x_p is defined as the average value of x_p^n over primes $p \leq B$ where E has good reduction. In Lecture 1 we saw that for an elliptic curve over $\mathbb{Q}$ without complex multiplication, the sequence of moment statistics $M_0, M_1, M_2, \ldots$ appear to converge to the integer sequence

$$1, 0, 1, 0, 2, 0, 5, 0, 14, 0, 42, \ldots,$$

whose odd terms are 0 and whose even terms are the Catalan numbers. Your goal is to determine an analogous sequence for elliptic curves over $\mathbb{Q}$ with complex multiplication.

To do this efficiently, use the `E.aplist()` method in Sage. The following block of code computes the moment statistics $M_0, \ldots, M_{10}$ of x_p using the bound $B = 2^k$.

```
k=12
E=EllipticCurve([0,1])
A=E.aplist(2^k)
P=prime_range(0,2^k)
X=[A[i]/sqrt(RR(P[i])) for i in range(0,len(A))]
M=[sum([a^n for a in X])/len(X) for n in [0..10]]
print M
```

(note that use of `RR(P[i])` to coerce the prime `P[i]` to a real number before taking its square root — without this Sage will use a symbolic representation of the square root as an algebraic number, which is not what we want). With this approach we are also including a few a_p values at bad primes (which will yield $x_p \approx 0$), but this is harmless as long as we make $B = 2^k$ large enough.

By computing moment statistics using bounds $B = 2^k$ with $k = 12, 16, 20, 24$, determine the integers to which the first ten moment statistics appear to converge, and come up with a conjectural formula for the nth moment (if you get stuck on this, look at parts (e) and (f) below). Then test your conjecture by computing the 12th and 14th moment statistics and comparing the results.

(c) Repeat the analysis in parts (a) and (b) for the following elliptic curves over $\mathbb{Q}$:

$$y^2 = x^3 - 595x + 5586,$$
$$y^2 = x^3 - 608x + 5776,$$
$$y^2 = x^3 - 9504x + 365904.$$

You will probably need to look at more a_p values than just up to $p \leq 200$ in order to formulate a criterion for the a_p that are zero. Do the x_p moment statistics for these elliptic curves appear to converge to the same sequence you conjectured in part (b)?

(d) Pick one of the three curves from part (c) and take its quadratic twist by the last four digits of your student ID. Does this change the sequence of a_p values? Does it change the moment statistics of x_p?

(e) Recall that the special orthogonal group $\mathrm{SO}(2)$ consists of all matrices of the form $R_\theta = \left(\begin{smallmatrix} \cos\theta & -\sin\theta \\ \sin\theta & \cos\theta \end{smallmatrix}\right)$. To generate a random matrix in $\mathrm{SO}(2)$, one simply picks θ uniformly at random from the interval $[0, 2\pi)$; this is the *Haar measure* on $\mathrm{SO}(2)$, the unique probability measure that is invariant under the group action. Derive a formula for the nth moment of the trace of a random matrix in $\mathrm{SO}(2)$ by integrating the nth power of the trace of R_θ over all $\theta \in [0, 2\pi)$. Be sure to normalize by $1/(2\pi)$ so that $M_0 = 1$.

(f) The normalizer $N(\mathrm{SO}(2))$ of $\mathrm{SO}(2)$ in the special unitary group $\mathrm{SU}(2)$ consists of all matrices of the form R_θ and JR_θ, where $J = \left(\begin{smallmatrix} i & 0 \\ 0 & -i \end{smallmatrix}\right)$. Derive a formula for the nth moment of the trace of a random matrix in $N(\mathrm{SO}(2))$ (under the Haar measure on $N(\mathrm{SO}(2))$ one picks $\theta \in [0, 2\pi)$ uniformly at random and then takes R_θ or JR_θ with equal probability). Compare the results to the formula you conjectured in part (b).

Problem 5. Survey

Complete the following survey by rating each of the problems you solved on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how difficult you found the problem (1 = "trivial," 10 = "brutal"). Also estimate the amount of time you spent on each problem to the nearest half hour.

	Interest	Difficulty	Time Spent
Problem 1			
Problem 2			
Problem 3			
Problem 4			

Please rate each of the following lectures that you attended on a scale of 1 to 10, according to the quality of the material (1="pointless", 10="priceless"), the quality of the presentation (1="epic fail", 10="perfection"), and the novelty of the material to you (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Novelty
2/3	Introduction			
2/5	Group Law			

Feel free to record any additional comments you have on the problem sets or lectures; in particular, how you think they might be improved.

18.783 Elliptic Curves
Spring 2015