18.783 Elliptic Curves **Spring 2019**
Problem Set #1 **Due: 02/18/2019**

These problems are related to the material covered in Lectures 1-3. Some of them require the use of Sage; you will need to either create a (free) CoCalc account, or download and install a copy of Sage to run on your own computer. Sage is based on the python programming language; you will find examples of Sage usage in the problem descriptions below, and there is a wealth of information to be found on the Sage website, including tutorials (a bit of googling will also yield answers to many common questions).

Instructions: Solve any combination of problems 1-5 that sums to 96 points, then complete the survey problem 6 (worth 4 points), 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. CoCalc 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). Your solutions are to be written up in latex and submitted as a pdf-file with a filename of the form `SurnamePset1.pdf` via e-mail to `drew@math.mit.edu` by **noon** on the date due.

Collaboration is permitted/encouraged, but you must identify your collaborators, and any references you consulted that are not listed in the course syllabus. If there are none, you should write "**Sources consulted: none**" at the top of your solution. The first person to spot each non-trivial typo/error in any of the problem sets or lecture notes will receive 1-5 points of extra credit.

Problem 1. Chebyshev's theorem (16 points)

Let $\pi(x)$ denote the prime counting function, which for any real number x counts the number of primes $p \le x$. The Prime Number Theorem is the asymptotic statement

$$\pi(x) \sim \frac{x}{\log x}$$

which means $\lim_{x\to\infty} \pi(x)/(x/\log x) = 1$. We won't prove the prime number theorem in this course, as we are happy to make do with the weaker statement that there exist $c_1, c_2 > 0$ such that

$$c_1 \frac{x}{\log x} \le \pi(x) \le c_2 \frac{x}{\log x} \tag{1}$$

holds for all sufficiently large x, as proved by Chebyshev. In fact, if we take $c_1 = (\log 2)/2$ and $c_2 = 6 \log 2$ then (1) holds for all $x \ge 2$, as you will now prove.

(a) Show that for all integers $n \ge 1$ we have

$$n^{\pi(2n)-\pi(n)} \le \prod_{n<p\le 2n} p \le \binom{2n}{n} \le 2^{2n},$$

where p ranges over primes. Conclude that $\pi(2n) - \pi(n) \le (2\log 2)n/(\log n)$.[1]

[1] When you are asked to "conclude" something on a problem set in this course, you need to prove it.

(b) Using **(a)**, prove that $\pi(2^n) \leq 3 \cdot 2^n/n$ for all integers $n \geq 1$, and use this to show

$$\pi(x) \leq (6\log 2)\frac{x}{\log x}$$

for all $x \geq 1$.

(c) For integers $n \geq 1$, let $v_p(n)$ denote the largest integer $e \geq 0$ such that $p^e|n$. Prove

$$v_p(n!) = \sum_{e\geq 1}\left\lfloor \frac{n}{p^e}\right\rfloor,$$

and then show that $v_p(\binom{2n}{n}) \leq (\log 2n)/(\log p)$. Using this, prove that

$$\frac{2^{2n}}{2n} \leq (2n)^{\pi(2n)}$$

holds for all integers $n \geq 1$.

(d) Using **(c)**, show that for $x \geq 2$ we have

$$\pi(x) \geq \frac{\log 2}{2}\frac{x}{\log x}.$$

Problem 2. Edwards curves (16 points)

(a) Let d be a non-square in a field k of characteristic different from 2, and consider the Edwards curve

$$E\colon x^2 + y^2 = 1 + dx^2y^2$$

with $(0,1)$ as the identity element. Using the group law defined in class, show that the rational point $(1,0)$ has order 4. Give an example of an elliptic curve over a finite field of odd characteristic that is not isomorphic to any Edwards curve.

(b) Explain how to modify the group law on E so that $(1,0)$ is the identity and $(0,1)$ is a point of order 4, and show that this group is isomorphic to the original one.

(c) Let n be the integer formed by the last 2 digits of your student ID (but set $n = 2$ if you student ID ends in 01), 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 3. Twists of elliptic curves (32 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 $c \in k^\times$ 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 $k^\times$, 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 $k^\times$ or not (in general, curves defined over k are *twists* if they are isomorphic over some extension of k).

(d) Show that when $B = 0$, replacing A by $A' := cA$ for some nonsquare c yields an elliptic curve E' that is not a quadratic twist of E but is a *quartic twist* of E, which becomes isomorphic to E over the extension $k(c^{1/4})$. Similarly show how to construct *cubic twists* and *sextic twists* of E when $A = 0$.

(e) Now let $k = \mathbb{F}_q$ be a finite field of odd characteristic, and let t be the unique integer for which

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

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

$$\#E_c(\mathbb{F}_q) = q + 1 - \chi(c)t,$$

where $\chi\colon \mathbb{F}_q^\times \to \{\pm 1\}$ is the quadratic character of $\mathbb{F}_q^\times$ (so $\chi(c) = 1$ iff c is a square).

(f) Continuing with $k = \mathbb{F}_q$, show that if $t \neq 0$ then E_c and $E_{c'}$ are isomorphic if and only if $\chi(c) = \chi(c')$ (this is also true when $t = 0$ but you need not prove this).

Problem 4. Four torsion subgroups (32 points)

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

$$E\colon \qquad y^2 = f(x) = x^3 + Ax + B,$$

and let $f'(x) := 3x^2 + A$ denote the formal derivative of $f(x)$. Let $E[n] := E(\bar{k})[n]$ denote the n-torsion subgroup of $E(\bar{k})$.

(a) Prove that $P \in E(\bar{k})$ has order 2 if and only if $P = (x_0, 0)$ with $f(x_0) = 0$. Conclude that $E[2] \simeq \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/2\mathbb{Z}$ and $E[2^r] \simeq \mathbb{Z}/2^r\mathbb{Z} \oplus \mathbb{Z}/2^r\mathbb{Z}$ for all $r \geq 1$.

(b) Let $Q = (x_0, 0) \in E(\bar{k})$ and let $P = (u, v) \in E(\bar{k})$. Prove that $2P = Q$ if and only if we have $f'(x_0) = (u - x_0)^2$.

Now let $k = \mathbb{F}_q$ be a finite field of odd characteristic and let $\chi\colon \mathbb{F}_q^\times \to \{\pm 1\}$ be its quadratic character.

(c) Prove that $E(\mathbb{F}_q)$ contains a point of order 4 only if $\chi(f'(x_0)) = 1$ for some rational root $x_0 \in \mathbb{F}_q$ of $f(x)$. Show that this necessary condition is not always sufficient.

(d) Suppose that $f(x)$ has three rational roots $x_1, x_2, x_3 \in \mathbb{F}_q$. Prove that

$$\chi(-1)\chi(f'(x_1))\chi(f'(x_2))\chi(f'(x_3)) = 1.$$

Conclude that if $q \equiv 3 \bmod 4$ then $E(\mathbb{F}_q)[4] \neq E[4]$.

Let $c \in \mathbb{F}_q^\times$ be a nonsquare and let E_c denote the quadratic twist of E, as in Problem 3. If $f(x)$ has no rational roots then $E(\mathbb{F}_q)[4] = E_c(\mathbb{F}_q)[4] = \{0\}$ (by **3b** and **4a**).

(e) Determine up to isomorphism the unordered pairs $(E(\mathbb{F}_q)[4], E_c(\mathbb{F}_q)[4])$ that can arise when $f(x)$ has exactly one rational root, where q and $f(x)$ are allowed to vary subject to this constraint.

(f) Determine up to isomorphism the unordered pairs $(E(\mathbb{F}_q)[4], E_c(\mathbb{F}_q)[4])$ that can arise when $f(x)$ has three rational roots and $q \equiv 3 \bmod 4$, and then do the same for $q \equiv 1 \bmod 4$, where q and f are allowed to vary subject to these constraints.

Problem 5. Sato-Tate for CM elliptic curves (32 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 $p \le 200$ 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 $p \le 2^{10}$ 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 $p \le B$ 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 **(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 $\mathbb{Q}$:

$$\begin{aligned} y^2 &= x^3 - 595x + 5586, \\ y^2 &= x^3 - 608x + 5776, \\ y^2 &= x^3 - 9504x + 365904. \end{aligned}$$

You will probably need to look at more a_p values than just up to $p \le 200$ 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 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 SO(2), one simply picks θ uniformly at random from the interval $[0, 2\pi)$; this is the *Haar measure* on 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 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 SO(2) in the special unitary group 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 6. Survey (4 points)

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			
Problem 5			

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"), the pace (1="watching paint dry", 10="head still spinning"), and the novelty of the material (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
2/6	Introduction				
2/11	The group law				
2/13	Finite field arithmetic				

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