18.783 Elliptic Curves **Spring 2017**
Problem Set #6

Description

These problems are related to the material covered in Lectures 12-13.

Instructions: Solve problem 1 and then solve **one** of Problems 2-4. Finally, complete Problem 5, which is a short survey. Your solutions are to be written up in latex and submitted as a pdf-file with a filename of the form `SurnamePset6.pdf`.

Collaboration is permitted/encouraged, but you must identify your collaborators, and any references not listed in the course syllabus. The first to spot each non-trivial typo/error in the problem sets or lecture notes will receive 1-5 points of extra credit.

Problem 1. A noncommutative endomorphism ring (30 points)

Let $p = 7$, and consider the finite field $\mathbb{F}_{p^2}$, which we may represent explicitly as

$$\mathbb{F}_{p^2} \simeq \mathbb{F}_p[i]/(i^2+1) = \{a + bi : a, b \in \mathbb{F}_p\}.$$

To create the field $\mathbb{F}_{p^2}$ in Sage using this particular representation, use

```
F7.<x>=PolynomialRing(GF(7))
F49.<i>=GF(49,modulus=x^2+1)
```

Now consider the elliptic curve $E/\mathbb{F}_{p^2}$ defined by

$$y^2 = x^3 + (1+i)x.$$

The group of $\mathbb{F}_{p^2}$-rational points on E is isomorphic to $\mathbb{Z}/6\mathbb{Z} \oplus \mathbb{Z}/6\mathbb{Z}$ and is generated by the affine points

$$P_1 = (i, i), \quad P_2 = (i+2, 2i),$$

which you can construct in Sage using `P1=E(i,i)` and `P2=E(i+2,2*i)`. Let π_E denote the Frobenius endomorphism of E.

(a) Prove that $\pi_E = 7$ in $\operatorname{End}(E)$.

Since π_E corresponds to an integer in $\operatorname{End}(E)$, you might be tempted to conclude that $\operatorname{End}(E) \simeq \mathbb{Z}$. But this is far from true.

(b) Show that the p-power Frobenius map π of degree $p = 7$ does not lie in $\operatorname{End}(E)$.

(c) Prove that nevertheless $\operatorname{End}(E)$ does contain an endomorphism α of degree 7 by exhibiting an explicit rational map $\alpha\colon E \to E$ that satisfies $\alpha^2 = -7$.

(d) Now find another endomorphism β that satisfies $\beta^2 = -1$ (give β explicitly).

(e) Prove that α and β do not commute, but that $\alpha\beta = -\beta\alpha$ holds.

Problem 2. The image of Galois (70 points)

Let $E/\mathbb{Q}$ be an elliptic curve, let ℓ be a prime, and let $K = \mathbb{Q}(E[\ell])$ be the associated *ℓ-torsion field* obtained by adjoining the coordinates of all the points in the ℓ-torsion subgroup $E[\ell]$ to $\mathbb{Q}$. As you proved in Problem Set 3, the ℓ-torsion field K is a Galois extension of $\mathbb{Q}$, and the Galois group $\mathrm{Gal}(K/\mathbb{Q})$ acts linearly on the vector space

$$E[\ell] \;\simeq\; \mathbb{Z}/\ell\mathbb{Z} \oplus \mathbb{Z}/\ell\mathbb{Z} \;\simeq\; \mathbb{F}_\ell^2.$$

This induces a group homomorphism

$$\rho_{E,\ell} : \mathrm{Gal}(K/\mathbb{Q}) \to \mathrm{Aut}(E[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$$

that maps each field automorphism $\sigma \in \mathrm{Gal}(K/\mathbb{Q})$ to an element of $\mathrm{GL}_2(\mathbb{F}_\ell)$ that we may view as an invertible 2×2 matrix with coefficients in $\mathbb{F}_\ell$, once we have fixed a choice of basis for $E[\ell] \simeq \mathbb{F}_\ell^2$.

As you may recall, a homomorphism from a group G to a group of linear transformations is called a (linear) *representation* of G. The map $\rho_{E,\ell}$ is a representation of the group $\mathrm{Gal}(K/\mathbb{Q})$, known as the *mod-$\ell$ Galois representation* attached to E.[1]

For each prime $p \neq \ell$ where E has good reduction there is a corresponding *Frobenius element* $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$. To construct Frob_p one picks a prime ideal $\mathfrak{p}$ of the ring of integers $\mathcal{O}_K$ (the integral closure of $\mathbb{Z}$ in K) that divides the ideal $p\mathcal{O}_K$, and then considers the *decomposition subgroup* $D_\mathfrak{p} := \{\sigma \in \mathrm{Gal}(K/\mathbb{Q}) : \sigma(\mathfrak{p}) = \mathfrak{p}\}$. Our conditions on p ensure that $D_\mathfrak{p}$ is naturally isomorphic to $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$, where $\mathbb{F}_\mathfrak{p} := \mathcal{O}_K/\mathfrak{p}$ is the *residue field* of $\mathfrak{p}$, which necessarily contains $\mathbb{F}_p$ as a subfield (because $\mathfrak{p}$ contains $p\mathcal{O}_K$); the isomorphism is given by restricting $\sigma \in D_\mathfrak{p}$ to $\mathcal{O}_K$ and reducing modulo $\mathfrak{p}$ to obtain an automorphism of $\mathcal{O}_K/\mathfrak{p} = \mathbb{F}_\mathfrak{p}$. The Galois group $\mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$ is cyclic, generated by the Frobenius automorphism $\pi\colon x \mapsto x^p$, and we take Frob_p to be the inverse image of π under the natural isomorphism $D_\mathfrak{p} \xrightarrow{\sim} \mathrm{Gal}(\mathbb{F}_\mathfrak{p}/\mathbb{F}_p)$. Now Frob_p depends on our choice of the prime ideal $\mathfrak{p}$ dividing $p\mathcal{O}_K$, but different choices lead to conjugate elements, and since the representation $\rho_{E,\ell}\colon \mathrm{Gal}(K/\mathbb{Q}) \simeq \mathrm{GL}_2(\mathbb{F}_\ell)$ is only determined up to conjugacy in any case (it depends on a choice of basis for $E[\ell]$), this ambiguity will not concern us.

The property of Frob_p that is relevant to us here is that we can make the identification

$$\rho_{E,\ell}(\mathrm{Frob}_p) = \pi_\ell \in \mathrm{End}(E_p[\ell]) \simeq \mathrm{GL}_2(\mathbb{F}_\ell).$$

Here $E_p/\mathbb{F}_p$ is the reduction of the elliptic curve $E/\mathbb{Q}$ modulo p obtained by reducing the coefficients of an integral equation $y^2 = x^3 + Ax + B$ for $E/\mathbb{Q}$ modulo p, and $\pi_\ell \in \mathrm{End}(E_p[\ell])$ is the restriction of the Frobenius endomorphism π_{E_p} to the ℓ-torsion subgroup $E_p[\ell]$. Both sides of the equality above are determined only up to conjugacy (each depends on a choice of basis), so there is no harm in making this identification, provided that we keep this in mind. The key point is that the conjugacy class of $\rho_{E,\ell}(\mathrm{Frob}_p) = \pi_\ell \in \mathrm{GL}_2(\mathbb{F}_\ell)$ is uniquely determined. In particular, we have

$$\mathrm{tr}\,\rho_{E,\ell}(\mathrm{Frob}_p) \equiv \mathrm{tr}\,\pi_{E_p} \bmod \ell \qquad \text{and} \qquad \det \rho_{E,\ell}(\mathrm{Frob}_p) \equiv p \bmod \ell.$$

(recall that we have assumed $p \neq \ell$).

[1] One can replace the ℓ-torsion field $K = \mathbb{Q}(E[\ell])$ with any algebraic extension of K, including an algebraic closure of $\mathbb{Q}$, but the representation is still determined by its restriction to K.

The Chebotarev density theorem implies that for any conjugacy class C of $\mathrm{Gal}(K/\mathbb{Q})$, the proportion of primes p (over $p \leq B$ as $B \to \infty$) for which Frob_p lies in C is exactly $\#C/\#\mathrm{Gal}(K/\mathbb{Q})$ Asymptotically, we can think of each prime p as being assigned a uniformly random Frobenius element $\mathrm{Frob}_p \in \mathrm{Gal}(K/\mathbb{Q})$ which is mapped by $\rho_{E,\ell}$ to a uniformly random element of the image of $\rho_{E,\ell}$ in $\mathrm{GL}_2(\mathbb{F}_\ell)$. For a typical elliptic curve $E/\mathbb{Q}$, the representation $\rho_{E,\ell}$ is surjective and its image is all of $\mathrm{GL}_2(\mathbb{F}_\ell)$, but this is not always the case. Number theorists (and others) are very interested in understanding these exceptional cases. The image of $\rho_{E,\ell}$ has a direct impact on the statistical behavior of $E_p[\ell]$ as p varies. For instance, the proportion of primes p for which $E_p[\ell] = E_p(\mathbb{F}_p)[\ell]$ is precisely $1/\#\operatorname{im}\rho_E$, since this occurs if and only if $\rho_E(\mathrm{Frob}_p) = \pi_\ell$ is the identity.

In this problem you will attempt to determine the image of $\rho_{E,\ell}$ for various elliptic curves $E/\mathbb{Q}$ by analyzing the statistics of π_ℓ as $p \neq \ell$ varies over primes of good reduction, by comparing these statistics to the corresponding statistics for various candidate subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$.

(a) Prove that for $\ell = 2$ the image of $\rho_{E,2}$ in $\mathrm{GL}_2(\mathbb{F}_2)$ is isomorphic to the Galois group of the splitting field of the cubic $f(x) := x^3 + Ax + B$. Conclude that (up to conjugacy) every possible subgroup of $\mathrm{GL}_2(\mathbb{F}_2)$ arises as the image of $\rho_{E,2}$ for some elliptic curve $E/\mathbb{Q}$ and give an explicit example of each case.

For $\ell > 2$, not every subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$ can arise as the image of $\rho_{E,\ell}$.

(b) Show that there exists a set of primes p of good reduction for E whose reductions modulo ℓ generates $(\mathbb{Z}/\ell\mathbb{Z})^\times$ (you don't need Dirichlet's theorem on primes in arithmetic progressions or the Chebotarev density theorem to do this). Conclude that the image of $\rho_{E,\ell}$ must contain elements of every possible determinant (all of $\mathbb{F}_\ell^\times$).

For $\ell = 3$ there are, up to conjugacy, 8 candidate subgroups G of $\mathrm{GL}_2(\mathbb{F}_3)$ for the image of $\rho_{E,3}$. These are listed in Table 1, and can also be found in this Sage worksheet.

group	order	description	generators
C_2	2	cyclic	$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}$
D_2	4	dihedral	$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 0 \\ 0 & 2 \end{pmatrix}$
$D_3 = S_3$	6	dihedral	$\begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix}, \begin{pmatrix} 1 & 0 \\ 1 & 2 \end{pmatrix}$
C_8	8	cyclic	$\begin{pmatrix} 1 & 1 \\ 1 & 0 \end{pmatrix}$
D_4	8	dihedral	$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 2 \\ 1 & 0 \end{pmatrix}$
D_6	12	dihedral	$\begin{pmatrix} 1 & 2 \\ 1 & 0 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
Q_{16}	16	semi-dihedral	$\begin{pmatrix} 1 & 1 \\ 2 & 1 \end{pmatrix}, \begin{pmatrix} 0 & 1 \\ 1 & 0 \end{pmatrix}$
$\mathrm{GL}_2(\mathbb{F}_3)$	48	general linear	$\begin{pmatrix} 2 & 0 \\ 0 & 1 \end{pmatrix}, \begin{pmatrix} 2 & 1 \\ 2 & 0 \end{pmatrix}$

Table 1. Candidates for the image of $\rho_{E,3}$ in $\mathrm{GL}_2(\mathbb{F}_3)$.

(c) The determinant $\det A$, trace $\operatorname{tr} A$, and multiplicative order $|A|$ of a matrix A in $\mathrm{GL}_2(\mathbb{F}_\ell)$ are invariant under conjugation. Prove that the pair $(\det A, \operatorname{tr} A)$ does not determine the conjugacy class of A in $\mathrm{GL}_2(\mathbb{F}_3)$, but the triple $(\det A, \operatorname{tr} A, |A|)$ does.

Part (c) implies that we can get more information about π_ℓ if, in addition to computing its trace, we also compute its multiplicative order in the ring $\operatorname{End}(E_p[\ell])$.

(d) Devise and prove a criterion for computing the order of π_2 in $\mathrm{GL}_2(\mathbb{F}_2)$ based on the number of roots the cubic $f(x)$ has in $\mathbb{F}_p$, where $y^2 = f(x)$ is the Weierstrass equation for E.

(e) Modify the function `trace_mod` that was used in our implementation of Schoof's algorithm in Lecture 9 (which can be found in this Sage workhseet) so that it also computes the order of π_ℓ and returns both the trace t_ℓ and the order $|\pi_\ell|$ of π_ℓ.

Important: The order of π_ℓ must be computed modulo the full division polynomial ψ_ℓ, not modulo one of its factors. So compute $|\pi_\ell|$ before computing q_ℓ, which is the first place where a division-by-zero error could occur, causing h to be replaced by a proper factor. Also, be sure to compute $|\pi_\ell|$ only the first time through the loop when you know that $h = \psi_\ell$, don't accidentally recompute it if the loop repeats.

Now address the first part of (c) in a different way: pick an elliptic curve $E/\mathbb{Q}$ and find two primes p and p' for which $\pi_3 \in \operatorname{End}(E_p[3])$ and $\pi_3' \in \operatorname{End}(E_{p'}[3])$ have the same characteristic polynomial but different orders in $\mathrm{GL}_2(\mathbb{F}_3)$.

(f) Write a program that, given an elliptic curve E, a prime ℓ, and an upper bound N, enumerates the primes $p \le N$ distinct from ℓ for which E has good reduction, and for each E_p, computes the triple $(\det \pi_\ell, \operatorname{tr} \pi_\ell, |\pi_\ell|)$. You can use `prime_range(N+1)` to efficiently enumerate primes $p \le N$. Keep a count of how often each distinct triple occurs (use a dictionary, as in the `group_stats` function in this Sage worksheet). Normalize the counts by dividing by the number of primes p you used, yielding a ratio for each triple.

For $\ell = 3$, use your program to provisionally determine the image of $\rho_{E,3}$ for each of the ten elliptic curves below, by comparing the statistics computed by your program with the corresponding statistics for each of the 8 candidate subgroups of $\mathrm{GL}_2(\mathbb{F}_3)$. With N around 5000 or 10000 you should be able to easily distinguish among the possibilities. The curves below are also listed in this Sage worksheet.

$y^2 = x^3 + x$

$y^2 = x^3 + 432$

$y^2 = x^3 + 21x + 26$

$y^2 = x^3 - 3915x + 113670$

$y^2 = x^3 + 5805x - 285714$

$y^2 = x^3 + 1$

$y^2 = x^3 + x + 1$

$y^2 = x^3 - 112x + 784$

$y^2 = x^3 + 4752x + 127872$

$y^2 = x^3 + 652509x - 621544482$

(g) Note that if a given triple $(\det \pi_3, \operatorname{tr} \pi_3, |\pi_3|)$ occurs for some E_p but does not occur in a candidate subgroup $G \subset \mathrm{GL}(\mathbb{F}_3)$, you can immediately rule out G as a possibility for the image of $\rho_{E,3}$. Analyze the 8 candidate subgroups in Table 1 to find a pair of triples that arise in $\mathrm{GL}_2(\mathbb{F}_3)$ but do not both arise in any of its proper subgroups. If for a given curve $E/\mathbb{Q}$ you can find both of these triples for some E_{p_1} and E_{p_2}, then you have unconditionally *proved* that $\rho_{E,3}$ is surjective.

Use this to devise an algorithm that attempts to prove $\rho_{E,3}$ is surjective. Your algorithm should return `true` as soon as it can determine $\operatorname{im}\rho_{E,3} = \mathrm{GL}_2(\mathbb{F}_3)$ (this should happen quite quickly, if it is true). If this fails to happen after computing triples for E_p for every prime up to, say, 10000, then your algorithm should give up and return `false`. You can think of this as a Monte Carlo algorithm with one-sided error: the "randomness" comes from the assumption that the Frobenius elements Frob_p is uniformly and independently distributed over $\mathrm{Gal}(K/\mathbb{Q})$ as p varies. If your program returns `true`, then $\rho_{E,3}$ is definitely surjective; if it returns `false` it is almost certainly not surjective, but there is a small probability of error. Give an upper bound on the probability of error under the assumption that Frobenius elements are independent and uniformly distributed.

(h) Using `ZZ.random_element(-100,100)`, generate random elliptic curves $E/\mathbb{Q}$ of the form $y^2 = x^3 + Ax + B$, with A and B uniformly distributed over the interval $[-100, 100]$. Excluding cases where $AB(4A^3 + 27B^2) = 0$, use your program to test whether the mod-3 Galois representation $\rho_{E,3}$ is surjective or not. List five curves for which your program returns `false`, and provisionally identify the image of $\rho_{E,3}$ in each such case as in part 3 above (you may need to test a few thousand curves to achieve this).

Problem 3. ECPP (70 points)

Let us define an *elliptic curve primality proof* (ECPP) for p as a sequence of *certificates* $C_1, C_2, \dots, C_k$, where each certificate C_i is of the form $(p_i, A_i, B_i, x_i, y_i, p_{i+1})$ with $p_1 = p$ and $p_{k+1} < (\log p)^4$. In each certificate C_i, the primes p_i and p_{i+1} satisfy

$$(\sqrt[4]{p_i} + 1)^2 < p_{i+1} < (\sqrt{p_i} + 1)^2/2, \tag{1}$$

and $P_i = (x_i, y_i)$ is a point of order p_{i+1} on $E_i \colon y^2 = x^3 + A_i x + B_i$ over $\mathbb{F}_{p_i}$.

(a) Let p be the least prime greater than $2^{128} \cdot N + 3^{64}$, where N is the first four digits of your student ID (use the `next_prime` function in Sage to compute p). Construct a short elliptic curve primality proof for p; this means each prime p_{i+1} should be close to the lower bound in (1) (you should not need more than 6 or 7 certificates). Note: the Goldwasser-Kilian algorithm typically will **not** produce a proof this short, it will have p_{i+1} closer to the upper bound in (1), so you will need to do something slightly different.

(b) Give an algorithm for verifying an elliptic curve primality proof and analyze its complexity. Express your answer solely in terms of $n = \log p$ and assume the worst-case (so the proof might not be as short as the one you generated in (a)).

(c) Analyze the asymptotic complexity of constructing an elliptic curve primality proof using the Goldwasser-Kilian algorithm given in class, under the heuristic assumption that the orders of random elliptic curves over $\mathbb{F}_p$ have factorizations comparable to random integers in the interval $[p, 2p]$. Assume that trial division and the Miller-Rabin test are used for attempted factorizations. Use an $O(n^5 \log\log n)$ complexity bound for point-counting via Schoof's algorithm.

(d) Now suppose that you want to construct an elliptic curve primality proof that can always be verified in $O(n\mathsf{M}(n))$ time, where $n = \log p$. Under the heuristic assumption above, give a probabilistic algorithm for constructing such a proof whose expected running time is bounded by $L_p[\alpha, c]$, using the smallest value of α that you can (hint: you can make $\alpha < 1/2$). Your answer should include a high-level description of the algorithm and a (heuristically proven) bound on its complexity.

Problem 4. Pomerance proofs (70 points)

A *Pomerance proof* is a special form of an elliptic curve primality proof that involves just a single certificate (p, A, x_0, k) and uses a Montgomery curve $By^2 = x^3 + Ax^2 + x$ over $\mathbb{F}_p$ on which there is a point (x_0, y_0) of point of order $2^k > (\sqrt[4]{p} + 1)^2 \geq 2^{k-1}$. Note that neither the y-coordinate nor B is needed to verify the certificate (no matter what $x_0^3 + Ax_0^2 + x_0$ is, there exists a nonzero B and a y_0 that will work and the verifier does not need to know what they are), but the verifier should check that $\gcd(A^2 - 4, p) = 1$ to ensure that the curve is not singular.

Every prime p has a Pomerance proof, but for a general prime p no efficient algorithm is known for finding one. In this problem you will develop a very efficient algorithm to construct a Pomerance proof for primes of a special form.

Let us first convince ourselves that every sufficiently large prime has a Pomerance proof. To do this we note the following theorem, which we will prove later in the course.

Theorem 1. *Let p be a prime. For every integer N in the Hasse interval*

$$\mathcal{H}(p) = [p + 1 - 2\sqrt{p},\ p + 1 + 2\sqrt{p}]$$

there exists an elliptic curve $E/\mathbb{F}_p$ for which $E(\mathbb{F}_p)$ is a cyclic group of order N.

(a) Using the theorem above, prove that every prime $p > 31$ has a Pomerance proof.

Now let E be the elliptic curve $y^2 = x^3 + 8$ over $\mathbb{F}_p$.

(b) Using the formula $\#E(\mathbb{F}_p) = p + 1 + \sum_{x \in \mathbb{F}_p} \left(\frac{x^3+8}{p}\right)$, prove that for every odd prime $p \equiv 2 \bmod 3$ we have $\#E(\mathbb{F}_p) = p + 1$.

(c) Prove that for any prime $p \equiv 11 \bmod 12$ the curve $E/\mathbb{F}_p$ can be put in Montgomery form $By^2 = x^3 + Ax^2 + x$. Give a deterministic algorithm that computes A and B in time $O(n\mathsf{M}(n))$, where $n = \log p$.

(d) Give a probabilistic algorithm to construct a Pomerance proof for primes of the form $p = 3 \cdot 2^m c - 1$, where c is odd and $2^m > (\sqrt[4]{p} + 1)^2$, and analyze its complexity. Be sure to address the fact that the algorithm you gave in part (c) assumes that p is prime, but now it must also handle composite values of p.

(e) Implement your algorithm and use it to construct a Pomerance proof for a prime of the form $p = 2^k \cdot 3^m - 1$ that is greater than 2^{1000}. Be sure to format you answer so that all of the digits in the certificate you construct fit on the page. To speed things up, you may wish to do some trial division by small primes to eliminate obviously composite values of p before attempting to construct a primality proof.

(f) As noted above, no efficient algorithm is known for constructing a Pomerance proof. On the other hand, there certainly *is* an algorithm; for example, one could simply enumerate all the possible certificates (clearly a finite set) and attempt to verify them. But you can certainly do better than this. Give the most efficient algorithm you can come up with for constructing a Pomerance proof for a given prime $p > 31$ and bound its complexity. Your algorithm need not be deterministic, and you should feel free to assume any heuristics you believe are reasonable.

Problem 5. Survey

Complete the following survey by rating each of the problems you attempted on a scale of 1 to 10 according to how interesting you found the problem (1 = "mind-numbing," 10 = "mind-blowing"), and how hard 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			

Also, please rate each of the following lectures that you attended, according to the quality of the material (1="useless", 10="fascinating"), the quality of the presentation (1="epic fail", 10="perfection"), the pace (1="way too slow", 10="way too fast", 5="just right") and the novelty of the material (1="old hat", 10="all new").

Date	Lecture Topic	Material	Presentation	Pace	Novelty
3/20	Elliptic curve primality proving				
3/22	Endomorphism algebras				

Please feel free to record any additional comments you have on the problem sets or lectures, in particular, ways in which they might be improved.

18.783 Elliptic Curves
Spring 2017