18.783 Elliptic Curves **Spring 2015**

Problem Set #13 **Due: 05/14/2015**

Description

These problems are related to the material covered in Lectures 23 and 25. As usual, the first person to spot each non-trivial typo/error will receive 1–3 points of extra credit (this is an all new problem set for this year, so there are sure to be some typos in it).

Instructions: As this is the last week of class this problem set is shorter than usual and only worth 50 points. You are only required to solve **one** of the following five problems. However, those who wish to do more have the following options:

1. Solve **two** problems and have this problem set weighted 100 points and your second worst problem set score divided in half and weighted out of 50 points.
2. Solve **three** problems and your best score will be counted for this problem set and the sum of your other two problem scores will replace your score on your second worst problem set (but only if that helps you).
3. For the truly ambitious, solve all **five** problems and your best score will counted for this problem set, and your other four scores will be used to replace your scores on your second and third worst problem sets (but only to the extent that it helps).

No matter which option you choose, your worst problem set score will be dropped.

Problem 1. Pairing attack on the discrete logarithm problem (50 points)

In the early days of elliptic curve cryptography supersingular curves were initially considered ideal candidates for discrete logarithm based cryptography (using a prime order subgroup of the rational points) because for these curves it is easy to determine the group order ($p+1$ over prime fields for $p > 3$) and there are special techniques to speed up scalar multiplication. However, supersingular curves were quickly ruled out once it was discovered by Menezes, Okamato, and Vanstone [2] that one can use the Weil pairing to reduce the computation of a discrete logarithm in an order N subgroup of $E(\mathbb{F}_q)$ to the computation of a discrete logarithm in a finite field $\mathbb{F}_{q^r}$ that contains the group $\mu_N \subseteq \overline{\mathbb{F}}_q$ of Nth roots of unity. As we saw in Lecture 11, there are subexponential-time algorithms to solve the discrete logarithm problem in a finite field, whereas no such algorithm is known for the discrete logarithm problem on an elliptic curve. In general r will be very large (exponential in $\log q$) and this reduction does not make the problem of computing discrete logarithms in $E(\mathbb{F}_q)$ any easier. But for supersingular curves this is not the case.

Let $p > 3$ be a prime, let $E/\mathbb{F}_p$ be a supersingular curve, let $N > \sqrt{p}$ be a prime dividing $p+1$, and let μ_N denote the multiplicative group of Nth roots of unity in $\overline{\mathbb{F}}_p$.

(a) Prove that $\mu_N \subseteq \mathbb{F}_{p^2}^\times$.

(b) Prove that $\#E(\mathbb{F}_{p^2}) = (p+1)^2$ and $E[N] \subseteq E(\mathbb{F}_{p^2})$.

Let $P \in E(\mathbb{F}_p)$ be a point of order N, and let $Q \in \langle P \rangle$. Consider the following algorithm Las Vegas algorithm to compute $\log_P Q$:

1. Generate a random point $R \in E(\mathbb{F}_{p^2})$ and compute $S = mR$, where $m = (p+1)/N$.
2. Compute $a = e_N(S, P)$, and if $a = 1$ then return to step 1.
3. Compute $b = e_N(S, Q)$.
4. Compute $\log_a b$ in $\mathbb{F}_{p^2}^\times$ and output the result.

(c) Prove that the expected number of times the algorithm executes step 1 is $1 + o(1)$.

(d) Prove that the algorithm correctly outputs $\log_P Q$.

The expected running time the algorithm is thus completely dominated by the time to compute $\log_a b$ in $\mathbb{F}_{p^2}^\times$, which can heuristically be accomplished in $L[1/3, c]$ time.

Let $N = 10^{14} + 2367$ (which is prime), let $p = 2N - 1$ (also prime), and let $E/\mathbb{F}_p$ be the elliptic curve $y^2 = x^3 - 35x - 98$ (which is supersingular). Viewing $\mathbb{F}_q$ as integers in $[0, q-1]$, choose $P_0 \in E(\mathbb{F}_q)$ so that $x(P_0)$ is the least integer greater than your student ID and $y(P_0)$ is minimal, and let $P = 2P_0$. Then choose $Q_0 \in E(\mathbb{F}_q)$ so that $x(Q_0)$ is the least integer greater than twice your student ID and $y(Q_0)$ is minimal, and let $Q = 2Q_0$. Then both P and Q lie in $E[N]$ and we can apply the above algorithm to compute $\log_P Q$, with $m = 2$. Here are a few tips to help you do this:

- To create the field $\mathbb{F}_{p^2}$ in Sage use `F2 = GF(p**2,'z')`.
- To generate R use `E.change_ring(F2).random_element()`.
- To compute $e_N(S, P)$ use `S.weil_pairing(P.change_ring(F2),N)`.
- To compute $\log_a b$ use `b.log(a)`.

(e) Compute $\log_P Q$. In your answer list the points P_0, P, Q_0, Q, the values of a and b, the integer $n = \log_a b$, and the running time of your algorithm (which should be well under a minute). Be sure to check your answer by verifying that $nP = Q$.

Remark. You should not be particularly impressed by this running time, since you can easily beat it with a careful implementation of the baby-steps giant-steps or Pollard rho algorithms. But for larger values of p and N this algorithm will easily outperform any generic method. Unfortunately Sage does not have a particularly fast implementation for computing discrete logarithms in non-prime finite fields, so I intentionally chose a small example.

Problem 2. A fast Las Vegas algorithm to compute $E(\mathbb{F}_p)$ (50 points)

Problem 3 of Problem Set 5 gave a Las Vegas algorithm to compute the structure of the group $E(\mathbb{F}_p) \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, but its running time was $\exp(\frac{1}{4}\log p + o(1))$, exponential in $\log p$. In this problem, following Miller [3], you will develop a much faster algorithm to compute $E(\mathbb{F}_p)$. Strictly speaking it is not polynomial-time because it requires the factoring the integer $d = \gcd(\#E(\mathbb{F}_p), p - 1)$, but typically d will either be small (in which case the problem is easy), or it will have only one large prime factor ℓ, in which case factoring d is easy but computing the structure of $E(\mathbb{F}_p)$ with the algorithm from Problem Set 5 will be very difficult if ℓ^2 divides $\#E(\mathbb{F}_p)$. In any case, this does give a subexponential-time Las Vegas algorithm, since we can always factor d in subexponential time using a Las Vegas algorithm (the best proven bound is $L[1/2, c]$, but heuristically this can be done in time $L[1/3, c]$).

(a) Let ℓ be a prime. Prove that if $E[\ell] \subseteq E(\mathbb{F}_p)$ then $\ell | (p-1)$ and $\ell^2 | \#E(\mathbb{F}_p)$.

Let $N = \#E(\mathbb{F}_p)$ and write N as $N = N_0 N_1$, where N_0 and N_1 are relatively prime and N_1 is divisible only by primes ℓ that divide $p-1$ and whose square divides N. By part (a), when computing the structure of $E(\mathbb{F}_p)$, we can restrict our attention to $E(\mathbb{F}_p)[N_1]$. Consider the following algorithm to compute the structure of $E(\mathbb{F}_p)$, which takes as input the elliptic curve $E/\mathbb{F}_p$, the integers N_0 and N_1, and the prime factorizations of N_1.

1. Generate random points $P_0, Q_0 \in E(\mathbb{F}_p)$ and put $P := N_0 P_0$ and $Q := N_0 Q_0$.
2. Using the prime factorization of N_1, compute $s := |P|$ and $t := |Q|$.
3. Let $r = \operatorname{lcm}(s,t)$ and compute $\zeta := e_r(P,Q)$.
4. Using the prime factorization of N_1, compute $n := |\zeta|$.
5. If $rn = N_1$ then put $m = rN_0$ and output $\mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$, otherwise go to step 1.

(c) Prove that when the algorithm terminates we have $E(\mathbb{F}_p) \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$.

(d) Prove that in step 3 we have $\zeta \in \mathbb{F}_p^\times$.

(e) Prove that the expected number of times the algorithm returns to step 1 is $O(1)$.

(f) Let $g \in G$ be an element of a generic group with exponent λ (so $\lambda g = 0$). Prove that, given the prime factorization of λ you can compute the order of g using $(\log \lambda)^{1+o(1)}$ group operations. (You may wish to review Lecture 10 on generic algorithms).

(g) Prove that the running time of the algorithm above is $(\log p)^{2+o(1)}$.

Remark. As noted above, this only gives a subexponential-time algorithm to compute $E(\mathbb{F}_p)$ if we are not given the factorization of N_1. But it is known that we can do this in *average polynomial time* [1], in the following sense: for any prime p, if we pick a random $A, B \in \mathbb{F}_p$ the expected time to compute $E(\mathbb{F}_p) \simeq \mathbb{Z}/m\mathbb{Z} \oplus \mathbb{Z}/n\mathbb{Z}$ for the curve $E\colon y^2 = x^2 + Ax + B$ is polynomial in $\log p$.

Problem 3. The Birch and Swinnerton-Dyer Conjecture (50 points)

The goal for this problem is to lead you to a formulation of the (weak) Birch and Swinnerton-Dyer conjecture. The main difficulty here is not for you to prove a precisely stated question, but rather for you to formulate a precise question, starting from some data and some general suggestions. This means that parts of the problem are deliberately vague; making the questions more precise is part of the problem. Other than part **(a)**, you are not expected to prove anything; heuristic arguments are fine.

One of the outstanding Millennium Prize Problems is the famous conjecture of Birch and Swinnerton-Dyer, which concerns the ranks of elliptic curves over $\mathbb{Q}$. Recall from Lecture 1 that the Mordell-Weil theorem implies

$$E(\mathbb{Q}) = E(\mathbb{Q})_{\text{tors}} \oplus \mathbb{Z}^r.$$

As opposed to the torsion subgroup, the rank r of the Mordell-Weil group $E(\mathbb{Q})$ is far less understood; we do not have a fully general algorithm to compute r, and mathematicians do not even agree on whether r should be bounded or not (so not only can't we prove a conjecture, we don't even know what the right conjecture is!). However, in the 1960s, Birch and Swinnerton-Dyer carried out computations on the EDSAC computer at Cambridge University that led them to conjecture a deep relationship between the L-series of E and the rank r of the Mordell-Weil group. In this problem you will develop a conjecture and investigate the evidence for it.

Recall from Lecture 25 that the L-series of $E/\mathbb{Q}$ is defined by

$$L_E(s) = \prod_p L_p(p^{-s})^{-1} = \prod_p (1 - a_p p^{-s} + \chi(p) p^{-2s+1})^{-1},$$

where the Dirichlet character $\chi(p) = 0$ if E has bad reduction at p and 1 otherwise.[1] This converges for $\Re(s) > 3/2$; however by the modularity theorem, it admits an analytic continuation to the entire complex plane.

(a) Assume that E is given in affine coordinates by the equation $y^2 = x^3 + Ax + B$ with $A, B \in \mathbb{Z}$.[2] A rational point $(x_0 : y_0 : z_0) \in E(\mathbb{Q})$ gives a solution to

$$y^2 z \equiv x^3 + Axz^2 + Bz^3 \pmod{p^n},$$

and hence a point on E mod p^n for almost every p. Let N_{p^n} denote the number of solutions to this congruence mod p^n. Using Hensel's lemma (see problem 1 of Problem Set 3) prove that

$$N_{p^n} = p^{n-1} N_p$$

for all $p \nmid \Delta(E)$. Conclude that

$$\lim_{n\to\infty} \frac{N_{p^n}}{p^n} = \frac{N_p}{p},$$

except for finitely many p. This quantity $\lim_{n\to\infty} \frac{N_{p^n}}{p^n}$ represents the density of p-adic points on E. Give a plausible relation with r.

(b) Let S be the set of primes of bad reduction of E. Define

$$f_E(X) = \prod_{\substack{p \notin S \\ p \le X}} \frac{N_p}{p},$$

What is the relationship between $f_E(X)$ and $L_E(s)$?

(c) Consider the elliptic curve[3] E with rank 3 given by

$$y^2 = x^3 - 82x.$$

Compute and plot the values of

$$f_E(X) = \prod_{\substack{p \notin S \\ p \le X}} \frac{N_p}{p}$$

[1] Recall that this assumes a minimal Weierstrass model for E.

[2] This need not be a minimal Weierstrass model, but you may assume it is if you wish.

[3] In 1938, this was the highest rank known, due to Billings.

for X up to at least 10^6 (or further if you like). What appears to be the asymptotic growth of this function? Make a plot of your results with an appropriate choice of scale on the coordinate axes so your answer is apparent. Attach relevant plots in your solutions.

(d) Repeat part **(c)** for the following curves of the form

$$E_i : y^2 = x^3 - d_i^2 x,$$

for the values:

	d_i	rank
E_1	1	0
E_2	5	1
E_3	34	2
E_4	1254	3
E_5	29274	4

Display your final plots (with the appropriate scaling of the axes) together.

(e) Combining your results from parts **(b)**, **(c)**, and **(d)** above, make a precise conjecture on the relationship between $L_E(s)$ and the rank of E. Your conjecture should be precise enough that different ranks give rise to different behaviors of the L-function. (Hint: You might need to do more work in **(b)** in order to give a more precise relationship – there is a natural interplay between conjecture and computation.)

(f) Choose 5 random elliptic curves with $|A|, |B| < 100$ and conjecturally assign their ranks. Note: you can use Sage to check your answer, but you must provide evidence based upon your work in previous parts to receive full credit.[4]

Problem 4. Classifying subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ (50 points)

Let E be an elliptic curve defined over $\mathbb{Q}$. Recall that for each integer $n > 1$, the n-torsion of $E(\overline{\mathbb{Q}})$ is a rank 2 $(\mathbb{Z}/n\mathbb{Z})$-module we denote by $E[n]$. As explained in Problem Set 5, the action of the absolute Galois group $G_{\mathbb{Q}} := \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q})$ on the coordinates of points gives rise to an action on the set $E(\overline{\mathbb{Q}})$ that commutes with the group law. Hence the action of $G_{\mathbb{Q}}$ preserves $E[n]$ and gives rise to a linear representation of the absolute Galois group

$$\rho_{E,n} \colon G_{\mathbb{Q}} \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}_2(\mathbb{Z}/n\mathbb{Z}),$$

which we call the *mod-n Galois representation* attached to E. In this problem an the next we are concerned only with the case that $n = \ell$ is prime.

In this case, a foundational result in the subject of Galois representations of elliptic curves is the following theorem of Serre:

Theorem (Serre, 1972)**.** *Let E be an elliptic curve over $\mathbb{Q}$ which does not have CM. Then for all but finitely many primes ℓ, the image of the mod-ℓ Galois representation is surjective:*

$$\rho_{E,\ell}(G_{\mathbb{Q}}) = \mathrm{GL}_2(\mathbb{F}_\ell).$$

[4] While we do not have a general algorithm to compute the rank of $E/\mathbb{Q}$, for small $|A|$ and $|B|$, Sage can easily do so.

Remark. It is conjectured that for all $E/\mathbb{Q}$ without CM we have $\rho_{E,\ell} = \mathrm{GL}_2(\mathbb{F}_\ell)$ for all $\ell > 37$. There has been some recent progress in proving this, but it remains a major open problem.

A key component of the proof of this theorem is understanding the maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ In order to discuss subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ in a basis-free manner, it is often convenient to write $\mathrm{GL}(V)$ where V is a 2-dimensional vector space over $\mathbb{F}_\ell$ and $\mathrm{GL}(V)$ denotes its group of automorphisms. In this problem you will give a complete classification of the maximal subgroups of $\mathrm{GL}_2(V)$.

Let L_1 and L_2 be distinct 1-dimensional subspaces of V, which we can think of as lines through the origin in V, and let C_s be the subgroup of $\mathrm{GL}(V)$ that preserves both L_1 and L_2 (individually, no swapping allowed).

(a) Show that for $\ell \neq 2$, the subgroup C_s uniquely determines the lines $L_1, L_2 \subset \mathrm{GL}(V)$ (and hence is equivalent to specifying two such lines).

We call such a C a *split Cartan subgroup* of $\mathrm{GL}(V)$. If we choose a basis for V compatible with the decomposition $V = L_1 \oplus L_2$, we then have

$$C_s = \begin{pmatrix} * & 0 \\ 0 & * \end{pmatrix},$$

where $*$ indicates any element of $\mathbb{F}_\ell^\times$. From this we see that $C \simeq \left(\mathbb{F}_\ell^\times\right)^2$ is an abelian group of order $(\ell-1)^2$.

As an $\mathbb{F}_\ell$-vector space, $\mathbb{F}_{\ell^2} \simeq \mathbb{F}_\ell^2$; but $\mathbb{F}_{\ell^2}$ also has a multiplicative structure, and so the action of the multiplicative group $\mathbb{F}_{\ell^2}^\times$ on $\mathbb{F}_{\ell^2} \simeq V$ gives a cyclic subgroup C_{ns} of $\mathrm{GL}(V)$ isomorphic to $\mathbb{F}_{\ell^2}^\times$. Such a subgroup C_{ns} is called a *non-split Cartan subgroup.* We collectively refer to split and non-split Cartan subgroups as Cartan subgroups.

(b) Show that for $\ell \neq 2$, if we fix a quadratic non-residue $\epsilon \in \mathbb{F}_\ell^\times$, then in an appropriate basis we have

$$C_{ns} = \left\{ \begin{pmatrix} x & \epsilon y \\ y & x \end{pmatrix} : x, y \in \mathbb{F}_\ell, (x,y) \neq (0,0) \right\}.$$

(c) Show that the intersection of any two distinct Cartan subgroups (either split or non-split) is the group of scalar matrices $Z = \left(\begin{smallmatrix} z & 0 \\ 0 & z \end{smallmatrix}\right)$ with $z \in \mathbb{F}_\ell^\times$.

(d) Show that any element $s \in \mathrm{GL}(V)$ with $\Delta(s) = \mathrm{tr}(s)^2 - 4 \cdot \det(s) \neq 0$ is contained in a unique Cartan subgroup, and determine a condition involving $\Delta(s)$ that specifies the type of Cartan. Deduce that the union of all Cartan subgroups of $\mathrm{GL}(V)$ is the set of elements of order prime to ℓ. (If you are stuck, look at part **(h)** below.)

(e) Let N denote the normalizer of a Cartan subgroup C in $\mathrm{GL}(V)$, that is all elements $s \in \mathrm{GL}(V)$ such that $sCs^{-1} = C$. Show that $(N : C) = 2$ and give an explicit description of this group in the split and non-split cases separately.

It is easy to show that the group Z of scalar matrices forms the center of $\mathrm{GL}(V)$. We define $\mathrm{PGL}(V)$ to be the quotient of $\mathrm{GL}(V)$ by its center, so $\mathrm{PGL}(V) := \mathrm{GL}(V)/Z$. Let $\varphi\colon \mathrm{GL}(V) \to \mathrm{PGL}(V)$ denote the quotient map.

(f) Show that if C is a split (resp. non-split) Cartan subgroup, then $\varphi(C) \subset \mathrm{PGL}(V)$ is cyclic of order $\ell-1$ (resp. $\ell+1$). Show that the image in $\mathrm{PGL}(V)$ of a normalizer of a Cartan subgroup is a dihedral group.[5]

By part **(d)** above, it remains to understand the elements of $\mathrm{GL}(V)$ of order divisible by ℓ. A Borel subgroup B of $\mathrm{GL}(V)$ is the group of automorphisms of V fixing a specified line (through the origin). A Borel subgroup of $\mathrm{GL}(V)$ has order $\ell(\ell-1)^2$. After choosing an appropriate basis, this has the form

$$B = \begin{pmatrix} * & * \\ 0 & * \end{pmatrix}.$$

(g) Show that any element $s \in \mathrm{GL}(V)$ of order ℓ is conjugate to the matrix $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$.

(h) Using the fact that $\mathrm{SL}(V)$ is generated $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $\left(\begin{smallmatrix} 1 & 0 \\ 1 & 1 \end{smallmatrix}\right)$, deduce that any subgroup of $\mathrm{GL}(V)$ of order divisible by ℓ either lies in a Borel subgroup, or contains $\mathrm{SL}(V)$.

Let k be any field. If H is a finite subgroup of $\mathrm{PGL}_2(k)$ of order prime to the characteristic of k that is not cyclic or dihedral, then H is isomorphic to either A_4, S_4, or A_5. (In the case $k = \mathbb{C}$, this result is well known and these subgroups correspond to the symmetry groups of the regular polyhedra: tetrahedron, cube/octahedron, and icosahedron/dodecahedron, respectively.)

(i) Using the above result, prove the classification theorem below.

Theorem (Maximal subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$)**.** *Let G be a subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$; let H denote the image of G in $\mathrm{PGL}_2(\mathbb{F}_\ell)$. Then one of the following holds:*

1. *G has order prime to ℓ and either:*

   (i) H is cyclic and G is contained in a Cartan subgroup of $\mathrm{GL}_2(\mathbb{F}_\ell)$;

   (ii) H is dihedral and G is contained in the normalizer of a Cartan subgroup C of $\mathrm{GL}_2(\mathbb{F}_\ell)$ but not in C;

   (iii) H is isomorphic to A_4, S_4 or A_5 and we call G exceptional;

2. *G has order divisible by ℓ and either:*

   (iv) G is contained in a Borel subgroup;

   (v) G contains $\mathrm{SL}_2(\mathbb{F}_\ell)$.

Problem 5. Surjectivity of Mod-ℓ Galois Representations (50 points)

This is a continuation of Problem 4, but you don't need to solve Problem 4 in order to do this problem, you can assume the classification theorem and any other results stated or proved in Problem 4. Let ℓ be an odd prime and let V be a 2-dimensional $\mathbb{F}_\ell$-vector space, with automorphism group $\mathrm{GL}(V)$, as in the previous problem, and let $\varphi\colon \mathrm{GL}(V) \twoheadrightarrow \mathrm{PGL}(V)$ denote the quotient map.

[5] For this problem, the product of two cyclic groups of order 2 (the Klein group) is a dihedral group.

(a) Let s be an element of $\mathrm{GL}(V)$ whose order is not divisible by ℓ, let $u = \mathrm{tr}(s)^2/\det(s)$, and let r be the order of $\varphi(s)$ in $\mathrm{PGL}(V)$. Prove that $u = \zeta_r + \zeta_r^{-1} + 2$, for some primitive rth root of unity $\zeta_r \in \mathbb{F}_{\ell^2}^\times$.

(b) Suppose that we are in case (iii) of the classification theorem, in which G is a subgroup of $\mathrm{GL}(V)$ whose image in $\mathrm{PGL}(V)$ is isomorphic to A_4, S_4, or A_5. Prove that for all elements $s \in G$, $u = \mathrm{tr}(s)^2/\det(s)$ is equal to $4, 0, 1, 2$ or satisfies $u^2 - 3u + 1 = 0$.

Now we are ready to use this classification to deduce some results about surjectivity of the mod-ℓ Galois representation

$$\rho_{E,n}\colon G_{\mathbb{Q}} \to \mathrm{Aut}(E[n]) \simeq \mathrm{GL}(V),$$

of an elliptic curve $E/\mathbb{Q}$.

(c) Let $G = \rho_{E,\ell}(G_{\mathbb{Q}})$. Using the Weil pairing, prove that the determinant map $G \to \mathbb{F}_\ell^\times$ is surjective. Show that the image H of the G in $\mathrm{PGL}(V)$ contains a (normal) subgroup of index 2. Deduce that if $G \neq \mathrm{GL}_2(\mathbb{F}_\ell)$ then one of the following is true:

1. G is contained in the normalizer of a Cartan subgroup;
2. G is contained in a Borel subgroup;
3. G is exceptional and $H = S_4$.

Remark. As noted in Problem 4, it is a famous conjecture that for $\ell > 37$, the mod-ℓ Galois representation is surjective for $E/\mathbb{Q}$ without CM. This has been proven in all of these cases except for G contained in the normalizer of a non-split Cartan.

(d) Prove that any element of the normalizer of a Cartan subgroup that does not lie in the Cartan subgroup itself has trace 0.

(e) Again let $G = \rho_{E,\ell}(G_{\mathbb{Q}})$. Determine three types of elements (specified by their trace and determinant) such that if G contains these elements, then $G = \mathrm{GL}_2(\mathbb{F}_\ell)$.

(f) Let E be the elliptic curve

$$y^2 + y = x^3 - x^2,$$

which has good reduction outside 11. By considering the Frobenius elements $\pi_2 = \rho_{\ell,E}(\mathrm{Frob}_2)$ and $\pi_3 = \rho_{\ell,E}(\mathrm{Frob}_3)$, and using your criterion above, show that $\rho_{E,\ell}$ is surjective for all $\ell \geq 13$ satisfying $\left(\frac{11}{\ell}\right) = -1$.

Problem 6. Survey

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

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
5/7	The Weil pairing				
5/12	Modular forms				

Finally, if you have any comments about the course as a whole, in particular, things that you think would improve it in the future, please let me know!

References

[1] J.B. Friedlander, C. Pomerance, I.E. Shparlinski, *Finding the group structure of elliptic curves over finite fields*, Bulletin of the Australian Mathematical Society **72** (2005), 251–263.

[2] A.J. Menezes, T. Okamato, and S.A. Vanstone, *Reducing elliptic curve logarithms to logarithms in a finite field*, IEEE Transactions on Information Theory **39** (1993), 1639–1646.

[3] V.S. Miller, *The Weil pairing and its efficient calculation*, J. Cryptology **17** (2004), 235–261.