18.783 Elliptic Curves **Fall 2023**

Problem Set #9 **Due: 11/20/2023**

Description: These problems are related to the material covered in Lectures 15–17.

Instructions: Pick any combination of problems to solve that sums to 100 points. Your solutions are to be written up in latex and submitted as a pdf-file to Gradescope.

Collaboration is permitted/encouraged, but you must identify your collaborators or your group on pset partners, as well any references you consulted that are not listed in the syllabus or lecture notes. If there are none write "**Sources consulted: none**" at the top of your solutions. Note that each student is expected to write their own solutions; it is fine to discuss the problems with others, but your writing must be your own.

The first person to spot each non-trivial typo/error in the problem sets or lecture notes will receive 1-5 points of extra credit.

In cases where your solution involves writing code, please either include your code in your write up (as part of the pdf), or the name of a notebook in your 18.783 CoCalc project containing you code (please use a separate notebook for each problem).

Problem 1. Complex multiplication (49 points)

Let $\tau = (1+\sqrt{-7})/2$. In problem 1 of Problem Set 8 you computed $j(\tau) = -3375$. In problem 3 of Problem Set 7 you proved that the endomorphism ring of the elliptic curve $y^2 = x^3 - 35x - 98$ with j-invariant -3375 is equal to $[1,\tau]$, the maximal order (ring of integers) of $\mathbb{Q}(\sqrt{-7})$. Let us now set $g_2 := -4(-35) = 140$ and $g_3 := -4(-98) = 392$ and work with the isomorphic elliptic curve $E/\mathbb{C}$ defined by

$$y^2 = 4x^3 - g_2x - g_3,$$

which is isomorphic to $y^2 = x^3 - 35x - 98$.

We should note that $g_2([1,\tau])$ and $g_3([1,\tau])$ are not equal to 140 and 392, but there is a lattice L homothetic to $[1,\tau]$ for which $g_2(L) = 140$ and $g_3(L) = 392$ (you computed this lattice L in problem 2 of Problem Set 8). In particular, $\tau L \subseteq L$, thus τ satisfies condition (1) of Theorem 16.4. The goal of this problem is to compute the polynomials $u, v \in \mathbb{C}[x]$ for which condition (2) of Theorem 16.4 holds, and the endomorphism ϕ for which condition (3) of Theorem 16.4 holds, and to explicitly confirm that the diagram

$$\begin{array}{ccc} \mathbb{C}/L & \xrightarrow{\ \Phi\ } & E(\mathbb{C}) \\ \downarrow{\scriptstyle \tau} & & \downarrow{\scriptstyle \phi} \\ \mathbb{C}/L & \xrightarrow{\ \Phi\ } & E(\mathbb{C}) \end{array}$$

commutes, where τ denotes the multiplication-by-τ map $z \mapsto \tau z$.

Recall that the Weierstrass $\wp$-function satisfying the differential equation

$$\wp'(z)^2 = 4\wp(z)^3 - g_2\wp(z) - g_3 \tag{1}$$

has a Laurent series expansion about 0 of the form $\wp(z) = z^{-2} + \sum_{n=1}^{\infty} a_{2n}z^{2n}$.

(a) Use g_2 and g_3 to determine a_2 and a_4, and then determine a_6 by comparing coefficients in the Laurent expansions of both sides of (1).

We now wish to compute the polynomials $u, v \in \mathbb{C}[x]$ for which

$$\wp(\tau z) = \frac{u\big(\wp(z)\big)}{v\big(\wp(z)\big)},$$

as in condition (2) of Theorem 16.4. Following Corollary 16.5, we have $\mathrm{N}(\tau) = \tau\bar{\tau} = 2$, so $\deg u = 2$ and $\deg v = 1$. We can make $u = x^2 + ax + b$ monic, and with $v = cx + d$ we must have

$$(c\wp(z) + d)\wp(\tau z) = \wp(z)^2 + a\wp(z) + b \tag{2}$$

(b) Use (2) to determine the coefficients a, b, c, d, expressing your answers in terms of τ. It will be convenient to work in the subfield $K = \mathbb{Q}(\tau)$, rather than $\mathbb{C}$. To define the field K and the polynomial ring $K[x]$ in Sage, use

```
RQ.<w>=PolynomialRing(QQ)
K.<tau>=NumberField(w^2-w+2)
RK.<x>=PolynomialRing(K)
```

Once you have determined $a, b, c, d \in K$, you can verify $u, v \in K[x]$ via[1]

```
RL.<z>=LaurentSeriesRing(K,100)
wp=EllipticCurve([-35,-98]).weierstrass_p(100).change_ring(K)
assert wp(tau*z) == u(wp(z))/v(wp(z))
```

(c) Following the proof of Theorem 16.4, construct polynomials $s, t \in K[x]$ that satisfy

$$\wp'(\tau z) = \frac{s\big(\wp(z)\big)}{t\big(\wp(z)\big)}\wp'(z).$$

You can verify your results in Sage via

```
wpp = wp.derivative()
assert wpp(tau*z) == s(wp(z))/t(wp(z))*wpp(z)
```

(d) Now let $\phi = \big(\frac{u(x)}{v(x)}, \frac{s(x)}{t(x)}y\big)$. Use Sage to verify that ϕ is an endomorphism by checking that its coordinate functions satisfy the curve equation $y^2 = 4x^3 - g_2x - g_3$.

The symbolic verifications in parts (b) and (d) confirm that $\Phi(\tau z) = \phi(\Phi(z))$, showing that the diagram commutes (at least for the first 100 terms in the Laurent expansion of $\wp(z)$). But we would like to explicitly check this for some specific values of $z \in \mathbb{C}$. In order to do this in Sage, we need to redefine τ and the polynomials u, v, s, t over $\mathbb{C}$, rather than K. You can use the following Sage script to do this:

```
R.<X>=PolynomialRing(CC)
pi = K.embeddings(CC)[0]
tauC = pi(tau)
def coerce(f,pi,X):
    c = f.coefficients(sparse=False)
```

[1] Sage effectively computes $\wp(z)$ using $y^2 = 4x^3 - g_2x - g_3$ when we define $E\colon y^2 = x^3 + Ax + B$ with $g_2 = -4A$ and $g_3 = -4B$.

```
        return sum([pi(c[i])*X^i for i in range(len(c))])
    uC = coerce(u,pi,X)
    vC = coerce(v,pi,X)
    sC = coerce(s,pi,X)
    tC = coerce(t,pi,X)
```

(e) Pick three "random" nonzero complex numbers z_1, z_2, z_3 of norm less than 0.1 (they need to be close to 0 in order for the Laurent series of $\wp(x)$ to converge quickly). You can approximate the point $P_1 = \Phi(z_1) = \big(\wp(z_1), \wp'(z_1)\big)$ on the elliptic curve $y^2 = 4x^3 - g_2x - g_3$ in Sage using[2]

```
wp = EllipticCurve([CC(-35),CC(-98)]).weierstrass_p(100)
wpp = wp.derivative()
P1=(wp.laurent_polynomial()(z1),wpp.laurent_polynomial()(z1))
```

For $i = 1, 2, 3$, compute the points $P_i = \Phi(z_i)$ and $Q_i = \Phi(\tau z_i)$ (remember to use the embedding of τ in $\mathbb{C}$). Check that the points all approximately satisfy the curve equation $y^2 = 4x^3 - g_2x - g_3$ (if not, use z_i with smaller norms). Then verify that Q_i and $\phi(P_i)$ are approximately equal in each case. Report the values of z_i, P_i, Q_i and $\phi(P_i)$.

Problem 2. Binary quadratic forms (49 points)

A *binary quadratic form* is a homogeneous polynomial of degree 2 in two variables:

$$f(x, y) = ax^2 + bxy + cy^2,$$

which we identify by the coefficient vector (a, b, c). We are interested in a particular set of binary quadratic forms, those that are *integral* ($a, b, c \in \mathbb{Z}$), *primitive* ($\gcd(a, b, c) = 1$), and *positive definite* ($b^2 - 4ac < 0$ and $a > 0$). Henceforth we shall use the word *form* to refer to an integral, primitive, positive definite, binary quadratic form. The *discriminant* of a form is the negative integer $D = b^2 - 4ac$, which is evidently a square modulo 4. We call such integers (imaginary quadratic) discriminants, and let $F(D)$ denote the set of forms with discriminant D.

(a) For each $\gamma = \left(\begin{smallmatrix} s & t \\ u & v \end{smallmatrix}\right) \in \mathrm{SL}_2(\mathbb{Z})$ and $f(x, y) \in F(D)$ define

$$f^\gamma(x, y) := f(sx + ty,\ ux + vy).$$

Show that $f^\gamma \in F(D)$, and that this defines a right group action of $\mathrm{SL}_2(\mathbb{Z})$ on the set $F(D)$ (this means $f^I = f$ and $f^{(\gamma_1\gamma_2)} = (f^{\gamma_1})^{\gamma_2}$).

Forms f and g are (properly) *equivalent* if $g = f^\gamma$ for some $\gamma \in \mathrm{SL}_2(\mathbb{Z})$. In this problem and the next, you will prove that the set $\mathrm{cl}(D)$ of $\mathrm{SL}_2(\mathbb{Z})$-equivalence classes of $F(D)$ forms a finite abelian group, and develop algorithms to compute in this group.

The group $\mathrm{cl}(D)$ is called the *class group*, and it plays a key role in the theory of complex multiplication. Our first objective is to prove that $\mathrm{cl}(D)$ is finite, and to develop an algorithm to enumerate unique representatives of its elements (which also allows us

[2] You need to use the `laurent_polynomial` method in order to evaluate `wp` at a complex number.

to determine its cardinality). We define the (principal) *root* τ of a form $f = (a, b, c)$ to be the unique root of $f(x, 1)$ in the upper half plane:

$$\tau = \frac{-b + \sqrt{D}}{2a}.$$

Recall that $\mathrm{SL}_2(\mathbb{Z})$ acts on the upper half plane $\mathcal{H}$ via linear fractional transformations

$$\begin{pmatrix} s & t \\ u & v \end{pmatrix} \tau = \frac{s\tau + t}{u\tau + v},$$

and that the set

$$\mathcal{F} = \big\{\tau \in \mathcal{H} : \mathrm{re}(\tau) \in [-1/2, 0] \text{ and } |\tau| \geq 1\big\} \cup \big\{\tau \in \mathcal{H} : \mathrm{re}(\tau) \in (0, 1/2) \text{ and } |\tau| > 1\big\}$$

is a fundamental region for $\mathcal{H}$ modulo the $\mathrm{SL}_2(\mathbb{Z})$-action.

(b) Prove that $\gamma \in \mathrm{SL}_2(\mathbb{Z})$ acts compatibly on forms and their roots by showing that if τ is the root of f, then $\gamma^{-1}\tau$ is the root of f^γ. Conclude that two forms are equivalent if and only if their roots are equivalent.

A form $f = (a, b, c)$ is said to be *reduced* if

$$-a < b \leq a < c \qquad \text{or} \qquad 0 \leq b \leq a = c.$$

(c) Prove that a form is reduced if and only if its root lies in the fundamental region $\mathcal{F}$. Conclude that each equivalence class in $F(D)$ contains exactly one reduced form.

(d) Prove that if f is reduced then $a \leq \sqrt{|D|/3}$. Conclude that the set $\mathrm{cl}(D)$ is finite, and show that in fact its cardinality $h(D)$ satisfies $h(D) \leq |D|/3$. Prove that $F(D)$ contains a unique reduced form (a, b, c) with $a = 1$, and conclude that $h(-3) = h(-4) = 1$.

The positive integer $h(D)$ is called the *class number* of the discriminant D. The bound $h(D) \leq |D|/3$ is a substantial overestimate. In fact, $h(D) = O(|D|^{1/2} \log |D|)$, but proving this requires some analytic number theory that is beyond the scope of this course. Under the generalized Riemann hypothesis one can show $h(D) = O(|D|^{1/2} \log\log |D|)$.

(e) Give an algorithm to enumerate the reduced forms in $F(D)$. Using the upper bound $h(D) = O(|D|^{1/2} \log |D|)$, prove that your algorithm runs in $O(|D|\mathsf{M}(\log |D|))$ time.

(f) Implement your algorithm and use it to enumerate the five reduced forms in $F(-103)$ and the six reduced forms in $F(-396)$. Then use it to compute $h(D)$ for the first three discriminants $D < -N$, where N is the integer formed by the first four digits of your student ID.

Problem 3. The class group (98 points)

In Problem 2 we proved that $\mathrm{cl}(D)$ is a finite set. In this problem you will prove that it is an abelian group, and develop an algorithm for computing the group operation.

To each form $f(x, y) = ax^2 + bxy + cy^2$ in $F(D)$ with root $\tau = (-b + \sqrt{D})/(2a)$, we associate the lattice $L(f) = L(a, b, c) = a[1, \tau]$.

(a) Show that two forms $f, g \in F(D)$ are equivalent if and only if the lattices $L(f)$ and $L(g)$ are homothetic (use may use part (b) of problem 2 if you wish).

For any lattice L, the *order* of L is the set

$$\mathcal{O}(L) = \{\alpha \in \mathbb{C} : \alpha L \subseteq L\}.$$

(b) Prove that either $\mathcal{O}(L) = \mathbb{Z}$ or $\mathcal{O}(L)$ is an order in an imaginary quadratic field, and that homothetic lattices have the same order. Prove that if L is the lattice of a form in $F(D)$, then $\mathcal{O}(L)$ is the order of discriminant D in the field $K = \mathbb{Q}(\sqrt{D})$.

For the rest of this problem let $\mathcal{O}$ denote the (not necessarily maximal) imaginary quadratic order of discriminant D, which may be represented as a lattice $[1, \omega]$, where ω is an algebraic integer whose minimal polynomial x^2+bx+c has discriminant $b^2-4c = D$.

Recall that an (integral) $\mathcal{O}$*-ideal* $\mathfrak{a}$ is an additive subgroup of O that is closed under multiplication by $\mathcal{O}$. Every $\mathcal{O}$-ideal $\mathfrak{a}$ is necessarily a sublattice of $\mathcal{O}$, and its *norm* $N(\mathfrak{a})$ is the index $[\mathcal{O} : \mathfrak{a}] = |\mathcal{O}/\mathfrak{a}|$. An $\mathcal{O}$-ideal $\mathfrak{a}$ is said to be *proper* if $\mathcal{O}(\mathfrak{a}) = \mathcal{O}$. In Lecture 18 we showed that $\mathfrak{a}$ is proper if and only if it is invertible as a fractional ideal, which explains our interest in this property. Note that we always have $\mathcal{O} \subseteq \mathcal{O}(\mathfrak{a})$, so when $\mathcal{O}$ is maximal every nonzero $\mathcal{O}$-ideal is proper.

(c) Prove that if $L(a, b, c) = a[1, \tau]$ is the lattice of a form in $F(D)$, then L is a proper $\mathcal{O}$-ideal of norm a, where $\mathcal{O} = \mathcal{O}(L) = [1, a\tau]$.

(d) Conversely prove that every proper $\mathcal{O}$-ideal $\mathfrak{a}$ is homothetic to the lattice of a form in $F(D)$. Show that the assumption that $\mathfrak{a}$ is proper is necessary by giving an explicit example of an $\mathcal{O}$-ideal $\mathfrak{a}$ that is not proper (so by (c) it cannot be homothetic to the lattice of a form in $F(d)$).

(e) Prove that if the norm of $\mathfrak{a}$ is relatively prime to the conductor $u = [\mathcal{O}_K : \mathcal{O}]$ of $\mathcal{O}$ then $\mathfrak{a}$ is proper. Give an explicit example showing that the converse is not true.

The product of two lattices $[\omega_1, \omega_2]$ and $[\omega_3, \omega_4]$ in $\mathbb{C}$ is the additive group generated by $\{\omega_1\omega_3,\ \omega_1\omega_4,\ \omega_2\omega_3,\ \omega_2\omega_4\}$.

(f) Show that, in general, the product of two lattices need not be a lattice, but the product of two lattices that are $\mathcal{O}$-ideals is a lattice.

(g) Let $\mathrm{cl}(\mathcal{O})$ denote the set of equivalence classes (under homothety) of lattices that are proper $\mathcal{O}$-ideals. Prove that the lattice product makes $\mathrm{cl}(\mathcal{O})$ into an abelian group. Conclude that the corresponding operation on the equivalence classes of $F(D)$ makes $\mathrm{cl}(D)$ into an abelian group that is isomorphic to $\mathrm{cl}(\mathcal{O})$.

To do explicit computations in $\mathrm{cl}(D)$ we need to translate the product operation on lattices $L(f_1)$ and $L(f_2)$ into a corresponding product operation on forms $f_1, f_2 \in F(D)$. This is known as *composition* of forms, and is performed as follows. If $f_1 = (a_1, b_1, c_1)$ and $f_2 = (a_2, b_2, c_2)$ are forms in $F(D)$, then let $s = (b_1+b_2)/2$ (this is an integer because b_1, b_2 and D all have the same parity). Use the extended Euclidean algorithm (twice) to compute integers u, v, w, and d such that $ua_1 + va_2 + ws = d = \gcd(a_1, a_2, s)$. The composition of f_1 and f_2 is then given by

$$f_1 * f_2 = (a_3, b_3, c_3) = \left(\frac{a_1a_2}{d^2},\ b_2 + \frac{2a_2}{d}(v(s-b_2) - wc_2),\ \frac{b_3^2 - D}{4a_3}\right).$$

It is a straight-forward but tedious task to verify that this composition formula satisfies $L(f_1 * f_2) = L(f_1) * L(f_2)$; you are not required to do this.

(h) Verify that the inverse of (a, b, c) is $(a, -b, c)$ and that the unique reduced from with $a = 1$ acts as the identity (see Problem 2 for the definition of a reduced form).

Unfortunately, even if f_1 and f_2 are reduced forms, the composition of f_1 and f_2 need not be reduced. In order to compute in $\mathrm{cl}(D)$ effectively, we need a reduction algorithm. Recall the matrices $S = \left(\begin{smallmatrix} 0 & -1 \\ 1 & 0 \end{smallmatrix}\right)$ and $T = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ that generate $\mathrm{SL}_2(\mathbb{Z})$.

(i) Let f be the form (a, b, c). Compute the forms f^S, f^{T^m}, and $f^{T^{-m}}$, for a positive integer m.

A form (a, b, c) with $-a < b \leq a$ is said to be *normalized*.

(j) Show that for any form f there is an integer m such that f^{T^m} is normalized, and give an explicit formula for m. Let us call f^{T^m} the *normalization* of f. Now let $f = (a, b, c)$ be a normalized form and prove the following:

(a) If $a < \sqrt{|D|}/2$ then f is reduced.

(b) If $a < \sqrt{|D|}$ and f is not reduced, then the normalization of Sf is reduced.

(c) If $a \geq \sqrt{|D|}$ then the normalization (a', b', c') of Sf has $a' \leq a/2$.

(k) Give an algorithm to compute the reduction of a form f in $F(D)$, and bound its complexity as a function of $n = \log |D|$, assuming that its coefficients are $O(n)$ bits in size. Then bound the complexity of computing the reduction of the product of two reduced forms (this corresponds to performing a group operation in $\mathrm{cl}(D)$).[3]

(l) Implement your algorithm and then use it to compute the reduction of a form $(a, b, c) \in F(D)$, with a equal to the least prime greater than $|D|^2$ for which $\left(\frac{D}{a}\right) = 1$. Do this for the discriminants $D = -103$ and $D = -396$, and for the first three discriminants $D < -N$, where N is the first four digits of your student ID. For the largest $|D|$, list the sequence of normalized forms computed during the reduction.

Problem 4. Subgroups of $\mathrm{GL}_2(\mathbb{F}_\ell)$ (49 points)

Let E be an elliptic curve defined over $\mathbb{Q}$. Recall that for each integer $n > 1$, the n-torsion subgroup of $E(\overline{\mathbb{Q}})$ is a rank 2 $(\mathbb{Z}/n\mathbb{Z})$-module we denote $E[n]$. As explained in Problem Sets 3 and 6, 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 $G_\mathbb{Q}$-action 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 we restrict our attention to prime $n = \ell$, in which case we have following theorem of Serre.

[3] A quasi-linear bound is known [1], but your bound does not need to be this tight. However it should be polynomial in n.

Theorem (Serre, 1972)**.** *Let E be an elliptic curve over $\mathbb{Q}$ for which $\mathrm{End}(E_{\overline{\mathbb{Q}}}) = \mathbb{Z}$. For all but finitely many primes ℓ, the image of the mod-ℓ Galois representation is surjective:*

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

Remark. For an elliptic curve over $\mathbb{Q}$ (or any number field) we know that $\mathrm{End}(E_{\overline{\mathbb{Q}}})$ is either $\mathbb{Z}$ or an order in an imaginary quadratic field. The latter case is quite special: it applies to only 13 $\overline{\mathbb{Q}}$-isomorphism classes of elliptic curves over $\mathbb{Q}$, corresponding to the 13 imaginary quadratic orders of class number one.[4]

Remark. It is conjectured that Serre's theorem actually applies to all primes $\ell > 37$ (independent of E). There is ample evidence and some recent progress toward a proof of this conjecture, but it remains a major open question.

A key component of the proof of Serre's 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 $L_1, L_2 \subset V$ (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 $*$ denotes any element of $\mathbb{F}_\ell^\times$. Thus $C \simeq \left(\mathbb{F}_\ell^\times\right)^2$ 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.)

[4]Elliptic curves $E/\mathbb{Q}$ with $\mathrm{End}(E_{\overline{\mathbb{Q}}}) \neq \mathbb{Z}$ are often said to have complex multiplication and called CM curves, even though this is not strictly true: the extra endomorphisms are only defined over a quadratic extension (it would be more correct to say these curves have "potential complex multiplication").

(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; these subgroups correspond to the symmetry groups of the regular polyhedra: tetrahedron, cube/octahedron, and icosahedron/dodecahedron, respectively.)

(i) Use parts (a) to (h) to prove the following classification theorem.

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 $\mathrm{SL}_2(\mathbb{F}_\ell)$.*

Serre's theorem states that except for elliptic curves $E/\mathbb{Q}$ with (potential) complex multiplication, for all but finitely many primes ℓ we are in case (v) of the classification above. On later problem sets we will see that for $\ell \neq 2$ this never happens if E has complex multiplication, so the hypothesis $\mathrm{End}(E_{\overline{\mathbb{Q}}}) = \mathbb{Z}$ in Serre's theorem is necessary.

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

Problem 5. Survey (2 points)

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 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			

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
11/14	Riemann surfaces, modular curves				
11/16	The modular equation				

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.

References

[1] A. Schönhage, *Fast reduction and composition of binary quadratic forms*, in International Symposium on Symbolic and Algebraic Computation–ISSAC'91, ACM, 1991, 128–133.