MODULAR FORMS

D. CULVER

Contents

1. Modular forms over $\mathbb{C}$

This section is essentially lifted from [5]. Let us begin by recalling that there is an action of the arithmetic group $\mathrm{SL}_2(\mathbb{Z})$ on the upper half plane

$$H := \{z \in \mathbb{C} \mid \operatorname{im} z > 0\}$$

given by Möbius transformations. Namely, if

$$g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in \mathrm{SL}_2\mathbb{Z}$$

and $z \in H$, then

$$gz := \frac{az+b}{cz+d}.$$

Here is where this group action comes from: Let $\mathcal{L}$ denote the set of lattices inside $\mathbb{C}$, and let $\mathcal{B}$ denote the set of ordered pairs (ω_1, ω_2) of elements in $\mathbb{C}^*$ such that $\operatorname{im}(\omega_1/\omega_2) > 0$. There is then a surjective map

$$\mathcal{B} \to \mathcal{L}; (\omega_1, \omega_2) \mapsto \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2.$$

So we regard $\mathcal{B}$ as the set of bases for lattices in $\mathcal{L}$. Suppose that two elements (ω_1, ω_2) and (ω_1', ω_2') of $\mathcal{B}$ gave the same lattice $L \subseteq \mathbb{C}$. Then we would be able to write

$$\omega_1' = a\omega_1 + b\omega_2, \qquad \omega_2' = c\omega_1 + d\omega_2 \tag{1.1}$$

for some integers $a, b, c, d \in \mathbb{Z}$. What this really describes is a linear automorphism of L whose matrix with respect to the basis (ω_1, ω_2) is

$$g := \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}).$$

Observe that the equations in (1.1) can be rewritten in terms of the action of $SL_2\mathbb{Z}$ on H:

$$g \cdot \frac{\omega_1}{\omega_2} = \frac{\omega_1'}{\omega_2'}.$$

This shows that the action of $SL_2\mathbb{Z}$ on the upper half plane is only meant to capture that two elements $\tau, \tau' \in H$ determine the same lattice in $\mathbb{C}$ if and only if they are in the same $SL_2\mathbb{Z}$ orbit. Note that we have also clearly defined an action of $SL_2\mathbb{Z}$ on $\mathcal{B}$.

Proposition 1.2. *The quotient $\mathcal{B}/SL_2(\mathbb{Z})$ is isomorphic to $\mathcal{L}$.*

Now let $\mathbb{C}^*$ act on $\mathcal{L}$ via homothety,

$$L \mapsto \lambda L,$$

and similarly $\mathbb{C}^*$ acts on $\mathcal{B}$ by

$$\lambda \cdot (\omega_1, \omega_2) := (\lambda\omega_1, \lambda\omega_2).$$

Observe the map

$$(\omega_1, \omega_2) \mapsto \omega_1/\omega_2$$

defines a map to H, which produces a bijection

$$\mathcal{B}/\mathbb{C}^* \cong H,$$

passing to the quotient by the $SL_2(\mathbb{Z})$ actions gives a bijection

$$\mathcal{L}/\mathbb{C}^* \cong H/SL_2(\mathbb{Z}).$$

A modular function will be a function on the set of lattices $\mathcal{L}$ satisfying a certain homogenity condition with respect to the action by $\mathbb{C}^*$. More specifically:

Definition 1.3. A *modular function F* of *weight* $2k$ is a complex-valued function $f : \mathcal{L} \to \mathbb{C}$ satisfying the following conditions:

(1) (homogeneity) For each $L \in \mathcal{L}$ and $\lambda \in \mathbb{C}^*$, F satisfies

$$F(\lambda L) = \lambda^{-2k} F(\Lambda);$$

(2) The function

$$f(\tau) := F(\mathbb{Z}\tau \oplus \mathbb{Z})$$

is a meromorphic function on H.

Let's translate this into a function on the upper half plane H. Let F be a modular function of weight $2k$, and let $(\omega_1, \omega_2) \in \mathcal{B}$. Then we can define a function $f : H \to \mathbb{C}$ by

$$F(\omega_1, \omega_2) = \omega_2^{-2k} f(\omega_1/\omega_2). \tag{1.4}$$

Since F is $SL_2\mathbb{Z}$-invariant, this translates into the following functional equation for f,

$$f(z) = (cz+d)^{-2k} f(gz), \qquad \text{for all } g = \begin{pmatrix} a & b \\ c & d \end{pmatrix} \in SL_2(\mathbb{Z}) \tag{1.5}$$

Conversely, if we have a function f on the upper half plane satisfying (1.5), then we can define a function F on $\mathcal{L}$ satisfying homogeneity.

Remark 1.6. Note that in the definition of a modular function, we could have defined modular functions of odd weight. However, all such functions are zero as

$$F(-\Lambda) = F(\Lambda)$$

but homogeneity requires that

$$F(-\Lambda) = -F(\Lambda)$$

and hence $F = 0$.

We can now define modular forms.

Definition 1.7. Let k be an integer. We say a function f is *weakly modular of weight* $2k$ if f is meromorphic on H and satisfies relation (1.5).

This can be expressed using differential forms. First note that for $g \in SL_2(\mathbb{Z})$

$$\frac{d}{dz}(gz) = (cz+d)^{-2}$$

which can also be written as

$$d(gz) = (cz+d)^{-2} dz.$$

We can consider the *weight k differential $dz^{\otimes k}$*, and we can rephrase what it means for $f(z)$ to be a weakly modular function (modular form) by regarding $f(z)dz^{\otimes k}$ as a $SL_2(\mathbb{Z})$-invariant weight k meromorphic form.

Fact 1. The arithmetic group $SL_2(\mathbb{Z})$ is generated by the following elements

$$S := \begin{pmatrix} 0 & -1 \\ 1 & 0 \end{pmatrix}$$

and

$$T := \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}.$$

The corresponding action on H is given by

$$Sz = -1/z$$

$$Tz = 1 + z.$$

A consequence of this fact is

Corollary 1.8. *A meromorphic function f on H is weakly modular of weight $2k$ if and only if*

$$f(1+z) = f(z) \tag{1.9}$$

and

$$f(-1/z) = z^{2k} f(z). \tag{1.10}$$

Because of the relation (1.9), we can make the change coordinates via $q := e^{2\pi i z}$. This defines a holomorphic map

$$e^{2\pi i z} : H \to D \setminus \{0\}$$

where D denotes the open unit disc. As a function in q, $f(q)$ is meromorphic on $D \setminus \{0\}$. If f is meromorphic at 0, then we say that f is *meromorphic at infinity*. In this case, f admits a Laurent expansion near the origin

$$f(q) = \sum_{-\infty}^{\infty} a_n q^n$$

where the a_n are all zero for sufficiently small n. If $f(q)$ is holomorphic at 0, then we say that f *holomorphic at infinity*, and in this case the q-expansion is

$$\sum_{n=0}^{\infty} a_n q^n.$$

Definition 1.11. A weakly modular function f is *modular* if it is meromorphic at infinity.

When f is holomorphic at infinity, we set $f(\infty) := f(0)$.

Definition 1.12. A modular function f is a *modular form* if it is holomorphic at infinity. If $f(\infty) = 0$, then we call f a *cusp form*.

1.1. **Eisenstein series.** Let $L \subseteq \mathbb{C}$ be a lattice. We define a lattice function as follows

$$G_{wk}(L) := \sum_{\gamma \in L \setminus \{0\}} \frac{1}{\gamma^{2k}}.$$

This clearly satisfies homogeneity can be shown to be meromorphic on H. So this defines a weakly modular function. If ω_1, ω_2 is a basis for L, then we can write

$$G_{2k}(L) = \sum_{m,n} \frac{1}{(m\omega_1 + n\omega_2)^{2k}}$$

The associated weakly modular function on the upper half plane is

$$G_{2k}(\tau) = \sum_{(m,n) \in \mathbb{Z} \times \mathbb{Z} \setminus \{(0,0)\}} \frac{1}{(m\tau + n)^{2k}},$$

and it turns out this is actually holomorphic everywhere, including at ∞. So G_{2k} is a modular form, and it is called the kth *Eisenstein series*. One has that

$$\lim_{\tau \to i\infty} G_{2k}(z) = 2\zeta(2k)$$

where ζ is the Riemann ζ-function. The q-expansions of the Eisenstein series is

$$G_{2k}(z) = 2\zeta(2k) + 2\frac{(2\pi i)^{2k}}{(2k-1)!} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

where

$$\sigma_k(n) = \sum_{d \mid n} d^k.$$

We can divide $G_{2k}(z)$ by $2\zeta(2k)$ to get the *normalized Eisenstein series*

$$E_{2k}(z) = 1 + (-1)^k \frac{4k}{B_{2k}} \sum_{n=1}^{\infty} \sigma_{2k-1}(n) q^n$$

where B_{2k} denotes the kth Bernoulli number.

1.2. **The algebra of modular forms.** Notice that the sum of two modular forms of weight $2k$ is clearly another modular form of weight $2k$, and the product of a weight $2k$ and weight 2ℓ modular form is of weight $2k + 2\ell$. If we let M_{2k} denote the space of weight $2k$ modular forms, then

$$MF_* = \bigoplus_{k \geq 0} M_{2k}$$

forms a graded algebra. Let M^0_{2k} denote the space of weight $2k$ cusp forms, i.e. those weight $2k$ modular forms f with $f(\infty) = 0$. Note the exact sequence

$$\begin{tikzcd} 0 \arrow[r] & M^0_{2k} \arrow[r] & M_{2k} \arrow[r] & \mathbb{C} \arrow[r] & 0 \end{tikzcd}$$

where the second map is evaluation at ∞. Since $E_{2k}(\infty) \neq 0$, this map is indeed surjective. So we get a decomposition

$$M_{2k} = M^0_{2k} \oplus \mathbb{C}\{E_{2k}\}.$$

It turns out that (cf. [5]) this graded algebra is a polynomial algebra on E_4 and E_6.

Theorem 1.13.

$$MF_* = \mathbb{C}[E_4, E_6].$$

This fact has interesting consequences. In particular, each space M_{2k} is finite dimensional, This allows one to find interesting relations between modular forms, such as the Eisenstein series, and to then deduce relations amongst the coefficients in their q-expansions. This can yield interesting arithmetic information.

Example 1.14. The space M_8 is one dimensional. This implies that for some $\alpha \in \mathbb{C}^*$, $E_8 = \alpha E_4^2$. As they are both 1 at ∞, $\alpha = 1$. Comparing the coefficients in the q-expansion yields the following equality

$$\sigma_7(n) = \sigma_3(n) + 120 \sum_{m=1}^{n-1} \sigma_3(m)\sigma_3(n-m).$$

2. Modular forms over $\mathbb{Z}$

I will now try to motivate the definition of modular forms over more general rings, in particular over the integers $\mathbb{Z}$. Fist, let's start by trying to think about what a complex modular form is.

Recall that if $\Lambda \subseteq \mathbb{C}$ is a lattice, then the quotient $\mathbb{C}/\Lambda$ has the structure of complex elliptic curve. This is obtained using the Weierstrass $\wp$ function:

$$x(z) = \wp(z;\Lambda) := \frac{1}{z^2} + \sum_{\omega \in \Lambda \backslash 0} \left(\frac{1}{(z-\omega)^2} - \frac{1}{\omega^2} \right).$$

Let

$$y(z) := \wp'(z;\Lambda).$$

Let $g_4 = 60G_4$ and $g_6 = 140G_6$. It can be shown that $\wp$ satisfies the differential equation

$$y^2 = 4x^3 - g_2(\Lambda)x - g_3(\Lambda),$$

which furnishes an embedding

$$\varphi_\Lambda : \mathbb{C}/\Lambda \to \mathbb{P}^2; z \mapsto [x(z);y(z);1].$$

Thus we have produced a map

$$\mathcal{L} \to \{\text{elliptic curves over}\mathbb{C}\}/\cong \tag{2.1}$$

This suggests that we might want to think of a modular form $f(z)$ as a function which gives a complex number $f(E/\mathbb{C})$ for every elliptic curve over the complex numbers $E/\mathbb{C}$, and we would like to think that this number is an isomorphism invariant. But that is actually not correct because the embeddings of $\mathbb{C}/\Lambda$ depend on Λ, but different choices of Λ may give isomorphic elliptic curves. In other words, the map (2.1) is surjective but not injective[1].

Observe that if $\lambda \in \mathbb{C}^*$, and $\lambda\Lambda_1 \subseteq \Lambda_2$, then scalar multiplication by λ induces a holomorphic homomorphism

$$f_\lambda : \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2; z \mapsto \lambda z \mod \Lambda_2.$$

Every map of elliptic curves arise in this way.

Proposition 2.2. *(cf.* [6]*) Let Λ_1, Λ_2 be lattices of $\mathbb{C}$. Then the map*

$$\{\lambda \in \mathbb{C}^* : \lambda\Lambda_1 \subseteq \Lambda_2\} \to \{\text{ holomorphic homomorphisms } \mathbb{C}/\Lambda_1 \to \mathbb{C}/\Lambda_2\}; \lambda \mapsto f_\lambda$$

is a bijection. Moreover, we can identify the target with the set of isogenies of the elliptic curves determined by Λ_1, Λ_2. Consequently, the elliptic curves $\mathbb{C}/\Lambda_1$ and $\mathbb{C}/\Lambda_2$ are isomorphic iff there is a scalar λ with $\lambda\Lambda_1 = \Lambda_2$.

[1] The fact that (2.1) is a non-trivial result going under the name of the Uniformization Theorem. For a proof, see [2].

Since g_2, g_3 are modular forms, it follows that

$$g_2(\lambda\Lambda) = \lambda^{-4} g_2(\Lambda)$$

and

$$g_3(\lambda\Lambda) = \lambda^{-6} g_3(\Lambda)$$

which means that the embedding gives different Weierstrass expressions for the same elliptic curve $\mathbb{C}/\lambda\Lambda \cong \mathbb{C}/\Lambda$. This suggests that the lattice Λ is carrying some extra structure which we missed.

Observe that there is a translation invariant differential dz on $\mathbb{C}$, modding out by a lattice produces Λ produces an invariant differential dz on $\mathbb{C}/\Lambda$. The Weierstrass embedding (2.1) carries the invariant differential dz to

$$\omega_\Lambda := \frac{dx}{y}.$$

This differential pulls back to dz under the embedding φ_Λ since

$$\varphi_\Lambda^*(\omega) = \frac{d\wp(z;\Lambda)}{\wp'(z;\Lambda)} = dz.$$

Proposition 2.3. *[cf. [6]] There is a bijection*

$$\mathcal{L} \to \{(E,\omega) \mid E \textit{ is an elliptic curve over } \mathbb{C}, \textit{ and } \omega \textit{ is an invariant differential}\}$$

Proof Sketch. Let E be an elliptic curve with invariant differential ω. Let $\gamma_1, \gamma_2 \in H_1(E,\mathbb{Z})$ denote the two generators of the first homology of E. Then we can integrate these with respect ω. This gives complex numbers

$$\omega_i := \int_{\gamma_i} \omega.$$

It turns out these are $\mathbb{R}$-linearly independent, and so generate a lattice Λ in $\mathbb{C}$. It turns out that φ_Λ determines the isomorphism between $\mathbb{C}/\Lambda$ and E, and carries dz to ω. □

This suggests that we can rephrase what it means to be a weight k modular form.

Definition 2.4. (version 3) A modular form of weight $2k$ over $\mathbb{C}$ is a function on pairs (E,ω) where E is an elliptic curve, and ω is an invariant differential of E satisfying the following condition:

(1) (homogeneity) For all $\lambda \in \mathbb{C}^*$, one has

$$f(E,\lambda\omega) = \lambda^{-2k} f(E,\omega)$$

(2) The function $f(\mathbb{Z}/(\mathbb{Z}\tau \oplus \mathbb{Z}), dz)$ is holomorphic in $\tau \in H$ and bounded as $\tau \to i\infty$.

Remark 2.5. We can translate between this definition of a modular form and the one given earlier as a functin on lattices. In particular, given a modular form in the sense of Definition 1.11, we define a modular form in the sense of 2.4 by using the isomorphism of Proposition 2.3, i.e. if $(E, \omega) \cong (\mathbb{C}/\Lambda, dz)$ then we set

$$f(E, \omega) = f(\mathbb{C}/\Lambda, dz) := f(\Lambda).$$

Since multiplication by λ induces a map of elliptic curves, carrying the differential dz to λdz, it follows from 2.3 that

$$(\mathbb{C}/\Lambda, dz) \leftrightarrow \Lambda$$

whereas

$$(\mathbb{C}/\Lambda, \lambda dz) \leftrightarrow \lambda\Lambda.$$

Thus the homogeneity condition is the same in both definitions.

It is this definition that we will generalize to more algebraic settings. Before proceeding with that, we will need some algebro-geoemtric preliminaries. In particular we need to introduce what a generalized elliptic curve is. For simplicity, we follow Rezk in [4] and give a coordinate definition.

Definition 2.6. A *generalized elliptic curve* over a base scheme S is a morphism of schemes $p : E \to S$ with a section $e : S \to E$ such that there is a cover by opens $U_i \to S$ such that over each U_i, the scheme $E|_{U_i} \to U_i$ is isomorphic to a Weierstrass curve with basepoint e. A morphism of generalized elliptic curve is a pullback diagram in schemes

$$\begin{tikzcd} E' \arrow[r, "\varphi"] \arrow[d, "p'"'] & E \arrow[d, "p"] \\ S' \arrow[r, "\varphi"] & S \end{tikzcd}$$

which is locally a map of Weierstrass curves[2].

Example 2.7. Consider the scheme over Spec($\mathbb{Z}$) given in affine coordinates via the Weierstrass equation

$$C_1 : y^2 = x^3 + 2x^2 + 6$$

[2] There is a coordinate free definition of a generalized elliptic curve. See [1] and [3].

In this case the section e is picking out the point at infinity over each point.

Remark 2.8. Let E be a Weierstrass curve over $\mathrm{Spec}(R)$, so in particular $E \to \mathrm{Spec}(R)$ is a generalized elliptic curve. By Katharine's talk, we know that there is a line bundle on $\mathrm{Spec}(R)$ called the sheaf of invariant differentials on E, denoted ω_E. She wrote the invariant differential

$$\omega = \frac{dx}{2y + a_1 x + a_3},$$

this is a nowhere vanishing section of E, witnessing that ω_E is a trivial line bundle. Given a generalized elliptic curve $E \to S$ with cover $\{U_i\}$, we have a sheaf of invariant differentials $\omega_{E|_{U_i}}$ for each U_i. From Katharine's description of how the invariant differential changes under change of coordinates allows us to glue these sheaves together. This gives the *sheaf of invariant differentials* $\omega_{E/S}$ for E. This is a line bundle on S.

The sheaf of invariant differentials can also be defined as:

Definition 2.9. Let $p : E \to S$ be a generalized elliptic curve. Let $\Omega^1_{E/S}$ be the sheaf of relative differentials, which is a sheaf on E. This is an invertible sheaf, and we define

$$\omega_{E/S} := e^* \Omega^1_{E/S}.$$

Observation 2.10. *If $\varphi : E'/S' \to E/S$ is a morphism of generalized elliptic curves, then*

$$\varphi^* \omega_{E/S} \cong \omega_{E'/S'}$$

This suggests the following generalization of modular forms (cf. [1]):

Definition 2.11. An *integral modular form of weight k* is a function f which assigns to each elliptic curve E/S over a base scheme S an element $f(E/S) \in H^0(S; \omega^{\otimes k})$ such that f is stable under base change.

To be stable under base change means that if we have a pullback diagram

$$\begin{tikzcd}
E' \arrow[r] \arrow[d] & E \arrow[d] \\
S' \arrow[r, "\varphi"] & S
\end{tikzcd}$$

where E/S is an elliptic curve over S, then

$$\varphi^* f(E/S) = f(E'/S') \in H^0(S', \omega_{E'/S'}^{\otimes k}).$$

This looks slightly different then Definition 2.4. Let's briefly relate these two definitions. Suppose that we have an elliptic curve $E \to \operatorname{Spec}(R)$ which is given globally via a Weierstrass equation. Let

$$\omega = \frac{dx}{2y + a_1 x + a_3}$$

be the invariant differential coming from the Weierstrass equation. This is a nowhere vanishing section of the sheaf ω_E. If f is a modular form of weight k, then we can write

$$f(E/R) = F(E/R, \omega) \cdot \omega^{\otimes k}$$

where $F(E/R, \omega) \in R$. The function F must satisfy:

(1) $F(E/R, \omega)$ depends only on the R-isomorphism class of the pair;
(2) F satisfies the identity

$$F(E/R, \lambda\omega) = \lambda^{-k} F(E/R, \omega)$$

for every $\lambda \in R^\times$.
(3) F is stable under pullback.

The condition (2) comes from the following: a modular form f relies only on the R-isomorphism type of E/R. However, the differential ω is extra data. If we had chosen another nowhere vanishing section ω' of ω_E, then the value $F(E/R, \omega')$ will be different from $F(E/R, \omega)$.

There a unit $\lambda \in R^\times$ such that $\omega' = \lambda\omega$. Thus we must have

$$\lambda^k F(E/R, \lambda\omega)\omega^{\otimes k} = F(E/R, \lambda\omega) \cdot (\lambda\omega)^{\otimes k} = f(E/R) = F(E/R, \omega) \cdot \omega^{\otimes k}$$

and for these equalities to hold we must have that

$$F(E/R, \lambda\omega) = \lambda^{-2k} F(E/R, \omega).$$

Examples 2.12. Let us quickly give some examples of modular forms in this sense. Let $E \to \operatorname{Spec}(R)$ be a Weierstrass curve. Recall that Katharine defined some polynomials c_4, c_6, and Δ from the coefficients of the Weierstrass equations. It turns out that $c_4\omega^{\otimes 4}$, $c_6\omega^{\otimes 6}$, and $\Delta\omega^{\otimes 12}$ are integral modular forms. To see why, note that under change of coordinates, there will be a unit u which alters c_4, c_6, Δ, and the differential ω, as follows

$$c_4' = u^4 c_4, \quad c_6' = u^6 c_6, \quad \Delta' = u^{12}\Delta, \quad \omega' = u^{-1}\omega.$$

Thus the sections $c_4\omega^{\otimes 4}, c_6\omega^{\otimes 6}$, and $\Delta\omega^{\otimes 12}$ are independent of the Weierstrass coordinates for E. For example

$$c_4'(\omega')^{\otimes 4} = u^4 c_4 \cdot u^{-4}\omega^{\otimes 4} = c_4\omega^{\otimes 4}.$$

This implies that we can define sections c_4, c_6 and Δ for any generalized elliptic curve $E \to S$, and these sections are clearly stable under pullback. Thus they define integral modular forms of weight 4, 6, and 12 respectively.

The following theorem of Deligne tells us what the algebra of integral modular forms is precisely.

Theorem 2.13 (Deligne)**.** *The ring of integral modular forms is generated over $\mathbb{Z}$ by c_4, c_6 and Δ and has exactly one relation*

$$c_4^3 - c_6^2 = 1728\Delta.$$

That is, the ring of integral modular forms is the ring

$$\mathbb{Z}[c_4, c_6, \Delta]/(c_4^3 - c_6^2 - 1728\Delta).$$

So I've defined modular forms over $\mathbb{Z}$ to be a function which assigns a section of $\omega_{E/S}^{\otimes *}$ for each elliptic curve E/S. One can show that the sheaves of invariant differentials $\omega_{E/S}$ glue together to give a sheaf ω on the moduli stack of elliptic curves $\mathcal{M}_{ell}$. Thus we also have

Definition 2.14. The space of weight k integral modular forms is the graded ring

$$H^0(\mathcal{M}_{ell}; \omega^{\otimes k}).$$

Corollary 2.15.

$$H^0(\mathcal{M}_{ell}; \omega^*) \cong \mathbb{Z}[c_4, c_6, \Delta]/(c_4^3 - c_6^2 - 1728\Delta).$$

References

[1] Pierre Deligne, *Courbes elliptique: Formulaire (d'après j. tate)*, Modular functions of one variable iv, 1972, pp. 53–73.

[2] Fred Diamond and Jerry Shurman, *A first course in modular forms*, Springer-Verlag, 2005.

[3] Haruzo Hida, *Geometric modular forms and elliptic curves*, 2nd ed., World Scientific Publishing, 2012.

[4] Charles Rezk, *Supplementary notes*. on author's webpage.
[5] Jean-Pierre Serre, *A course in arithmetic*, Springer-Verlag, 1973.
[6] Joseph H. Silverman, *The arithmetic of elliptic curves*, Springer-Verlag, 2009.

University of Notre Dame
E-mail address: dculver@nd.edu