

A Non-Gorenstein Eisenstein Descent

Frank Calegari William Stein

April 21, 2011

1 Introduction

Let $X_0(N)$ be the modular curve parameterizing isomorphism classes of (generalized) elliptic curves together with a cyclic subgroup of order N . Let $J_0(N)$ be the Jacobian of $X_0(N)$, and \mathbf{T} the ring of Hecke operators acting on $J_0(N)$. It is well known that we can associate to any maximal ideal \mathfrak{m} of the Hecke algebra a self-dual two-dimensional residual Galois representation

$$\bar{\rho}_{\mathfrak{m}} : \text{Gal}(\bar{\mathbf{Q}}/\mathbf{Q}) \rightarrow \text{GL}_2(\mathbf{T}/\mathfrak{m})$$

that arises from the natural action of Galois on the division points of $J_0(N)$ (see, e.g., [9]). Assume that the representation $\bar{\rho}_{\mathfrak{m}}$ is reducible, in which case one says that \mathfrak{m} is an *Eisenstein* prime. Mazur's analysis [3] of the Eisenstein ideal when N is prime allows for a thorough understanding of the arithmetic of the \mathfrak{m} -adic Tate module of $J_0(N)$, and through this the “Eisenstein quotients” of $J_0(N)$ that can naturally be associated to \mathfrak{m} . For example, when N is prime Mazur proved for Eisenstein primes \mathfrak{m} that:

1. The maximal ideal \mathfrak{m} satisfies multiplicity one; namely, $J_0(N)[\mathfrak{m}] = \mathbf{Z}/p\mathbf{Z} \oplus \mu_p$ if $p > 2$, and $J_0(N)[\mathfrak{m}] = D/\mathbf{Z}$ if $p = 2$, where D/\mathbf{Z} is the unique nontrivial group scheme extension of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 killed by 2. [Todo: give precise ref]
2. $\mathbf{T}_{\mathfrak{m}}$ is a Gorenstein ring.
3. The \mathfrak{m} -adic Tate module

$$J^{(\mathfrak{m})} := \mathbf{T}_{\mathfrak{m}} \otimes_{\mathbf{T}} \varprojlim J[p^n]$$

is free of rank two as a $\mathbf{T}_{\mathfrak{m}}$ -module.

There is a strong synergy between these results, and indeed their proofs. A notable consequence is the following theorem ([3, Cor. 3.5, Prop. 3.6, p. 150]):

Theorem 1.1 (Mazur). *Assume that N is prime, and let \mathfrak{m} be an Eisenstein prime of \mathbf{T} . If M is the Mordell-Weil group of $J_0(N)$ over \mathbf{Q} then $M \otimes_{\mathbf{T}_p} \mathbf{T}_{\mathfrak{m}}$ is finite; equivalently, the \mathfrak{m} -Eisenstein quotient J has finite Mordell-Weil group. Suppose moreover that the residue characteristic of \mathfrak{m} is odd. Then $\text{III}(J) \otimes_{\mathbf{T}_p} \mathbf{T}_{\mathfrak{m}} = 0$; equivalently, $\text{III}(J)[\mathfrak{m}] = 0$.*


If one tries to extend these results to non-prime level one quickly finds that the situation is more complicated. For example, there exist modular elliptic curves E/\mathbf{Q} with nontrivial torsion and positive rank. Such curves are examples of Eisenstein quotients of nonzero rank. On the other hand, many of Mazur's arguments continue to apply in a more general situation. In this note, we concentrate on a particular Eisenstein quotient of non-prime level, namely a 15 dimensional quotient A of $J_0(559)$ (defined more precisely below), and an associated Eisenstein maximal ideal \mathfrak{m} of residue characteristic 7. This example is particularly interesting in several respects. First, we already start to see pathologies not present in the case of prime conductor, namely, the failure of multiplicity one. On the other hand, we are still able to prove the following analogue of Theorem 1.1:

Theorem 1.2. *The Mordell–Weil group of A over \mathbf{Q} is finite. Furthermore $\text{III}(A)[\mathfrak{m}] = 0$.*

We do not strive for generality, but rather instead try by example to highlight the issues and difficulties one might expect in this more general context. Another guiding and motivating problem for us is the following:

Question 1.1. Let A be a modular abelian variety. Can one practically determine the following invariants of A ?

1. The rational torsion subgroup,
2. The endomorphism ring,
3. The minimal degree of a polarization $A \rightarrow A^\vee$.

A positive answer to this question would give a way of computing some of the invariants of A that appear in the BSD conjecture. Although there exist various algorithms for computing the torsion subgroup of an abelian variety, they usually require a concrete description of A in terms of equations. Our hold on the abelian varieties A is decidedly more fleeting: we have, concretely, a q -expansion f_A that is canonically associated to A . However, the form f_A only determines A up to *isogeny*, which is not enough to determine the torsion subgroup. In practise one can often use f_A to determine a multiple of the order of the torsion subgroup, and then hope to physically realize this subgroup by some geometric construction, say by considering the cuspidal subgroup (see [AS05, §3.5–3.6]). This is not always effective, however. ¹ Initial computations [Todo: reference paper in progress that explains how to do such computations.] performed by Tseno Tselkov suggested that there always existed a polarization $A \rightarrow A^\vee$ of degree some power of 2. We produce an explicit example to show that this is false. Namely, suppose that A is the 15 dimensional quotient  $J_0(559)$ mentioned above. Then we have the following:

Theorem 1.3. *Any polarization $A \rightarrow A^\vee$ has degree divisible by 7.*

We suspect that A might be the modular abelian variety of lowest level that exhibits this phenomenon.²

¹Frank: William says something about 2 and 3.

²William: William, is there any better way to search Tseno's data to determine how difficult this computation should be?

2 The Abelian Variety A

Let \mathbf{T} be the Hecke algebra of level $N = 559 = 13 \cdot 43$ associated to $J = J_0(559)$, and let \mathcal{I} be the ideal generated by $T_\ell - 1 - \ell$ for all $\ell \neq 13, 43$, and by $U_{13} + 1$ and $U_{43} - 1$. We call \mathcal{I} the *Eisenstein ideal*, but note that a choice has been made, and that there are two “Eisenstein ideals” of this level; the other choice is to replace $U_{13} + 1$ and $U_{43} - 1$ with $U_{13} - 1$ and $U_{43} + 1$. (The two other choices of sign corresponds to factors of J where the L -function is forced to vanish because the sign in the functional equation is -1 .) We find (see Section 4.1) that $\mathbf{T}/\mathcal{I} \simeq \mathbf{Z}/(2 \cdot 7^2)\mathbf{Z}$. Let $\mathfrak{m} = (7) + \mathcal{I}$, and note that \mathfrak{m} is maximal since $\mathbf{T}/((7) + \mathfrak{I}) \cong \mathbf{Z}/7\mathbf{Z}$. Let

$$\mathfrak{J} = \bigcap_{k \geq 0} (7, \mathfrak{m}^k)$$

and let $\mathbf{T}_7 = \mathbf{T} \otimes_{\mathbf{Z}} \mathbf{Z}_7$ be the 7-adic completion of \mathbf{T} .

Let A be the new simple abelian subvariety at J such that $A[\mathfrak{m}]$ is nontrivial. This determines A uniquely.³ It is a fifteen-dimensional geometrically-simple abelian variety, and is associated to a normalized Hecke eigenform $f = \sum a_n q^n \in S_2(\Gamma_0(559), \overline{\mathbf{Q}})$. There are two natural degeneracy maps $\alpha, \beta : J_0(43) \rightarrow J$. Since $X_0(p\ell) \rightarrow X_0(p)$ is totally ramified [7], it follows that both maps are injections.⁴ Let J_{old} be the sum of the images of α and β . The kernel of $J_0(43) \times J_0(43) \rightarrow J_{\text{old}}$ is isomorphic to the Shimura subgroup Σ anti-diagonally embedded in the product (see [8, Thm. 4.3]).

Let \mathcal{O} be the ring generated over \mathbf{Z} by the coefficients a_n of f . The surjection $\mathbf{T} \rightarrow \mathcal{O}$ gives rise to a map $\mathbf{T}_{\mathfrak{m}} \rightarrow \mathcal{O}_{\mathfrak{m}}$. The ring $\mathcal{O}_{\mathfrak{m}}$ has index 7 inside its integral closure.⁵ One usually says in this situation that 7 is a prime of “self-fusion”, since it implies the existence of a congruence between f and a Galois conjugate f^σ , modulo some prime above 7. Congruences $f \equiv g$ between non-conjugate eigenforms give rise to primes of fusion. The prime 7 is also a prime of fusion for A , since f is congruent modulo \mathfrak{m} to g , where g is one of the two old forms associated to the unique cusp form of level 43. These simultaneous pathologies (Eisenstein, fusion, self-fusion) occur for levels less than 559 only at the prime two.⁶ We shall also see that 7 divides the degree of the modular polarization $A \rightarrow A^\vee$. We start by proving the following:

Theorem 2.1. *We have the following equalities and identifications, where all dimensions are over $\mathbf{F}_7 \cong \mathbf{T}/\mathfrak{m}$:*

- (1) $\dim A[\mathfrak{m}] = 3$.
- (2) $\mathfrak{J}\mathbf{T}_7 = (\mathfrak{m}^k, 7)\mathbf{T}_7$ for $k \geq 2$.

³William: A computation.

⁴William: I couldn’t find the totally ramified assertion in [7]; if it is there we should give a precise reference. Also, why this implies injective is a general fact, but I still think we should give a reference for that. If [7] doesn’t work out as a reference, Ribet’s level raising paper discusses this sort of thing and certainly has enough to get injectivity (since he proves that the kernel of the sum of both maps is the anti-diagonal Shimura subgroup).

⁵William: A calculation.

⁶William: A computation that requires justification.

(3) $\dim A[(\mathfrak{m}^k, 7)] = 4$, for $k \geq 2$.

(4) If $A_{\text{old}} := A \cap J_{\text{old}}$, then

(a) $\dim A_{\text{old}}[\mathfrak{m}] = 2$,

(b) $\mathbf{Z}/7\mathbf{Z} \subset A_{\text{old}}[\mathfrak{m}]$, where $\mathbf{Z}/7\mathbf{Z}$ is the intersection of A with the image of the cuspidal subgroup of J_{old} .

Proof. The identification of \mathfrak{J} follows by a consideration of q -expansions. All the other results can essentially be proved by computations over the complex numbers.⁷ The only arithmetic input is to understand the cuspidal subgroup of J_{old} , but this is completely described by [3]. For part (1) it suffices to consider finitely many Hecke operators, by the Sturm bound (see the appendix to [2]). \square

Part (1) of Theorem 2.1 shows that A does not satisfy “multiplicity one” at the Eisenstein prime \mathfrak{m} . Calculation (2) reflects the fact that $\mathcal{O}_{\mathfrak{m}}$ has rank two over \mathbf{Z}_7 . Calculation (3) uses William’s exact “intersection” routine inside J .⁸

Let us consider further the Hecke algebra structure of \mathbf{T} on A .

Definition 2.2. Let \mathcal{O} be the image of \mathbf{T} in $\text{End}(A)$. Let $\mathcal{O}_{\mathfrak{m}}$ denote the localization of \mathcal{O} at the image of \mathfrak{m} .

Lemma 2.3. *The ring $\mathcal{O}_{\mathfrak{m}}$ is the unique index 7 ring inside the Witt vectors $W(\mathbf{F}_{49})$. There is an isomorphism*

$$\mathcal{O}_{\mathfrak{m}}/(7) \simeq \mathbf{F}_7[\epsilon]/\epsilon^2.$$

Proof. The Hecke algebra is finitely generated, and an explicit list of generators may be found from [2, App.]. The lemma follows by calculation.⁹ \square

These rings are *explicitly computable*, i.e., one may find a Hecke operator $\epsilon \in \mathbf{T}$ that gives rise to this isomorphism. This will be important below. One way to construct an element ϵ is to consider the Hecke operators

$$\eta_{\ell} = 1 + \ell - T_{\ell}$$

for various primes $\ell \neq 13, 43$. They will *a priori* land in \mathfrak{m} , but by the Chebotarev density theorem will land in \mathfrak{J} infinitely often. If $\mathcal{O}_{\mathfrak{m}}/7$ is generated by η_{ℓ} over \mathbf{F}_7 then we say that ℓ is a *good prime*. Note that $\mathfrak{m}\mathcal{O}_{\mathfrak{m}}$ is equal to $(7, \eta_{\ell})$ for a good prime ℓ , but $\mathfrak{m}\mathcal{O}_{\mathfrak{m}}$ is not generated by η_{ℓ} ; indeed, the maximal ideal $\mathfrak{m}\mathcal{O}_{\mathfrak{m}}$ cannot be generated by a single element since $\mathcal{O}_{\mathfrak{m}}$ is not a discrete valuation ring.

⁷Frank: as William explains

⁸William: I’ll rewrite.

⁹William: A calc.

Definition 2.4. Consider its Jordan–Hölder factors of a Galois module G . Let $\delta(G)$ denote the number of times $\mathbf{Z}/7\mathbf{Z}$ occurs as a factor minus the number of occurrences of μ_7 . For an abelian variety B , let $\delta_B(n)$ denote $\delta(B[7^n])$.

Lemma 2.5. *We have $\delta_A(n) = \delta_{A^\vee}(n) = 0$, and $\delta(A[\mathfrak{J}]) = \delta(A[\mathfrak{m}^2, 7]) = 0$.*

Proof. Note that δ is additive in exact sequences. Since $A[7^n]$ has a filtration by copies of $A[7]$ it follows that $\delta_A(n) = n\delta_A(1)$. Since A^\vee is dual to A it follows that $\delta_{A^\vee}(n) = -\delta_A(n)$. Thus

$$\delta_A(n) - \delta_{A^\vee}(n) = 2n\delta_A(1).$$

Yet A is isogenous to A^\vee , and thus $\delta_A(n) - \delta_{A^\vee}(n) = O(1)$. Hence $\delta_A(n) = \delta_{A^\vee}(n)$; but $\delta_A(n) = -\delta_{A^\vee}(n)$, so this proves the first part of the lemma. For the second it suffices to note that \mathfrak{m} is the unique Eisenstein prime (of A) with residue characteristic 7. \square

It follows from Lemma 2.5 that $A[\mathfrak{J}]$ has a filtration by two copies of $\mathbf{Z}/7$ and two copies of μ_7 . We may also control the constant and multiplicative submodules of $A[\mathfrak{J}]$:

Lemma 2.6. *The maximal constant Galois submodule of $A[\mathfrak{J}]$ is contained in $A[\mathfrak{m}]$. The maximal μ -type subgroup of $A[\mathfrak{J}]$ is also contained in $A[\mathfrak{m}]$.*

Proof. It suffices to prove that both constant Galois modules and μ -type Galois modules are killed by the Eisenstein ideal. Let M be a constant Galois module, and suppose that $M \subseteq A[\mathfrak{J}]$. Let $\ell \neq 7, 13, 43$. By the Eichler–Shimura relations the Frobenius element σ_ℓ acting on M satisfies the polynomial $x^2 - T_\ell x + \ell = 0$. Thus if M is constant it follows that $\eta_\ell = 1 + \ell - T_\ell$ kills M . Choosing ℓ to be a good prime it follows that M is killed by $(7, \eta_\ell) = \mathfrak{m}$, since $7 \in \mathfrak{J}$. Yet for good primes ℓ we have that $(7, \eta_\ell)\mathcal{O}_\mathfrak{m} = \mathfrak{m}\mathcal{O}_\mathfrak{m}$, and thus M is killed by \mathfrak{m} , and $M \subseteq A[\mathfrak{m}]$. An identical argument works for μ -type subgroups. \square

2.1 Determining the Jordan–Hölder factors of $A[\mathfrak{m}]$

As in [3] (§14, p.114), we see that the Galois module $A[\mathfrak{m}]$ has a filtration by modules of the form $\mathbf{Z}/7\mathbf{Z}$ and μ_7 , and correspondingly $A[\mathfrak{m}]$ considered as a group scheme over $\text{Spec}(\mathbf{Z}_7)$ or $\text{Spec}(\mathbf{F}_7)$ also has such a filtration (as one sees from [5]). By Theorem 2.1, we see that there is at least one copy of $\mathbf{Z}/7\mathbf{Z}$ that includes into $A[\mathfrak{m}]$. A general argument of Mazur [3] shows that all the other filtered pieces of μ_7 must be isomorphic to μ_7 .

Lemma 2.7. *Let N be an integer, let $p \nmid 2N$ be a prime, and let \mathfrak{m} be a maximal ideal of the Hecke algebra of residue characteristic p . Let $J[\mathfrak{m}]_{\mathbf{F}_p}^{\text{ét}}$ be the étale part of the group scheme $J_0(N)[\mathfrak{m}]_{\mathbf{F}_p}$. Then $J[\mathfrak{m}]_{\mathbf{F}_p}^{\text{ét}}$ is one dimensional.*

Proof. The argument of Mazur ([3], Cor 14.8, p.119) applies *mutatis mutandis*. \square

Note that this result does not imply that the p -torsion subgroup of $J_0(N)$ is cyclic, for $p \nmid N$, since different rational cyclic subgroups may be killed by different maximal Eisenstein ideals. The point is that the argument requires the q -expansion principal, which

is only valid if one works with the full Hecke algebra (i.e. specifying the action of U_ℓ for bad primes ℓ). Thus we infer that $A[\mathfrak{m}]/(\mathbf{Z}/7\mathbf{Z})$ has a filtration by two copies of μ_7 . We show that this second piece is a direct summand.

Lemma 2.8. *Let N be an integer, let $p \nmid 2N$, and let \mathfrak{m} be a maximal ideal of the Hecke algebra of residue characteristic p . Let V be a Galois module subquotient of $J[\mathfrak{m}]$ whose filtration consists either entirely of $(\mathbf{Z}/p\mathbf{Z})$'s or μ_p 's. Then V is a direct summand.*

Proof. We apply the same argument as in the proof of [3], Lemma 16.7, p. 126. Since V is a subquotient of $J[\mathfrak{m}]$, by the Eichler-Shimura relations any Frobenius element σ_ℓ satisfies the minimal polynomial $(x-1) \cdot (x-\ell) = 0$. Choose a prime $\ell \not\equiv 1 \pmod{p}$, possible since $p \neq 2$. Suppose that V has a filtration by constant pieces. Then $(\sigma_\ell - \ell)$ is an isomorphism on each filtered piece and thus has no kernel on V . It follows that $\sigma_\ell = 1$ on V . By the Chebotarev density theorem it follows that V is constant, so it is clearly a direct sum of constant modules. If V has a filtration by μ_p 's, then the same argument applied to V^\vee shows that V^\vee is also a direct summand of constant modules and thus V is a direct summand of multiplicative Galois modules. \square

Thus we have the following:

Lemma 2.9. 1. $\delta(A[\mathfrak{m}]) = -1$, and $A[\mathfrak{m}]$ sits inside an exact sequence of the form:

$$0 \rightarrow \mathbf{Z}/7\mathbf{Z} \rightarrow A[\mathfrak{m}] \rightarrow \mu_7 \oplus \mu_7 \rightarrow 0.$$

2. $A[\mathfrak{J}]/A[\mathfrak{m}] \simeq \mathbf{Z}/7\mathbf{Z}$.

Proof. The second claim follows from Lemma 2.5 which implies that

$$0 = \delta(A[\mathfrak{J}]) = \delta(A[\mathfrak{J}]/A[\mathfrak{m}]) + \delta(A[\mathfrak{m}]).$$

\square

2.2 Determining $A[\mathfrak{m}]$

We show now that the extension (1) of Lemma 2.9 is nontrivial.

Lemma 2.10. *Suppose that $A[\mathfrak{m}] \simeq \mathbf{Z}/7\mathbf{Z} \oplus (\mu_7)^2$. Then*

$$\eta_\ell = T_\ell - 1 - \ell \notin \mathfrak{J}$$

(equivalently, ℓ is a good prime) if and only if both conditions are satisfied:

1. $\ell \not\equiv 1 \pmod{7}$
2. ℓ is not a 7th power modulo 43.

Proof. Choosing an appropriate basis for $A[\mathfrak{J}]$ as a four dimensional \mathbf{F}_7 vector space we may write the action of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ as

$$\rho = \begin{pmatrix} 1 & 0 & 0 & a \\ 0 & \chi & 0 & b \\ 0 & 0 & \chi & c \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where χ is the cyclotomic character, and a , b and c are functions on $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. We compute that

$$(\rho(\sigma) - 1)(\rho(\sigma) - \chi(\sigma)) = (\chi(\sigma) - 1) \begin{pmatrix} 0 & 0 & 0 & a(\sigma) \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

Since $\mathfrak{J} \neq \mathfrak{m}$ it follows that a is nontrivial. Moreover, we see that a prime ℓ is good if and only if $\ell \not\equiv 1 \pmod{7}$ and $a(\text{Frob}_\ell)$ is nontrivial. The function a defines an extension class inside $\text{Ext}^1(\mathbf{Z}/7\mathbf{Z}, \mathbf{Z}/7\mathbf{Z})$. These extensions are taking place inside the category of finite flat group schemes over $\mathbf{Z}[1/559]$. Such extensions are étale, and thus the generic fibre defines a degree 7 field unramified over \mathbf{Q} outside 559. The only such extension is the degree 7 extension inside $\mathbf{Q}(\zeta_{43})$, since $7 \nmid 13 - 1$. Thus if $\sigma = \text{Frob}_\ell$, then $a(\sigma) = 0$ if and only if ℓ splits completely in this degree 7 field. This is equivalent to ℓ being a 7th power modulo 43. This proves one implication. Now assume that either $\ell \equiv 1 \pmod{7}$ or ℓ is a 7th power modulo 43. Then if $\sigma = \text{Frob}_\ell$ and $x = \rho(\sigma)$, then $(x - 1)(x - \ell) = 0$. Thus

$$0 = x^2 - T_\ell x + \ell = (x - 1)(x - \ell) + (T_\ell - 1 - \ell)x = \eta_\ell x.$$

Since $x = \rho(\sigma)$ is invertible, this implies that $\eta_\ell = 0$, and thus ℓ is not a good prime. This proves the lemma. \square

It is easy to compute that $\eta_2 \in \mathfrak{J}$ and thus 2 is not a good prime. By the previous lemma this implies that $A[\mathfrak{m}] \neq \mathbf{Z}/7\mathbf{Z} \oplus \mu_7 \oplus \mu_7$.

To sum up what we know so far, the action of Galois on $A[\mathfrak{J}] = A[7, \mathfrak{m}^2]$ can be written as follows:

$$\rho(\sigma) = \begin{pmatrix} 1 & x & y & a \\ 0 & \chi & 0 & b \\ 0 & 0 & \chi & c \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

Where x , y , a , b and c are all continuous functions of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$, and x and y are not both zero. We may also assume that the first 2×2 matrix represents the action of Galois on $A_{\text{old}}[\mathfrak{m}]$. Since $A^\vee[\mathfrak{J}]$ is the Cartier dual to $A[\mathfrak{J}]$ we also understand the Galois action on

$A^\vee[\mathfrak{J}]$. Explicitly, it is given by $\chi\rho^{-1}$ which is

$$\rho^\vee(\sigma) = \begin{pmatrix} \chi & -c & -b & a' \\ 0 & 1 & 0 & -y \\ 0 & 0 & 1 & -x \\ 0 & 0 & 0 & \chi \end{pmatrix},$$

Lemma 2.11. *At least one of b and c is nonzero, and thus there is no surjection $A[\mathfrak{J}] \rightarrow \mu_7 \oplus \mu_7$ and no inclusion $\mathbf{Z}/7\mathbf{Z} \oplus \mathbf{Z}/7\mathbf{Z} \rightarrow A^\vee[\mathfrak{J}]$.*

Proof. If both b and c are zero then one finds that any $\ell \equiv 1 \pmod{7}$ cannot be a good prime (that is, η_ℓ must kill $A[\mathfrak{J}]$). Yet this contradicts the fact that 29 is a good prime (as one can compute).¹⁰ □ 10

It follows that the torsion subgroup of $A^\vee[\mathfrak{J}]$ has order at most 7.

Lemma 2.12. *We have $c \neq 0$, and $b = 0$.*

Proof. There is an injective map $A[\mathfrak{J}]/A_{\text{old}}[\mathfrak{m}] \rightarrow A^\vee[\mathfrak{m}]$.¹¹ If $c = 0$ then the image contains a rational 7-torsion point. Yet the intersection of the image with the cuspidal torsion group of A^\vee is zero,¹² and thus $A^\vee[\mathfrak{J}]$ would contain two linearly disjoint rational subgroups of order 7, contradicting Lemma 2.11. Thus $c \neq 0$. On the other hand, there is a rational torsion point of order 7 in $A^\vee[\mathfrak{m}]$,¹³ and thus (changing bases slightly if necessary) we have that $b = 0$. □ 13

Let us now determine the extensions c and x .

Lemma 2.13. *The extensions c and x are unramified at 13, and the class y is nontrivial.*

Proof. The claim for x follows from the fact that $A_{\text{old}}[\mathfrak{m}]$ is unramified at 13, by the criterion of Néron–Ogg–Shafarevich applied to $J_0(43)$. This determines the class of x uniquely. The class c corresponds to an extension of the form $\mathbf{Q}(\zeta_7, \sqrt[7]{D})$, where $D = 43 \cdot 13^k$ for some k or $D = 13$. To determine it explicitly we prove the following Sub-lemma, which is a variation on Lemma 2.10:

Sub-lemma 1. *Fix a D whose only prime divisors lie in the set $\{13, 43\}$. Let $K = \mathbf{Q}(\zeta_7, \sqrt[7]{D})$. Suppose that the class c becomes trivial over K . Let $\ell \equiv 1 \pmod{7}$ and suppose that ℓ splits completely in K . Then η_ℓ is not a good prime. Equivalently,*

$$\eta_\ell = T_\ell - 1 - \ell \equiv 0 \pmod{\mathfrak{J}}.$$

¹⁰William: A calc.

¹¹Frank: This is this a calculation for William.

¹²William: A calc.

¹³William: a calc.

Proof. Choosing an appropriate basis for $A[\mathfrak{J}]$ as a four dimensional \mathbf{F}_7 vector space we may write the action of $\sigma \in \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ as

$$\rho(\sigma) = \begin{pmatrix} 1 & x & y & a \\ 0 & \chi & 0 & 0 \\ 0 & 0 & \chi & c \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

where χ is the cyclotomic character, and a, c, x, y are functions on $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. Suppose that $\sigma = \text{Frob}_\ell$, and that $\ell \equiv 1 \pmod{7}$ so $\chi(\sigma) = 1$. We compute that

$$(\rho(\sigma) - 1)^2 = \begin{pmatrix} 0 & 0 & 0 & c(\sigma)y(\sigma) \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \\ 0 & 0 & 0 & 0 \end{pmatrix}$$

If ℓ splits completely in K then $c(\text{Frob}_\ell) = 0$. Now letting $x = \rho(\sigma)$, and remembering that $\ell \equiv 1 \pmod{7}$, we find that

$$0 = x^2 - T_\ell x + 1 = (x - 1)^2 + \eta_\ell x = \eta_\ell x.$$

Since x is invertible, it follows that η_ℓ annihilates $A[\mathfrak{J}]$ and thus $\eta_\ell \in \mathfrak{J}$. □

The following table gives the smallest prime that splits completely in $\mathbf{Q}(\zeta_7, \sqrt[7]{D})$ for various D :¹⁴

D	43	$43 \cdot 13$	$43 \cdot 13^2$	$43 \cdot 13^3$	$43 \cdot 13^4$	$43 \cdot 13^5$	$43 \cdot 13^6$	13
ℓ	631	211	29	337	281	197	239	421
$T_\ell \in \mathfrak{J}$	Yes	No	No	No	No	No	No	No

Thus the only possibility for c is that it becomes trivial in $\mathbf{Q}(\zeta_7, \sqrt[7]{43})$. As a double check of our computations, we find the next few primes that split completely in $\mathbf{Q}(\zeta_7, \sqrt[7]{43})$. They are 659, 1009, 1289 and 1933. We check in all of these cases that $T_\ell \in \mathfrak{J}$. Thus $D = 43$ and c is unramified at 13. We also conclude from these calculations that $y \neq 0$, completing the proof of Lemma 2.13. □

2.3 The torsion subgroup of A and A^\vee

We may write the action of Galois on $A[\mathfrak{J}] = A[7, \mathfrak{m}^2]$ as follows:

$$\rho(\sigma) = \begin{pmatrix} 1 & x & y & a \\ 0 & \chi & 0 & b \\ 0 & 0 & \chi & c \\ 0 & 0 & 0 & 1 \end{pmatrix},$$

¹⁴William: Explain how computed.

Where x, y, a, b and c are all continuous functions of $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$. We may also assume that the first 2×2 matrix represents the action of Galois on $A_{\text{old}}[\mathfrak{m}]$.

Theorem 2.14. *The rational 7-torsion subgroups of A and A^\vee are exactly $\mathbf{Z}/7$.*

Proof. The cuspidal torsion subgroup of $A^\vee[7]$ is $\mathbf{Z}/7$, as can be computed.¹⁵ Suppose that there was an inclusion $\pi : \mathbf{Z}/7 \oplus \mathbf{Z}/7 \subseteq A^\vee[7]$. Then considering the Cartier dual there would be a section

$$\pi^\vee : A[\mathfrak{J}] \rightarrow \mu_7 \oplus \mu_7$$

which contradicts lemma 2.11. □

Note, that this just proves that the rational 7-torsion of A^\vee has rank one. We prove now that there are no points of order 49.

Theorem 2.15. *The 7-Sylow subgroups of $A_{\text{tors}}(\mathbf{Q})$ and $A_{\text{tors}}^\vee(\mathbf{Q})$ have degree 7.*

Proof. Since all rational torsion of A is contained in $A[\mathfrak{m}]$ by Lemma 2.6, the first claim has already been proved. For the second, consider the variety $A' = A^\vee/\mu_7$. Then from our explicit description of the Galois action on 7-torsion we find that $\mathbf{Z}/7 \oplus \mathbf{Z}/7 \subset A'[7]$. Suppose that $\mathbf{Z}/49\mathbf{Z} \subset A_{\text{tors}}^\vee(\mathbf{Q})$. Then since the torsion of A^\vee injects into the torsion of A' the torsion subgroup of A' must have order divisible by 343. This contradicts the multiple of torsion computed earlier.¹⁶ □

2.4 Conjectural Computations with the BSD conjecture

17

2.5 Remarks on the Structure of the Tate Module

An important ingredient in our calculations was explicitly working with the action of the completed Hecke algebra $\mathbf{T}_\mathfrak{m}$ on the Tate module $A^{(\mathfrak{m})}$. What is the structure of this module? We know that as a $\mathbf{T}_\mathfrak{m}$ module, it is torsion free, and has “rank two” in the sense that $A^{(\mathfrak{m})} \otimes \mathbf{Q}$ is a free $\mathbf{T}_\mathfrak{m} \otimes \mathbf{Q}$ of rank two. In general the structure of finite rank torsion free modules over a local domain can be quite difficult (except in the case of a discrete valuation ring, of course!). However, certain special rings admit a nice description of their finite rank modules.

Definition 2.16. Let R be a local domain of dimension one with maximal ideal \mathfrak{m} . Let \tilde{R} denote the integral closure of R . Suppose that every ring R' such that $R \subseteq R' \subseteq \tilde{R}$ is Gorenstein. Then R is a Bass ring.

¹⁵William: A calc.

¹⁶William: Ref to the calc.

¹⁷Frank: Here William writes down BSD and shows how in this case it implies that the odd part of $\text{III}(A)$ is trivial.

For example, let \tilde{R} be the Witt vectors $W(\mathbf{F}_q)$ for $q = p^f$, let π be the reduction map $\pi : \tilde{R} \rightarrow \mathbf{F}_q$, and let $R = \pi^{-1}(\mathbf{F}_p)$. Then R is a Bass ring. Taking the example $q = 49$ and $f = 2$ we find that $R = \mathbf{T}_m$ is a Bass ring.

The following theorem answers our questions about modules for Bass rings.

Theorem 2.17. *Let R be a Bass ring. Then any torsion free module of rank n is a direct sum of rank one modules M isomorphic to a subring R' satisfying*

$$R \subseteq R' \subseteq \tilde{R}.$$

In our examples, this implies that the only rank one modules of \mathcal{O}_m are either \mathcal{O}_m or $\tilde{\mathcal{O}}_m$. Since $\dim(\mathcal{O}_m/\mathfrak{m}) = 1$ and $\dim(\tilde{\mathcal{O}}_m/\mathfrak{m}) = 2$ we conclude the following:

Lemma 2.18. *There is an isomorphism of Hecke modules*

$$A^{(\mathfrak{m})} \simeq \mathcal{O}_m \oplus \tilde{\mathcal{O}}_m.$$

3 The Descent

The goal of this section is to prove that $\text{III}(A)[\mathfrak{m}]$ is trivial and that $A(\mathbf{Q})$ has rank 0.

It turns out to be easier to compute the descent on A^\vee rather than A . Let $S = \text{Spec}(\mathbf{Z})$. Let \mathcal{A} be the Néron model of A^\vee over S , and note that $\mathcal{A}[\mathfrak{J}]$ equals $\mathcal{A}[7] \otimes_{\mathbf{T}_7} \mathbf{T}_m$. For a group scheme G/S and a finite set of primes Σ let $G^{b(\Sigma)}$ denote the quasi-finite group scheme over S obtained from G by removing the special fibres at primes in Σ . We have the following exact diagram of quasi-finite group schemes over S :

$$\begin{array}{ccccccc}
 & & 0 & & & & \\
 & & \downarrow & & & & \\
 & & \mathcal{M} & & & & \\
 0 & \longrightarrow & \mu_7 & \longrightarrow & \mathcal{M} & \longrightarrow & (\mathbf{Z}/7\mathbf{Z})^{b(43)} \longrightarrow 0 \\
 & & \updownarrow & & \updownarrow & & \\
 & & \mathcal{A}[\mathfrak{m}] & & \mathcal{A}[\mathfrak{J}] & & \\
 0 & \longrightarrow & \mathcal{A}[\mathfrak{m}] & \longrightarrow & \mathcal{A}[\mathfrak{J}] & \longrightarrow & (\mu_7)^{b(\Sigma)} \longrightarrow 0 \\
 & & \updownarrow & & \updownarrow & & \\
 & & \mathbf{Z}/7\mathbf{Z} & & & & \\
 & & \downarrow & & & & \\
 & & 0 & & & &
 \end{array}$$

Where the up and down arrows correspond to the fact that there exists sections, and Σ is a subset of $\{13, 43\}$. The inclusions $\mu_7, \mathbf{Z}/7\mathbf{Z} \rightarrow \mathcal{A}[\mathfrak{m}]$ exist because of the corresponding inclusions of Galois modules and the Néron mapping property applied to \mathcal{A} . The identity $\mathcal{M}/\mu_7 = (\mathbf{Z}/7\mathbf{Z})^{\flat(43)}$ similarly follows from the fact that the Galois module underlying \mathcal{M} is ramified at 43 and unramified at 13 (the corresponding extension class is c , which we identified by Lemma 2.13) and the Néron mapping property. We note that $43 \in \Sigma$ because the extension class x is ramified at 43, by Lemma 2.13. Now we make the following observations on *fppf* cohomology for $S = \text{Spec}(\mathbf{Z})$ (see for example [3], p.48):

Lemma 3.1. *The following hold.*

1. $H^i(S, \mathbf{Z}/7\mathbf{Z}) = H^i(S, \mu_7) = 0$ for $i = 1, 2$.
2. $H^1(S, (\mathbf{Z}/7\mathbf{Z})^{\flat(43)}) = 0$, and $H^2(S, (\mathbf{Z}/7\mathbf{Z})^{\flat(43)})$ is one dimensional.
3. $H^1(S, \mathcal{M}) = 0$, and $H^2(S, \mathcal{M}) = H^2(S, (\mathbf{Z}/7\mathbf{Z})^{\flat(43)})$.
4. $H^1(S, \mathcal{A}[\mathfrak{m}]) = 0$, and $H^2(S, \mathcal{A}[\mathfrak{m}]) = H^2(S, (\mathbf{Z}/7\mathbf{Z})^{\flat(43)})$.
5. $H^1(S, \mathcal{A}[\mathfrak{J}]) = 0$.
6. If Φ is the component group of \mathcal{A} then $H^0(S, \Phi) \otimes \mathbf{Z}_7 = \mathbf{Z}/7\mathbf{Z}$.
7. The map $H^0(\mathcal{A}) \rightarrow H^0(\Phi)$ is surjective.

Proof. We prove each item in turn.

1. This follows from the discussion in [3], p.48, p.49.
2. Again we follow [3], p.48, p.49. There is an exact sequence

$$0 \rightarrow (\mathbf{Z}/7\mathbf{Z})^{\flat(43)} \rightarrow \mathbf{Z}/7\mathbf{Z} \rightarrow \phi \rightarrow 0$$

for some skyscraper sheaf ϕ supported in characteristic 43. Taking global sections we see that $H^0(S, \mathbf{Z}/7\mathbf{Z})$ surjects onto $H^0(S, \phi) = \mathbf{Z}/7\mathbf{Z}$ and thus $H^1(S, (\mathbf{Z}/7\mathbf{Z})^{\flat(43)})$ injects into $H^1(S, \mathbf{Z}/7\mathbf{Z}) = 0$. On the other hand, from part one we also conclude that $H^2(S, (\mathbf{Z}/7\mathbf{Z})^{\flat(43)}) = H^1(S, \phi)$ is one dimensional.

3. This follows from the long exact sequence of cohomology, and parts one and two.
4. Since $\mathcal{A}[\mathfrak{m}] = \mathcal{M} \oplus \mathbf{Z}/7\mathbf{Z}$, we have $H^i(S, \mathcal{A}[\mathfrak{m}]) = H^i(S, \mathcal{M}) \oplus H^i(S, \mathbf{Z}/7\mathbf{Z})$.
5. The long exact sequence of cohomology gives an exact sequence

$$0 \rightarrow H^1(S, \mathcal{A}[\mathfrak{J}]) \rightarrow H^1(S, (\mu_7)^{\flat(\Sigma)}) \rightarrow H^2(S, \mathcal{A}[\mathfrak{m}])$$

Now the exact sequence

$$0 \rightarrow (\mu_7)^{\flat(\Sigma)} \rightarrow \mu_7 \rightarrow \psi \rightarrow 0$$

shows that $H^0(S, \psi) = H^1(S, (\mu_7)^{b(\Sigma)})$. Since

$$H^0(S, \psi) = \bigoplus_{p \in \Sigma} \mu_7(\mathbf{F}_p)$$

and since \mathbf{F}_{13} has no 7th roots of unity we see that the dimension of $H^1(S, (\mu_7)^{b(\Sigma)})$ is the dimension of $\mu_7(\mathbf{F}_{43})$, which is one. On the other hand, the target of the coboundary map $H^2(S, \mathcal{A}[\mathfrak{m}]) \simeq H^1(S, (\mathbf{Z}/7\mathbf{Z})^{b(43)})$ is one dimensional also. Thus it suffices to show that the coboundary map

$$\mu_7(\mathbf{F}_{43}) \simeq H^1(S, (\mu_7)^{b(\Sigma)}) \longrightarrow H^1(S, (\mathbf{Z}/7\mathbf{Z})^{b(43)}) \simeq H^1(S, \phi)$$

is nontrivial. Perhaps more helpfully, this boundary map is the same as the one coming from the associated long exact sequence of the following long exact sequence:

$$0 \rightarrow (\mathbf{Z}/7\mathbf{Z})^{b(43)} \rightarrow \mathcal{N} \rightarrow (\mu_7)^{b(\Sigma)} \rightarrow 0,$$

Where $\mathcal{N} = \mathcal{A}[\mathfrak{J}]/(\mathbf{Z}/7\mathbf{Z} \oplus \mu_7)$. The Galois extension corresponding to the generic fibre of \mathcal{N} is given by extension class y .¹⁸

18

6. This follows from the [3], Appendix, Thm. A.1.

7. This follows from the identification of Φ above and a computation...¹⁹

19

□

Let us consider the usual descent sequence:

$$\begin{array}{ccccccc} 0 & \longrightarrow & \mathcal{A}^0 & \longrightarrow & \mathcal{A} & \longrightarrow & \Phi \longrightarrow 0 \\ & & \uparrow & \nearrow 7 & \uparrow & & \\ 0 & \longrightarrow & \mathcal{A}[\mathfrak{J}] & \longrightarrow & \mathcal{A} & \longrightarrow & \mathcal{A}^0 \longrightarrow 0 \end{array}$$

Let M be the Mordell–Weil group of A . By the Néron mapping property $M = \mathcal{A}(S)$. Let $M^0 = \mathcal{A}^0(S)$. Taking cohomology and using parts 5 & 7 of Lemma 3.1, we get the following exact diagram²⁰, where by abuse of notation we consider everything (as in [3] p.150) in the category of \mathbf{T} -modules modulo the category of \mathbf{T} -modules whose support lies in some finite set Δ containing all primes of characteristic seven besides \mathfrak{m} .

¹⁸Frank: To myself, this is what needs to be completed.

¹⁹Frank: Is this right? Or is it obvious

²⁰William, Make the map $M \rightarrow \mathbf{Z}/7\mathbf{Z}$ a surjective arrow

$$\begin{array}{ccccccccccccccc}
0 & \longrightarrow & M^0 & \longrightarrow & M & \longrightarrow & \mathbf{Z}/7\mathbf{Z} & \longrightarrow & H^1(\mathcal{A}^0) & \longrightarrow & H^1(\mathcal{A}) \\
& & \uparrow & \nearrow 7 & \uparrow & & & & \uparrow & \nearrow 7 & \uparrow \\
0 & \longrightarrow & \mathbf{Z}/7\mathbf{Z} & \longrightarrow & M & \longrightarrow & M^0 & \longrightarrow & 0 & \longrightarrow & H^1(\mathcal{A}) & \longrightarrow & H^1(\mathcal{A}^0)
\end{array}$$

From this diagram we easily conclude that $M \simeq \mathbf{Z}/7\mathbf{Z}$. It also follows that the multiplication by 7 map on $H^1(\mathcal{A})$ is injective (modulo \mathbf{T} -modules with support outside \mathfrak{m}), and thus that $H^1(\mathcal{A})[\mathfrak{m}] = 0$. By [4], Prop, p.263, the Tate–Shafarevich group $\text{III}(A)$ injects into $H^1(\mathcal{A})$, and thus it follows that $\text{III}(A)[\mathfrak{m}] = 0$.

4 Algorithms

In this section we explain the algorithms we use to verify the computational assertions that appear elsewhere in this paper.

4.1 The quotient by the Eisenstein ideal

References

- [AS05] Agashe Agashe and William Stein, *Visible evidence for the Birch and Swinnerton-Dyer conjecture for modular abelian varieties of analytic rank zero*, Math. Comp. **74** (2005), no. 249, 455–484 (electronic), With an appendix by J. Cremona and B. Mazur, <http://wstein.org/papers/shacomp/>.
- [1] F. Calegari, M. Emerton. *Ramification of Hecke Algebras at Eisenstein Primes*, submitted.
- [2] Joan-C. Lario and René Schoof, *Some computations with Hecke rings and deformation rings*, Experiment. Math. **11** (2002), no. 2, 303–311, With an appendix by Amod Agashe and William Stein.
- [3] B. Mazur. *Modular curves and the Eisenstein ideal*, Publ. Math. IHES **47**(1977), 33–186
- [4] B. Mazur. *Rational points of abelian varieties with values in towers of number fields*, Invent. Math. **18**(1972), 183–266.
- [5] F. Oort, J. Tate. *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3**(1970) 1–21.

- [6] M. Raynaud. *Schémas en groupes de type (p, \dots, p)* , Bull. Soc. Math. France **102**(1974), 241–280.
- [7] K. A. Ribet. *A modular construction of unramified p -extensions of $\mathbf{Q}(\zeta_p)$* , Invent. Math. **34**, (1976), no. 3, 151–162.
- [8] Kenneth A. Ribet, *Congruence relations between modular forms*, Proc. International Congress of Mathematicians (1983), 503–514.
- [9] K. A. Ribet and W. A. Stein, *Lectures on Serre’s conjectures*, Arithmetic algebraic geometry (Park City, UT, 1999), IAS/Park City Math. Ser., vol. 9, Amer. Math. Soc., Providence, RI, 2001, pp. 143–232.