Kolyvagin Derivatives of Modular Points on Elliptic Curves

Richard Hatton

Abstract

Let $E/\mathbb{Q}$ and $A/\mathbb{Q}$ be elliptic curves. We can construct modular points derived from $A$ via the modular parametrisation of $E$. With certain assumptions we can show that these points are of infinite order and are not divisible by a prime $p$. In particular, using Kolyvagin’s construction of derivative classes, we can find elements in certain Shafarevich-Tate groups of order $p^n$.

INTRODUCTION

Let $E/\mathbb{Q}$ be an elliptic curve with conductor $N_E$. Then due to the modularity theorem, there exists a surjective morphism

$$\phi_E : X_0(N_E) \to E$$

defined over $\mathbb{Q}$ known as the modular parametrisation of $E$, where $\infty$ on the modular curve $X_0(N_E)$ is mapped to $O$. We can view $X_0(N_E)$ as a moduli space of points $x_{A,C} = (A, C)$ for $A$ an elliptic curve and $C$ a cyclic subgroup of $A$ of order $N_E$. Fixing $A/\mathbb{Q}$, the image of $x_{A,C}$ under $\phi_E$ is known as a modular point, which we will denote $P_{A,C} \in E(\mathbb{Q}(C))$ where $\mathbb{Q}(C)$ is the field of definition of $C$. We denote the compositium of all such $\mathbb{Q}(C)$ as $K_{N_E}$. This is the smallest field $K$ such that its absolute Galois group $G_K$ acts by scalars on $A[N_E]$. This has Galois group $G_{N_E} := \text{Gal}(K_{N_E}/\mathbb{Q})$ which can be identified as a subgroup of $\text{PGL}_2(\mathbb{Z}/N_E\mathbb{Z})$ via the mapping

$$\tau_{Q,A,N_E} : G_Q \to \text{Aut}(A[N_E]) \cong \text{GL}_2(\mathbb{Z}/N_E\mathbb{Z}) \to \text{PGL}_2(\mathbb{Z}/N_E\mathbb{Z})$$.

We can also define higher modular points above $P_{A,C}$. These are points of the form $\phi_E(B, D)$ for an elliptic curve $B$ isogenous to $A$ over $\overline{\mathbb{Q}}$ and $D \leq B$ cyclic of order $N_E$. We look at isogenies of degree $p^n$ for some prime $p$ of good or multiplicative reduction with respect to $E$ and $n \geq 1$.

Kolyvagin initially looked at how Heegner points can be used to bound Selmer groups in [9]. This involved creating cohomology classes coming from these points and using the classes to bound the Selmer groups from above.

Wuthrich then worked on an analogue system to Kolyvagin’s work in [13] where he uses a type of modular point known as self points to create derivative classes and finds lower bounds of Selmer groups over certain fields. In this paper, we look to extend the idea of self points to a general modular point. We end up with similar findings to that in [13] but can also show further that Selmer groups over certain fields must contain points of prime power order when the higher modular points satisfy certain conditions.

In the first section, we look at the divisibility of the modular points in $E(\mathbb{Q}(C))$. Initially, we want to see when the modular points are of infinite order. We obtain the following result.
Lemma 0.1. Let $E/\mathbb{Q}$ be an elliptic curve of conductor $N_E$. Let $A/\mathbb{Q}$ be an elliptic curve such that the $j$ invariant of $A$ is not in $\frac{1}{2}\mathbb{Z}$ and the degree of any isogeny of $A$ defined over $\mathbb{Q}$ is coprime to $N_E$. Then the modular points $P_{A,C}$ are of infinite order for all cyclic subgroups $C$ of order $N_E$ in $A$.

From this, we can show that if $p$ is a prime with specific conditions related to $E$, then $P_{A,C}$ is not $p$-divisible in $E(\mathbb{Q}(C))$ as seen in Lemma 2.4. We also find relationships between the modular points. That is, if $d$ is a divisor of $N_E$ and $B \leq A$ is cyclic of order $d$, then the sum of $P_{A,C}$ over $C \supset B$ is torsion. This reduces the rank of the group generated by these points.

If we let $G_n := \text{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ for $n \geq 0$, we will see that we can relate the group generated by the modular points to certain $\mathbb{Z}_p[G_n]$-lattices in $V_n = \ker \left( \mathbb{Q}_p[G_n/B_n] \rightarrow \mathbb{Q}_p \right)$ for $p$ prime and $B_n$ a Borel subgroup of $G_n$. We can view $V_n$ in the following way

$$V_n = \left\{ f : P^1_n \rightarrow \mathbb{Q}_p : \sum_C f(C) = 0 \right\}$$

where $P^1_n := P^1(\mathbb{Z}/p^{n+1}\mathbb{Z})$. This contains the standard lattice

$$T_n = \ker \left( \mathbb{Z}_p[G_n/B_n] \rightarrow \mathbb{Z}_p \right),$$

which we can easily understand the cohomology of with respect to subgroups of $G_n$. Hence, we take a look at the representation theory of $G_n$ and will later look at the application of this to the modular points.

We then take a look at a specific case of creating higher modular points for a prime $p$ of either good ordinary or multiplicative reduction with respect to $E$. Here, we will look at the case where $p$ is coprime to $N_E$. Let $D$ be a cyclic subgroup of $A$ of order $p^{n+1}$ for prime $p$ and $n \geq 0$. We look at the higher modular point coming from $(A/D, \psi(C))$ where $\psi : A \rightarrow A/D$ is the isogeny defined by $D$. We define $Q_{A,D} = \phi_E(A/D, \psi(C)) \in E(\mathbb{Q}(C,D))$. We see that the higher modular points form a trace-compatible system with

$$a_p(E) \cdot Q_{A,D} = \sum_{D' \supset D} Q_{A,D'}$$

where the sum is taken over the subgroups $D'$ of $A$ of order $p^{n+2}$ containing $D$ and $a_p(E)$ is the $p$-th Fourier coefficient for the modular form associated to the isogeny class of $E$. This results in showing that the higher modular points generate a group of rank $p^{n+1} + p^n$ as seen in Lemma 4.3.

We then look to follow a similar procedure to Wuthrich in [13] from the ideas of Kolyvagin in [9]. We create derivative classes coming from higher modular points of infinite order which are not $p$-divisible over $E(\mathbb{Q}(C))$ as shown in Lemma 2.4.

Let $p$ be a prime such that it is one of the following:

- A prime of non-split multiplicative reduction for $E$,
- A prime of split multiplicative reduction for $E$ and $p \nmid \text{ord}_p(\Delta_E)$,
- A non-anomalous prime of good ordinary reduction for $E$,
where $\Delta_E$ is the minimal discriminant of $E$. This ensures that the higher modular points are not $p$-divisible in $E(\mathbb{Q}(C))$. Let

$$F_n := \begin{cases} K_{p^{n+1}N_E} & \text{if } p \nmid N_E, \\ K_{p^nN_E} & \text{if } p | N_E, \end{cases}$$

for $n \geq -1$ with $F := F_{-1}$. We assume

$$\tau_{F,A,p} : \text{Gal}(\overline{F}/F) \to \text{PGL}_2(\mathbb{Z}_p)$$

is surjective giving $\text{Gal}(F_n/F) = G_n$. We let $A_n$ be a non-split Cartan subgroup of $G_n$. This is a cyclic subgroup of order $p^{n+1} + p^n$. Then we define $L_n$ to be the subfield of $F_n$ fixed by $A_n$. We are able to construct a mapping

$$\delta_n : H^1(A_n, S_n) \to \text{III}(E/L_n)$$

where $S_n$ denotes the saturated group generated by the higher modular points in $E(F_n)$. This leads to the following.

**Theorem 0.2.** Let $p > 2$ be a prime. Let $E/\mathbb{Q}$ and $A/\mathbb{Q}$ be elliptic curves of conductor $N_E$ and $N_A$ respectively. Let $F_n$ be as defined above. Assume that:

1. $A$ is semistable,
2. $E$ has either split multiplicative reduction at $p$ with $p \nmid \text{ord}_p(\Delta_E)$, non-split multiplicative reduction at $p$ or good ordinary non-anomalous reduction at $p$,
3. The degree of any isogeny of $A$ defined over $\mathbb{Q}$ is coprime to $N_E$,
4. $\rho_{Q,A,p} : G_{\mathbb{Q}} \to \text{Aut}(A[p]) \cong \text{GL}_2(\mathbb{F}_p)$ is surjective,
5. $\rho_{Q,E,p} : G_{\mathbb{Q}} \to \text{Aut}(E[p]) \cong \text{GL}_2(\mathbb{F}_p)$ is surjective,
6. Any prime $\ell$ of bad reduction of $E$ and good reduction of $A$ such that $\ell \neq p$ has $a_\ell(A)^2 - 4\ell$ square modulo $p$.

Then there exists an element of order $p^n$ in $\text{Sel}^{p^n}(E/L_n)$.

With the conditions on $p$, we can show that the source of $\delta_n$ is a cyclic group of order $p^n$. This result comes from the link between the construction of the derivative classes and modular representation theory. The group $S_n$ defined earlier is isomorphic to a $\mathbb{Z}_p[G_n]$-lattice containing $T_n$. Due to the structure of $S_n$, we can use the following.

**Lemma 0.3.** Let $U$ be a $\mathbb{Z}_p[G_n]$-lattice of $V_n$ such that $U^{B_n} = T_n^{B_n}$ where $B_n$ is a Borel subgroup of $G_n$. Then $U \cong T_n$.

Hence, we have $S_n \cong T_n$ under the conditions we have stated and as we understand the cohomology of $T_n$ associated to subgroups for $G_n$, we obtain this result.

However, we still do not fully understand all potential $\mathbb{Z}_p[G_n]$-lattices $S_n$ could be isomorphic to. Further research into the modular representation theory of $F_p[G_n]$ would improve our understanding of the structure of the saturated group of higher modular points and further still, understand the properties of the derivative classes constructed.
1 PRELIMINARIES

Let $K$ be a number field. For an elliptic curve $E$ over $K$ and $m > 1$ an integer, we let $E[m]$ be the $m$-torsion subgroup of $E(K)$. We have $G_K$ acting on $E[m]$ where $G_K := \text{Gal}(\overline{K}/K)$ is the absolute Galois group of $K$. This leads to a Galois representation

$$\overline{\rho}_{K,E,m} : G_K \rightarrow \text{Aut}(E[m]) \cong \text{GL}_2(\mathbb{Z}/m\mathbb{Z}).$$

Let $T_pE = \varprojlim_n E[p^n]$ be the $p$-adic Tate module of $E$ for a prime $p$. Then $G_K$ acts on $T_pE$ which leads to the Galois representation

$$\rho_{K,E,p} : G_K \rightarrow \text{Aut}(T_pE) \cong \text{GL}_2(\mathbb{Z}_p).$$

We define the mapping $\tau_{K,E,m} := s_m \circ \overline{\rho}_{K,E,m}$ where $s_m$ is the quotient mapping to $\text{PGL}_2(\mathbb{Z}/m\mathbb{Z})$ and the mapping $\tau_{K,E,p} := s_p \circ \rho_{K,E,p}$ where $p$ is prime and $s$ is the quotient mapping to $\text{PGL}(\mathbb{Z}_p)$. Throughout, we will denote the centre of $\text{GL}_2(\mathbb{Z}/m\mathbb{Z})$ as $Z_m$ and define $G_n := \text{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ for a prime $p$ and $n \geq 0$.

In this article, we will be looking at the links between the modular points we have constructed and the representation theory associated to $G_n$. We let $B_n$ denote a Borel subgroup of $G_n$. We see that $G_n$ acts on the projective line over $\mathbb{Z}/p^{n+1}\mathbb{Z}$ for $n \geq 0$ via linear substitution, which will be denoted $\mathbb{P}^1_n$ throughout.

2 MODULAR POINTS ON ELLIPTIC CURVES

We would like to understand when the modular points are of infinite order over certain fields. We prove the following.

**Lemma 2.1.** Let $A/\mathbb{Q}$ and $E/\mathbb{Q}$ be elliptic curves of conductor $N_A$ and $N_E$ respectively. Suppose the $j$-invariant of $A$ is not in $\frac{1}{2}\mathbb{Z}$. Then there exists a $C \leq A$ cyclic of order $N_E$ such that $P_{A,C} \in E(\overline{\mathbb{Q}}_p)$ is non-torsion.

**Proof.** Let $p$ be a prime which divides the denominator of the $j$-invariant of $A$. If $p^2 \mid N_A$, we know $A$ acquires multiplicative reduction at $p$ over some extension of $\mathbb{Q}$. Fix an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$. We consider the modular parametrisation over $\mathbb{Z}_p$. The modular curve $X_0(N_E)$ over $\mathbb{Z}_p$ has a neighbourhood of the cusp $\infty$ consisting of couples $(J, C)$ of the Tate curve of the form $J(\mathbb{Q}_p) = \mathbb{Q}_p^*/q^2$ together with a cyclic subgroup $C$ of order $N_E$ generated by the $N_E^{\frac{1}{2}}$ root of unity. The parameter $q$ is a $p$-adic analytic uniformiser at $\infty$, so that the Spf $\mathbb{Z}_p[[q]]$ is the formal completion of $X_0(N_E)/\mathbb{Z}_p$ at the cusp $\infty$, as seen in [S, Chapter 8].

Since $A$ has multiplicative reduction over $\mathbb{Z}_p$, there is exactly one point $x_{A,C}$ in the neighbourhood of $\infty$ on $X_0(N_E)$ which is represented by the $p$-adic Tate parameter $q_A$ associated to $A$ and $C$ is isomorphic to $\mu[N_E]$. Let $f_E = \sum a_n(E)q^n$ be the normalised newform associated to $E$ and let $\omega_E$ be the invariant differential on $E$. Then we have $\phi_E(\omega_E) = c_E \cdot f_E/q \cdot dq$ where $c_E$ is the Manin constant of $E$. Hence

$$\log_E(\phi_E(x_{A,C})) = \int_0^{\phi_E(x_{A,C})} \omega_E = c_E \cdot \int_0^{a_n} f_E \frac{dq}{q} = c_E \cdot \sum_{n=1}^{\infty} \frac{a_n(E)}{n} \cdot q_A^n$$
where \( \log_E \) is the formal logarithm associated to \( E \) from the formal group \( \hat{E}(\mathbb{m}) \) to the maximal ideal \( \mathbb{m} \) of \( \mathbb{Z}_p \). We let \( q \cdot |\cdot|_p \) be the normalised absolute value such that \( |p|_p = p^{-1} \). We then have the following lemma.

**Lemma 2.2.** Let \((J,C)\) be a point on \( Y_0(N_E)(\mathbb{Q}_p) \) such that \( J \) is isomorphic to the Tate curve with parameter \( q_0 \neq 0 \) and \( C \) is isomorphic to \( \mu[N_E] \). If \( |q_0|_p < p^{-\frac{1}{N}} \) then \( \phi_E(J,C) \) is a point of infinite order in \( E(\mathbb{Q}_p) \).

Hence, we have for \( p \neq 2 \) that

\[
|q_A|_p = |j(A)|^{-1} \leq p^{-1} < p^{-\frac{1}{N}}
\]

and if \( p = 2 \) then

\[
|q_A|_2 = |j(A)|^2 \leq p^{-2} < p^{-\frac{1}{N}}.
\]

Therefore, by Lemma 2.2, we have that \( P_{A,C} = \phi_E(x_{A,C}) \) is a point of infinite order in \( E(\mathbb{Q}_p) \). \( \square \)

We assume for primes \( \ell \) of bad reduction for \( E \), there exists no \( \ell \)-isogeny on \( A \). Hence the set of modular points \( \{P_{A,C}\} \) form a single orbit under the action of \( G_{N_E} \) and so for all \( C \), \( P_{A,C} \) is of infinite order in \( E(\mathbb{Q}(C)) \). However, we do have a relation with respect to sums of these modular points.

**Proposition 2.3.** The sum of the modular points \( P_{A,C} \) as \( C \) varies through all cyclic subgroups of \( A \) of order \( N_E \) is a torsion point defined over \( \mathbb{Q} \). Let \( d \neq N_E \) be an integer dividing \( N_E \). Then

\[
\sum_{C \in \mathcal{B}} P_{A,C} \in E(K_d)
\]

is a torsion point where \( B \) is a cyclic subgroup of \( A \) of order \( d \) and the sum is taken over all cyclic subgroups of \( A \) of order \( N_E \) containing \( B \).

**Proof.** Identical to the proof of \[13\] Proposition 7]. \( \square \)

Hence, we know that there exists at least one \( P_{A,C} \in E(\mathbb{Q}(C)) \) of infinite order and there is a relationship between them. We next observe the divisibility of the points in \( E(\mathbb{Q}(C)) \).

**Lemma 2.4.** Suppose \( j(A) \notin \frac{1}{2}\mathbb{Z} \) and \( p > 2 \) is a prime such that its satisfies one of the following:

- A prime of non-split multiplicative reduction for \( E \),
- A prime of split multiplicative reduction for \( E \) and \( p \nmid \text{ord}_p(\Delta_E) \),
- A non-anomalous prime of good reduction for \( E \).

Then \( P_{A,C} \notin p^{r_E(A)} \cdot E(\mathbb{Q}(C)) \).

**Proof.** Let \( p \) be the place \( \mathbb{Q}(C) \) corresponding to the chosen embedding \( \mathbb{Q} \) to \( \mathbb{Q}_p \). Then we have \( \mathbb{Q}(C)_p = \mathbb{Q}_p \). As \( p \) is one of the primes in the lemma with respect to \( E \), then the order of the group of components of \( E \) over \( \mathbb{Q}_p \) and the number of non-singular points in the reduction \( E(\mathbb{F}_p) \) are both prime to \( p \). Hence, if \( P_{A,C} \) is divisible by \( p \) in \( E(\mathbb{Q}_p) \) then it is divisible by \( p \) in \( E(p\mathbb{Z}_p) \). But the valuation of \( \log_E(P_{A,C}) \) shows this cannot happen. Let \( z = \log_E(P_{A,C}) \) and denote
We have now seen the divisibility of the modular points in $c_p(A)$ as the Tamagawa number for $A$ at $p$. As $\mathbb{Q}(C)_p = \mathbb{Q}_p$, then we have $\text{ord}_p(q_A) = c_p(A)$. We then see that

$$\text{ord}_p(z) = \min\{\text{ord}_p(q_A), \text{ord}_p(a_p(E)) + p \cdot \text{ord}_p(q_A) - \text{ord}_p(p)\} = \min\{c_p(A), \text{ord}_p(a_p(E)) + p \cdot c_p(A) - 1\} = c_p(A)$$

as $a_p(E)$ is an integer. Therefore, we have that $P_{A,C} \in E(p^{\phi(A)}\mathbb{Z}_p)$. If $p \neq 2$, then we have

$$\text{ord}_p(z - q_A) = \text{ord}_p(a_p(E)) + p \cdot \text{ord}_p(q_A) - 1 = \text{ord}_p(a_p(E)) + p \cdot c_p(A) - 1 \geq (p - 1)c_p(A) \geq 2c_p(A).$$

Hence, we have $z$ is congruent to $q_A$ modulo $p^{2\phi(A)}$. So the value $z$ is non zero and hence $P_{A,C} \notin p^{\phi(A)} \cdot E(\mathbb{Q}(C))$.}

We have now seen the divisibility of the modular points in $E(\mathbb{Q}(C))$. This will become important when we study the representation theory of the group generated by the modular points on $E$.

3 REPRESENTATIONS OF $\text{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$

We are interested in the representations that will appear in the study of modular points. We let

$$V_{(n)} = \mathbb{Q}_p[G_n/B_n]$$

which is a $\mathbb{Q}_p[G_n]$-module of dimension $p^{n+1} + p^n$. We can view $V_{(n)} = \text{Maps}(\mathbb{P}_n^1 \rightarrow \mathbb{Q}_p)$. This decomposes as

$$V_{(n)} := \bigoplus_{i=1}^{n} W_i$$

where $W_i$ are irreducible $\mathbb{Q}_p[G_n]$-modules as seen in [13, Theorem 8]. These take the form $W_{-1} = \mathbb{Q}_p$ and

$$W_i = \ker\left(\mathbb{Q}_p[G_i/B_i] \rightarrow \mathbb{Q}_p[G_{i-1}/B_{i-1}]\right) = \left\{ f : \mathbb{P}_i^1 \rightarrow \mathbb{Q}_p : \sum_{C \supseteq D} f(C) = 0 \text{ for all } D \in \mathbb{P}_{i-1}^1 \right\}$$

for $i \geq 0$. We define the standard $\mathbb{Z}_p[G_n]$-lattice inside $V_{(n)}$ as

$$T_{(n)} = \mathbb{Z}_p[G_n/B_n] = \text{Maps}(\mathbb{P}_n^1 \rightarrow \mathbb{Z}_p).$$

Define

$$V_n := V_{(n)}/W_{-1} = \ker\left(\mathbb{Q}_p[G_n/B_n] \rightarrow \mathbb{Q}_p\right)$$

and let

$$T_n := \ker\left(\mathbb{Z}_p[G_n/B_n] \rightarrow \mathbb{Z}_p\right) = \left\{ f : \mathbb{P}_n^1 \rightarrow \mathbb{Z}_p : \sum_{C} f(C) = 0 \right\}$$

be the standard $\mathbb{Z}_p[G_n]$-lattice in $V_n$. We initially look at the cohomology of $B_n$ with respect to the lattice $T_{(n)}$. 

6
Lemma 3.1. For all \( n \geq 0 \), we have \( H^1(B_n, T_{(n)}) = 0 \).

**Proof.** We know that \( T_{(n)} \cong \text{Ind}_{B_n}^G(Z_p) \). Then
\[
H^1(B_n, T_{(n)}) \cong \text{Ext}^1_{Z_pB_n}(T_{(n)}, Z_p) \cong \text{Ext}^1_{Z_pG_n}(T_{(n)}, T_{(n)}).
\]
We see by [3, Corollary 3.3.5 (vi)] that
\[
\text{Ext}^1_{Z_pG_n}(T_{(n)}, T_{(n)}) \cong \bigoplus_{B_n g B_n} \text{Ext}^1_{Z_p[B_n \cap g B_n g^{-1}]}(\text{Res}^G_{B_n \cap g B_n g^{-1}}(Z_p), \text{Res}^G_{B_n \cap g B_n g^{-1}}(Z_p))
\]
where the sum is taken over the double cosets \( B_n g B_n \). However, for all such double cosets, we have \( B_n \cap g B_n g^{-1} \leq G_n \) and acts trivially on \( Z_p \). Therefore we have
\[
\text{Ext}^1_{Z_pG_n}(T_{(n)}, T_{(n)}) \cong H^1(B_n \cap g B_n g^{-1}, Z_p)
\]
\[
\cong \text{Hom}(B_n \cap g B_n g^{-1}, Z_p) = 0.
\]
for all double cosets \( B_n g B_n \). Hence we have \( \text{Ext}^1_{Z_pG_n}(T_{(n)}, T_{(n)}) = 0 \).

We then use this for the following.

**Lemma 3.2.** For all \( n \geq 0 \), we have \( H^1(B_n, T_n) = 0 \).

**Proof.** We have the short exact sequence
\[
0 \rightarrow T_n \rightarrow T_{(n)} \xrightarrow{2} Z_p \rightarrow 0
\]
which induces
\[
0 \rightarrow T_n^{B_n} \rightarrow T_{(n)}^{B_n} \xrightarrow{2} Z_p \rightarrow H^1(B_n, T_n) \rightarrow 0
\]
as \( B_n \) acts trivially on \( Z_p \) and \( H^1(B_n, T_{(n)}) = 0 \) by Lemma 3.1. As \( B_n \) fixes a point of \( P^1_n \), let \( C \in P^1_n \) be the fixed point. The characteristic function \( \epsilon_C : P_n \rightarrow Z_p \) in \( T_n^{B_n} \) is mapped to 1 in \( Z_p \) by \( g \). Therefore, \( g \) is surjective and \( H^1(B_n, T_n) = 0 \).

We would like to focus on the \( Z_p[G_n] \)-lattices \( U \) of \( V_n \) such that \( U^{B_n} \cong T_n^{B_n} \). All such lattices can be scaled such that they contain \( T_n \) and are contained in \( \frac{1}{k} T_n \) for some \( k \geq 1 \). We have the exact sequence
\[
0 \rightarrow T_n \rightarrow U \rightarrow U / T_n \rightarrow 0.
\]
By Lemma 3.2 if \( U^{B_n} \cong T_n^{B_n} \) then \( (U / T_n)^{B_n} = 0 \). We will initially focus on the \( k = 1 \) case. We now define \( X := X \otimes_{Z_p} F_p \) for any \( Z_p(G_n) \)-module \( X \). We look at the fixed part by \( B_n \) of the \( \mathbb{F}_p[G_n] \)-submodules of \( T_{(n)} := \mathbb{F}_p[G_n / B_n] \).

**Lemma 3.3.** Let \( W \) be a non-trivial \( \mathbb{F}_p[G_n] \)-submodule of \( T_{(n)} \). Then \( W^{B_n} \neq 0 \).
Proof. Let $W$ be a non-trivial $\mathbb{F}_p[G_n]$-submodule of $\mathcal{T}_{(n)}$. We will show that the only irreducible submodules of $\mathcal{T}_{(n)}$ are the trivial module and the Steinberg representation

$$W_{st} = \left\{ f : \mathbb{P}^1_n \to \mathbb{F}_p : f(C) = t_D \text{ for } C \supset D \in \mathbb{P}^1_0 \text{ and } \sum_D t_D = 0 \right\}$$

and these modules have non-trivial fixed part by a Borel subgroup.

We will first show these are the only irreducible $\mathbb{F}_p[G_n]$-submodules of $\mathcal{T}_{(n)}$. Let $W$ be an irreducible $\mathbb{F}_p[G_n]$-module and let

$$W_H = W/\langle (h-1)W : h \in H \rangle$$

where $H \leq G_n$. We let $B_n$ be a Borel subgroup and

$$\Pi_n = \left\{ \begin{pmatrix} a & b \\ 0 & 1 \end{pmatrix} \in G_n : a \equiv 1 \pmod{p} \right\}.$$

This is a Sylow $p$-subgroup of $B_n$. We will look at the $n = 0$ case first. Then $\Pi_0$ is generated by $u = \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix}$. We see that

$$\text{Hom}_{\mathbb{F}_p[G_0]}(W, \mathcal{T}_{(0)}) \cong \text{Hom}_{\mathbb{F}_p[B_0]}(W, \mathbb{F}_p)$$

$$\cong \text{Hom}_{\mathbb{F}_p}(W_{B_0}, \mathbb{F}_p)$$

$$\cong \text{Hom}_{\mathbb{F}_p[G_0/\Pi_0]}(W_{\Pi_0}, \mathbb{F}_p).$$

We see in [6, pg. 87] that the irreducible $\mathbb{F}_p[G_0]$ representations take either the form

$$\tau_{j,1} = \text{Sym}^{j-1} \otimes \text{det}^{-\frac{j-1}{2}}$$

or

$$\tau_{j,2} = \tau_{j,1} \otimes \tau_1$$

where $\tau_1$ is the unique non-trivial 1-dimensional $\mathbb{F}_p[G_0]$-representation and $j \in \{1, 3, ..., p\}$. We can view $\text{Sym}^{j-1}$ as an $\mathbb{F}_p$-subspace of $\mathbb{F}_p[x, y]$ of degree $j - 1$ homogeneous polynomials where $\text{GL}_2(\mathbb{F}_p)$ acts on $\text{Sym}^{j-1}$ by linear substitution. Then

$$(u - 1) \text{Sym}^{j-1} \oplus \mathbb{F}_p y^{j-1} = \text{Sym}^{j-1}.$$

Therefore if we twist by $\text{det}^{-\frac{j-1}{2}}$, we have $(\text{Sym}^{j-1} \otimes \text{det}^{-\frac{j-1}{2}})_{\Pi_0} \cong \mathbb{F}_p y^{j-1} \otimes \text{det}^{-\frac{j-1}{2}}$. This means that if $W$ is an irreducible $\mathbb{F}_p[G_0]$-module, then $W$ must have the underlying representation $\tau_{j,1}$ or $\tau_{j,2}$ for $j \in \{1, 3, ..., p\}$. Hence $W_{\Pi_0}$ is a 1-dimensional irreducible $\mathbb{F}_p[G_0/\Pi_0]$-module. We see that

$$B_{0j/\Pi_0} \cong \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in G_0 \right\}$$

and $y^{j-1} \in \text{Sym}^{j-1} \otimes \text{det}^{-\frac{j-1}{2}}$ is an eigenvector of $(\begin{pmatrix} 0 & 1 \\ 0 & 0 \end{pmatrix})$ with eigenvalue $a^{-\frac{j-1}{2}}$. We also have

$$\tau_1 \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} = a^{\frac{j-1}{2}}.$$

We see from [6] that $\mathbb{F}_p$ and $W_{st}$ have underlying representations $\tau_{1,1}$ and $\tau_{p,2}$ respectively. Therefore, $W_{\Pi_0} = \mathbb{F}_p \iff W = \mathbb{F}_p$ or $W = W_{st}$.

For $n \geq 1$, we see that $\text{Irr}_{\mathbb{F}_p}(G_n) = \text{Irr}_{\mathbb{F}_p}(G_0)$ where $\text{Irr}_{\mathbb{F}_p}(G)$ are the irreducible representations for the group $G$ over $\mathbb{F}_p$. As $W$ is an irreducible $\mathbb{F}_p[G_n]$-module, then we can again view $W$ having
Lemma 3.4. We would like to see when these lattices have non-trivial fixed part by a Borel subgroup. Hence for $\mathfrak{g}$, we see that $\tau_j = \tau_1 \otimes \tau_1$ for $j \in \{1, 3, \ldots, p\}$. We have $G_n$ acting on it by linear substitution. We also see that

$$\Pi_n = \left\{ \begin{pmatrix} 1 & 1 \\ 0 & 1 \end{pmatrix} \right\} \times \left\{ \begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in G_n : a \equiv 1 \pmod{p} \right\}$$

which is no longer cyclic. We therefore need to look at the action of the right hand side group on $\text{Sym}^j$. Let $\pi$ represent the element $\begin{pmatrix} a & 0 \\ 0 & 1 \end{pmatrix} \in \Pi_n$ where $a \equiv 1 \pmod{p}$. Looking at the 1-dimensional $F_p[G_n]$-representation $\det : G_n \to F_p$, we see that $\text{det} - \frac{j}{p} \pi = 1$ as $a \equiv 1 \pmod{p}$. Also, as $\text{Sym}^j$ can be viewed as degree $j-1$ homogeneous polynomials over $F_p$, then

$$\pi \cdot x^{j-1}y^i = a^{j-1}x^{j-1}y^i = x^{j-1}y^i$$

as $a \equiv 1 \pmod{p}$. Therefore, this shows that $\text{Sym}^j \otimes \text{det} - \frac{j}{p} \pi$ and so

$$Hom_{F_p[G_n]}(W, T_{\langle \alpha \rangle}) \cong Hom_{F_p[B_n]}(W, F_p) \cong Hom_{F_p[B_n]}(W_{H_n}, F_p) \cong Hom_{F_p[B_n]}(W, F_p).$$

We see that if $\pi$ is a representative of a coset in $B_n/\Pi_n$, the representation underlying $\text{Sym}^j \otimes \text{det} - \frac{j}{p} \pi$ maps $\pi$ to $a^{-\frac{j}{p}}$ and the representation underlying $\text{Sym}^j \otimes \text{det} - \frac{j}{p} \pi \otimes \tau_1$ maps $\pi$ to $a^{-\frac{j}{p}}$. Hence for $W_{H_n} = F_p$, we need $j = 1$ in the first case or $j = p$ in the second, so $W$ is either $F_p$ or $W_{st}$. We finally need to show these irreducible modules have non-trivial fixed part by a Borel subgroup. The trivial $F_p[G_n]$-module has $G_n$ acting trivially on it and hence so does every Borel subgroup. Also, for a fixed element of $F_p^1$, denoted $D_0$, then a Borel subgroup acts transitively on the set of $C \not\supset D_0$ for $C \in P_1$. As the number of all elements $C \not\supset D_0$ is divisible by $p$, then the fixed part of $W_{st}$ by a Borel subgroup contains the function $f$ such that

$$f(C) = \begin{cases} 1 & \text{if } C \not\supset D_0, \\ 0 & \text{otherwise}, \end{cases}$$

and hence is non-trivial.

Therefore, if $U$ is a $Z_p[G_n]$-lattice inside $\frac{1}{p} T_n$ containing $T_n$ with $U_{B_n} = T_{B_n}$, then we know that $(U/T_n)_{B_n} = 0$. Hence by Lemma 3.3 we have $U/T_n = 0$ meaning $U \cong T_n$.

We now look at the $Z_p[G_n]$-lattices containing $T_n$ that are contained in $\frac{1}{k^p} \cdot T_n$ for some $k \geq 1$. We would like to see when these lattices have non-trivial fixed part by a Borel subgroup.

**Lemma 3.4.** Let $W$ be a non-trivial $\mathbb{Z}/p^k\mathbb{Z}[G_n]$-module contained in $T_{\langle \alpha \rangle}/p^k T_{\langle \alpha \rangle}$ for $k \geq 1$. Then $W_{B_n} \neq 0$. 

9
Proof. We do this by induction. The \( k = 1 \) case is Lemma 3.3 so assume this is true for \( k \). We have a short exact sequence
\[
0 \to T_n^{(n)} \to T_n^{(n)/p^{k+1}T_n^{(n)}} \to T_n^{(n)/p^{k}T_n^{(n)}} \to 0
\]
so we can view \( T_n^{(n)} \) as a \( \mathbb{Z}/p^{k+1}\mathbb{Z}[G_n] \)-submodule of \( T_n^{(n)/p^{k+1}T_n^{(n)}} \). Let \( W \) be a non-trivial \( \mathbb{Z}/p^{k+1}\mathbb{Z}[G_n] \)-module contained in \( T_n^{(n)/p^{k+1}T_n^{(n)}} \). If \( W \cap T_n^{(n)} \neq 0 \), then \( W \) contains an irreducible \( \mathbb{F}_p[G_n] \)-module \( U \) such that \( U^{B_n} \neq 0 \) by Lemma 3.3. Hence we can assume \( W \cap T_n^{(n)} = 0 \). Then by the second isomorphism theorem, we have
\[
\frac{W + T_n^{(n)}}{T_n^{(n)}} \cong \frac{W}{W \cap T_n^{(n)}} \cong W.
\]
Hence
\[
W \cong \frac{W + T_n^{(n)}}{T_n^{(n)}} \leq \frac{T_n^{(n)/p^{k+1}T_n^{(n)}}}{T_n^{(n)}} \cong T_n^{(n)/p^{k}T_n^{(n)}}.
\]
As \( W \neq 0 \), then by induction, \( W^{B_n} \neq 0 \).

Therefore we can prove the following.

**Lemma 3.5.** Let \( U \) be a \( \mathbb{Z}_p[G_n] \)-lattice of \( V_n \) such that \( U^{B_n} = T_n^{B_n} \). Then \( U \cong T_n \).

**Proof.** We see there exists a \( k \geq 1 \) such that \( U \subseteq T_n^{\frac{1}{p^k}} \). As \( U^{B_n} = T_n^{B_n} \), then we have seen that \( (U/T_n)^{B_n} = 0 \). Therefore by Lemma 3.3 \( U \cong T_n \). \( \square \)

### 4 HIGHER MODULAR POINTS

We now investigate the properties of higher modular points and their relationship with the representation theory we have looked at in the previous section. Let \( E/\mathbb{Q} \) and \( A/\mathbb{Q} \) be elliptic curves of conductor \( N_E \) and \( N_A \) respectively and \( D \) a cyclic subgroup of \( A \). We then take the isogenous curve \( A/D \) and a cyclic subgroup of order \( N_E \) in this isogenous curve. We look at two cases of these higher modular points.

#### 4.1 MULTIPLICATIVE CASE

Let \( E/\mathbb{Q} \) be an elliptic curve of conductor \( N_E \) and let \( p \) be a prime of multiplicative reduction. We let \( N_E = pM \) and define \( F_n := K_{p^{n+1}M} \) for all \( n \geq -1 \) with \( F := F_{-1} \). We can view \( \Delta_n = \text{Gal}(F_n/F) \) as a subgroup of \( G_n \).

Let \( B \leq A \) be cyclic of order \( M \). Let \( n \geq 0 \) and \( D \leq A \) be a cyclic subgroup of order \( p^{n+1} \). Let \( C = D[p] \oplus B \) which is a cyclic subgroup of order \( N_E \) and let \( \psi : A \to A/D \) be the isogeny associated with \( D \) with dual \( \hat{\psi} \). We define
\[
C' = \ker(\hat{\psi})[p] \oplus \psi(B).
\]
This is a cyclic subgroup of \( A/D \) of order \( N_E \). We then define \( y_{A,D} = (A/D, C') \in X_0(N_E) \). We define a higher modular point above \( P_{A,C} \) as the point \( Q_{A,D} = \phi_E(y_{A,D}) \in E(F_n) \).
When \( n = 0 \), we see from above that we have \( y_{A,D} = w_p(x_{A,C}) \) where \( w_p \) is the Atkin-Lehner involution on \( X_0(N_E) \). Therefore, we have \( Q_{A,D} = -a_p(E) \cdot P_{A,C} + T \) for some \( T \in E(\mathbb{Q})[2] \) and \( a_p(E) \in \{ \pm 1 \} \) is the Hecke eigenvalue of the newform \( f \) attached to \( E \).

Let \( D \leq A \) be cyclic of order \( p^n+1 \). Let \( T_p \) be the Hecke operator \( T_p \) on \( J_0(N_E) \). Then

\[
T_p((y_{A,D})-(\infty)) = \sum_{D' \supseteq D} ((y_{A,D'})-(\infty))
\]

where the sum runs over all cyclic subgroups \( D' \) of order \( p^n+2 \) in \( A \). This then leads to the trace relation

\[
a_p(E) \cdot Q_{A,D} = \sum_{D' \supseteq D} Q_{A,D'}.
\]

Hence, by induction, if \( P_{A,C} \) is of infinite order then so is \( Q_{A,D} \). In particular, if \( P_{A,C} \notin p \cdot E(F_0) \) then \( Q_{A,D} \notin p \cdot E(F_n) \).

**Lemma 4.1.** Fix a cyclic subgroup \( B \) of \( A \) of order \( M \) and let \( n \geq 0 \). Then \( \sum_D Q_{A,D} \) is a torsion point in \( E(F) \) where the sum is over all cyclic subgroups \( D \) of \( A \) of order \( p^n+1 \) such that \( D[p] \oplus B \) is a cyclic subgroup of \( A \) of order \( N_E \).

This is proven identically to [13, Lemma 19]. If we fix a cyclic subgroup \( B \) of \( M \) in \( A \), then we have a \( \Delta_n \)-morphism

\[
V_n \rightarrow E(F_n) \otimes \mathbb{Q}_p
\]

\[
e_D \mapsto Q_{A,D}
\]

where \( e_D \) is the characteristic function on \( D \). If we then assume that \( \tau_{F,A,p} \) is surjective, then we have \( \Delta_n \cong G_n \).

**Lemma 4.2.** Let \( E/\mathbb{Q} \) and \( A/\mathbb{Q} \) be elliptic curves of conductor \( N_E \) and \( N_A \) respectively. Let \( p \) be a prime of multiplicative reduction of \( E \) and let \( P_{A,C} \subseteq E(F_0) \) have infinite order. Suppose \( \tau_{F,A,p} \) is surjective. Then all higher modular points \( Q_{A,D} \) above \( P_{A,C} \) are of infinite order and generate a group of rank \( p^n+1 + p^n - 1 \) in \( E(F_n) \otimes \mathbb{Q}_p \).

### 4.2 Good Case

Let \( p \) be a prime of good reduction for \( E \). We define \( F_n := K_{p^n+1,N_E} \) where \( F := K_{p-1} \) is a number field such that \( P_{A,C} \) is of infinite order in \( E(F) \). Hence, we can view \( \Delta_n = \text{Gal}(F_n/F) \) as a subgroup of \( G_n \).

For \( n \geq 0 \), we let \( D \) be a cyclic subgroup of \( A \) of order \( p^n+1 \) and then we can construct the higher modular points. We let \( \psi : A \rightarrow A/D \) be the isogeny associated to \( D \). Then we have \( y_{A,D} = (A/D, \psi(C)) \in X_0(N_E) \). We then define the higher modular point above \( P_{A,C} \) as \( Q_{A,D} = \phi_E(y_{A,D}) \in E(F_n) \).

As before, if we use the Hecke operator \( T_p \), we obtain the trace relation

\[
a_p(E) \cdot Q_{A,D} = \sum_{D' \supseteq D} Q_{A,D'}
\]

for all \( n \geq 0 \) and \( D \) as defined before. Here, the sum runs over all cyclic subgroups \( D' \) of order \( p^n+2 \). Hence, this means that we have

\[
a_p(E) \cdot P_{A,C} = \sum_D Q_{A,D}
\]
where the sum runs over all cyclic subgroups of order \( p \). Therefore, as \( P_{A,C} \) is of infinite order in \( E(F) \), then for all cyclic subgroups \( D \) of order \( p^{n+1} \) and all \( n \geq 0 \), \( Q_{A,D} \) is of infinite order in \( E(F_n) \).

Therefore, we can define a \( \Delta_n \)-morphism

\[
V(n) \to E(F_n) \otimes \mathbb{Q}_p \\
\epsilon_D \mapsto Q_{A,D}.
\]

If we then assume that \( \tau_{F,A,p} \) is surjective, then we have \( \Delta_n \cong G_n \).

**Lemma 4.3.** Let \( E/\mathbb{Q} \) and \( A/\mathbb{Q} \) be elliptic curves of conductor \( N_E \) and \( N_A \) respectively. Let \( p \) be a prime of good ordinary reduction of \( E \) ensuring \( a_p(E) \neq 0 \) and let \( P_{A,C} \in E(F) \) have infinite order. Suppose \( \tau_{F,A,p} \) is surjective. Then all higher modular points \( Q_{A,D} \) above \( P_{A,C} \) are of infinite order and generate a group of rank \( p^{n+1} + p^n \) in \( E(F_n) \otimes \mathbb{Q}_p \).

### 5 DERIVATIVES

Let \( E/\mathbb{Q} \) and \( A/\mathbb{Q} \) be elliptic curves of conductors \( N_E \) and \( N_A \) respectively. Let \( p \) be a prime of good ordinary or multiplicative reduction with respect to \( E \). We assume that \( \tau_{F,A,p} \) is surjective. Hence, if we let \( F_n \) be the smallest field extension of \( F \) such that \( \Delta_n := \text{Gal}(F_n/F) \) acts as scalars on \( E[p^{n+1}] \), then we have \( \Delta_n \cong G_n \).

We define \( A_n \) to be a non-split Cartan subgroup of \( G_n \). This is a cyclic subgroup of order \( p^{n+1} + p^n \). We then let \( L_n \) be the subfield of \( F_n \) fixed by \( A_n \).

**Theorem 5.1.** Let \( p > 2 \) be a prime. Let \( E/\mathbb{Q} \) and \( A/\mathbb{Q} \) be elliptic curves of conductor \( N_E \) and \( N_A \) respectively and let \( F \) be as defined above. Assume that:

1. \( A \) does not have potentially good supersingular reduction for any prime of additive reduction,
2. \( E \) has either split multiplicative reduction at \( p \) with \( p \nmid \text{ord}_p(\Delta_E) \), non-split multiplicative reduction at \( p \) or good ordinary non-anomalous reduction at \( p \),
3. The degree of any isogeny of \( A \) defined over \( \mathbb{Q} \) is coprime to \( N_E \),
4. \( \tau_{F,A,p} \) is surjective,
5. \( \overline{\rho}_{Q,E,p} \) is surjective,
6. Any prime \( \ell \) of bad reduction of \( E \) and good reduction of \( A \) such that \( \ell \neq p \) has \( a_\ell(A)^2 - 4\ell \) square modulo \( p \).

Then there exists an element of order \( p^n \) in \( \text{Sel}^n(E/L_n) \).

We show that the elements in the Selmer groups in the above theorem originate from non-trivial elements in \( \text{III}(E/L_n)[p^n] \). In order to show this, we need to look at the splitting of primes in the field extension \( F_n/L_n \).

**Lemma 5.2.** [13] Lemma 25] \( A_n \) intersects trivially with any Borel subgroup in \( G_n \).

This then implies that any generator of \( A_n \) acts transitively on \( \mathbb{P}^1_{\mathbb{F}_n} \). We want to prove the following.
Proposition 5.3. Suppose none of the primes of additive reduction for $A$ are potentially good supersingular. Then the extension $F_{\nu}/L_{\nu}$ is nowhere ramified. Furthermore, all places above $\infty$, $p$ and $N_A$ split completely in the extension as well as all places above a prime $\ell$ dividing $N_E$ but not $p$ or $N_A$ such that $a_\ell(\mathcal{A})^2 - 4\ell$ is a square modulo $p$.

We will first need the following lemma.

Lemma 5.4. [13] Lemma 26] Let $\nu$ be either a place of ordinary reduction above $p$, an infinite place or a place of potentially multiplicative reduction all with respect to $A$. Then the image of $\tau_{F_{\nu},A,p^{n+1}}$ lies in a Borel subgroup of $G_n$.

Therefore, we now need to look at the places of $F$ of bad reduction with respect to $E$ such that they are not above $p$ or $N_A$. Let $\nu$ be such a place. Then the Frobenius element $\text{Fr}_\nu$ of $\Delta_n$ generates the decomposition group.

Let $A_\nu$ be the reduced elliptic curve at $\nu$ and $R_\nu$ the subring of $\text{End}(A_\nu)$ generated by the Frobenius endomorphism. We define

$$u_\nu := \text{disc}(R_\nu), \quad \delta_\nu := 0, 1 \text{ depending on when } u_\nu \equiv 0, 1 \pmod{4},$$

and $b_\nu$ the unique positive integer such that $u_\nu b_\nu^2 = a_\nu(\mathcal{A})^2 - 4q_\nu$. We then associate to $\nu$ the integral matrix

$$M_\nu = \begin{pmatrix} a_\nu(\mathcal{A}) + b_\nu \delta_\nu & b_\nu \\ b_\nu^2(u_\nu - \delta_\nu) & a_\nu(\mathcal{A}) - b_\nu \delta_\nu \end{pmatrix}.$$ 

Lemma 5.5. [3] Theorem 2.1] Let $A$ be an elliptic curve over $F$. Let $\nu$ be a place of $F$ of good reduction for $A$ such that $\nu \nmid p$. Then $\nu$ is unramified in $F(A[p^{n+1}])$ and the integral matrix $M_\nu$, when reduced modulo $p^{n+1}$, represents the conjugacy class of the Frobenius of $\nu$ in $\text{Gal}(F(A[p^{n+1}])/F)$.

Thus, we want to see when $M_\nu$ reduced modulo $p^{n+1}$ lies in a Borel subgroup. To do this, we look at the conjugacy classes of $M_\nu$ in $\text{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$.

Definition 5.6. A matrix $A \in \text{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ is cyclic if $A$ is not a scalar matrix modulo any power of $p$.

Using this we are able to write each matrix of $\text{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ in a specific form.

Lemma 5.7. [3] Lemma 2.1] Let $X \in \mathbb{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$. Then $X$ is either cyclic or can be written in the form $dI_2 + p^{j}\beta$ for some $1 \leq j \leq n+1$ such that $d \in (\mathbb{Z}/p^{n+1}\mathbb{Z})^\times$ and $\beta \in M_2(\mathbb{Z}/p^{n+1-j}\mathbb{Z})$ cyclic.

Then we can find a representative of the conjugacy class each matrix in $\text{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ lies in.

Lemma 5.8. [3] Theorem 2.2] Let $A \in \text{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ be of the form $dI_2 + p^{j}\beta$. Then $A$ is conjugate to

$$\begin{pmatrix} d & p^{j} \\ -p^{j} \cdot \text{det}(\beta) & d + p^{j} \cdot \text{tr}(\beta) \end{pmatrix}.$$ 

We can use this form on $M_\nu$ to prove the following.

Lemma 5.9. If $a_\nu(\mathcal{A})^2 - 4q_\nu$ is a square modulo $p$ then $M_\nu$ reduced modulo $p^{n+1}$ lies in a Borel subgroup of $\text{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$. 

13
Proof. First assume \((b_\nu, p) = 1\). Then \(M_\nu\) is conjugate to
\[
\begin{pmatrix}
0 & 1 \\
-q_\nu & a_\nu(A)
\end{pmatrix}.
\]
This matrix lies in a Borel subgroup if \(a_\nu(A)^2 - 4q_\nu\) is a square modulo \(p\).

If \(b_\nu = p^jt\) for some \(j \geq 1\) and \((t, p) = 1\) then as \(\det(M_\nu) = q_\nu\) is not divisible by \(p\) then neither is \(a_\nu(A)^2\). Therefore, \(M_\nu\) is conjugate to
\[
\begin{pmatrix}
a_\nu(A)/2 & p^j \\
p^j/a_\nu(A)/4 & \frac{a_\nu(A)}{2}
\end{pmatrix}.
\]
This matrix lies in a Borel subgroup if \(u_\nu\) is a square modulo \(p\). But as \(u_\nu b_\nu^2 = a_\nu(A)^2 - 4q_\nu\), this is true if \(a_\nu(A)^2 - 4q_\nu\) is a square modulo \(p\).

We would like to find conditions for \(a_\nu(A)^2 - 4q_\nu\) to be a square modulo \(p\). We let \(\ell\) be a prime of good reduction with respect to \(A\). Then the arithmetic Frobenius \(\text{Fr}_\ell\) has characteristic polynomial
\[
x^2 - a_\ell(A)x + \ell \quad \text{with roots } \alpha \text{ and } \beta.
\]
Then we obtain \(a_\ell^n(A) = \alpha^n + \beta^n\) and \(\ell^n = \alpha^n \beta^n\) for \(n \geq 1\).

Proposition 5.10. Let \(A/\mathbb{Q}\) be an elliptic curve and \(p\) a prime. Let \(\ell\) be a prime of good reduction with respect to \(A\) such that \(\ell \neq p\). Then for all \(n \geq 1\)
\[
a_\ell(A) - 4\ell \text{ is a square mod } p \text{ if and only if } a_\ell^n(A) - 4\ell^n \text{ is a square mod } p.
\]
The proof will follow later. From now on, we let \(t_n := \text{tr}(\text{Fr}_\ell^n)\).

Proposition 5.11. We have \(t_n = t_1 t_{n-1} - \ell t_{n-2}\) for \(n \geq 3\).

Proof. For \(n \geq 3\), we have
\[
t_n = \alpha^n + \beta^n = (\alpha + \beta)(\alpha^{n-1} + \beta^{n-1}) - \alpha \beta (\alpha^{n-2} + \beta^{n-2}) = t_1 t_{n-1} - \ell t_{n-2}
\]
which gives our formula. \(\square\)

We will first look at the cases where \(n\) is odd.

Lemma 5.12. For all \(n \geq 0\)
\[
t_{2n+1}^2 - 4\ell^{2n+1} = (t_1^2 - 4\ell)(1 - 2n)\ell^n + \sum_{j=1}^{n} \ell^{n-j} t_j^2.
\]

Proof. Let \(\alpha\) and \(\beta\) be as before. Then we have
\[
t_{2n+1}^2 - 4\ell^{2n+1} = (\alpha^{2n+1} - \beta^{2n+1})^2.
\]
and \( t_1^2 - 4\ell = (\alpha - \beta)^2 \). Therefore we have

\[
\alpha^{2n+1} - \beta^{2n+1} = (\alpha - \beta) \left( \sum_{j=0}^{2n} \alpha^j \beta^{2n-j} \right)
\]

\[
= (\alpha - \beta) \left( \sum_{j=1}^{n} \alpha^n \beta^j + \sum_{j=1}^{n} \alpha^{n+j} \beta^{n-j} + \alpha^{n-j} \beta^{n+j} \right)
\]

\[
= (\alpha - \beta) \left( 1 - 2n \alpha^n \beta^n + \sum_{j=1}^{n} (\alpha^{n+j} \beta^{n-j} + 2\alpha^n \beta^n + \alpha^{n-j} \beta^{n+j}) \right)
\]

\[
= (\alpha - \beta) \left( 1 - 2n \alpha^n \beta^n + \sum_{j=1}^{n} \alpha^{n-j} \beta^{n-j} (\alpha^{j} + \beta^{j})^2 \right)
\]

\[
= (\alpha - \beta) \left( 1 - 2n \ell^n + \sum_{j=1}^{n} \ell^{n-j} t_j^2 \right)
\]

Squaring both sides gives the equation. \( \square \)

We then just need to check the case for \( n \) even. We first need the following lemma.

**Lemma 5.13.** For all \( n \geq 1 \), we have \( t_2^n = t_2^n - 2\ell^n \).

**Proof.** Let \( \alpha \) and \( \beta \) be as above. Then we have

\[
t_2^n = \alpha^{2n} + \beta^{2n} = (\alpha^n + \beta^n)^2 - 2\alpha^n \beta^n = t_2^n - 2\ell^n.
\]

\( \square \)

**Proof of Proposition 5.10.** We see from Lemma 5.12 that if \( n \) is odd, this is true. If \( n \) is even, then we can show by induction and Lemma 5.13 that if \( n = 2^m \) with \( m \) odd then

\[
t_2^n - 4\ell^n = (t_2^m - 4\ell^m) \left( \prod_{j=0}^{r-1} t_{2^m} \right)^2.
\]

\( \square \)

**Proof of Proposition 5.3.** As \( F_n \subset F(A[p^\infty]) \), then it is unramified outside \( \infty \), \( p \) and \( N_A \). We see by Lemma 5.4 that the decomposition group of a place in \( F \) dividing \( \infty \cdot p \cdot N_A \) inside \( \Delta_n \) is contained in a Borel. Furthermore, by Lemma 5.5 and Lemma 5.9 the decomposition group of a place \( \nu \) in \( F \) dividing \( N_E \) but not \( p \) or \( N_A \) such that \( a_\nu(A)^2 - 4q_\nu \) is a square modulo \( p \) inside \( \Delta_n \) is contained in a Borel. Since any Borel intersects trivially with \( A_n \) then these places must split completely in \( F_n/L_n \).

\( \square \)

**Proof of Theorem 5.1.** We have an injection

\[
\mu : V_n \to E(F_n) \otimes \mathbb{Q}_p
\]

\[
f \mapsto \sum_D f(D) \cdot Q_{A,D}
\]

where \( Q_{A,D} \) are the higher modular points. Let

\[
S_n = \{ P \in E(F_n) : \text{there exists a } k \geq 0 \text{ such that } p^k \cdot P \in \mathbb{Z}_p G_n \cdot Q_{A,D} \}
\]

15
be the saturated group generated by the higher modular points in $E(F_n)$. This group contains all torsion points in $E(F_n)$ and there exists a short exact sequence

$$0 \to E(F_n)_{\text{tors}} \to S_n \to U_n \to 0$$

where $U_n$ can be identified as a $G_n$-stable lattice in the image of $\mu$ which has no $A_n$-fixed elements. As seen in the proof of [13, Theorem 24], if $E(F_n)[p] = 0$, we have

$$|H^1(A_n, S_n)| = |H^1(A_n, U_n)| = p^n.$$  

However, we have the following,

**Lemma 5.14.** If $\mathcal{P}_{Q,E,p}$ is surjective then for all $n \geq 0$, $E(F_n)[p] = 0$.

**Proof.** Let $K_n = F_n \cap \mathbb{Q}(E[p])$ and let $H = \text{Gal}(E(E[p])/K_n) \leq \text{GL}_2(\mathbb{F}_p)$. If $p \geq 5$, then either $H \supseteq \text{SL}_2(\mathbb{F}_p)$ or $H \subseteq \mathbb{Z}_p$, and if $p = 3$, then either $H \supseteq \text{SL}_2(\mathbb{F}_3)$, $H \subseteq \mathbb{Z}_3$ or $H = \mathbb{Q}_8 \subset \text{SL}_2(\mathbb{F}_3)$ by [11, Theorem 4.9] where $Q_8$ is a quaternion group.

Let $\nu$ be a place of $F_n$ above $p$. As $p$ is a prime of good ordinary or multiplicative reduction with respect to $E$, if we let $I_n$ be the inertia subgroup of $G_{F_n}$, then $\mathcal{P}_{F_n,E,p}(I_\nu)$ contains the set of matrices of the form $(\begin{smallmatrix} * & \nu \\ 0 & * \end{smallmatrix})$. Therefore $H$ contains this set and so $H \supseteq \text{SL}_2(\mathbb{F}_p)$. But then the mapping $\det : H \to \mathbb{F}_p^\times$ is surjective and has kernel $\text{SL}_2(\mathbb{F}_p)$ meaning $H = \text{GL}_2(\mathbb{F}_p)$. Therefore we must have $H = \text{GL}_2(\mathbb{F}_p)$ and so $K_n = \mathbb{Q}$. As $E(Q)[p] = 0$ then this means $E(F_n)[p] = 0$. □

If we consider the natural inclusion of $S_n$ in $E(F_n)$, then the cokernel $Y_n$ is a free $\mathbb{Z}$-module and we obtain a long exact sequence

$$0 \to E(L_n)_{\text{tors}} \to E(L_n) \to Y_n^{A_n} \to H^1(A_n, S_n) \to H^1(A_n, E(F_n))$$

where $Y_n^{A_n}$ has the same rank as $E(L_n)$.

If we compose the last map with the inflation map we obtain

$$\delta_n : H^1(A_n, S_n) \to H^1(L_n, E)$$

known as the derivation map. In particular, we have

$$\left(\frac{S_n}{p^nS_n}\right)^{A_n}_{\mathbb{F}_p} \cong H^1(A_n, S_n).$$

We thus call the image of $\delta_n$ the derived classes of higher modular points.

**Lemma 5.15.** The image of $\delta_n$ is contained in $\text{III}(E/L_n)$.

**Proof.** We let $\eta$ be a lift of an element in the image of $\delta_n$ in the map

$$H^1(L_n, E[m]) \to H^1(L_n, E)[m]$$

for a sufficiently large $m$. The extension $F_n/L_n$ is unramified at a place $\nu$ outside the set of places in $L_n$ above $N_E$, $p$ or $\infty$ and so the restriction of $\eta$ to $H^1(L_{n,\nu}, E[m])$ will lie in $H^1(L_{n,\nu}, E[m])$.

If $\nu$ is a place of $L_n$ lying above $\infty$, $p$ or $N_A$ or is a place that lies above $N_E$ but not above $\infty$, $p$ or $N_A$, then Proposition 5.3 shows that $\nu$ splits completely in the extension $F_n/L_n$. Then the restriction of $\eta$ to $H^1(L_{n,\nu}, E[m])$ is trivial as it comes from the inflation

$$H^1(F_n/L_n, E(F_n)) \to H^1(L_n, E).$$

Hence, $\eta$ belongs to $\text{Sel}^m(E/L_n)$. □
We therefore have the map
\[ \delta_n : H^1(A_n, S_n) \to \text{III}(E/L_n). \]
However, if \( Q_{A,D} \nmid p \cdot E(F_n) \) then \( S_{B_n} = T_{B_n} \). Therefore \( S_n \cong T_n \) by Lemma 3.5. Hence we can look at the cohomology with respect to the standard \( Z_p[\Delta_n] \)-lattice in \( V_n \).

**Lemma 5.16.** We have \( H^1(A_n, T_n) = Z/p^n Z \).

**Proof.** Identical to the proof of Lemma 28 which looks at \( Z[\Delta_n] \)-modules.

We thus have two options. Firstly, if \( \delta_n \) is not injective, then from the long exact sequence we must have the rank of \( Y^\text{An} \) positive and hence so must \( E(L_n) \). Then \( E(L_n) \) will contribute a copy of \( Z/p^n Z \) in \( \text{Sel}^{p^\nu}(E/L_n) \) as \( E(L_n)[p^n] = 0 \).

If \( \delta_n \) is injective, then \( \text{III}(E/L_n)[p^n] \) must contain a cyclic subgroup of order \( p^n \). Therefore, \( \text{Sel}^{p^\nu}(E/L_n) \) must contain an element of order \( p^n \) by lifting the image of \( \delta_n \) from \( \text{III}(E/L_n)[p^n] \).

We can look further at Theorem 5.1 by taking semistable \( A/Q \) and assuming \( p_{Q,A,p} \) is surjective. We will require the following.

**Proposition 5.17.** If we let \( A/Q \) be semistable and \( p_{Q,A,p} \) be surjective, then \( \tau_{F,A,p} \) is surjective.

**Proof.** Let \( K = \mathbb{Q}(A[p]) \cap F \) and \( H = \text{Gal}(\mathbb{Q}(A[p])/K) \triangleleft \text{GL}_2(\mathbb{F}_p) \). As \( A \) is semistable, all primes of \( F \) lying above \( p \) are of good or multiplicative reduction. Let \( \nu \) be a place of \( F \) above \( p \) and \( I_\nu \) be the inertia subgroup of \( G_F \). Then by Lemma 11, \( p_{F,A,p}(I_\nu) \) either contains the set \( \{ (1,0,0) \} \) or a non-split Cartan subgroup of \( \text{GL}_2(\mathbb{F}_p) \) depending on whether \( \nu \) is a place of good ordinary or multiplicative reduction for the first case and good supersingular reduction in the second.

The first case gives \( H = \text{GL}_2(\mathbb{F}_p) \) as seen in the proof of Lemma 5.14. For the good supersingular reduction case, Theorem 4.9 shows that \( H \cong \text{SL}_2(\mathbb{F}_p) \) or \( H \leq \mathbb{Z}_p \) for \( p > 3 \) and also \( H \) could be the quaternion group \( Q_8 \) if \( p = 3 \). Therefore as a non-split Cartan subgroup has order \( p^2 - 1 \), then for all \( p \geq 3 \), we have \( H \cong \text{SL}_2(\mathbb{F}_p) \). However, \( \det : H \to \mathbb{F}_p^\times \) is surjective as \( H \) contains a non-split Cartan subgroup giving \( H = \text{GL}_2(\mathbb{F}_p) \).

Therefore \( H \cong \text{Gal}(F(A[p])/F) \) meaning \( p_{F,A,p} \) is surjective. But \( A \) is semistable which implies \( p_{F,A,p} \) is surjective and hence \( \tau_{F,A,p} \) is also.

Therefore when \( A/Q \) is semistable, we can reduce Theorem 5.1 to the following.

**Theorem 5.18.** Let \( p > 2 \) be a prime. Let \( E/Q \) and \( A/Q \) be elliptic curves of conductor \( N_E \) and \( N_A \) respectively. Let

\[ F := \begin{cases} K_{N_E} & \text{if } p \nmid N_E, \\ K_{N_E}/F & \text{if } p|N_E. \end{cases} \]

Assume that:

1. \( A \) is semistable,
2. \( E \) has either split multiplicative reduction at \( p \) with \( p \nmid \text{ord}_p(\Delta_E) \), non-split multiplicative reduction at \( p \) or good ordinary non-anomalous reduction at \( p \),
3. The degree of any isogeny of \( A \) defined over \( Q \) is coprime to \( N_E \),
4. \( p_{Q,A,p} \) is surjective,
5. \( p_{Q,E,p} \) is surjective,

6. Any prime \( \ell \) of bad reduction of \( E \) and good reduction of \( A \) such that \( \ell \neq p \) has \( a_\ell(A)^2 - 4\ell \) square modulo \( p \).

Then there exists an element of order \( p^n \) in \( \text{Sel}^{p^n}(E/L_n) \).

6 EXAMPLES

We now look at applying Theorem 5.18 to a few examples. For information on specific elliptic curves, we obtained our data from [12].

**Example.** Let

\[ E : y^2 + y = x^3 - x^2 - x - 2 \]

be the elliptic curve with Cremona label 143a1 and

\[ A : y^2 + y = x^3 + x^2 + 9x + 1 \]

be the elliptic curve with Cremona label 35a1. Then if we let \( p = 7 \), then this is a prime of good ordinary non-anomalous reduction for \( E \). We see that the only \( \mathbb{Q} \)-isogeny on \( A \) is of degree 3, which is coprime to \( N_E \) and both \( p_{Q,A,7} \) and \( p_{Q,E,7} \) are surjective. Also,

\[
\begin{align*}
a_{11}(A)^2 - 4 \cdot 11 &= -35 \equiv 0 \pmod{7} \\
a_{13}(A)^2 - 4 \cdot 13 &= -27 \equiv 1 \pmod{7}
\end{align*}
\]

which are both squares modulo 7. Therefore by Theorem 5.18, there exists an element of order \( 7^n \) in \( \text{Sel}^{7^n}(E/L_n) \) for all \( n \geq 1 \).

We also see that \( E \) doesn’t necessarily have to be a semistable elliptic curve.

**Example.** Let

\[ E : y^2 + xy = x^3 - x^2 - 5 \]

be the elliptic curve with Cremona label 45a1 and

\[ A : y^2 + xy = x^3 + x \]

be the elliptic curve with Cremona label 21a4. Then if we let \( p = 5 \), then this is a prime of non-split multiplicative reduction for \( E \). We see that the only \( \mathbb{Q} \)-isogeny on \( A \) is of degree 2, 4 or 8, which are coprime to \( N_E \) and both \( p_{Q,A,5} \) and \( p_{Q,E,5} \) are surjective. Also,

\[
\begin{align*}
a_3(A)^2 - 4 \cdot 3 &= -11 \equiv 4 \pmod{5}
\end{align*}
\]

which is a square modulo 5. Therefore by Theorem 5.18, there exists an element of order \( 5^n \) in \( \text{Sel}^{5^n}(E/L_n) \) for all \( n \geq 1 \).

Depending on the curves \( E \) and \( A \), we can vary the prime \( p \) if it is of good ordinary non-anomalous reduction for \( E \).

**Example.** Let

\[ E : y^2 + xy = x^3 - 3x + 1 \]

be the elliptic curve with Cremona label 34a1 and

\[ A : y^2 + y = x^3 + x^2 - 3x + 1 \]
be the elliptic curve with Cremona label 37b3. We know by \cite{10} Lemma 8.18 that 3 is the only prime of good anomalous reduction for \(E\). Therefore, we let \(p > 3\) be a prime of good ordinary reduction such that \(p \equiv 1, 3 \pmod{8}\). We see that the only \(\mathbb{Q}\)-isogeny on \(A\) is of degree 3 or 9, which are coprime to \(N_E\) and both \(\tilde{\rho}_{Q,A,p}\) and \(\tilde{\rho}_{Q,E,p}\) are surjective. Also,

\[
\begin{align*}
a_2(A)^2 - 4 \cdot 2 &= -8 \\
a_{17}(A)^2 - 4 \cdot 17 &= -32
\end{align*}
\]

which are square modulo \(p\) as \(p \equiv 1, 3 \pmod{8}\). Therefore by Theorem \[5.18\] there exists an element of order \(p^n\) in \(\text{Sel}^{p^n}(E/L_n)\) for all \(n \geq 1\). The first such prime is \(p = 11\).

We can even vary the curves \(E\) and \(A\) if they both have prime conductor.

**Example.** Let \(E/\mathbb{Q}\) and \(A/\mathbb{Q}\) be elliptic curves of prime conductor \(p\) and \(q\) respectively. We see from \cite{4} Proposition 2 that if \(p\) is a prime of split multiplicative reduction for \(E\) then \(p \nmid \text{ord}_p(\Delta_E)\) and \(\tilde{\rho}_{Q,A,p}\) is surjective for all \(p\). We also have that \(\tilde{\rho}_{Q,E,p}\) is surjective as \(p \geq 11\). In particular, \(A\) has no \(\mathbb{Q}\)-isogeny defined over \(\mathbb{Q}\). Hence, by Theorem \[5.18\] \(\text{Sel}^{p^n}(E/L_n)\) contains an element of order \(p^n\) for all \(p\) prime and \(n \geq 1\).

We also show a specific example for \(E\) with conductor \(pq\) for \(p, q\) prime such that \(p \neq q\).

**Example.** Let \(a, b \in \mathbb{Z}\) such that at least one of \(a\) or \(b\) is not divisible by 3 and

\[
a^{12} - 9a^4b + 27a^2b^2 - 27b^3
\]

is not a square. Then by \cite{17} there exists infinitely many \(m \in \mathbb{Z}\) such that

\[
E_m : y^2 + y = x^3 + ax^2 + bx + m
\]

is an elliptic curve where \(|\Delta_{E_m}| = pq\). Here, \(p\) is an odd prime and \(q\) is either 1 or an odd prime different from \(p\). If we pick \(m\) such that \(p \geq 11\), then as \(E_m\) is semistable, \(\tilde{\rho}_{Q,E_m,p}\) is surjective. In particular, \(p\) is a prime of multiplicative reduction such that \(\text{ord}_p(\Delta_{E_m}) = 1\).

Suppose there exists an elliptic curve \(A/\mathbb{Q}\) of conductor \(q\). Then there exists no \(\mathbb{Q}\)-isogeny of \(A\) of degree \(p\) or \(q\) and \(\tilde{\rho}_{Q,A,p}\) is surjective as \(p \geq 11\). Therefore, by Theorem \[5.18\] \(\text{Sel}^{p^n}(E_m/L_n)\) contains an element of order \(p^n\) for all \(n \geq 1\).

**References**

1. E. Artin. *Geometric algebra*. Interscience Publishers, Inc., New York-London, 1957.

2. N. Avni, U. Onn, A. Prasad, and L. Vaserstein. Similarity classes of 3 × 3 matrices over a local principal ideal ring. *Comm. Algebra*, 37(8):2601–2615, 2009.

3. D. J. Benson. *Representations and cohomology. I*, volume 30 of *Cambridge Studies in Advanced Mathematics*. Cambridge University Press, Cambridge, 1991. Basic representation theory of finite groups and associative algebras.

4. C. Delaunay and C. Wuthrich. Self-points on elliptic curves of prime conductor. *Int. J. Number Theory*, 5(5):911–932, 2009.

5. W. Duke and A. Tóth. The splitting of primes in division fields of elliptic curves. *Experiment. Math.*, 11(4):555–565 (2003), 2002.
[6] R. Greenberg. Iwasawa theory, projective modules, and modular representations. *Mem. Amer. Math. Soc.*, 211(992):vi+185, 2011.

[7] S. Howe and K. Joshi. Asymptotics of conductors of elliptic curves over \( \mathbb{Q} \), 2012.

[8] N. M. Katz and B. Mazur. *Arithmetic moduli of elliptic curves*, volume 108 of *Annals of Mathematics Studies*. Princeton University Press, Princeton, NJ, 1985.

[9] V. A. Kolyvagin. Euler systems. In *The Grothendieck Festschrift, Vol. II*, volume 87 of *Progr. Math.*, pages 435–483. Birkhäuser Boston, Boston, MA, 1990.

[10] B. Mazur. Rational points of abelian varieties with values in towers of number fields. *Invent. Math.*, 18:183–266, 1972.

[11] J.-P. Serre. Propriétés galoisiennes des points d’ordre fini des courbes elliptiques. *Invent. Math.*, 15(4):259–331, 1972.

[12] The LMFDB Collaboration. The L-functions and Modular Forms Database. [http://www.lmfdb.org](http://www.lmfdb.org) 2019. [Online; accessed 14 October 2019].

[13] C. Wuthrich. Self-points on elliptic curves. *Algebra Number Theory*, 3(3):283–315, 2009.