Algebra & Number Theory

Volume 3
2009
No. 3

Self-points on elliptic curves

Christian Wuthrich

mathematical sciences publishers

ALGEBRA AND NUMBER THEORY 3:3(2009)

Self-points on elliptic curves

Christian Wuthrich

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N and let p be a prime. We consider trace-compatible towers of modular points in the noncommutative division tower $\mathbb{Q}(E[p^\infty])$. Under weak assumptions, we can prove that all these points are of infinite order and determine the rank of the group they generate. Also, we use Kolyvagin's construction of derivative classes to find explicit elements in certain Tate–Shafarevich groups.

1. Introduction

1.1. ***Definition of self-points.*** Let $E/\mathbb{Q}$ be an elliptic curve and write N for its conductor. As proved in [Breuil et al. 2001], there exists a modular parametrisation

$$\varphi_E : X_0(N) \to E$$

that is a surjective morphism defined over $\mathbb{Q}$ and maps the cusp ∞ on the modular curve $X_0(N)$ to O. The open subvariety $Y_0(N)$ in $X_0(N)$ is a moduli space for the set of pairs (A, C), where A is an elliptic curve and C is a cyclic subgroup in A of order N. More precisely, if $k/\mathbb{Q}$ is a field, then $Y_0(N)(k)$ is in bijection with the set of such pairs (A, C) with A and C defined over k, up to isomorphism over the algebraic closure $\bar{k}$.

In particular, we may consider the pairs $x_C = (E, C)$ for any given cyclic subgroup C of order N in E as a point in $Y_0(N)(\mathbb{C})$. Its image $P_C = \varphi_E(x_C)$ under the modular parametrisation is called a *self-point* of E. The field of definition of the point P_C on E is the same as the field of definition $\mathbb{Q}(C)$ of C. The compositum of all $\mathbb{Q}(C)$ will be denoted by K_N; it is the smallest field K such that the Galois group $\mathrm{Gal}(\overline{K}/K)$ acts by scalars on $E[N]$.

More generally, for any integer m we define a number field K_m as follows. There is a Galois representation attached to the m-torsion points on E, given by

$$\bar{\rho}_m : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \longrightarrow \mathrm{Aut}(E[m]) \cong \mathrm{GL}_2(\mathbb{Z}/m\mathbb{Z}) \longrightarrow \mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z}).$$

MSC2000: primary 11G05; secondary 11G18, 11G40.
Keywords: elliptic curves, modular point, modular curves.
The author was supported by a fellowship of the Swiss National Science Foundation.

The field K_m is the field fixed by the kernel of $\bar{\rho}_m$. The Galois group of the extension $K_m/\mathbb{Q}$ can be viewed via $\bar{\rho}_m$ as a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})$.

We will call *higher self-point* the image under φ_E of any pair (A, C) in which A is an elliptic curve that is isogenous to E over $\overline{\mathbb{Q}}$, though the most interesting case of higher self-points is the case when the isogeny between E and A is of degree a prime power p^n. In particular, this prime p is allowed to divide the conductor N.

This construction imitates the definition of Heegner points, where one uses pairs (A, C) with A having complex multiplication. More generally, modular points on elliptic curves were considered earlier by Harris [1979] without any restriction on A. This article is a sequel to the articles [Delaunay and Wuthrich 2008] and [Wuthrich 2007] on self-points, where we have emphasised already that the theory of self-points differs from the well-known theory of Heegner points. For instance, there does not seem to be a link between the root numbers and the question of whether the self-points are of infinite order.

We present here not only a generalisation of the previous results on self-points, but also we introduce the construction of derivative classes à la Kolyvagin. Indeed, Kolyvagin [1990] was able to find upper bounds on certain Selmer groups by constructing cohomology classes starting from Heegner points. We propose here to do the analogue for self-points. But the situation is radically different as the Galois groups involved are noncommutative; rather than finding upper bounds of Selmer groups over the base field, we will find *lower* bounds on Selmer groups over certain number fields.

1.2. ***The results for self-points.*** The main question that arises first is whether we can determine if the self-points are of infinite order in the Mordell–Weil group $E(\mathbb{Q}(C))$. It was shown in [Delaunay and Wuthrich 2008] that the self-points are always of infinite order if the conductor is a prime number. We extend here the method and provide a framework to treat the general case. In Section 5.2 we will prove the following.

Theorem 12. *Let $E/\mathbb{Q}$ be a semistable elliptic curve of conductor $N \neq 30$ or 210. Then all the self-points are of infinite order.*

But the methods are more general and we are able to prove that they are of infinite order in most cases. In fact, we conjecture that this holds whenever E does not admit complex multiplication. In Section 6.2 we will give a self-point of finite order on a curve with complex multiplication. In the largest generality, we are able to prove in Theorem 2 that there is at least one self-point of infinite order under the assumption that $j(E) \notin \frac{1}{2}\mathbb{Z}$.

Next we address the question of the rank of the group generated by self-points in $E(K_N)$. If N is prime, we saw that the only relation among the self-points is that the sum of all of them is a torsion point in $E(\mathbb{Q})$. For a general conductor, we

find that for all proper divisors d of N and all cyclic subgroups B in E of order d, the sum of all self-points P_C with $C \supset B$ is torsion. This is proved in Proposition 4 as a consequence of the existence of the degeneracy maps on modular curves. For a lot of semistable curves, the following result shows that these are the only relations among self-points.

Theorem 14. *Let $E/\mathbb{Q}$ be a semistable elliptic curve. Suppose that N is not equal to* 30 *or* 210. *Suppose that for each prime $p \mid N$ such that $\bar{\rho}_p$ is not surjective, there is a prime $\ell \mid N$ such that the Tamagawa number c_ℓ is not divisible by p. Then the group generated by the self-points is of rank N.*

We think that this may hold more generally.

Conjecture. *Let $E/\mathbb{Q}$ be an elliptic curve without complex multiplication. Then all the self-points are of infinite order and the only relations among them are produced by the degeneracy maps as described in Proposition 4. In particular, the rank of the group generated by self-points is equal to*

$$\delta(N) = \prod_{p|N} \lceil (1 - p^{-2}) \cdot p^{\mathrm{ord}_p(N)} \rceil,$$

where $\lceil x \rceil$ denotes the smallest integer no less than x.

The expression $\delta(N)$ in the conjecture is equal to N if and only if N is square-free.

1.3. ***The results for higher self-points.*** We are particularly interested in higher self-points that are modular points coming from a pair (E', C') in which E' has an isogeny to E of degree a power of a prime p. We treat two cases: when p is a prime of good reduction and when p is a prime of multiplicative reduction.

For simplicity we only sketch the results for the good case here, that is, $p \nmid N$. See Section 7 for more details.

We fix now a cyclic subgroup C in E of order N; the following construction depends on this choice, but our notation will not reflect this. Let D be a cyclic subgroup of E of order p^{n+1} and let $E' = E/D$. Given any self-point P_C, we may consider the image C' of C under the isogeny $E \to E'$. The higher self-point Q_D is defined to be the image of $(E', C') \in Y_0(N)$ under the modular parametrisation φ_E. It is a point in the Mordell–Weil group of E over the field $\mathbb{Q}(C, D)$, which is contained in $K_{p^{n+1}N}$. In Corollary 20, we are able to prove that the higher self-points are all of infinite order in some cases.

Theorem 1. *Let $E/\mathbb{Q}$ be a semistable curve of conductor N not equal to* 30 *or* 210. *Suppose that p is a prime such that $p > N$, and such that the Galois representation $\bar{\rho}_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_p)$ is surjective. Let s be the rank of the group generated by the self-points in $E(K_N)$. Then the higher self-points in $E(K_{p^{n+1}N})$ generate a group of rank $s \cdot (p+1) \cdot p^n$.*

If one assumes that the prime is of ordinary reduction for E, one can weaken the condition on the bad reduction substantially.

Furthermore these higher self-points are trace-compatible in the following sense. Let D be a cyclic subgroup of order p^{n+1}, and let a_p be the p-th Fourier coefficient of the modular form associated to the isogeny class of E. Then we have

$$\sum_{D' \supset D} Q_{D'} = a_p \cdot Q_D,$$

where the sum runs over all cyclic subgroups D' of order p^{n+2} containing D. For any number field F, we will write

$$\rho_{F,p} : \mathrm{Gal}(\bar{F}/F) \longrightarrow \mathrm{Aut}(T_p E) \cong \mathrm{GL}_2(\mathbb{Z}_p) \longrightarrow \mathrm{PGL}_2(\mathbb{Z}_p)$$

for the representation of $\mathrm{Gal}(\bar{F}/F)$ on the Tate module $T_p E$. If the Galois representation $\rho_{K_N,p}$ is surjective, then we can reformulate the above relation by saying that the trace of $Q_{D'}$ from its field of definition to the field of definition of Q_D is equal to $a_p \cdot Q_D$. This trace compatibility reminds one of the definition of an Euler system. However, the field $\mathbb{Q}(C, D)$ is not Galois over $\mathbb{Q}$ and the Galois closure is not an abelian extension, and worse not even a solvable extension.

The higher self-points are the only known towers of points of infinite order in the division tower $\mathbb{Q}(E[p^\infty])$ of E. Nevertheless the growth of the rank of the Mordell–Weil group should often be faster than the lower bound $(p+1)p^n$ that we establish here in many cases. This is due to changing signs in the functional equations and the corresponding parity results on the corank of Selmer groups. See [Coates et al. 2009; Mazur and Rubin 2008]. These results predict, under the assumption of the finiteness of the Tate–Shafarevich group, that there should be more points of infinite order in the division tower that are not accounted for by higher self-points. Furthermore the higher self-points do not seem to be linked in any obvious way to root numbers. Also it is completely unknown if there is a relation to L-functions (or to noncommutative p-adic L-functions as in [Coates et al. 2005]) in analogy to the Gross–Zagier formula for Heegner points.

1.4. ***Derivatives.*** Kolyvagin [1990] has used Heegner points of infinite order to construct cohomology classes that obstruct the existence of further points of infinite order. We aim to use a similar construction to build cohomology classes from higher self-points of infinite order.

Let p be a prime of either good ordinary reduction or of multiplicative reduction. If p does not divide the conductor N, define $F_n = K_{p^{n+1}N}$; otherwise let $F_n = K_{p^n N}$. Put $F = F_{-1}$. If we suppose that $\rho_{F,p} : \mathrm{Gal}(\bar{F}/F) \to \mathrm{PGL}_2(\mathbb{Z}_p)$ is surjective, then $\mathrm{Gal}(F_n/F) = \mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$. We are interested in a particular cyclic subgroup A in $\mathrm{Gal}(F_n/F)$. Choosing a $\mathbb{Z}_p$-basis of the quadratic unramified extension $\mathbb{O}$ of $\mathbb{Z}_p$

gives a map

$$\mathbb{O}^\times \to \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{PGL}_2(\mathbb{Z}_p) \to \mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}),$$

whose image is a cyclic group A_n of order $(p+1)\cdot p^n$. By a slight abuse of notation we will denote the subfield of F_n fixed by A_n by F_n^A.

The construction of derivatives provides us with a map

$$\partial_n : \mathrm{H}^1(A_n, S) \to Ш(E/F_n^A).$$

The source is a cohomology group of the saturated group S of higher self-points (see Section 8 for the definitions). Although we do not know its exact structure, we can prove that it contains at least p^n elements. It seems plausible to think that the map ∂_n is very often injective, but we do have no means to prove this in a single case. Nevertheless, we are able to show the existence of points of infinite order in $E(F_n^A)$ whenever the map is not injective. Here is the final result:

Theorem 21. *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose E does not have potentially good supersingular reduction for any prime of additive reduction. Let p be a prime of either good ordinary or multiplicative reduction. Assume that $\rho_{F,p}$ is surjective and that K_N contains a self-point of infinite order. Then we have*

$$\#\,\mathrm{Sel}_{p^n}(E/F_n^A) \geqslant p^n.$$

The construction of derivatives relies on a property of modular representation theory. The higher self-points generate in the Mordell–Weil group a copy of the irreducible Steinberg representation. More precisely, if H_n denotes $\mathrm{Gal}(F_n/F)$, there is a certain $\mathbb{Q}[H_n]$-module in $E(F_n)\otimes\mathbb{Q}$ that is irreducible, but this module is no longer irreducible over $\mathbb{F}_\ell[H_n]$ when ℓ divides $(p+1)\cdot p^n$. Perhaps the idea of using modular representation theory to study Selmer groups, which was developed in [Greenberg 2008], could shed new light on these derivatives.

2. The fundamental theorem

Theorem 2. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. If the j-invariant of E is not in $\frac{1}{2}\mathbb{Z}$, then there is at least one self-point P_C of infinite order in $E(K_N)$.*

Proof. Let p be a prime that divides the denominator of the j-invariant of E. If possible, we avoid $p=2$. Note that p^2 may divide N, but we know that E acquires multiplicative reduction over some extension of $\mathbb{Q}$ at p.

First we fix an embedding of $\overline{\mathbb{Q}}$ into $\overline{\mathbb{Q}}_p$. We consider the modular parametrisation over $\overline{\mathbb{Z}}_p$. The modular curve $X_0(N)$ over $\overline{\mathbb{Z}}_p$ has a neighbourhood of the cusp ∞ consisting of pairs (A, C) of a Tate curve of the form $A = \overline{\mathbb{Q}}_p^\times/q^{\mathbb{Z}}$, together with a cyclic subgroup C of order N generated by the N-th root of unity. The parameter q is a p-adic analytic uniformiser at ∞, so that the $\mathrm{Spf}\,\overline{\mathbb{Z}}_p[\![q]\!]$ is

the formal completion of $X_0(N)/\overline{\mathbb{Z}}_p$ at the cusp ∞; see [Katz and Mazur 1985, Chapter 8].

Let $f_E = \sum a_n q^n$ be the normalised newform associated to E. Then $f_E/q \cdot dq$ is the associated differential. Let c_E be the Manin constant (of the not necessarily strong Weil curve E), that is, the number such that $\varphi_E^*(\omega_E) = c_E \cdot f_E/q \cdot dq$, where ω_E is the invariant differential on E. The rigid analytic map induced by φ_E on the completion can now be characterised as

$$\log_E(\varphi_E(q)) = \int_O^{\varphi_E(q)} \omega_E = c_E \cdot \int_0^q f_E \frac{dq}{q} = c_E \cdot \sum_{n \geqslant 1} \frac{a_n}{n} \cdot q^n. \tag{1}$$

Here $\log_E$ denotes the formal logarithm associated to E from the formal group $\hat{E}(\overline{\mathfrak{m}})$ to the maximal ideal $\hat{\mathbb{G}}_a(\overline{\mathfrak{m}}) = \overline{\mathfrak{m}}$ of $\overline{\mathbb{Z}}_p$. We deduce from this description the following lemma that will be useful later. Write $|\cdot|_p$ for the normalised absolute value such that $|p|_p = p^{-1}$.

Lemma 3. *Let (A, C) be a point in $Y_0(N)(\overline{\mathbb{Q}}_p)$ such that A is isomorphic to the Tate curve with parameter $q_0 \neq 0$ and C is isomorphic to the Galois module of N-th roots of unity $\mu[N]$. If $|q_0|_p < p^{-1/(p-1)}$, then $\varphi_E(A, C)$ is a point of infinite order on $E(\overline{\mathbb{Q}}_p)$.*

Proof. Under the condition on the absolute value of q_0, we know that the sum on the right-hand side of (1) converges. We consider the sum

$$z = c_E \cdot \sum_{n \geqslant 1} \frac{a_n}{n} \cdot q_0^n.$$

Since the Manin constant is known to be an integer (see [Edixhoven 1991]), the absolute value of the right-hand side is

$$|z|_p = |c_E|_p \cdot \left| q_0 + \frac{a_p}{p} q_0^p \right|_p$$

as these are the terms of large absolute value. However note that the condition on q_0 implies that the second term on the right side is actually slightly smaller that the first, and hence the absolute value of the sum is bounded by

$$|z|_p = |c_E|_p \cdot |q_0|_p < p^{-1/(p-1)}.$$

Therefore the value of z lies in the domain of convergence of the p-adic elliptic exponential $\exp_E$, and we obtain that $\varphi_E(A, C) = \exp_E(z)$. Since we know that $|z|_p \neq 0$, we can deduce that $\exp_E(z)$ is not a torsion point in $E(\overline{\mathbb{Q}}_p)$. □

We may now finish proving the theorem. Since E has multiplicative reduction over $\overline{\mathbb{Z}}_p$, exactly one of the $x_C = (E, C)$ if in the neighbourhood of ∞ on $X_0(N)$;

it is represented by the p-adic Tate parameter q_E associated to E together with the group C isomorphic to $\mu[N]$. If $p \neq 2$, then we know that

$$|q_E|_p = |j(E)|_p^{-1} \leqslant p^{-1} < p^{-1/(p-1)},$$

and if p had to be chosen to be equal to 2 in the beginning then we know that

$$|q_E|_2 = |j(E)|_2^{-1} \leqslant p^{-2} < p^{-1/(p-1)}.$$

Hence in any case, the lemma applies and provides us with a point of infinite order among the self-points. □

If the chosen prime p is such that p^2 does not divide N, then q_E lies in $p^v\mathbb{Z}_p$, where $v = -\operatorname{ord}_p(j(E))$. Hence the proof's point P_C will be defined over $\mathbb{Q}_p$.

The restriction at $p = 2$ seems unnecessary. Often one can deduce the result of the theorem by hand for curves whose j-invariant is an odd integer divided by 2. We present here an easy example. For the curve 2450o1 in Cremona's tables [1997] with j-invariant $-189/2$, the 2-adic Tate parameter is equal to $2+2^2+2^4+\mathbf{O}(2^9)$ and the newform is $f_E = q - q^2 + q^4 + \mathbf{O}(q^8)$. From this one concludes that $\log_E(P_C) = 2^3 + \mathbf{O}(2^5)$. So P_C is of infinite order. Nevertheless we do not see any easy argument to prove that $P_C \neq O$ for a general curve with $j(E) \in \frac{1}{2}\mathbb{Z} \setminus \mathbb{Z}$, as it seems that the 2-adic valuation of $\log_E(P_C)$ can be arbitrarily large.

2.1. ***A torsion self-point.*** We believe that this theorem is still valid if E is a curve with integral j-invariant as long as the curve does not admit complex multiplication. But not all self-points are of infinite order. We present here a surprisingly easy example of a self-point that is torsion.

The curve 27a2 admits a cyclic isogeny of degree 27 defined over $\mathbb{Q}$ to the curve 27a4. Let E be either of the two curves. Then E has exactly one cyclic subgroup of order 27 defined over $\mathbb{Q}$, that is, E admits a self-point in $E(\mathbb{Q})$. Since the rank of $E(\mathbb{Q})$ is zero, the self-point has to be of finite order. Note that these curves have complex multiplication. See Section 6.2 for more detailed computations on these self-points.

3. Relations

In [Delaunay and Wuthrich 2008] it is shown that the self-points on a curve of prime conductor satisfy exactly one relation. What kind of relations could occur among the self-points for a curve of conductor N? Here is a first part of an answer. First, we need some more notation. The Galois group $G = G_N = \mathrm{Gal}(K_N/\mathbb{Q})$ was identified with a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$. For any divisor d of N, we define the image of G_N under the projection $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z}) \to \mathrm{PGL}_2(\mathbb{Z}/d\mathbb{Z})$ as G_d and by K_d its fixed field in K_N. In other words, K_d is the smallest number field for which the absolute Galois groups acts by scalars on $E[d]$.

Proposition 4. *The sum of all self-points is a torsion point defined over $\mathbb{Q}$. If $d \neq N$ is an integer dividing N, then there are relations of the form*

$$R_B: \quad \sum_{C \supset B} P_C \text{ is torsion in } E(K_d),$$

where B is any given cyclic subgroup of order d and C runs through all cyclic groups of order N containing B.

Proof. The degeneracy map $\pi : X_0(N) \to X_0(d)$ induces $\pi^* : J_0(d) \to J_0(N)$ on Jacobians. Given a cyclic subgroup B of order d on E, we may consider the point $x_B = (E, B)$ on $X_0(d)$. The divisor class

$$\pi^*[(x_B) - (\infty)] = \sum_{C \supset B} [(x_C)] - \pi^*[(\infty)]$$

is in the image of π^* in $J_0(N)$ and hence in the kernel of the map $\varphi_E : J_0(N) \to E$ because N is the exact conductor of E. This gives the relation R_B.

Taking $d = 1$ gives the result that the sum of all self-points is a torsion point. Since this sum is fixed by the Galois group, it has to be a rational point. □

4. The Steinberg representations

The aim is to describe certain irreducible representations that will appear in the study of self-points. Let $N > 1$ be an integer. We are interested in the group $P = \mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$. We will decompose the $\mathbb{Q}[P]$-module V whose basis $\{e_C\}$ as a $\mathbb{Q}$-vector space is in bijection with the projective line $\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$ and on which the P-action is given by the usual permutation on the basis. So it can be written as

$$V = \bigoplus_{C \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} \mathbb{Q}e_C = \mathrm{Ind}_B^P(\mathbb{1}_B),$$

where B is a Borel subgroup of P and $\mathbb{1}_B$ is its trivial representation.

Theorem 5. *The $\mathbb{Q}[\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})]$-module V splits into the sum $V = \bigoplus_{D|N} W_D$ of irreducible $\mathbb{Q}[\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})]$-modules W_D, where D runs through all divisors of N. Let $D = \prod_p p^{d_p}$ be the prime decomposition of a divisor D of N. Define*

$$\delta_p = \left\lceil p^{d_p} - p^{d_p - 2} \right\rceil = \begin{cases} 1 & \text{if } d_p = 0, \\ p & \text{if } d_p = 1, \\ p^{d_p} - p^{d_p - 2} & \text{if } d_p > 1. \end{cases}$$

Then W_D has dimension $\delta(D) = \prod_{p|D} \delta_p$ as a $\mathbb{Q}$-vector space.

Proof. We split the proof into three parts according to whether N is a prime, a prime power or any integer. The first two cases could also be treated by invoking [Silberger 1970, Theorem 3.3 on page 58], but, since we need the explicit description of W_D later on, we prefer to prove this theorem in detail. Since the proof is inductive on N, we will now write P_N for $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$ and V_N for its V.

Case: N is prime. Write $p = N$. The claim is simply that the $\mathbb{Q}[P]$-module V_p splits into two irreducible components $W_1 \oplus W_p$. We define W_1 to be the 1-dimensional subspace of V generated by the vector $v_1 = \sum_C e_C$, where the sum runs over all C in $\mathbb{P}^1(\mathbb{F}_p)$. Of course, $W_1 = V_p^P$ is an irreducible $\mathbb{Q}[P]$-submodule of V_p and the space

$$W_p = \Big\{ \sum a_C \cdot e_C \;\Big|\; \sum a_C = 0 \Big\}$$

is a complement to it. It remains to show that W_p is irreducible. Let g be an element of order p in P, such as the class of $\left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$. On $V_p \otimes \mathbb{C}$ the element g acts with eigenvalues 1, 1, ζ, ζ^2, …, ζ^{p-1}, where ζ is a primitive p-th root of unity. Hence on W_p every p-th root of unity appears exactly once as an eigenvalue. So the only possibility for W_p to split up into two $\mathbb{Q}[P]$-submodules would have to involve a 1-dimensional and a $(p-1)$-dimensional submodule.

As we can see from the fact that $\mathrm{PSL}_2(\mathbb{F}_p)$ is a simple group when $p > 3$ and by direct calculations for $p = 2$ and 3, there are only two one-dimensional representations of $\mathrm{PGL}_2(\mathbb{F}_p)$: the trivial representation and the one with kernel $\mathrm{PSL}_2(\mathbb{F}_p)$ of index 2. Since $\mathrm{PSL}_2(\mathbb{F}_p)$ acts transitively on $\mathbb{P}^1(\mathbb{F}_p)$, the one-dimensional subrepresentations of V_p must be contained in $V_p^{\mathrm{PSL}_2(\mathbb{F}_p)} = W_1$.

Case: N is a prime power. We write $N = p^k$ with p prime. We prove the statement by induction on k. The case $k = 1$ has been treated already; thus we may assume that $k \geqslant 2$. The claim is that V_{p^k} splits as $\bigoplus W_{p^m}$, where m runs from 0 to k.

There is a reduction map $\alpha : \mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z}) \to \mathbb{P}^1(\mathbb{Z}/p^{k-1}\mathbb{Z})$ that is surjective and all of whose fibres contain p elements. Define

$$V' = \Big\{ \sum a_C e_C \;\Big|\; a_C = a_{C'} \text{ whenever } \alpha(C) = \alpha(C') \Big\}.$$

It is easy to see that V' is canonically isomorphic to $V_{p^{k-1}}$ as a vector space, so we will identify them. The action of P_{p^k} factors through the quotient $P_{p^k} \to P_{p^{k-1}}$ induced by reduction. By induction, V' splits as a $\mathbb{Q}[P_{p^{k-1}}]$-module into the sum $V' = \bigoplus_{m=0}^{k-1} W_{p^m}$; this also decomposes V' into irreducible $\mathbb{Q}[P_{p^k}]$-modules. As a complement to V', we define

$$W_{p^k} = \Big\{ \sum a_C e_C \;\Big|\; \sum_{\alpha(C)=D} a_C = 0 \text{ for all } D \text{ in } \mathbb{P}^1(\mathbb{Z}/p^{k-1}\mathbb{Z}) \Big\}.$$

It is clear that W_{p^k} is a $\mathbb{Q}[P_{p^k}]$-submodule of V_{p^k}. If $k > 1$ then its dimension is equal to

$$\begin{aligned}\dim_{\mathbb{Q}} W_{p^k} &= \#\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z}) - \#\mathbb{P}^1(\mathbb{Z}/p^{k-1}\mathbb{Z}) \\ &= (p+1)\cdot p^{k-1} - (p+1)\cdot p^{k-2} = p^k - p^{k-2}.\end{aligned}$$

It remains to show that W_{p^k} is irreducible.

Let ∞ be any point in $\mathbb{P}^1(\mathbb{F}_p)$ and write U^∞ for the preimage of ∞ under the reduction map $\mathbb{P}^1(\mathbb{Z}/p^k\mathbb{Z}) \to \mathbb{P}^1(\mathbb{F}_p)$. Within V, we define a linear subspace

$$V^\infty = \left\{ \sum a_C e_C \;\middle|\; a_C = 0 \text{ if } C \in U^\infty \right\}$$

of dimension p^k and let $W^\infty = W_{p^k} \cap V^\infty$ and $V'^\infty = V' \cap V^\infty$. Let g be an element of P_{p^k} of order p^k whose fixed points lie in U^∞. If ∞ is $(0:1)$, then we may take the class of the matrix $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$. The element g acts on $V^\infty \otimes \mathbb{C}$ such that every p^k-th root of unity appears exactly once. The eigenvalues of g on the subspace V'^∞ are all p^{k-1}-st roots of unity. Hence on W^∞ every primitive p^k-th root of unity appears exactly once as an eigenvalue. So W^∞ is an irreducible $\mathbb{Q}[\langle g\rangle]$-module, and so if W_{p^k} splits as a $\mathbb{Q}[P_{p^k}]$-module, then W^∞ has to be completely contained in one of the summands. But for any two distinct points ∞ and ∞' in $\mathbb{P}^1(\mathbb{F}_p)$ the spaces W^∞ and $W^{\infty'}$ span the whole of W_{p^k}. Hence W_{p^k} cannot be reducible.

The general case follows fairly easily from the previous cases. Let $N = \prod p^{n_p}$ be the prime decomposition of N. We may suppose that N is not a prime power, since we have treated this case already. Now the group P_N splits as

$$P_N = \mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z}) = \prod_{p|N} \mathrm{PGL}_2(\mathbb{Z}/p^{n_p}\mathbb{Z}) = \prod_{p|N} P_{p^{n_p}}$$

by the Chinese remainder theorem. Similarly, we have

$$\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z}) = \prod_{p|N} \mathbb{P}^1(\mathbb{Z}/p^{n_p}\mathbb{Z}) \quad \text{and so} \quad V_N = \bigotimes_{p|N} V_{p^{n_p}}$$

as a $\mathbb{Q}[P_N]$-module. Now we use the previous case to rewrite

$$V_N = \bigotimes_{p|N} \bigoplus_{m=0}^{n_p} W_{p^m}.$$

Let D be any divisor of N and $\prod p^{d_p}$ its prime factorisation. Then define

$$W_D = \bigotimes_{p|D} W_{p^{d_p}}.$$

It is clear from the representation theory of direct products that W_D is irreducible. Rearranging the above decomposition of V_N, we arrive at the desired expression $V_N = \bigoplus_{D|N} W_D$. □

Proposition 6. *Let p be a prime. Let G be a subgroup of a Borel subgroup of* $\mathrm{PGL}_2(\mathbb{F}_p)$ *acting on $V_p = \bigoplus \mathbb{Q}e_C$. Suppose that the class of $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ belongs to G. Then V_p decomposes into irreducible $\mathbb{Q}[G]$-modules as $W_1 \oplus W_1' \oplus W_p'$, where W_p' is an irreducible $\mathbb{Q}[G]$-module of dimension $p-1$.*

Proof. Let C_0 be the element of $\mathbb{P}^1(\mathbb{F}_p)$ fixed by the Borel group containing G. By assumption, we know that C_0 is the only fixed point of G acting on $\mathbb{P}^1(\mathbb{F}_p)$. Hence V_p contains two linearly independent vectors that are fixed by G, namely e_{C_0} and $v_0 = \sum_{C \neq C_0} e_C$. The $\mathbb{Q}[G]$-submodule

$$W_p' = \Big\{ \sum_{C \neq C_0} a_C \cdot e_C \;\Big|\; \sum_{C \neq C_0} a_C = 0 \Big\}$$

is a complement to V_p^G. Now use the class g of the matrix $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$ as before to show that W_p' is irreducible since the eigenvalues of g on W_p' are exactly the set of all primitive p-th roots of unity. □

In fact one can show that Theorem 5 holds even for the complex representation $V \otimes \mathbb{C}$ as $\mathbb{C}[\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})]$-modules. On the other hand, Proposition 6 really relies on the fact that we are only considering decompositions as $\mathbb{Q}[G]$-modules. For instance, we may well take G to be the cyclic group generated by the matrix $\left(\begin{smallmatrix}1 & 1\\ 0 & 1\end{smallmatrix}\right)$; then of course $W_p' \otimes \mathbb{C}$ will split into 1-dimensional representations. But since the p-th roots of unity are not all defined over $\mathbb{Q}$, at least if $p > 2$, this decomposition does not hold in general for W_p'.

We can now reformulate the statement of Proposition 4 as follows. There is a G-equivariant map $\iota : V_N \to E(K_N) \otimes \mathbb{Q}$, defined by sending e_C to P_C. It has a kernel containing all submodules W_d for $d \neq N$ dividing N. So it induces a map $\iota : W_N \to E(K_N) \otimes \mathbb{Q}$ that is G-equivariant. By the fundamental Theorem 2, this morphism is nontrivial if $j \notin \frac{1}{2}\mathbb{Z}$. Hence we can deduce the following corollary.

Corollary 7. *The self-points generate a group of rank at most $\delta(N)$ inside $E(K_N)$. If W_N is an irreducible $\mathbb{Q}[G_N]$-module and the j-invariant is not in $\frac{1}{2}\mathbb{Z}$, then the self-points generate a group of rank $\delta(N)$ and the Galois group acts like the Steinberg representation W_N on it.*

5. Self-points on semistable curves

We will suppose in this section that the curve $E/\mathbb{Q}$ is semistable. In particular, the j-invariant cannot belong to $\frac{1}{2}\mathbb{Z}$ since all primes dividing N must appear in the

denominator of $j(E)$ and there is no curve of conductor 2. Hence the fundamental Theorem 2 applies to E.

5.1. ***Some lemmata.*** Recall that K_m was defined to be the field fixed by the kernel of $\bar{\rho}_m$. We denote the Galois group $\mathrm{Gal}(K_m/\mathbb{Q})$ by G_m and think of it as a subgroup in $\mathrm{PGL}_2(\mathbb{Z}/m\mathbb{Z})$.

In what follows, we often have to split up the primes dividing N into two groups. Let s, standing for "surjective", be the product of all primes p dividing N such that the representation $\bar{\rho}_p$ is surjective. Let m, standing for "méchant", be the product of the remaining primes dividing N. Note that there are not many choices for m as described in the following lemma.

Lemma 8. *We have* $m \in \{1, 2, 3, 4, 5, 6, 7, 10\}$. *If* $p \mid m$, *then* G_p *is contained in a Borel group of* $\mathrm{PGL}_2(\mathbb{F}_p)$ *and hence is either a cyclic or a metacyclic*[1] *group.*

Proof. Let $p \mid m$. By a theorem of Serre [1996], the curve admits a p-isogeny $E \to E'$ defined over $\mathbb{Q}$, and either E or E' must have a point of order p defined over $\mathbb{Q}$. Then by Mazur's theorem [1978] on torsion points on elliptic curves over $\mathbb{Q}$, and we know now that $p \leqslant 7$ and that $m \leqslant 10$. □

Lemma 9. *Let* $E/\mathbb{Q}$ *be a semistable elliptic curve. Then the largest prime* p *dividing* N *is such that the representation* $\bar{\rho}_p$ *is surjective, and* $p - 1 > m$ *unless* N *is* 30 *or* 210.

Proof. If N is divisible by a prime $p \geqslant 13$, then the largest prime p dividing N cannot divide m and satisfies $p - 1 > m$ because $m \leqslant 10$ by the previous lemma. Hence we are left with a finite list of possible N to check. This can be done easily; to illustrate it we show in Table 1 the list of curves of square-free conductors N whose prime divisors are among $\{2, 3, 5, 7\}$. For the full proof, we would need to list also conductors divisible by 11, but then the list will be far too long to be included here. However the only three exceptional isogeny classes can already be seen in this table.

To each isogeny class, we give the number i of isogenous curves, the maximal degree d of an isogeny among them, the value of m, and the largest $p \mid N$ such that $\bar{\rho}_p$ is surjective. This ends the proof. □

Lemma 10. *Let* $E/\mathbb{Q}$ *be a semistable elliptic curve with* $6 \mid N$ *and such that the representation* $\bar{\rho}_2$ *is surjective onto* $\mathrm{PGL}_2(\mathbb{F}_2)$. *If there exists a prime* $p \mid N$ *such that* $3 \nmid c_p$, *then* K_2 *cannot be contained in* K_3.

Proof. We wish to derive a contradiction from the assumption that K_2 is contained in K_3. By assumption, the Galois group G_2 of the extension $K_2/\mathbb{Q}$ is $\mathrm{PGL}_2(\mathbb{F}_2)$, which is isomorphic to the symmetric group on three letters $\mathfrak{S}_3$. The Galois group

[1] metacyclic: a semidirect product of cyclic groups

N	14a	15a	21a	**30a**	35a	42a	70a	105a	**210a**	**210b**	210c	210d	210e
i	6	8	6	**8**	3	6	4	4	**8**	**8**	6	4	8
d	18	16	8	**12**	9	8	4	4	**12**	**12**	8	4	16
m	2	1	1	**6**	1	2	2	1	**6**	**6**	2	2	2
p	7	5	7	**5**	7	7	7	7	**7**	**7**	7	7	7

Table 1. Some of the "evil curves" to be treated separately in Lemma 9.

G_3 is contained in $\mathrm{PGL}_3(\mathbb{F}_3) = \mathfrak{S}_4$. Therefore the Galois group $\mathrm{Gal}(K_3/K_2)$ is contained in the Klein group V_4 of $\mathfrak{S}_4$.

Suppose first that the reduction of E at p is split multiplicative. Let q_E be the Tate parameter of E over $\mathbb{Q}_p$. Choose a place v above p in K_2 and a place w above v in K_3. Then the completion $K_{3,w}$ is equal to $\mathbb{Q}_p(\zeta_3, \sqrt[3]{q_E})$ and $K_{2,v}$ is equal to $\mathbb{Q}_p(\sqrt{q_E})$. Since 3 does not divide $c_p \geqslant 1$, we know that q_E cannot be a cube. Therefore the degree of $K_{3,w}/K_{2,v}$ is divisible by 3. This is impossible since the degree of K_3/K_2 must be a power of 2.

If the reduction is nonsplit multiplicative at p, one can do the same argument but transposed to the extension L of $\mathbb{Q}_p$ over which E acquires split multiplicative reduction. As $L/\mathbb{Q}_p$ is of degree 2, we still find that the degree of $K_{3,w}/K_{2,v}$ must be a multiple of 3. □

Lemma 11. *Let $E/\mathbb{Q}$ be a semistable elliptic curve. For* (ii) *and* (iii) *below, we assume that if $2 \mid N$ and $3 \mid N$, then there is a prime $p \mid N$ such that $3 \nmid c_p$.*

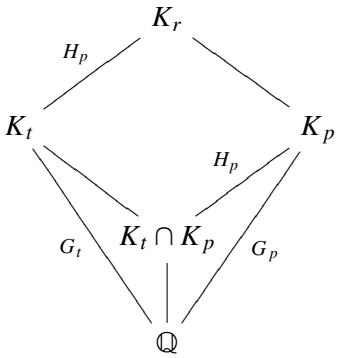
(i) *G_s acts transitively on the set $\mathbb{P}^1(\mathbb{Z}/s\mathbb{Z})$ of cyclic subgroups of order s in E.*

(ii) *The Steinberg representation W_s is irreducible as a $\mathbb{Q}[G_s]$-module.*

(iii) *Suppose W_m decomposes into irreducible $\mathbb{Q}[G_m]$-modules as $U_1 \oplus \cdots \oplus U_k$. Then W_N decomposes into irreducible $\mathbb{Q}[G_N]$-modules as*

$$W_N = \bigoplus_{i=1}^{k} (U_i \otimes W_s).$$

Proof. We will first prove by induction the statement in (ii) with s replaced by any of its divisors r, assuming the additional hypothesis. If $r = p$ is prime then $G_p = \mathrm{PGL}_2(\mathbb{F}_p)$ and Theorem 5 shows that W_p is irreducible as a $\mathbb{Q}[G_p]$-module. Let p be the largest prime factor of r. We may suppose that r is composite and so $p > 2$. Put $t = r/p \geqslant 2$. We assume that W_t is an irreducible $\mathbb{Q}[G_t]$-module. We wish to prove that W_r is an irreducible $\mathbb{Q}[G_r]$-module.



The Galois group $H_p = \mathrm{Gal}(K_r/K_t)$ is isomorphic to that of the extension $K_p/K_t \cap K_p$. Hence H_p is a normal subgroup of $G_p = \mathrm{PGL}_2(\mathbb{F}_p)$. We use the fact that $\mathrm{PSL}_2(\mathbb{F}_p)$ is simple for $p > 3$. So H_p is either all of G_p, $\mathrm{PSL}_2(\mathbb{F}_p)$, the trivial group or, in the case $p = 3$, the Klein group V_4 in $\mathrm{PGL}_2(\mathbb{F}_3) = \mathfrak{S}_4$. Treating the four cases separately, we will prove that W_p is an irreducible $\mathbb{Q}[H_p]$-module.

If H_p is all of G_p, then W_p is irreducible as a $\mathbb{Q}[H_p]$-module by Theorem 5. If H_p is equal to $\mathrm{PSL}_2(\mathbb{F}_p)$, then W_p could split at most into two subspace of equal dimension since $\mathrm{PSL}_2(\mathbb{F}_p)$ has index 2 in $\mathrm{PGL}_2(\mathbb{F}_p)$. But the dimension of W_p is odd unless $p = 2$, which we excluded. Hence W_p is irreducible.

Next, we will exclude the case when H_p is trivial. If it were so, then there is a surjective map from G_t onto $G_p = \mathrm{PGL}_2(\mathbb{F}_p)$. The group G_t is contained in $\mathrm{PGL}_2(\mathbb{Z}/t\mathbb{Z})$, whose order is

$$\prod_{\ell \mid t} \ell \cdot (\ell + 1) \cdot (\ell - 1).$$

So the order of G_t cannot be divisible by p since p is larger than any of the ℓ, unless $p = 3$ and $t = 2$. It is also impossible that there is a surjective map from $\mathrm{PGL}_2(\mathbb{F}_2)$ onto $\mathrm{PGL}_2(\mathbb{F}_3)$. So H_p is not trivial.

Finally, we treat the case when H_p is the Klein group in $\mathrm{PGL}_2(\mathbb{F}_3)$. Since $p = 3$, we have $t = 2$. As $G_2 = \mathrm{PGL}_2(\mathbb{F}_2) = \mathfrak{S}_3$, the only possibility for this case is when K_2 is contained in K_3. But it was shown in Lemma 10 that this is not possible under our additional hypothesis.

Let X be a sub-$\mathbb{Q}[G_r]$-module of $W_r = W_p \otimes W_t$. As H_p acts trivially on W_t, we deduce that there is a subspace Z of W_t such that $X = W_p \otimes Z$. By the induction hypothesis, we know that W_t is irreducible as a $\mathbb{Q}[G_t]$-module. Hence $Z = W_t$ and we have shown that W_r is $\mathbb{Q}[G_r]$-irreducible.

Now we will prove (i). If the additional hypothesis is verified, then W_s is an irreducible $\mathbb{Q}[G_s]$-module by (ii); hence G_s acts transitively on $\mathbb{P}^1(\mathbb{Z}/s\mathbb{Z})$. But the only place where we used the additional hypothesis in the proof of (ii) is when we excluded the possibility that H_p is the Klein group in $\mathrm{PGL}_2(\mathbb{F}_3)$. But since the

Klein group acts transitively on $\mathbb{P}^1(\mathbb{F}_3)$, we can prove directly the truth of (i) in general.

Finally we must prove (iii). We follow again along the same lines as the proof of (ii). Of course, we may assume that $m > 1$. Let $1 \leqslant i \leqslant k$, and let $r \mid s$. We will prove by induction that $U_i \otimes W_r$ is an irreducible $\mathbb{Q}[G_{rm}]$-module. Let p be the largest prime dividing r and let $t = r/p$. By induction, we may suppose that $U_i \otimes W_t$ is G_{tm}-irreducible. Let $H_p = \mathrm{Gal}(K_{rm}/K_{tm}) \subset \mathrm{PGL}_2(\mathbb{F}_p)$. As before, if we can prove that W_p is an irreducible $\mathbb{Q}[H_p]$-module, then we know that $U_i \otimes W_r = U_i \otimes W_t \otimes W_p$ is G_{rm}-irreducible. Once again we must exclude only the possibility that H_p is trivial or equal to the Klein group V_4 in $\mathrm{PGL}_2(\mathbb{F}_3)$.

Suppose first that $p = 2$. By maximality of p, we must have $t = 1$. If H_p is trivial, then there is a surjective map from G_m to $\mathrm{PGL}_2(\mathbb{F}_2)$. Running through all the possible odd m in Lemma 8, we find that only $m = 3$ can be possible. Moreover in this case we must have $K_2 = K_3$. Again we use Lemma 10 to exclude this possibility.

We treat now the case that $p = 3$. Then $t = 1$ or $t = 2$. Suppose that H_p is trivial. There must be a surjective map from G_{tm} to $\mathrm{PGL}_2(\mathbb{F}_3) \cong \mathfrak{S}_4$. We can check that if $t = 1$, then we must have $m = 7$ since otherwise $\#G_m$ will not be a multiple of 3. But $\#G_7$ is not divisible by 24. If $t = 2$, then m can only be 5 or 7. Again it cannot be 7. So we must have $G_{tm} \subset \mathfrak{S}_3 \times (\mathbb{Z}/4\mathbb{Z} \ltimes \mathbb{Z}/5\mathbb{Z})$, and it is easy to check that the latter group does not have a subquotient isomorphic to $\mathfrak{S}_4$.

Continuing with the case $p = 3$, we suppose now that H_p is the Klein group in $\mathrm{PGL}_2(\mathbb{F}_3)$. This time we have a surjection of G_{tm} onto $\mathfrak{S}_3$. If $t = 1$, we can again check that there is no possibility for G_m. So suppose that $t = 2$. Then G_{tm} is contained in $\mathfrak{S}_3 \times G_m$. Then the only possibility for the surjection is that G_m lies in its kernel and $\mathrm{PGL}_2(\mathbb{F}_2)$ maps isomorphically onto $\mathfrak{S}_3$. In this case we would have that K_2 is contained in K_3. Once again Lemma 10 excludes this.

The very last step is to assume that $p > 3$ and that H_p is trivial. Then there is a surjective map from G_{tm} to $\mathrm{PGL}_2(\mathbb{F}_p)$. By the maximality of p, we know that $\#\mathrm{PGL}_2(\mathbb{Z}/t\mathbb{Z})$ is not divisible by p. Therefore $p \neq m$ must divide $\#G_m$. Running through the list of possible groups in Lemma 8, we find that this is not possible. □

5.2. *Results for semistable curves.*

Theorem 12. *Let $E/\mathbb{Q}$ be a semistable elliptic curve of conductor N with N not equal to* 30 *or* 210. *Then all the self-points P_C are of infinite order in $E(\mathbb{Q}(C))$.*

Proof. By Lemma 9, we may choose a prime p dividing N such that $\bar{\rho}_p$ is surjective and such that $p - 1 > m$.

Any cyclic subgroup C of order N may be written as $C = A \oplus B$, with A of order m and B of order $s = N/m$. Now we use the previous lemma. For any fixed A, the group G_N acts transitively on the set $\{A \oplus B\}_B$ as B runs over all cyclic

subgroups of order s in E. Hence all self-points $\{P_C\}$ with the m-part A fixed are conjugate in $E(K_N)$. In particular, if $m = 1$, then all self-points are conjugate and the fundamental Theorem 2 proves the theorem. So suppose now that $m > 1$.

Now we use the p-adic proof of Theorem 2. We identify the curve $E/\overline{\mathbb{Q}}_p$ with the Tate curve $\overline{\mathbb{Q}}_p^\times/q_E^{\mathbb{Z}}$. Fix a cyclic subgroup A of order m in E, and let $B = \mu[s]$ and $C = A \oplus B$. Since any self-point is conjugate to such a point, it is sufficient to prove that P_C is of infinite order.

For each $\ell \mid m$, let A_ℓ be the ℓ-torsion part of A. Write A'' for the direct sum of all A_ℓ such that A_ℓ is generated by the ℓ-th roots of unities $\mu[\ell]$ in $E(\overline{\mathbb{Q}}_p)$. Write A' for the sum of all other A_ℓ. So $A = A' \oplus A''$. Denote the order of A' by m' and likewise the order of A'' by m''. Now we consider the isogeny ψ with kernel A', given by

$$0 \longrightarrow A' \longrightarrow E \xrightarrow{\psi} E' \longrightarrow 0.$$

If $\hat{A}'$ is the kernel of the dual isogeny $\hat{\psi} : E' \to E$, then we may consider the point

$$x'_C = (E', \hat{A}' \oplus \psi(A'') \oplus \psi(B)) \in X_0(N)(\overline{\mathbb{Q}}_p),$$

which is nothing other than the Atkin–Lehner involution $w_{m'}$ applied to the point $x_C = (E, C)$. We know already that $\psi(B) = \mu[k]$ and $\psi(A'') = \mu[m'']$, but we also see that the group $\hat{A}'$ is isomorphic to $\mu[m']$. Hence the point x'_C lies now close to the cusp ∞ and its Tate-parameter will be a certain m'-th root u of q_E. Since

$$|u|_p = (|q_E|_p)^{1/m'} = p^{-c_p/m'} < p^{-1/(p-1)}$$

because $m' \leqslant m < p-1$, we can apply Lemma 3 to show that $\varphi_E(x'_C)$ is of infinite order. But the Atkin–Lehner involutions w_ℓ act like multiplication by $-a_\ell \in \{\pm 1\}$ for all primes ℓ dividing N, as shown in [Atkin and Lehner 1970]. Therefore $P_C = \varphi_E(x_C) = \pm\varphi_E(x'_C) + T$, where T is a point of finite order, and hence P_C is of infinite order. □

As remarked earlier we have a G_N-equivariant map

$$\iota : W_N \to E(K_N) \otimes \mathbb{Q}$$

Part (ii) of Lemma 11 shows this:

Theorem 13. *Let $E/\mathbb{Q}$ be a semistable elliptic curve with N not equal to* 30 *or* 210. *Suppose all the representations $\bar{\rho}_p$ for all primes $p \mid N$ are surjective. Then the group generated by the self-points is of rank N and the Galois group acts like the irreducible Steinberg representation W_N on it.*

We prove now an extension of this theorem to the case when $m \neq 1$. In particular W_N might not be irreducible anymore. Unfortunately we cannot prove that the rank is N in general for a semistable curve since we have to exclude the possibility

that the curve has two distinct isogenies of the same degree defined over $\mathbb{Q}$: If the curve has two isogenies of degree p over $\mathbb{Q}$, then in the decomposition of W_N into irreducible $\mathbb{Q}[G]$-modules, there will be a representation that appears with multiplicity 2. The second hypothesis in the following theorem excludes this possibility, but it is also needed elsewhere to be able to apply the lemmata from the previous section.

Theorem 14. *Let $E/\mathbb{Q}$ be a semistable elliptic curve. Suppose that N is not equal to 30 or 210. Suppose that for each prime $p \mid N$ such that $\bar{\rho}_p$ is not surjective, there is a prime $\ell \mid N$ such that the Tamagawa number c_ℓ is not divisible by p. Then the group generated by the self-points is of rank N.*

Proof. As a consequence of the second hypothesis, we know that for each $p \mid N$ there is an element of order p in G_p. See the appendix of [Serre 1968]. Since either G_p is all of $\mathrm{PGL}_2(\mathbb{F}_p)$ or it is contained in the Borel subgroup, we conclude that either G_p acts transitively on $\mathbb{P}^1(\mathbb{F}_p)$ or it has one single fixed point, which we will call $C_p \in \mathbb{P}^1(\mathbb{F}_p)$.

Let $p \mid m$. Then by Proposition 6, the $\mathbb{Q}[G_p]$-module W_p decomposes as the sum of the trivial part W_1' and an irreducible part W_p' of dimension $p-1$. If m is not prime it can only be either $2 \cdot 3$ or $2 \cdot 5$ by Mazur's theorem. If $m = 6$, then W_6 decomposes as $W_1' \oplus W_2' \oplus W_3' \oplus W_6'$, where $W_6' = W_2' \otimes W_3'$. To see that the latter is also irreducible one needs only to note that the dimension of W_2' is 1. In the same way, for $m = 10$, we have an irreducible component W_{10}'.

Using Lemma 11, we know now that W_N decomposes as

$$W_N = \bigoplus_{d \mid m} (W_d' \otimes W_s)$$

into irreducible $\mathbb{Q}[G_N]$-modules. We must now prove that none of the components belongs to the kernel of the map $\iota : W_N \to E(K) \otimes \mathbb{Q}$.

First recall the definition of $W_d' \otimes W_s$. It contains all elements

$$\sum_{C \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} a_C e_C \in \bigoplus_{C \in \mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})} \mathbb{Q} e_C,$$

subject to the following three conditions.

- For all $N \neq b \mid N$ and all cyclic subgroups B of order b, the sum $\sum_{C \supset B} a_C$ vanishes.
- For all primes $p \mid d$ and all $C \supset C_p$, we have $a_C = 0$.
- For all primes $p \mid (m/d)$ and all $C \not\supset C_p$, we have $a_C = 0$.

Let $d \mid m$. Define A to be the direct sum of C_p for all $p \mid (m/d)$. So A is a cyclic group of order m/d. The map ι on $W_d' \otimes W_s$ is induced from the map

$$\iota_d : \bigoplus_D \mathbb{Q} e_{A\oplus D} \longrightarrow E(K) \otimes \mathbb{Q},$$

where D runs through all the cyclic subgroups D in E of order $d \cdot s$ such that D does not contain any of the C_p with $p \mid d$. Since this map sends $e_{A\oplus D}$ to the self-point $P_{A\oplus D}$, it follows from Theorem 12 that the map ι_d is not trivial.

Now we use the relations in Proposition 4 to see that, for all $b \mid ds$ and all cyclic groups B of order b not containing any of the C_p, we have $\sum_{D\supset B} e_{A\oplus D} \in \ker \iota_d$. Hence the only irreducible part of the domain of ι_d that does not lie in the kernel is $W_d' \otimes W_s$ Hence ι_d induces an injection $W_d' \otimes W_s \to E(K) \otimes \mathbb{Q}$. □

The hypothesis in this last theorem is fulfilled for the very large part of semistable curves. We could not find a strong Weil curve with $N < 10{,}000$ for that the theorem would not apply. The first curve which does not satisfy the hypothesis with $p = 3$ is 651e2 since it has $G_3 = \mathbb{Z}/2\mathbb{Z}$, and the Tamagawa numbers are $c_3 = 3$, $c_7 = 3$, and $c_{31} = 3$. For $p = 2$, the examples that do not satisfy the hypothesis are exactly those that have all 2-torsion points defined over $\mathbb{Q}$, as for instance 30a2.

6. Examples

Table 2 shows some computations done for the optimal curves (with one exception) of smallest conductor. We do not give the complete explanation of how one obtains these results. For more detail, we refer the reader to [Delaunay and Wuthrich 2008] and [Wuthrich 2007]. We will consider two curves in more detail later.

N	11a1	14a1	15a1	17a1	19a1	20a1	21a1	24a1	26a1
torsion	5	$2\cdot 3$	$2\cdot 4$	4	3	$2\cdot 3$	$2\cdot 4$	$2\cdot 4$	3
isogeny	25	18	16	4	9	6	8	8	9
W_N	1	2	1	1	1	2	1	4	1
rank	11	14	15	17	19	15	21	18*	26

N	26b1	27a**2**	30a1	32a1	33a1	34a1	35a1	37a1	38a1
torsion	7	3	$2\cdot 3$	4	$2\cdot 2$	$2\cdot 3$	3	1	3
isogeny	7	27	12	4	4	6	9	1	9
W_N	1	5	4	?	1	2	1	1	1
rank	26	**20**	30*	**12***	33	34	35	37	38

Table 2. The ranks of the group generated by self-points for some curves.

We label the curves as in Cremona's tables [1997]. The first line of our table shows the structure of the torsion group over $\mathbb{Q}$; for example, $2 \cdot 4$ means that $E(\mathbb{Q})_{\text{tors}} = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. The next line indicates the largest degree of a cyclic isogeny defined over $\mathbb{Q}$ on E. The last two lines are those containing information about self-points: First we counted the number of irreducible $\mathbb{Q}[G_N]$-modules in W_N, and finally we computed the rank of the group generated by self-points in $E(K_N)$.

The two values in bold face are lower than the usual conjectured rank, which is no surprise since these two curves have complex multiplication. When there is no $*$ sign next to the rank, the value is proved using the results in the previous section. The sign $*$ indicates that we have only empirically computed the rank using the following method.

Using high precision computation we may find a very good approximation to the values of

$$z_C = \int_{x_C}^{\infty} f_E(q) \frac{dq}{q}$$

as elements of $\mathbb{C}$, where C runs over all cyclic subgroups of order N in E. Hence z_C maps to P_C under $\mathbb{C} \to \mathbb{C}/\Lambda_E \to E(\mathbb{C})$, where $\Lambda_E = \mathbb{Z}\omega_1 \oplus \mathbb{Z}\omega_2$ is the period lattice of E. Let t be the order of the torsion subgroup of E over $\mathbb{Q}$. Consider the abelian group spanned by $\frac{1}{t}\omega_1$, $\frac{1}{t}\omega_2$ and all the z_C in a complex vector space of dimension $2 + \#\mathbb{P}^1(\mathbb{Z}/N\mathbb{Z})$. Using the LLL algorithm, we find small vectors in this lattice. These are likely to give relations

$$b_1\omega_1 + b_2\omega_2 + \sum_C a_C z_C = 0$$

with b_1, b_2, and a_C all integers. This yields a probable relation among the self-points. Unfortunately we might not catch those relations involving torsion points on E not defined over $\mathbb{Q}$. So to increase the likelihood of finding all relations we multiply t by a product of small primes. For all cases for which we were able to determine the rank, this empirical computation gave the same answer. In principle these computations could be made rigorous by considering exact estimates for the error terms.

6.1. ***Conductor 24.*** We present here an example of a curve where we are unable to determine the rank of the group generated by self-points. The Mordell–Weil group of the curve 24a1, given by the equation

$$E: \quad y^2 = x^3 - x^2 - 4 \cdot x + 4,$$

is $E(\mathbb{Q}) = \mathbb{Z}/2\mathbb{Z} \oplus \mathbb{Z}/4\mathbb{Z}$. The situation is rather complicated and we do not explain all computations here. The field K_4 turns out to be $\mathbb{Q}(i, \sqrt{3})$, which happens to be equal to $\mathbb{Q}(E[4])$. There is are two nontrivial Galois-orbits of 4-torsion points,

one over $\mathbb{Q}(\sqrt{3})$ and the other over $\mathbb{Q}(\sqrt{-3})$. Hence the representation V_4 splits as

$$V_4 = \mathbb{1} \oplus \mathbb{1} \oplus \mathbb{1} \oplus \mathbb{1} \oplus \mathbb{1}(\sqrt{3}) \oplus \mathbb{1}(\sqrt{-3}),$$

where $\mathbb{1}(\sqrt{d})$ is the one-dimensional representation corresponding to the Dirichlet character associated to $\mathbb{Q}(\sqrt{d})$. Now the field K_8 can be computed too; it coincides with $\mathbb{Q}(E[8])$ in this case. It is a degree 16 extension of discriminant $2^{36} \cdot 3^{12}$, and contains the extension $\mathbb{Q}(i, \sqrt{2}, \sqrt{3})$. The subextension K_4 is fixed by the centre of the Galois group G_8. The group G_8 admits two irreducible 2-dimensional representations, one of which we call Z_2. Then the representation V_8 splits in many components and we find that

$$W_8 = \mathbb{1}(\sqrt{2}) \oplus \mathbb{1}(\sqrt{-2}) \oplus Z_2 \oplus Z_2.$$

The first two factors correspond to two pairs of lines in $E[8]$ defined over $\mathbb{Q}(\sqrt{2})$ and $\mathbb{Q}(\sqrt{-2})$ respectively. The other lines are defined over fields of degree 4.

Using that the field K_3 intersects K_8 in $\mathbb{Q}(\sqrt{-3})$, we find that W_{24} splits into 4 irreducible factors $W_{24} = W_3(\sqrt{2}) \oplus W_3(\sqrt{-2}) \oplus Z_6 \oplus Z_6$. Here $Z_6 = W_3 \otimes Z_2$ is an irreducible representation of dimension 6. In particular, this representation appears with multiplicity 2. So the usual proof that there are no further relations among self-points will not work.

The cyclic subgroup of order 8 in E that corresponds to $\mu[8]$ over $\mathbb{Q}_3$ contains the rational 4-torsion point. So one of the two factors of dimension 3 in W_{24} certainly appears in $E(K_N) \otimes \mathbb{Q}$. But we are unable to show that any other self-points are of infinite order by means of Theorem 12.

Though we can only conclude that the rank r of the group generated by the self-points satisfies $3 \leqslant r \leqslant 18$, we strongly believe that $r = 18$, as suggested by the empirical computations.

6.2. ***Conductor 27.*** There are four curves of conductor 27 forming the isogeny graph

$$27\text{a}2 \leftarrow 27\text{a}1 \leftarrow 27\text{a}3 \leftarrow 27\text{a}4$$

The isogenies $\leftarrow$ are all of degree 3, and in the sense that they are drawn here, the kernels are $\mathbb{Z}/3\mathbb{Z}$ while the dual isogenies have kernel $\mu[3]$. Over the field $F = \mathbb{Q}(\sqrt{-3}) = \mathbb{Q}(\zeta)$, with ζ a third root of unity, the curves 27a1 and 27a3 become isomorphic, the same holds for the curves 27a2 and 27a4. The first pair has complex multiplication by the maximal order $\mathbb{Z}[\zeta]$, while the second pair has complex multiplication by $\mathbb{Z}[3\zeta]$.

Let E be the curve 27a2 defined by $y^2 + y = x^3 - 270 \cdot x - 1708$.

Theorem 15. *The self-points on the curve* 27*a*2 *generate a group of rank* 20 *in* $E(K_{27})$. *There are exactly two linearly independent self-points defined over* $K_3 = \mathbb{Q}(\sqrt[6]{-3})$, *and they generate a subgroup of finite index in* $E(K_3)$.

The proof is contained in the following explanations, but we do omit certain computations.

The field K_3 is equal to $\mathbb{Q}(\sqrt[6]{-3})$, and the Galois group G_3 is a dihedral group of order 6. In fact some 3-torsion points are defined over $F = \mathbb{Q}(\sqrt{-3})$, some others are over $\mathbb{Q}(\sqrt[3]{-3})$, and we have $V_3 = \mathbb{1} \oplus \mathbb{1}(\sqrt{-3}) \oplus Z_2$, where Z_2 is the unique irreducible 2-dimensional representation of G_3.

In order to determine the structure of V_{27}, we need to use the theory of complex multiplication. Let H_{27} be the subgroup $\mathrm{Gal}(K_{27}/F)$ inside G_{27}. We know that the representation $\bar{\rho}_{27,F}$ now maps to

$$\bar{\rho}_{27,F} : H_{27} \rightarrowtail \frac{\mathrm{Aut}_{\mathbb{O}/27\mathbb{O}}(E[27])}{(\mathbb{Z}/27\mathbb{Z})^\times} = \frac{(\mathbb{O}/27\mathbb{O})^\times}{(\mathbb{Z}/27\mathbb{Z})^\times}$$

$$\xrightarrow{\cong} \left\{ \left(\begin{smallmatrix} 1 & * \\ 0 & 1 \end{smallmatrix}\right) \in \mathrm{PGL}_2(\mathbb{Z}/27\mathbb{Z}) \right\} \xrightarrow{\cong} \mathbb{Z}/27\mathbb{Z},$$

where $\mathbb{O} = \mathbb{Z}[3\zeta]$ is the ring of endomorphisms of E/F. It is possible to verify that H_{27} is equal to this group, and hence G_{27} is a dihedral group of order 54 generated by $h = \left(\begin{smallmatrix} 1 & 1 \\ 0 & 1 \end{smallmatrix}\right)$ and $s = \left(\begin{smallmatrix} 1 & 0 \\ 0 & -1 \end{smallmatrix}\right)$. The computation of V_{27} is now easy and one finds

$$W_{27} = \mathbb{1} \oplus \mathbb{1}(\sqrt{-3}) \oplus Z_2 \oplus Z_2 \oplus Z_{18}.$$

Here Z_2 is the unique 2-dimensional irreducible $\mathbb{Q}[G_{27}]$-module (the action of h has trace -1), and Z_{18} is the unique irreducible 18-dimensional $\mathbb{Q}[G_{27}]$-module (it splits over $\mathbb{C}$ into six 2-dimensional representations). Since the curve 27a2 is not the strong Weil curve in the isogeny class, the modular parametrisation φ_E from the elliptic curve $X_0(27)$ to E is not an isomorphism but an isogeny of degree 3. The curve $X_0(27)$ has six cusps represented by the classes $\{\infty, 0, \frac{1}{3}, \frac{2}{3}, \frac{2}{9}, \frac{4}{9}\}$. The group $X_0(27)(\mathbb{Q})$ contains the cusps ∞ and 0 and the self-point obtained from the isogeny 27a2$\rightarrow$27a4. They form exactly the kernel of φ_E. The other cusps are mapped to the 3-torsion points defined over F on E. In fact $E(F) = \mathbb{Z}/3\mathbb{Z}$ and $E(K_3)_{\mathrm{tors}} = \mathbb{Z}/3\mathbb{Z} \oplus \mathbb{Z}/3\mathbb{Z}$. A two-descent over K_3 shows that the 2-Selmer group of E/K_3 has two copies of $\mathbb{Z}/2\mathbb{Z}$ in it.

The trivial factor in W_{27} corresponds to the self-point obtained from the 27-isogeny defined over $\mathbb{Q}$ on 27a2. We know that it is the point O in $E(\mathbb{Q})$. The factor $\mathbb{1}(\sqrt{-3})$ in W_{27} must also belong to the kernel of $\iota : W_{27} \rightarrow E(K_{27}) \otimes \mathbb{Q}$ since the Mordell–Weil group $E(F)$ is of rank 0. Of the factors Z_2 at least one must be in the kernel since the rank of $E(K_3)$ is bounded by 2 from above. It is not hard to check by looking at traces of Frobenii that the torsion subgroup of $E(K_{27})$ only contains nine 3-torsion points. Since the degree of φ_E is 3, there are at most 27 points in $X_0(27)(K_{27})$ that map to torsion points in $E(K_{27})$ under φ_E. Since there are 36 points x_C, we conclude that at least 9 self-points are of infinite order.

Looking at the decomposition of W_{27}, we see that Z_{18} cannot belong to the kernel of ι.

Finally we have to show that there is a self-point of infinite order in $E(K_3)$. This will show that the second copy of Z_2 does not belong to the kernel of ι. This can be done numerically. The point $\tau_C = \frac{1}{6} \cdot (-1 + \sqrt{-3})$ in the upper half plane corresponds to a point x_C in $X_0(27)$. We find that

$$-\tfrac{1}{8}(36 \cdot s^5 + 15 \cdot s^4 - 45 \cdot s^3 - 18 \cdot s^2 + 69 \cdot s + 99) \quad \text{with } s = \sqrt[6]{-3}$$

is the x-coordinate of the self-point P_C in $E(K_3)$. Its canonical height is 1.5191 and hence P_C is of infinite order. This point P_C and its conjugates over F will generate a group of rank 2 in $E(K_3)$. Since we have computed the 2-Selmer group earlier, we conclude that the rank of $E(K_3)$ is as claimed equal to 2.

It seems plausible that this P_C can also be constructed as an "exotic Heegner point" using the construction of Bertolini, Darmon and Prasanna [$\geq$ 2009], but the authors exclude there explicitly the case of conductor $N = 27$.

7. Higher self-points

In this section, we investigate three particular cases of higher self-points. Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. For any cyclic subgroup D in E we may consider the isogenous curve E/D with a suitable choice of a cyclic subgroup of order N in it. In the first case, we use subgroups D defined over $\mathbb{Q}$ to construct new points and for the two other cases we use subgroups D of prime-power order p^n, first when p divides the conductor and then when it does not divide the conductor.

7.1. ***Self-points via rational isogenies.*** Let D be a cyclic subgroup in E defined over $\mathbb{Q}$. Suppose for simplicity that the order of D is prime to N. Then for any cyclic subgroup C of order N on E,

$$Q_D = \varphi_E(E/D, (C + D)/D)$$

is a higher self-point defined over the same field as P_C. It would be interesting to know in general when P_C and Q_D are linearly independent. For instance this can be shown on the curves of conductor 11: There are 3 curves in the isogeny class, and hence we find, for any fixed C, one self-point and two higher self-points on E defined over $\mathbb{Q}(C)$. Using the canonical height pairing, we can prove the linear independence of these three points computed explicitly on E. So the rank of $E(\mathbb{Q}(C))$ will have to be at least 3. See [Delaunay and Wuthrich 2008] and [Wuthrich 2007] for more details on this example.

In some cases the method of the proof of Theorem 12 can be used to show that Q_D is also of infinite order. But the methods of the proof of Theorem 14 will not be sufficient to prove the independence of P_C and Q_D.

7.2. ***The multiplicative case.*** Let now p be a prime dividing N exactly once, that is, E has multiplicative reduction at p. Let M be such that $N = p \cdot M$. As a base-field we will consider here the number field $F = K_M$, the smallest field such that its absolute Galois group acts as scalars on $E[M]$. In the particular situation when $N = p$ is prime then $F = \mathbb{Q}$; the same is true for instance if E is a curve of conductor 14 and $p = 7$.

For any $n \geqslant 0$, we define now F_n to be the field $K_{p^n N}$ and H_n to be the Galois group of F_n/F. Via the Galois representation

$$\rho_{F,p} : \mathrm{Gal}(\bar{F}/F) \longrightarrow \mathrm{Aut}(T_p E) \cong \mathrm{GL}_2(\mathbb{Z}_p) \longrightarrow \mathrm{PGL}_2(\mathbb{Z}_p),$$

the group H_n identifies with a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$.

Fix a subgroup B of order M in E. Let $n \geqslant 0$, and let D be a cyclic subgroup of order p^{n+1} in E. Let $A = D[p]$ and $C = A \oplus B$, which is a cyclic subgroup of order N. Write ψ for the isogeny $E \to E'$ of kernel D and $\hat{\psi}$ for its dual. Define

$$C' = \ker(\hat{\psi})[p] \oplus \psi(B),$$

which is a cyclic subgroup of E' of order $M \cdot p = N$. The image of the point $y_D = (E', C') \in Y_0(N)$ through the map φ_E will be denoted by Q_D. It is by definition a higher self-point. We will say that "Q_D lies over P_C" or "over B".

In particular, if $n = 0$, then $D = A$ is a cyclic subgroup of order p. From the construction above, we see that the point y_D is nothing but $w_p(x_C)$, where w_p is the Atkin–Lehner involution on $X_0(N)$. Hence we have that $Q_D = -a_p \cdot P_C + T$ for some 2-torsion point T defined over $\mathbb{Q}$. Here $a_p = \pm 1$ is, as before, the Hecke eigenvalue of the newform f_E attached to the isogeny class of E.

Let D be a cyclic subgroup of E of order p^{n+1}. By the definition of the Hecke operator T_p on $J_0(N)$, we have $T_p((y_D) - (\infty)) = \sum_{D' \supset D}((y_{D'}) - (\infty))$, where the sum runs over all cyclic subgroups D' in E of order p^{n+2} containing D. This gives us the relation

$$a_p \cdot Q_D = \sum_{D' \supset D} Q_{D'}. \tag{2}$$

Hence by induction, we know that Q_D is of infinite order if the self-point P_C is.

Lemma 16. *Let B be a fixed subgroup of order M in E, and let $n \geqslant 0$. Then $\sum_D Q_D$ is a torsion point in $E(F)$, where the sum is over all cyclic subgroups D of E of order p^{n+1}.*

Proof. Suppose first that $n = 0$. Then we sum over all cyclic subgroups $D = A$ of order p, which gives

$$\sum_D Q_D = \sum_{C \supset B} (-a_p P_C + T) = (p+1) \cdot T - a_p \sum_{C \supset B} P_C.$$

The first term on the right side is clearly torsion and the second term contains exactly one of the relations from Proposition 4. Now by induction, we assume that the statement holds for n. But then $\sum_{D'} Q_{D'}$, with the sum running over all cyclic subgroups D' of order p^{n+2}, is, by (2), equal to $a_p \cdot \sum_D Q_D$, with the sum now running over cyclic subgroups of order p^{n+1}. □

The $\mathbb{Q}$-vector space with basis $\{e_D\}_D$ in bijection with $\mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z})$ is a natural $\mathbb{Q}[H_n]$-module. Define

$$V'_{(n)} = \frac{\bigoplus_A \mathbb{Q} e_D}{\mathbb{Q}(\sum_D e_D)},$$

which is a vector space of dimension $p^{n+1} + p^n - 1$.

Fix a cyclic subgroup B of order M in E. By the previous lemma, there is a morphism of $\mathbb{Q}[H_n]$-modules given by

$$\iota_n = \iota_{B,n} : V'_{(n)} \longrightarrow E(F_n) \otimes \mathbb{Q}, \quad e_D \longmapsto Q_D$$

We assume that the Galois representation $\rho_{F,p}$ is surjective onto $\mathrm{PGL}_2(\mathbb{Z}_p)$. So H_n is isomorphic to $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$ and the $\mathbb{Q}[H_n]$-module $V'_{(n)}$ is the Steinberg representation, which was denoted by V_{p^n}/W_1 in Section 4.

Theorem 17. *Suppose $E/\mathbb{Q}$ is an elliptic curve and p a prime of multiplicative reduction. Suppose that $\rho_{F,p}$ is surjective and that there is a self-point P_C of infinite order in $E(F_0)$. Then for all $n \geqslant 0$ and all cyclic subgroups D of order p^{n+1} with $D[p] \subset C$, the point Q_D is of infinite order. They generate in $E(F_n) \otimes \mathbb{Q}$ a $\mathbb{Q}[H_n]$-module isomorphic to the representation $V'_{(n)}$ of dimension $p^{n+1} + p^n - 1$.*

As a special case, we recover [Delaunay and Wuthrich 2008, Theorem 8] in the case when $N = p$ is prime and $F = \mathbb{Q}$.

Proof. We only have to show that ι_n is injective. Suppose $n \geqslant 0$ is the smallest value such that ι_n is not injective. Since $V'_{(n)} = W_{p^{n+1}} \oplus V'_{(n-1)}$ if $n > 0$ and $V'_{(0)} = W_p$, this means that ι_n induced on $W_{p^{n+1}}$ is not injective. Since this is an irreducible $\mathbb{Q}[H_n]$-module when $\rho_{F,p}$ is surjective, this means that ι_n is trivial on $W_{p^{n+1}}$. This is impossible since we have shown that all Q_D above P_C are of infinite order. □

7.3. ***The good case.*** Let p be a prime not dividing N, that is, of good reduction for E. Let F be a number field such that $E(F)$ contains a self-point P_C of infinite order. We fix the corresponding cyclic subgroup C of order N in E.

For any $n \geqslant 0$, let F_n be the smallest Galois extension of F such that the absolute Galois group $\mathrm{Gal}(\bar{F}/F)$ acts via scalars on $E[p^{n+1}]$; hence $F_n = F \cdot K_{p^{n+1}}$. Define H_n to be the Galois group $\mathrm{Gal}(F_n/F)$, which will be considered as a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$.

For any $n \geqslant 0$ and any cyclic subgroup D of order p^{n+1}, we construct a higher self-point Q_D in $E(F_n)$ as follows. Let $\psi : E \to E/D$ be the isogeny associated

to D. Put $y_D = (E/D, \psi(C)) \in Y_0(N)$ and $Q_D = \varphi_E(y_D)$. This is a higher self-point "above P_C".

Again we may use the definition of the Hecke operator T_p to prove that, for all $n \geqslant 0$ and D as before,

$$a_p \cdot Q_D = \sum_{D' \supset D} Q_{D'}, \tag{3}$$

where the sum runs over all cyclic subgroups D' of order p^{n+2} in E containing D. Furthermore we have

$$a_p \cdot P_C = \sum_{D} Q_D, \tag{4}$$

with the sum running over all cyclic subgroups D of order p in E.

Let $V_{(n)} = V_{p^{n+1}}$ be the $\mathbb{Q}[H_n]$-module whose basis $\{e_D\}_D$ as a vector space over $\mathbb{Q}$ is in bijection with $\mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z})$. We have a H_n-morphism defined by

$$\iota_n = \iota_{C,n} : V_{(n)} \longrightarrow E(F_n) \otimes \mathbb{Q}, \quad e_D \longmapsto Q_D$$

Theorem 18. *Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let p be a prime of good and ordinary reduction for E. Let F be a number field such that $E(F)$ contains a self-point P_C of infinite order. Suppose that the representation $\rho_{F,p}$ is surjective. Then all higher self-points Q_D constructed above are of infinite order and they generate a group of rank $p^n \cdot (p+1)$.*

Proof. By induction on n, using the formulae (3) and (4) and the hypothesis that p is ordinary to guarantee that $a_p \neq 0$. □

The above easy proof of the theorem breaks down if E has supersingular reduction at p, for a_p is then almost always equal to 0.

Theorem 19. *Let $E/\mathbb{Q}$ be a semistable elliptic curve of conductor N not equal to* 30 *or* 210*. Let $p > N$ be a supersingular prime for E. Let $F = K_N$. Suppose that the representation $\rho_{F,p}$ is surjective. Then all higher self-points Q_D above a given self-point P_C are of infinite order, and they generate a group of rank $p^n \cdot (p+1)$.*

Proof. We follow the proof of Theorem 12. Let $\ell > 2$ be a prime dividing N. We proved that the self-points are of infinite order by showing that when a certain Atkin–Lehner involution is applied to one of the conjugates of x_C, one obtains a point ℓ-adically close to the cusp ∞ on $X_0(N)(\overline{\mathbb{Q}}_\ell)$.

Let Q_D be a higher self-point above the self-point P_C. Since $\rho_{F,p}$ is surjective, the point Q_D will be conjugate over K_N to all other higher self-points above the same self-point. Therefore without loss of generality we may assume that the cyclic subgroup D on E corresponds to $\mu[p^{n+1}]$ in $E(\overline{\mathbb{Q}}_\ell)$. Then the point $y_D = (E', C')$ is represented by a Tate curve over $\overline{\mathbb{Q}}_\ell$ with parameter $q_{E'}$ equal to the p^{n+1}-st power of q_E.

Let r be a divisor of N such that $w_r(y_D)$ is the pair $(E'', \mu[N])$, with E'' the Tate curve with parameter $q_{E'}^{1/r}$. Using that $p > N \geqslant r$, we find that

$$|q_{E'}^{1/r}|_\ell = |q_E|_\ell^{p^{n+1}/r} \leqslant \ell^{-(p/r)\cdot p^n} \leqslant \ell^{-1} < \ell^{-1/(\ell-1)},$$

and hence Lemma 3 shows that $\varphi_E(E'', \mu[N])$ is of infinite order. Then as usual Q_D differs from $\pm\varphi_E(w_r(y_D))$ by a torsion point. So Q_D is of infinite order.

Since the representation W_{p^n} is irreducible for $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$, we can show by induction that the rank of the group generated by higher self-points is $\dim(V_{(n)}) = p^n \cdot (p+1)$. □

Putting the previous two results together, we are able to show a corollary that holds for all but finitely many primes p.

Corollary 20. *Suppose $E/\mathbb{Q}$ is a semistable curve of conductor N not equal to* 30 *or* 210*. Let p be a prime such that $p > N$, (so it is of good reduction), and such that $\bar\rho_p : \mathrm{Gal}(\overline{\mathbb{Q}}/\mathbb{Q}) \to \mathrm{PGL}_2(\mathbb{F}_p)$ is surjective. Let s be the rank of the group generated by self-points in $E(K_N)$. Then the higher self-points in $E(K_{p^{n+1}N})$ generate a group of rank $s \cdot (p+1) \cdot p^n$.*

Proof. Take $F = K_N$ in the previous theorems. We only have to show the condition that $\rho_{F,p}$ is surjective. It is enough to show that $\bar\rho_{F,p} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{PGL}_2(\mathbb{F}_p)$ has all of $\mathrm{PSL}_2(\mathbb{F}_p)$ in its image, since the representation V_{p^n} will still have the same decomposition.

Let H_p be the group $\mathrm{Gal}(K_{Np}/K_N)$, that is, the image of $\bar\rho_{F,p}$. It is equal to the normal subgroup in $\mathrm{Gal}(K_p/\mathbb{Q}) \cong \mathrm{PGL}_2(\mathbb{F}_p)$ corresponding to the subextension $K_p/K_N \cap K_p$. Since $p > 11$ when $p > N$, we have that $\mathrm{PGL}_2(\mathbb{F}_p)$ has only three normal subgroups, namely itself, $\mathrm{PSL}_2(\mathbb{F}_p)$ and $\{1\}$. By the remark above, we only have to exclude that H_p is not trivial.

If H_p was trivial, then p, dividing the order of $\mathrm{PGL}_2(\mathbb{F}_p)$, would have to divide the order of G_N, which is a subgroup of $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$. But if $p > N$, then p cannot divide the order of $\mathrm{PGL}_2(\mathbb{Z}/N\mathbb{Z})$, except when $p = 3$ and $N = 2$, which cannot occur as a conductor. □

8. Derivatives

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Let p be an *odd* prime of *ordinary*, either good or multiplicative, reduction. To treat the cases of higher self-points discussed in the Sections 7.2 and 7.3 simultaneously, we choose now a base field F. If E has good ordinary reduction at p, then F is any number field such that $E(F)$ contains a self-point P_C of infinite order. If p divides N, then F is a number field such that the absolute Galois group of F acts by scalars on $E[N/p]$.

We will suppose from now on that $\rho_{F,p} : \mathrm{Gal}(\overline{F}/F) \to \mathrm{PGL}_2(\mathbb{Z}_p)$ is surjective.

We suppose that F_n is the smallest extension of F such that the Galois group $H_n = \mathrm{Gal}(F_n/F)$ acts by scalars on $E[p^{n+1}]$. By assumption the map $\rho_{F,p}$ induces an isomorphism from H_n to $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$. Also, this implies that $E(F_n)$ has no p-torsion elements.

Let $\mathbb{O}$ be the ring of integers in the unramified quadratic extension of $\mathbb{Q}_p$. Choosing a basis of $\mathbb{O}$ over $\mathbb{Z}_p$ and viewing each element $u \in \mathbb{O}^\times$ as the ($\mathbb{Z}_p$-linear) multiplication by u on $\mathbb{O}$, we get a homomorphism

$$\Psi : \mathbb{O}^\times \to \mathrm{GL}_2(\mathbb{Z}_p) \to \mathrm{PGL}_2(\mathbb{Z}_p),$$

whose kernel is $\mathbb{Z}_p^\times$. The image of the composition

$$\mathbb{O}^\times \to \mathrm{PGL}_2(\mathbb{Z}_p) \to \mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z}) \to H_n$$

will be denoted by A_n. This is a cyclic group of order $(p+1)\cdot p^n = \#\mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z})$. It is the projective version of the nonsplit Cartan group in $\mathrm{GL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$. To simplify notation, we will write F_n^A for the subfield of F_n fixed by A_n.

Theorem 21. *Let $E/\mathbb{Q}$ be an elliptic curve. Suppose E does not have potentially good supersingular reduction for any prime of additive reduction. Let p be a prime of either good ordinary or multiplicative reduction. Let F be the number field as above and assume that $\rho_{F,p}$ is surjective. Then we have $\#\mathrm{Sel}_{p^n}(E/F_n^A) \geqslant p^n$, where A is any nonsplit Cartan group in* $\mathrm{PGL}_2(\mathbb{Z}_p)$.

The proof of this theorem will be completed in Section 8.3.

Since there are no p-torsion points in $E(F_n)$, as $\rho_{F,p}$ is assumed to be surjective, there is an isomorphism $\mathrm{H}^1(F_n^A, E[p^k]) \to \mathrm{H}^1(F_n, E[p^k])^{A_n}$ induced by the restriction map. This implies that the map

$$\mathrm{Sel}_{p^n}(E/F_n^A) \to \mathrm{Sel}_{p^n}(E/F_n)^{A_n}$$

is injective. We conjecture that the elements in the Selmer group constructed in Theorem 21 do not lie in the image of the Kummer map, but represent nontrivial elements in the Tate–Shafarevich group $Ш(E/F_n^A)$. If so, these classes in the Tate–Shafarevich group will capitulate in the extension F_n/F_n^A, since the elements of the Selmer group in the theorem restrict to elements in the image of the higher self-points inside $\mathrm{Sel}_{p^n}(E/F_n)$. It would be very interesting to verify this conjecture in some cases, but even for the smallest cases like $p = 11$ it seems completely impossible to compute the classes explicitly. Nevertheless it is natural to make this conjecture when comparing it to Kolyvagin's conjecture on the nontriviality of derivative classes of Heegner points (as investigated in [Jetchev et al. 2007]).

8.1. *The field extension.*

Lemma 22. *The cyclic group A_n intersects trivially any Borel subgroup in H_n.*

Proof. We prove the statement that the image of Ψ in $\mathrm{PGL}_2(\mathbb{Z}_p)$ intersects trivially any of its Borel subgroups B. Let L be the $\mathbb{Z}_p$-line in $\mathbb{C}$ such that B is the stabiliser under the action of $\mathrm{PGL}_2(\mathbb{Z}_p)$ on $\mathbb{P}^1(\mathbb{Z}_p)$ viewed as the set of $\mathbb{Z}_p$-modules in $\mathbb{C}$ generated by a unit. Let $\alpha \in \mathbb{C}^\times$ be any element with a nontrivial image under Ψ. Then $\alpha \notin \mathbb{Z}_p^\times$ cannot fix L. □

This implies in particular that any generator α_n of A_n acts simply transitively on the set $\mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z})$.

Lemma 23. *Let v be either a place of ordinary reduction above p or an infinite place or a place of potentially multiplicative reduction. Then the image of*

$$\bar{\rho}_{F_v,p} : \mathrm{Gal}(\bar{F}_v/F_v) \to \mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$$

lies in a Borel subgroup of $\mathrm{PGL}_2(\mathbb{Z}/p^{n+1}\mathbb{Z})$.

Proof. First suppose that v divides p. Since E is of ordinary reduction at v, there is a cyclic subgroup of $E[p^{n+1}]$ of order p^{n+1} that is fixed by the Galois group $\mathrm{Gal}(\bar{F}_v/F_v)$. This subgroup consists of all elements of $E[p^{n+1}]$ with trivial reduction over $\bar{F}_v$. Therefore the image of $\bar{\rho}_{F_v,p}$ is contained in the stabiliser of this point in $\mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z})$, which is a Borel subgroup.

Now, let v be a place of split multiplicative reduction for E. From the description of E as a Tate curve over F_v, we see that there is subgroup isomorphic to $\mu[p^{n+1}]$ inside $E[p^{n+1}]$. As before $\mathrm{Gal}(\bar{F}_v/F_v)$ will fix this subgroup and hence the image of $\bar{\rho}_{F_v,p}$ is contained in a Borel subgroup.

Next, we suppose that v is a place of bad reduction, but not of split multiplicative type. Then by hypothesis, E has either nonsplit multiplicative or additive and potentially multiplicative reduction. In both cases there exists a quadratic extension L of F_v, unramified in the first case and ramified in the second, such that E has split multiplicative reduction over L; see [Serre 1972, page 312]. Hence $E[p^{n+1}]$ can be described as the set of $\zeta^i \cdot a^j$, with ζ a primitive p^{n+1}-st root of unity, a a p^{n+1}-st root of the Tate-parameter q and $0 \leqslant i, j < p^{n+1}$; the action of $\sigma \in \mathrm{Gal}(\bar{F}_v/F_v)$ is given by $\sigma * (\zeta^i \cdot a^j) = \chi_L(\sigma) \cdot \sigma(\zeta)^i \cdot \sigma(a)^j$, where χ_L is the quadratic character associated to L/F_v. Therefore the subgroup generated by ζ is still fixed under $\mathrm{Gal}(\bar{F}_v/F_v)$.

Finally, we have to treat the case when v is an infinite place. But for any p, there is a cyclic subgroup of order p^{n+1} in $E(\mathbb{R})$; hence the image is contained in a Borel subgroup. □

Remark: We used here in a crucial way the assumption that p is a prime of ordinary reduction. Certainly it will not hold for places of additive reduction that are potentially supersingular.

Proposition 24. *Suppose that none of the primes of additive reduction for E are potentially good supersingular. Then then extension F_n/F_n^A is nowhere ramified. Moreover all places above ∞, p, and N split completely in this extension.*

Proof. Since F_n is a subfield of $F(E[p^\infty])$, it is unramified outside ∞, p, and N. By the previous lemma, the decomposition group of a place v dividing $\infty \cdot p \cdot N$ in F inside H_n is contained in a Borel. Since any Borel intersects $A_n = \mathrm{Gal}(F_n/F_n^A)$ trivially by Lemma 22, the places above $\infty \cdot p \cdot N$ in F_n^A split completely. □

8.2. ***The A-cohomology of the Steinberg representation.*** Let

$$V_n' = \left\{ f : \mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z}) \to \mathbb{Q} \;\middle|\; \textstyle\sum_D f(D) = 0 \right\}$$

be the $\mathbb{Q}[H_n]$-module considered earlier in Section 7.2. It is a $\mathbb{Q}$-vector space of dimension $m-1$ with $m = (p+1)\cdot p^n$. There is a natural lattice T_n' in V_n' that is fixed by H_n, defined by

$$T_n' = \left\{ f : \mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z}) \to \mathbb{Z} \;\middle|\; \textstyle\sum_D f(D) = 0 \right\}.$$

Lemma 25. $\mathrm{H}^1(A_n, T_n') = \mathbb{Z}/m\mathbb{Z}$.

Proof. The A_n-fixed part of V_n' is trivial, since A_n acts transitively on $\mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z})$: A function $f : \mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z}) \to \mathbb{Q}$ that is fixed by A_n would necessarily be constant, but then $\sum_D f(D) = 0$ implies that $f = 0$. Consider now the exact sequence

$$0 \to T_n' \to V_n' \to V_n'/T_n' \to 0$$

of H_n-modules, which induces an isomorphism $(V_n'/T_n')^{A_n} \to \mathrm{H}^1(A_n, T_n')$ since $\mathrm{H}^1(H_n, V_n') = 0$ as V_n' is divisible. So we are looking to determine the A_n-fixed functions in

$$V_n'/T_n' = \left\{ f : \mathbb{P}^1(\mathbb{Z}/p^{n+1}\mathbb{Z}) \to \mathbb{Q}/\mathbb{Z} \;\middle|\; \textstyle\sum_D f(D) = 0 \right\}.$$

Such a function must be constant, since A_n acts transitively. Say $f(D) = f_0$. Then $m \cdot f_0 = 0$, so $f_0 \in (1/m)\mathbb{Z}$ gives the result. □

Proposition 26. *If U is any lattice in V_n' fixed by H_n, then $\#\,\mathrm{H}^1(A_n, U) = m$.*

Proof. The lattice U is contained in a scaled version of T_n' with finite index, say $0 \to U \to T_n' \to Z \to 0$. Since the Herbrand quotient[2] satisfies $h(A_n, Z) = 1$ for the finite A_n-module Z, we have $\#\,\mathrm{H}^1(A_n, U) = h(A_n, U) = h(A_n, T_n') = \#\,\mathrm{H}^1(A_n, T_n') = m$. □

It is not true in general that $\mathrm{H}^1(A_n, U)$ is cyclic. For $n = 0$, it can have up to three cyclic factors.

[2] We set $h(G, A) = \#\,\mathrm{H}^1(G, A)/\#\,\mathrm{H}^2(G, A)$ for a finite cyclic group G acting on a G-module A.

8.3. ***Proof of Theorem 21.*** We have an injection

$$\iota : V_n' \to E(F_n) \otimes \mathbb{Q}, \quad f \mapsto \sum_D f(D) \cdot Q_D,$$

where Q_D is the higher self-point constructed in Sections 7.2 and 7.3. Let S_n be the saturated group generated by the higher self-points in $E(F_n)$, that is,

$$S_n = \left\{ P \in E(F_n) \;\middle|\; \text{there is a } k > 0 \text{ such that } k \cdot P \in \mathbb{Z}[H_n] \cdot Q_D \right\}.$$

By definition all torsion points in $E(F_n)$ belong to S_n; moreover we have

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

where U_n can be identified as a H_n-stable lattice in the image of ι. Because there are no A_n-fixed elements in U_n, we find

$$\begin{aligned} 0 \longrightarrow \mathrm{H}^1(A_n, E(F_n)_{\text{tors}}) \longrightarrow \mathrm{H}^1(A_n, S_n) \longrightarrow \mathrm{H}^1(A_n, U_n) \\ \longrightarrow \mathrm{H}^2(A_n, E(F_n)_{\text{tors}}) \longrightarrow \mathrm{H}^2(A_n, S_n) \longrightarrow 0. \end{aligned}$$

Since the Herbrand quotient $h(A_n, E(F_n)_{\text{tors}})$ is trivial, we find

$$\begin{aligned} \#\mathrm{H}^1(A_n, S_n) &= \#\mathrm{H}^1(A_n, U_n) \cdot \#\mathrm{H}^1(A_n, S_n) \\ &\geqslant \#\mathrm{H}^1(A_n, U_n) = m = (p+1) \cdot p^n \end{aligned}$$

by Proposition 26. Note also that since $E(F_n)$ has no p-torsion points, we know that $\#\mathrm{H}^1(A_n, S_n)[p^n] = \#\mathrm{H}^1(A_n, U_n)[p^n] = p^n$. Consider the natural inclusion of S_n into $E(F_n)$. The cokernel of this inclusion Y_n is a free $\mathbb{Z}$-module. The long exact sequence

$$0 \longrightarrow E(F_n^A)_{\text{tors}} \longrightarrow E(F_n^A) \longrightarrow {Y_n}^{A_n} \longrightarrow \mathrm{H}^1(A_n, S_n) \longrightarrow \mathrm{H}^1(A_n, E(F_n)) \quad (5)$$

shows that ${Y_n}^{A_n}$ has the same rank as $E(F_n^A)$.

Composing the last map in the above sequence with the inflation map will be called the *derivation map*

$$\partial_n : \mathrm{H}^1(A_n, S_n) \longrightarrow \mathrm{H}^1(A_n, E(F_n)) \xrightarrow{\text{inf}} \mathrm{H}^1(F_n^A, E).$$

Since S_n has no p-torsion elements, we can identify the p^n-torsion part of the source with

$$\left(\frac{S_n}{p^n S_n}\right)^{A_n} \xrightarrow{\cong} \mathrm{H}^1(A_n, S_n)[p^n] \ ,$$

and therefore we call the image of ∂_n the *derived classes* of higher self-points.

Lemma 27. *The image of ∂_n is contained in* $Ш(E/F_n^A)$.

Proof. Let κ be the lift of an element in the image of ∂_n under the map

$$\mathrm{H}^1(F_n^A, E[m']) \longrightarrow \mathrm{H}^1(F_n^A, E)[m']$$

for a sufficiently large m'. Since the extension F_n/F_n^A is nonramified at a place v outside the set Σ of places in F_n^A above p, N or ∞, the restriction of κ to $\mathrm{H}^1(F_{n,v}^A, E[m'])$ will lie in $\mathrm{H}^1_f(F_n^A, E[m'])$. Now for any place v in Σ, the place v splits completely in extension F_n/F_n^A by Proposition 24. Therefore the restriction of κ to $\mathrm{H}^1(F_{n,v}^A, E)[m']$ is trivial since it comes from the inflation

$$\mathrm{H}^1(F_n/F_n^A, E(F_n)) \longrightarrow \mathrm{H}^1(F_n^A, E).$$

Hence κ belongs to the Selmer group within $\mathrm{H}^1(F_n^A, E[m'])$. □

We can now end the proof of Theorem 21. Denote by s the minimal number of generators of the kernel of ∂_n. From the long exact sequence (5), we see that the rank of ${Y_n}^{A_n}$ is at least s. So, if ∂_n is not injective, then $\mathrm{rank}(E(F_n^A))$ is positive. So either the image of ∂, lifted to the Selmer group, will contribute p^n elements or else $E(F_n^A)$ will give rise to a copy of $\mathbb{Z}/p^n\mathbb{Z}$ in $\mathrm{Sel}_{p^n}(E/F_n^A)$. □

We add here a comment on the case when E has supersingular reduction at p. It turns out that construction of derivative classes in $\mathrm{H}^1(F_n^A, E)$ using higher self-points works the same, provided that the higher self-points are of infinite order. The main difference is that the cohomology classes do not belong to the Tate–Shafarevich group. In fact, under the assumption that the derivative map is not trivial, they will provide classes that are orthogonal to elements from the Selmer group and could be used to bound the Selmer group from above, just like Kolyvagin's classes built from Heegner points. Unfortunately we do not know a way of proving the assumption; hence these derivative classes cannot be used to say something about the Selmer group.

8.4. ***Derivative of self-points.*** Besides constructing derivative classes of higher self-points, we can also produce cohomology classes from self-points. We only sketch here the results whose proofs are similar to the previous sections.

Let $E/\mathbb{Q}$ be an elliptic curve of conductor N. Assume for simplicity that $N = p$ is prime. Put $K = K_p$. It is known that ρ_p is surjective; for more details see [Delaunay and Wuthrich 2008]. So the Galois group $G = \mathrm{Gal}(K/\mathbb{Q})$ is isomorphic to $\mathrm{PGL}_2(\mathbb{F}_p)$. Let A be any cyclic subgroup of order $p+1$ in G.

Theorem 28. *There is map ∂ to the Tate–Shafarevich group $Ш(E/K^A)$ from a group of order at least $p+1$. If r is the difference of the rank of $E(\mathbb{Q}(C))$ and $E(\mathbb{Q})$, then*

$$\#\,\mathrm{Sel}_{p+1}(E/K^A) \geqslant (p+1)^r \cdot \#E(\mathbb{Q})[p+1].$$

As before we consider the saturation of the self-points S in $E(K)$. We know that S modulo its torsion part is a lattice U in the Steinberg representation of $\mathrm{PGL}_2(\mathbb{F}_p)$. As we have seen in Section 8.2, the cohomology group $\mathrm{H}^1(A, U)$ will have $p+1$ elements. In [Delaunay and Wuthrich 2008, Section 4], we computed the torsion subgroup of $E(K)$. Using this we obtain that $E(K^A)_{\mathrm{tors}} = E(\mathbb{Q})_{\mathrm{tors}}$ and

$$\mathrm{H}^1(A, E(K)_{\mathrm{tors}}) = \mathrm{H}^2(A, E(K)_{\mathrm{tors}}) = \begin{cases} \mathbb{Z}/2\mathbb{Z}, \\ 0, \end{cases}$$

the nontrivial case occurring exactly when E is one of the curves 17a2, 17a3, 17a4 or any Neumann–Setzer curve. As before, this shows that $\mathrm{H}^1(A, S)$ has either $p+1$ or $2(p+1)$ elements. The derivative map is again

$$\partial : \mathrm{H}^1(A, S) \longrightarrow \mathrm{H}^1(A, E(K)) \longrightarrow \mathrm{H}^1(K^A, E),$$

and its image is in the Tate–Shafarevich group $Ш(E/K^A)$. Denote by Y the quotient of $E(K)$ by S. Then $\ker \partial$ is the quotient of Y^A by $E(K^A)$. If this map ∂ is not injective, then there is a $y \in Y^G$, lifting to a point of infinite order $Q \in E(K)$, such that Q does not belong to $E(K^A)$ but a nonzero multiple of it does. So either ∂ is surjective or there are points of infinite order defined over K^A that only become divisible in $E(K)$.

We should add that the control theorem for the Selmer group is not necessarily perfect; the kernel of $\mathrm{Sel}_{p+1}(E/K^A) \to \mathrm{Sel}_{p+1}(E/K)$ can be of order 1 or 2.

It is also worth adding another particular property of K^A: the L-series of E over K^A is the product of $\prod_\rho L(E, \rho, s)$, where ρ runs over all distinct irreducible representations of $\mathrm{PGL}_2(\mathbb{F}_p)$ except the Steinberg representation and the nontrivial 1-dimensional representation. It is not known whether this L-series admits analytic continuation.

Acknowledgments

It is a pleasure to thank John Coates, Henri Darmon, Christophe Delaunay, Ralph Greenberg, Masato Kurihara, and Marusia Rebolledo for helpful and interesting discussions concerning self-points.

References

[Atkin and Lehner 1970] A. O. L. Atkin and J. Lehner, "Hecke operators on $\Gamma_0(m)$", *Math. Ann.* **185** (1970), 134–160. MR 42 #3022 Zbl 0177.34901

[Bertolini, Darmon and Prasanna ≥ 2009] M. Bertolini, H. Darmon, and K. Prasanna, "Exotic Heegner points", in preparation.

[Breuil et al. 2001] C. Breuil, B. Conrad, F. Diamond, and R. Taylor, "On the modularity of elliptic curves over $\mathbb{Q}$: Wild 3-adic exercises", *J. Amer. Math. Soc.* **14**:4 (2001), 843–939. MR 2002d:11058 Zbl 0982.11033

[Coates et al. 2005] J. Coates, T. Fukaya, K. Kato, R. Sujatha, and O. Venjakob, "The GL_2 main conjecture for elliptic curves without complex multiplication", *Publ. Math. Inst. Hautes Études Sci.* 101 (2005), 163–208. MR 2007b:11172

[Coates et al. 2009] J. Coates, T. Fukaya, K. Kato, and R. Sujatha, "Root numbers, Selmer groups, and non-commutative Iwasawa theory", *J. Algebraic Geom.* (2009).

[Cremona 1997] J. E. Cremona, *Algorithms for modular elliptic curves*, 2nd ed., Cambridge University Press, 1997. MR 99e:11068 Zbl 0872.14041

[Delaunay and Wuthrich 2008] C. Delaunay and C. Wuthrich, "Self-points on elliptic curves of prime conductor", preprint, 2008. To appear in *Internat. J. Number Theory*.

[Edixhoven 1991] B. Edixhoven, "On the Manin constants of modular elliptic curves", pp. 25–39 in *Arithmetic algebraic geometry* (Texel, 1989), edited by G. van der Geer et al., Progr. Math. **89**, Birkhäuser, Boston, 1991. MR 92a:11066 Zbl 0749.14025

[Greenberg 2008] R. Greenberg, "Iwasawa theory, projective modules, and modular representations", preprint, 2008, Available at http://www.math.washington.edu/~greenber/NewMod.pdf.

[Harris 1979] M. Harris, "Systematic growth of Mordell–Weil groups of abelian varieties in towers of number fields", *Invent. Math.* **51**:2 (1979), 123–141. MR 80i:14015 Zbl 0429.14013

[Jetchev et al. 2007] D. Jetchev, K. Lauter, and W. Stein, "Explicit Heegner points: Kolyvagin's conjecture and nontrivial elements in the Shafarevich–Tate group", preprint, 2007. arXiv 0707.0032

[Katz and Mazur 1985] N. M. Katz and B. Mazur, *Arithmetic moduli of elliptic curves*, Annals of Mathematics Studies **108**, Princeton University Press, 1985. MR 86i:11024 Zbl 0576.14026

[Kolyvagin 1990] V. A. Kolyvagin, "Euler systems", pp. 435–483 in *The Grothendieck Festschrift, II*, edited by P. Cartier et al., Progr. Math. **87**, Birkhäuser, 1990. MR 92g:11109 Zbl 0742.14017

[Mazur 1978] B. Mazur, "Rational isogenies of prime degree", *Invent. Math.* **44**:2 (1978), 129–162. MR 80h:14022 Zbl 0386.14009

[Mazur and Rubin 2008] B. Mazur and K. Rubin, "Growth of Selmer rank in nonabelian extensions of number fields", *Duke Math. J.* **143**:3 (2008), 437–461. MR 2423759 Zbl 1151.11023

[Serre 1968] J.-P. Serre, *Abelian l-adic representations and elliptic curves*, Benjamin, New York, 1968. MR 41 #8422 Zbl 0186.25701

[Serre 1972] J.-P. Serre, "Propriétés galoisiennes des points d'ordre fini des courbes elliptiques", *Invent. Math.* **15**:4 (1972), 259–331. MR 52 #8126 Zbl 0235.14012

[Serre 1996] J.-P. Serre, "Travaux de Wiles (et Taylor, ...), I", pp. 319–332 in *Séminaire Bourbaki, 1994/95*, Astérisque **237,** Exposé 803, Société Math. de France, Paris, 1996. MR 97m:11076 Zbl 0957.11027

[Silberger 1970] A. J. Silberger, PGL_2 *over the p-adics: its representations, spherical functions, and Fourier analysis*, Lecture Notes in Mathematics **166**, Springer, Berlin, 1970. MR 44 #2891 Zbl 0204.44102

[Wuthrich 2007] C. Wuthrich, "Self-points on an elliptic curve of conductor 14", pp. 189–195 in *Proceedings of the Symposium on Algebraic Number Theory and Related Topics*, edited by K. Hashimoto, RIMS Kôkyûroku Bessatsu **B4**, Res. Inst. Math. Sci., Kyoto, 2007. MR 2402010 Zbl 05258116

Communicated by Karl Rubin
Received 2008-06-10 Revised 2009-02-23 Accepted 2009-02-24

christian.wuthrich@nottingham.ac.uk
School of Mathematical Sciences, University of Nottingham, Nottingham NG7 2RD, United Kingdom