Mazur's Conjecture on higher Heegner points

Christophe Cornut

March 16, 2001

Abstract

In this article, we establish a non-triviality statement for Heegner points which was conjectured by B. Mazur [10], and has subsequently been used as a working hypothesis by a few authors in the study of the arithmetic of elliptic curves.

Introduction

Let $\mathbb{E}_{/\mathbb{Q}}$ be an elliptic curve and $\pi : X_0(N)_{/\mathbb{Q}} \to \mathbb{E}_{/\mathbb{Q}}$ a modular parametrisation. Let $K \subset \mathbb{C}$ be an imaginary quadratic field, O_K its ring of integers and d_K its discriminant. Assume the following *Heegner Hypothesis*: all prime factors of N split in K. Choose an ideal $\mathcal{N}$ of O_K such that $O_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$. Then the complex tori $\mathbb{C}/O_K$ and $\mathbb{C}/\mathcal{N}^{-1}$ define elliptic curves related by a cyclic N-isogeny, i.e., a complex point x_1 of $X_0(N)$. More generally, if c is a positive integer prime to N, let $O_c = \mathbb{Z} + cO_K$ be the order of conductor c in K, put $\mathcal{N}_c = O_c \cap \mathcal{N}$, and define:

$$x_c = [\mathbb{C}/O_c \to \mathbb{C}/\mathcal{N}_c^{-1}] \in X_0(N)$$

The theory of complex multiplication shows that this *Heegner point* is rational over $K[c]$, the ring class field of conductor c of K — see [4] for the basic properties of these fields. Put $y_c = \pi(x_c) \in \mathbb{E}(K[c])$.

The Heegner Hypothesis implies that the L-function of $\mathbb{E}_{/K}$ vanishes to *odd* order at $s = 1$. B.H. Gross and D. Zagier [6] established a formula which relates the value of its derivative at 1 to the canonical height of the point $\mathrm{Tr}_{K[1]/K}(y_1)$ in $\mathbb{E}(K)$, thus proving in particular that:

$$\mathrm{Tr}_{K[1]/K}(y_1) \notin \mathbb{E}(K)_{\mathrm{tors}} \iff L'(\mathbb{E}/K, 1) \neq 0$$

In a subsequent work, V.A. Kolyvagin [8] showed the implication:

$$\mathrm{Tr}_{K[1]/K}(y_1) \notin \mathbb{E}(K)_{\mathrm{tors}} \implies \mathrm{rank}(\mathbb{E}(K)) = 1$$

Kolyvagin's method (together with the input from the Gross-Zagier formula) actually yields almost the complete Conjecture of Birch and Swinnerton-Dyer, *provided that* the analytic rank $\mathrm{ord}_{s=1} L(\mathbb{E}/K, s)$ equals 1.

In the general case, B. Mazur suggested that higher Heegner points may still have their word to say about the arithmetic of $\mathbb{E}_{/K}$. More precisely, let $p \nmid N$ be a prime number[1]. Then $K[p^\infty] = \bigcup_{n\geq 0} K[p^n]$ is a finite extension of the *anticyclotomic* $\mathbb{Z}_p$-extension H_∞ of K, and Mazur's conjecture [10], which we will prove here, is the following:

Theorem. *There exists $n \geq 0$ such that:* $\mathrm{Tr}_{K[p^\infty]/H_\infty}(y_{p^n}) \notin \mathbb{E}(H_\infty)_{\mathrm{tors}}$.

Let us quote some known consequences. Besides extra technical conditions – see the references for further details – all of these corollaries assume that $\mathbb{E}_{/\mathbb{Q}}$ has (good) *ordinary* reduction at p.

The theorem signifies that Heegner points yield non-trivial input for the Iwasawa theory of the elliptic curve $\mathbb{E}$ along H_∞/K. Extending Kolyvagin's method to this Iwasawa setting, M. Bertolini [1] has proved:

- Put $\Gamma = \mathrm{Gal}(H_\infty/K)$ and $\Lambda = \mathbb{Z}_p[[\Gamma]]$. Let H_n/K be the fixed field of Γ^{p^n}. Then the Pontryagin dual of $\mathrm{Sel}_{p^\infty}(\mathbb{E}/H_\infty) = \varinjlim(\mathrm{Sel}_{p^\infty}(\mathbb{E}/H_n))$ is a Λ-module of rank one.

The information thus obtained partially descends to K by control theorems due to Mazur. In this direction, J. Nekovář and N. Schappacher [11] have shown:

- The Selmer group $\mathrm{Sel}_{p^\infty}(\mathbb{E}/K) = \varinjlim \mathrm{Sel}_{p^n}(\mathbb{E}/K)$ contains a copy of $\mathbb{Q}_p/\mathbb{Z}_p$. In other words: $\mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(\mathbb{E}/K)) \geq 1$. If the p-part of the Tate-Šafarevič group of $\mathbb{E}_{/K}$ is finite, then $\mathrm{rank}(\mathbb{E}(K)) \geq 1$.

Using his theory of Selmer Complexes, J. Nekovář has recently [12] obtained:

- For any elliptic curve $\mathbb{E}_{/\mathbb{Q}}$,

$$\mathrm{ord}_{s=1} L(\mathbb{E}, \mathbb{Q}) \equiv \mathrm{corank}_{\mathbb{Z}_p}(\mathrm{Sel}_{p^\infty}(\mathbb{E}/\mathbb{Q})) \pmod 2$$

A central ingredient of our proof is taken from V. Vatsal who, in a preprint of Spring 2000 [19], used a theorem of M. Ratner to deduce an equidistribution statement for Gross points on the connected components of a "definite Shimura curve" (see [5]). In the meantime, Vatsal has also derived a proof of Mazur's conjecture, under the extra assumption that d_K is *prime* and not equal to p. He uses Jochnowitz congruences to relate his previous results to the setting of classical Heegner points on modular curves [20]. Our more direct and geometrical approach enables us, on the one hand, to relax the assumption on d_K, and on the other to generalize Mazur's conjecture in various ways – see below and section 4 for precise statements. Our analog of Vatsal's equidistribution result, (Theorem 3.1) may also be of independent interest.

Our proof starts from the simple (but crucial) observation that the torsion subgroup of $\mathbb{E}(K[\infty])$ is *finite*, where $K[\infty] = \bigcup_{c\geq 1} K[c]$ (Lemma 4.1). It follows

[1] See section 5 below for the case where p divides N.

for instance that *almost all* points $y_c \in \mathbb{E}(K[\infty])$ $(c \geq 1)$ have infinite order, since only a finite number of the distinct points $x_c \in X_0(N)(K[\infty])$ can map to the finite set $\mathbb{E}(K[\infty])_{\mathrm{tors}}$. In the same way, Mazur's conjecture would be proven once we knew that the set $\{\mathrm{Tr}_{K[p^\infty]/H_\infty}(y_{p^n}) \mid n \geq 0\}$ is infinite. This would obviously be true if the set

$$\left\{(\sigma x_{p^n})_{\sigma \in G_0} \mid n \geq 0\right\} \subset X_0(N)^{G_0}$$

were *Zariski dense*, where we put $G_0 = \mathrm{Gal}(K[p^\infty]/H_\infty)$.

This is however usually not the case. Indeed, let Q be a *ramified* prime of $K/\mathbb{Q}$ with residue characteristic $q \neq p$, and put $\sigma = \mathrm{Frob}_Q(K[p^\infty]/K) \in \mathrm{Gal}(K[p^\infty]/K)$. The relation $Q^2 = qO_K$ implies that $\sigma^2 = 1$, hence $\sigma \in G_0$ since G_0 is precisely the torsion subgroup of $\mathrm{Gal}(K[p^\infty]/K)$. But if $\sigma \neq 1$, the Zariski closure of the set $\{(x_{p^n}, \sigma x_{p^n}) \mid n \geq 0\}$ in $X_0(N) \times X_0(N)$ is a curve, namely the image of the modular curve $X_0(Nq)$ under the product of the two classical degeneracy maps $X_0(Nq) \to X_0(N)$ (cf. section 4.1).

In view of this obstruction, we are led to consider the "genus" subgroup:

$$G_1 = \left\langle \mathrm{Frob}_Q(K[p^\infty]/K) \mid\ Q^2 = qO_K,\, q \mid d_K,\, q \neq p \right\rangle \subset G_0.$$

The Galois action of G_1 on the Heegner points is of geometric nature. More precisely, pick a minimal family of primes $q_1 \ldots q_g \mid d_K$ whose corresponding Frobeniuses generate G_1, and put $M = q_1 \cdots q_g$. Then we construct (section 4.1) a family of points $(x'_{p^n})_{n \geq 0} \in X_0(NM)(K[p^\infty])$ and a non-constant morphism $\pi' : X_0(NM) \to \mathbb{E}$ defined over $\mathbb{Q}$ such that:

$$\forall n \geq 0: \qquad \pi'(x'_{p^n}) = \mathrm{Tr}_{G_1}(y_{p^n}) \in \mathbb{E}(K[p^\infty]).$$

Note that the Heegner Hypothesis does *not* hold for NM and K (unless G_1 is trivial, and we have not changed anything).

Choosing a complete set of representatives $\mathcal{R} \subset G_0$ of G_0/G_1, we now want the set $\left\{\sum_{\sigma \in \mathcal{R}} \sigma \cdot \pi'(x'_{p^n}) \mid n \geq 0\right\}$ to be infinite, and this is again related to the fact that

$$\left\{(\sigma x'_{p^n})_{\sigma \in \mathcal{R}} \mid n \geq 0\right\} \subset X_0(NM)^{\mathcal{R}}$$

is very large. In this direction, a sufficiently strong statement does indeed follow from our Theorem 3.1 on the reduction of *CM points* at inert primes.

This theorem holds without the Heegner Hypothesis on N and K. We say that $x = [E_1 \to E_2] \in X_0(N)(\mathbb{C})$ is a *CM point* if E_1 (and hence also E_2) has complex multiplication by K, i.e., if $\mathrm{End}^0_{\mathbb{C}}(E_1) = \mathrm{End}_{\mathbb{C}}(E_1) \otimes \mathbb{Q} \simeq K$; the *Heegner points* are special cases of CM points, for which we furthermore require that $\mathrm{End}_{\mathbb{C}}(E_1) = \mathrm{End}_{\mathbb{C}}(E_2)$. Let $E_{/\mathbb{C}}$ be an elliptic curve with CM by K, and $C \subset E(\mathbb{C})$ a cyclic subgroup of order N. Define $\mathcal{L}_p$ to be the set of all cyclic subgroups $a \subset E(\mathbb{C})$ of order p^n for some $n \geq 0$. Since $p \nmid N$, we can associate to each $a \in \mathcal{L}_p$ a CM point $H(a) = [E/a \to E/(a \oplus C)] \in X_0(N)(K[\infty])$. Let $\ell \nmid pN$ be a rational prime which is *inert* in K, and v_ℓ a place of $K[\infty]$ above ℓ. By Class Field Theory, the residue field k of v_ℓ is then isomorphic to $\mathbb{F}_{\ell^2}$. Theorem 3.1 states that *under a technical assumption on the finite set* $\mathcal{R} \subset \mathrm{Gal}(K[\infty]/K)$, the following map is surjective:

$$\begin{array}{rccl} \mathrm{RED}: & \mathcal{L}_p & \to & X_0^{\mathrm{ss}}(N)(k)^{\mathcal{R}} \\ & a & \mapsto & \left(\mathrm{red}_\ell(\sigma \cdot H(a))\right)_{\sigma \in \mathcal{R}} \end{array}$$

where $\mathrm{red}_\ell : X_0(N)(K[\infty]) \to X_0(N)(k)$ is the reduction map at v_ℓ and $X_0^{\mathrm{ss}}(N)(k)$ is the set of supersingular points in $X_0(N)(k)$.

The technical assumption alluded to above is needed to avoid the behaviour that we saw with G_1. It is verified for any set of representatives of G_0/G_1, so that by the argument sketched above, Mazur's conjecture easily follows from the surjectivity of RED (take $\ell \gg 0$). However, to get the most out of this surjectivity, we furthermore use a theorem of Ihara to obtain refined and generalized versions of Mazur's conjecture – Theorem A and B of section 4. For instance, we find:

Theorem. *Assume that the kernel of* $\pi_* : J_0(N) = \mathrm{Pic}^0(X_0(N)) \to \mathbb{E}$ *is connected. Then for all prime* $q \nmid \#\left(\mathbb{Z}/Nd_K\mathbb{Z}\right)^*$*, the* $\mathbb{F}_q$*-vector span of*

$$\left\{\mathrm{Tr}_{K[p^\infty]/H_\infty}(y_{p^n}) \otimes 1 \mid n \geq 0\right\} \subset \mathbb{E}(H_\infty) \otimes \mathbb{F}_q$$

has infinite dimension.

To prove Theorem 3.1, we first rewrite the map RED in p-adic terms, by means of a well-known adelic description of $X_0^{\mathrm{ss}}(N)(k)$ (section 2). Care must be taken to keep track of the Galois action on CM points. Theorem 3.1 then reduces to the surjectivity of a map

$$\begin{array}{ccl} PSL_2(\mathbb{Q}_p) & \to & \prod_{\sigma \in \mathcal{R}} PSL_2(\mathbb{Z}_p) \setminus PSL_2(\mathbb{Q}_p)/\Gamma_\sigma^1 \\ x & \mapsto & ([x], ..., [x]) \end{array}$$

where Γ_σ^1 is a discrete and cocompact subgroup of $PSL_2(\mathbb{Q}_p)$ associated to $\sigma \in \mathcal{R}$. This very same map also arises in the context of Gross points on definite Shimura curves [19], and we then follow Vatsal's proof with only minor improvements: put $G = PSL_2(\mathbb{Q}_p)$, $\Gamma^1 = \prod_{\sigma \in \mathcal{R}} \Gamma_\sigma^1$, and let Δ be the diagonal in $G^{\mathcal{R}}$. The asserted surjectivity follows from the topological statement that $\Delta\Gamma^1$ is dense in $G^{\mathcal{R}}$. A theorem of M. Ratner [14] states that the closure of $\Delta\Gamma^1$ equals $H\Gamma^1$, for a *closed subgroup* $H \supset \Delta$ of $G^{\mathcal{R}}$. A purely group-theoretical result (section 3.6) forces H to be equal to the full group $G^{\mathcal{R}}$, as soon as the Γ_σ^1's are non-commensurable. The technical assumption on $\mathcal{R}$ guarantees just this non-commensurability.

Acknowledgement: It is a pleasure to thank Norbert Schappacher for guiding me through the realms of complex multiplication, Bas Edixhoven and Jan Nekovář for their patience and constant support. I have also benefited from many valuable suggestions by Jean-Louis Colliot-Thélène, and Julien Haristoy carefully read the manuscript. Last but not least, I am indebted to Nike Vatsal

for the key idea to use Ratner's Theorem and for freely sharing his work with me during a visit to Strasbourg.

Notations: We write $\overline{F}$ for an algebraic closure of a field F, and $F^{\mathrm{ab}} \subset \overline{F}$ for its maximal abelian subextension. We fix once and for all an algebraically closed field $\Omega \supset K$ ($\Omega = \mathbb{C}$), and for $F \subset \Omega$ we take $\overline{F}$ within Ω. For a commutative group M and a prime number p, we put $\widehat{M} = M \otimes \widehat{\mathbb{Z}}$, $M_p = M \otimes \mathbb{Z}_p$ and $\widehat{M}^{(p)} = M \otimes \widehat{\mathbb{Z}}^{(p)}$, where $\widehat{\mathbb{Z}}$, $\mathbb{Z}_p$ and $\widehat{\mathbb{Z}}^{(p)}$ are the profinite, p-adic and "prime-to-p-adic" completions of $\mathbb{Z}$.

The formalism of $\mathfrak{a}$-Transforms: If R is a ring (unitary, but not necessarily commutative) acting on a commutative group scheme $G_{/S}$, then for any left R-module M, we define a presheaf of abelian group G^M on the category of S-schemes by the rule:

$$T_{/S} \longmapsto G^M(T) = \mathrm{Hom}_R\left(M, G(T)\right).$$

This construction is covariant and left exact in G, contravariant and left exact in M. If $G_{/S}$ is an abelian scheme, and M is a finite type left R-module, then $G^M_{/S}$ is a proper commutative group scheme. If M is furthermore projective (resp. locally free of rank r), then $G^M_{/S}$ is an abelian scheme (resp. of relative dimension $r \times \dim(G_{/S})$). For a left R-ideal $I \subset R$, we put $G[I] = G^{R/I}$ — References: [16], [3].

1 CM points

1.1 Normalization of $K \simeq \mathbf{End}^0_{\overline{F}}(E)$

We say that an elliptic curve E over a field F has complex multiplication (CM) by K if $\mathrm{End}^0_{\overline{F}}(E)$ is isomorphic to K. If F is a subfield of Ω, the action of $\mathrm{End}_{\overline{F}}(E)$ on the one dimensional Ω-vector space $\mathrm{Lie}(E)(\Omega)$ induces an embedding $\mathrm{End}^0_{\overline{F}}(E) \hookrightarrow \Omega$ which is onto K. *We shall always identify K and $\mathrm{End}^0_{\overline{F}}(E)$ in this way.* $\mathrm{End}_{\overline{F}}(E)$ is then an order $O_c \subset K$ for a positive integer c, the conductor of E, and we also say that E has CM by O_c. Furthermore:

$$K \subset F \Longleftrightarrow E \text{ has CM by } K \textit{ over } F \text{ (i.e. } \mathrm{End}_F(E) = O_c).$$

With this normalization, any isogeny $f : E_1 \to E_2$ between elliptic curves with CM by O_{c_1} and O_{c_2} respectively over a subfield F of Ω commutes with $O_{c_1} \cap O_{c_2}$: we say that f is K-linear.

1.2 Families of isogenous points in $X_0(N)$

Let $E_{/F}$ be an elliptic curve, with $F \subset \Omega$. Let $\hat{T}(E) = \varprojlim E[n](\overline{F}) = \prod_q T_q(E)$ be its Tate module, and $\hat{V}(E) = \hat{T}(E) \otimes \mathbb{Q}$, so that $\hat{V}(E)$ is the restricted product of $V_q(E) = T_q(E) \otimes \mathbb{Q}$ with respect to $T_q(E)$, as q varies over the set of all rational primes. The inductive limit of

$$n^{-1}\hat{T}(E)/\hat{T}(E) \xrightarrow{\sim} E(\overline{F})[n]$$

is a Galois equivariant isomorphism

$$\hat{V}(E)/\hat{T}(E) \xrightarrow{\sim} E(\overline{F})_{\text{tors}}.$$

In particular, if $\mathcal{L}$ is the set of $\widehat{\mathbb{Z}}$-submodules of $\hat{V}(E)$ that contains $\hat{T}(E)$ with a finite index, we obtain a Galois equivariant bijection between $\mathcal{L}$ and the set of finite subgroups of $E(\overline{F})$. For $a \in \mathcal{L}$, we denote by X_a the corresponding subgroup of $E(\overline{F})_{\text{tors}}$, and put $d(a) = \#X_a$. Using the special element $e = \hat{T}(E)$ of $\mathcal{L}$, we shall view $(\mathcal{L}, e)$ as a pointed indexing set, and we thus write $\hat{T}(a) = a$ to refer to the submodule of $\hat{V}(E)$ indexed by $a \in \mathcal{L}$; it admits a decomposition $\hat{T}(a) = \prod_q T_q(a)$.

To each $a \in \mathcal{L}$, we can associate the $\overline{F}$-isogeny $g_a : E \to E/X_a$. We have identifications:

$$\begin{array}{ccc} \hat{V}(E)/\hat{T}(E) & \xrightarrow{\sim} & E(\overline{F})_{\text{tors}} \\ \downarrow & & \downarrow g_a \\ \hat{V}(E)/\hat{T}(a) & \xrightarrow{\sim} & (E/X_a)(\overline{F})_{\text{tors}} \end{array}$$

If $\hat{T}(a)$ is stable under $\mathrm{Gal}(\overline{F}/F')$ for some algebraic extension F' of F, then the same holds for X_a, which thus descends to a finite subgroup scheme of $E_{/F'}$. In this situation, we simply say that E/X_a and g_a are defined over F'.

Let furthermore $C \subset E(\overline{F})$ be a cyclic subgroup of order $N \geq 1$, and define

$$\mathcal{L}' = \{a \in \mathcal{L} \mid \gcd(d(a), N) = 1\}.$$

Then for each $a \in \mathcal{L}'$, $E/X_a \to E/(X_a \oplus C)$ is a cyclic N-isogeny, hence defines a point

$$H(a) = \left[E/X_a \to E/(X_a \oplus C)\right] \in X_0(N)(\overline{F}).$$

We refer to the map $H : \mathcal{L}' \to X_0(N)(\overline{F})$ as the family of points associated to $E_{/F}$ and C.

1.3 Families of isogenous CM points

Assume now that E *has complex multiplication by* O_c *over* $F \subset \Omega$, so that H is a family of CM points. For any integer $d \geq 1$, we let $F[d] \subset F^{\text{ab}}$ be the composite of F and $K[d]$. Since $K[c] = K(j(E)) \subset F$ by [16], we thus have $F[d] = F[\mathrm{lcm}(c, d)]$.

For each $a \in \mathcal{L}$, the *conductor* of a is the unique integer $c(a) \geq 1$ such that:

$$\forall q: \quad \{x \in K_q \mid xT_q(a) \subset T_q(a)\} = (O_{c(a)})_q.$$

$T_q(a)$ is then free of rank one over $(O_{c(a)})_q$, and E/X_a has complex multiplication by $O_{c(a)}$. If $e' \in \mathcal{L}$ corresponds to C, and a belongs to $\mathcal{L}'$, then $E/(X_a \oplus C)$ has complex multiplication by $O_{c'(a)}$, where $c'(a) = c(a) \times (c(e')/c(e))$.

In particular, $T_q(E)$ is free of rank one over $(O_c)_q$. Since the action of $\mathrm{Gal}(\overline{F}/F)$ on $T_q(E)$ is $(O_c)_q$-linear, it factors through a morphism:

$$\rho_q : \mathrm{Gal}(F^{\mathrm{ab}}/F) \to (O_c)_q^*.$$

This implies that $E(\overline{F})_{\mathrm{tors}} = E(F^{\mathrm{ab}})_{\mathrm{tors}}$. If furthermore F *is a number field,* we use class field theory to view ρ_q as a morphism $\rho_q : I_F \to (O_c)_q^*$, where I_F is the idele group of F. Then:

Proposition 1.1 *If $O_c^* = \{\pm 1\}$, $\mathrm{Gal}(F^{\mathrm{ab}}/F[c(a)])$ fixes $\hat{T}(a)$ for all $a \in \mathcal{L}$.*

Proof: Put $d = \mathrm{lcm}(c, c(a))$. We want: $\forall \sigma \in \mathrm{Gal}(F^{\mathrm{ab}}/F[d])$, $\sigma \hat{T}(a) = \hat{T}(a)$.

There exists a continuous homomorphism $\varepsilon : I_F \to K^*$ such that:

$$\forall s \in I_F,\ \forall q : \qquad \rho_q(s) = \varepsilon(s) N_{F/K}(s_q^{-1}) \in (O_c)_q^*,$$

where s_q is the q-component of s. This is Theorem 10 of [17] in case $c = 1$ ($\mathrm{End}_F(E) = O_K$). The general case reduces to it, since there exists a finite subgroup $D \subset E(\overline{F})$, defined over F, and such that E/D has complex multiplication by O_K over F: simply take $D = \{x \in E(\overline{F}) \mid cO_K \cdot x = 0\}$.

Let $[F^{\mathrm{ab}}/F, \star] : I_F \to \mathrm{Gal}(F^{\mathrm{ab}}/F)$ be the Artin reciprocity map, and pick $s \in I_F$ such that $[F^{\mathrm{ab}}/F, s] = \sigma \in \mathrm{Gal}(F^{\mathrm{ab}}/F[d])$. Since

$$\sigma \mid_{K[d]} = 1 = \left[K[d]/K, N_{F/K}(s)\right],$$

$N_{F/K}(s)$ belongs to the norm subgroup of I_K corresponding to the abelian extension $K[d]/K$, namely $K^*(\widehat{O}_d^* \times \mathbb{C}^*)$. Writing $N_{F/K}(s) = \lambda(\hat{x} \times \mu)$ with $\lambda \in K^*$, $\hat{x} \in \widehat{O}_d^* \subset \widehat{O}_c^*$ and $\mu \in \mathbb{C}^*$, we obtain:

$$\forall q : \qquad \varepsilon(s)\lambda^{-1} = \rho_q(s)\hat{x}_q$$

The l.h.s. belongs to K and the r.h.s to $(O_c)_q^*$, so that finally $\varepsilon(s)\lambda^{-1}$ belongs to $O_c^* = \{\pm 1\}$. But then $\rho_q(s) = \pm \hat{x}_q^{-1} \in (O_d)_q^*$, hence $\rho_q(s)\hat{T}_q(a) = \hat{T}_q(a)$ for all q since $O_d \subset O_{c(a)}$, so that indeed $\sigma \hat{T}(a) = \hat{T}(a)$. $\square$

As a consequence, $E \to E/X_a$ is defined over $F[c(a)]$, and for $a \in \mathcal{L}'$, $H(a)$ belongs to $X_0(N)\big(F\left[\mathrm{lcm}\,(c(a), c'(a))\right]\big)$. We shall refine this latter fact below.

1.4 The Galois action on CM points

1.4.1 Fields of definition

Proposition 1.2 *Let $x = [f : E_1 \to E_2] \in X_0(N)(\Omega)$ be a CM point, with $\mathrm{End}(E_1) = O_{c_1}$ and $\mathrm{End}(E_2) = O_{c_2}$. Put $c = \mathrm{lcm}(c_1, c_2)$. Let S be a finite set of rational primes subject to the condition: if $d_K = -3$ or -4 and c is a power of p, then $p \notin S$. Then there exist elliptic curves $E'_{1/K[c]}$ and $E'_{2/K[c]}$ with good* *reduction above S, and a $K[c]$-isogeny $f' : E_1' \to E_2'$, whose base change to Ω fits in a commutative diagram*

$$\begin{array}{ccc} E_1' & \xrightarrow{\sim} & E_1 \\ f' \downarrow & & \downarrow f \\ E_2' & \xrightarrow{\sim} & E_2 \end{array}$$

In particular, $x = [f' : E_1' \to E_2'] \in X_0(N)(K[c])$.

Proof: Our assumption on S implies by a theorem of Serre-Tate [17, p. 507] that there exists an elliptic curve $E_{/K[c]}$ with good reduction above S and complex multiplication by O_c. Since $E_{/\Omega}$ is isogenous to E_1 and E_2, we can find two subgroups H_1 and H_2 of $E(K[c]^{\mathrm{ab}})$ and a commutative diagram of Ω-isogenies:

$$\begin{array}{ccc} E/H_1 & \xrightarrow{\sim} & E_1 \\ f' \downarrow & & \downarrow f \\ E/H_2 & \xrightarrow{\sim} & E_2 \end{array}$$

If $d_K = -3, -4$ and $c = 1$, we can take $H_1 = H_2 = 0$ since $\mathrm{Pic}(O_K) = \{1\}$; then f' belongs to $\mathrm{End}_{K[1]}(E)$. In all other cases, we take for f' the projection induced by an inclusion $H_1 \subset H_2$, and then apply Proposition 1.1. $\square$

1.4.2 The Galois action

Let $x = [f : E_1 \to E_2] \in X_0(N)(\Omega)$ be a CM point, with $\mathrm{End}(E_1) = O_{c_1}$ and $\mathrm{End}(E_2) = O_{c_2}$, so that x is rational over $K[c]$ with $c = \mathrm{lcm}(c_1, c_2)$. Following Serre [16], we shall describe the action of $\mathrm{Gal}(K[c]/K)$ on x using the formalism of $\mathfrak{a}$-transforms (cf. Introduction).

Recall the isomorphism from class field theory:

$$\left(\frac{K[c]/K}{\star}\right) : \mathrm{Pic}(O_c) \xleftarrow{\sim} \widehat{K}^*/K^*\widehat{O}_c^* \xrightarrow{\sim} \mathrm{Gal}(K[c]/K).$$

Proposition 1.3 *Let $\sigma = \left(\frac{K[c]/K}{Q}\right)$ for some O_c-proper fractional ideal Q of K. Then: $\sigma \cdot x = [f^Q : E_1^Q \to E_2^Q]$.*

Proof: A straightforward generalization of the case $N = 1$, proven in [16]. $\square$

Remark: Due to our chosen identification of K with $\mathrm{End}^0_\Omega(E_1)$ and $\mathrm{End}^0_\Omega(E_2)$, f is linear with respect to the action of $O_c = O_{c_1} \cap O_{c_2}$ on E_1 and E_2, so that f^Q is well-defined, and $\ker(f^Q)(\Omega) = \mathrm{Hom}_{O_c/NO_c}\big(Q/NQ, \ker(f)(\Omega)\big)$. Since $Q/NQ \simeq O_c/NO_c$, f^Q is indeed a cyclic N-isogeny.

Remark: Let $d \geq 1$ be an integer such that $c \mid d$, hence $K[c] \subset K[d]$ and $O_d \subset O_c$. Then we can also describe the action of $\sigma \in \mathrm{Gal}(K[d]/K)$ on x using transforms with respect to the action of O_d on the elliptic curves, and an O_d-proper fractional ideal $Q \subset K$ such that $\sigma = \left(\frac{K[d]/K}{Q}\right)$.

2 The supersingular locus $X_0^{\mathrm{ss}}(N)$

Let N be a positive integer, $\ell \nmid N$ a prime number and k a finite field of characteristic ℓ. Let $E_{/k}$ be a supersingular elliptic curve such that $\mathrm{End}_k(E) = \mathrm{End}_{\overline{k}}(E) = R$. Then R is an order in $B = \mathrm{End}_k^0(E)$, a quaternion algebra that ramifies exactly at ℓ and ∞ [18, V.3]. The aim of this section is to describe the supersingular locus $X_0^{\mathrm{ss}}(N)(\overline{k})$ of $X_0(N)(\overline{k})$ with these data, using the formalism of $\mathfrak{a}$-transforms (cf. Introduction).

2.1 Step 1: Inclusions of left R-ideals

We refer to nonzero finite type left R-submodules of B as *left R-ideals*. The right order of such an ideal I is $O_r(I) = \{x \in B \mid Ix \subset I\} \simeq \mathrm{End}_R(I)$. For left R-ideals $I \subset J$, we write $I \subset_{N,N} J$ as a shorthand for: $J/I \approx (\mathbb{Z}/N\mathbb{Z})^2$. Let $\mathrm{Cl}(R, N)$ be the orbit set for the obvious right action of B^* on the set of those inclusions. We will prove below the following:

Proposition 2.1 *R is a maximal order in B, all supersingular points of $X_0(N)(\overline{k})$ are rational over k and there exists a well-defined bijection*

$$\begin{array}{ccc} \mathrm{Cl}(R,N) & \to & X_0^{\mathrm{ss}}(N)(\overline{k}) \\ [I \subset_{N,N} J] & \mapsto & [E^J \to E^I] \end{array}$$

We first *assume* the (well-known) fact that R is a maximal order. Then:

Lemma 2.2 *1. For any left R-ideal I, $E^I_{/k}$ is a supersingular elliptic curve.*

2. *For any left R-ideals I and J, $E^\star : \mathrm{Hom}_{\mathrm{R}}(I, J) \to \mathrm{Hom}_k(E^J, E^I)$ is an isomorphism, and $\mathrm{Hom}_k(E^J, E^I) = \mathrm{Hom}_{\overline{k}}(E^J, E^I)$.*

3. *Any supersingular elliptic curve $E'_{/\overline{k}}$ is isomorphic to $E^I_{/\overline{k}}$ for some I.*

4. *If $0 \to N \to M \to P \to 0$ is an exact sequence of finite type left R-modules, then $0 \to E^P \to E^M \to E^N \to 0$ is* fppf*-exact.*

5. *If M is a* finite *left R-module, then $E^M_{/k}$ is a finite commutative group scheme of rank $\sqrt{\#M}$.*

6. *For any nonzero R-linear map $f : I \to J$ between left R-ideals,*

$$E^f : E^J \to E^I \text{ is a cyclic } N\text{-isogeny} \iff f(I) \subset_{N,N} J.$$

Proof: 1-3) Every left R-ideal I is locally principal, hence defines an elliptic curve $E^I_{/k}$, which is supersingular since $E^I(\overline{k})[\ell] = \mathrm{Hom}_R\big(I, E(\overline{k})[\ell]\big) = 0$. Since the number of isomorphism classes of left R-ideals equals the number of supersingular j-invariant (see [5, p. 117] and [18, V.4]), 3) follows from 2). Since $\mathrm{Hom}_k(E^J, E^I)$ is a direct factor of $\mathrm{Hom}_{\overline{k}}(E^J, E^I)$ (a $\mathbb{Z}$-module of rank 4), the injectivity of $E^\star$, which is easy, implies the last equality of 2). It remains to show that $E^\star$ is surjective. When $I = J$, this follows from the fact that $O_r(I)$ is a maximal order. In the general case, we may thus replace (R, E) by $(O_r(J), E^J)$ and use the identifications

$$\mathrm{Hom}_R(I, J) \simeq \mathrm{Hom}_{O_r(J)}(J^{-1}I, O_r(J)) \quad \text{and} \quad E^I \simeq (E^J)^{J^{-1}I},$$

(where $J^{-1} = \{x \in B \mid JxJ \subset J\}$) to reduce to the case where $J = R$. It is then routine to check that the subset $\mathrm{Hom}_k(E, E^I)$ of $E^I(E) = \mathrm{Hom}_R(I, E(E))$ equals $\mathrm{Hom}_R(I, \mathrm{End}_k(E)) = \mathrm{Hom}_R(I, R)$.

4) We want: $E^M \to E^N$ is faithfully flat. By a formal argument, we may assume that $N = I$ is a left R-ideal within $M = R$. Then $E^R = E \to E^I$ is an isogeny (hence faithfully flat), since its kernel $E^{R/I}$ is finite.

5) Considering a surjective map $R^n/\#MR^n \to M$, we see that the rank of $E^M_{/k}$ divides a power of $\#M$. The statement is then a formal consequence of the fact that both $\mathrm{rank}(E^M_{/k})$ and $\sqrt{\#M}$ are multiplicative on exact sequences of finite left R-modules by 4), and agree with the reduced norm of α when $M = R/R\alpha$, $\alpha \in R$, $\alpha \neq 0$.

6) Put $M = J/f(I)$, so that $\ker(E^f) \simeq E^M$. Since $E^M[d] \simeq E^{M/dM}$ for any positive integer d, we obtain using 5): $E^J \to E^I$ is a cyclic N-isogeny $\Leftrightarrow$ $\forall d$, $\mathrm{rank}(E^M[d]) = \gcd(N, d) \Leftrightarrow \forall d$, $\#M/dM = \gcd(N, d)^2$. The result easily follows. □

We may now prove Proposition 2.1: still assuming that R is a maximal order, part 2) and 6) of the Lemma imply that the map $[I \subset_{N,N} J] \in \mathrm{Cl}(R, N) \mapsto [E^J \to E^I] \in X_0^{\mathrm{ss}}(N)(k)$ is well-defined and injective, whereas part 2), 3) and 6) imply that it is onto $X_0^{\mathrm{ss}}(N)(\overline{k})$. Finally, to prove that R is indeed maximal, we merely need to construct a supersingular elliptic curve $E'_{/k}$ whose endomorphism ring R' is a maximal order, since the lemma then implies that the endomorphism ring of *any* supersingular elliptic curve is isomorphic to the right order of a left R'-ideal, hence maximal. But for any maximal order R' in B, the reduced connected component of $E^{RR'}$ is easily seen to be such an elliptic curve.

We shall also need the following straigthforward corollary of Lemma 2.2:

Lemma 2.3 *Let $h : E \to E'$ be a k-isogeny and $I = \{\alpha \in R \mid \alpha \cdot \ker(h) = 0\}$. Then $E[I] = \ker(h)$, so that there exists a commutative diagram*

$$\begin{tikzcd}
E \arrow[r] \arrow[dr, "h"'] & E^I \arrow[d, "\simeq"] \\
 & E'
\end{tikzcd}$$

2.2 Step 2: Adelisation

Since R is finite over $\mathbb{Z}$, $\widehat{R} = \prod_q R_q$, and $\widehat{B} = \prod'_q B_q$ is the restricted product of the B_q's with respect to the R_q's, as q varies over all prime numbers. For a left R-ideal I and a finite idele $\hat{b} = (b_q) \in \widehat{B}^*$, we define the left R-ideal $I\hat{b} \subset B$ by the rule: $(I\hat{b})_q = I_q b_q$ for all q. Equivalently, $I\hat{b} = \widehat{I}\hat{b} \cap B$ in $\widehat{B}$. The right order of $I\hat{b}$ is $O_r(I\hat{b}) = \hat{b}^{-1}O_r(I)\hat{b}$. If $I \subset_{N,N} J$, then $I\hat{b} \subset_{N,N} J\hat{b}$, and we thus obtain a right action of $\widehat{B}^*$ (extending that of B^*) on the set of those inclusions. The stabilizer of $(I \subset_{N,N} J)$ is easily seen to be $\widehat{O_r(J/I)}^*$, where $O_r(J/I) = O_r(J) \cap O_r(I)$ (an Eichler order). Furthermore:

Lemma 2.4 *This action is transitive.*

Proof: Let $(I \subset_{N,N} J)$ and $(I' \subset_{N,N} J')$ be inclusions of left R-ideals. The question is local, so we must show that for any q, there exists $b_q \in B_q^*$ such that $(I'_q \subset J'_q)b_q = (I_q \subset J_q)$. Note that if q^r exactly divides N, then $I'_q \subset_{q^r,q^r} J'_q$ and $I_q \subset_{q^r,q^r} J_q$. If $q = \ell$, let $\pi \in R_\ell$ be a uniformising element; since left R_ℓ-ideals can be written as $R_\ell \pi^n$ for some n, the existence of b_ℓ is clear. If $q \neq \ell$, then $R_q \approx M_2(\mathbb{Z}_q)$ and the Morita correspondence reduces the problem to a similar and classical statement on lattices in $\mathbb{Z}_q^2$. $\square$

Thus, fixing an inclusion of left R-ideals $(I_0 \subset_{N,N} J_0)$, we obtain a bijection:

$$\widehat{O_r(J_0/I_0)}^* \setminus \widehat{B}^*/B^* \xrightarrow{\sim} \mathrm{Cl}(R,N).$$

Since $\widehat{\mathbb{Z}}^*\mathbb{Q}^* = \widehat{\mathbb{Q}}^*$ ($\mathbb{Z}$ is principal),

$$\widehat{O_r(J_0/I_0)}^* \setminus \widehat{B}^*/B^* = \widehat{O_r(J_0/I_0)}^* \widehat{\mathbb{Q}}^* \setminus \widehat{B}^*/B^*.$$

2.3 Step 3: Strong approximation

Fix a prime number $p \neq \ell$ and define $R_0 = O_r(J_0/I_0)$, an (Eichler) order in B. The strong approximation theorem [21, p. 81] implies that the embedding $B_p^* \to \widehat{B}^*$ induces a *surjective* map $B_p^* \to \widehat{R}_0^*\widehat{\mathbb{Q}}^* \setminus \widehat{B}^*/B^*$. If Γ is the image of $R_0[1/p]^*$ in B_p^*, an easy computation shows that:

$$R_{0,p}^*\mathbb{Q}_p^* \setminus B_p^*/\Gamma \xrightarrow{\sim} \widehat{R}_0^*\widehat{\mathbb{Q}}^* \setminus \widehat{B}^*/B^*.$$

We finally obtain a sequence of bijections:

$$\begin{array}{ccccccc} R_{0,p}^*\mathbb{Q}_p^* \setminus B_p^*/\Gamma & \to & \widehat{R}_0^*\widehat{\mathbb{Q}}^* \setminus \widehat{B}^*/B^* & \to & \mathrm{Cl}(R,N) & \to & X_0^{\mathrm{ss}}(N)(k) \\ [b \in B_p^*] & \mapsto & [b \in \widehat{B}^*] & \mapsto & [I_0 b \subset J_0 b] & \mapsto & [E^{J_0 b} \to E^{I_0 b}] \end{array}$$

3 The reduction of CM points at inert primes

3.1 Notations and Result

Let $E_{/\Omega}$ be an elliptic curve with complex multiplication by K, together with a cyclic subgroup $C \subset E(\Omega)$ of order N. Let

$$H : \mathcal{L}' \to X_0(N)(K[\infty])$$

be the associated family of CM points, where $K[\infty] = \bigcup_{c \geq 1} K[c]$ – see section 1 for the definition, and all related notations. We do *not* require any hypothesis on N relative to K in this section. Let $p \nmid N$ be a prime number, and define

$$\mathcal{L}_p = \{a \in \mathcal{L} \mid X_a \approx \mathbb{Z}/p^n\mathbb{Z} \quad \text{for some } n \geq 0\} \subset \mathcal{L}'.$$

Let S be a *finite* set of rational primes $\ell \nmid Np$ which are *inert in* K; choose for each $\ell \in S$ a place v_ℓ of $K[\infty]$ above ℓ, and let $k(\ell)$ be its residue field, so that $k(\ell) \approx \mathbb{F}_{\ell^2}$. Since $\ell \nmid N$ is inert in K, the reduction map at v_ℓ,

$$\mathrm{red}_\ell : X_0(N)(K[\infty]) \to X_0(N)(k(\ell)),$$

maps any CM point (relative to K) to the supersingular locus $X_0^{\mathrm{ss}}(N)(k(\ell))$ of $X_0(N)(k(\ell))$ [3, 3.3.4]. Finally, let $\mathcal{R}$ be a *finite* subset of $\mathrm{Gal}(K[\infty]/K)$.

Denote $[K[\infty]/K, \star] : \widehat{K}^* \twoheadrightarrow \mathrm{Gal}(K[\infty]/K)$ the Artin reciprocity map. This section will be devoted to the proof of the following theorem.

Theorem 3.1 *Assume that* $\forall(\sigma \neq \sigma') \in \mathcal{R}^2$, $\sigma^{-1}\sigma' \notin \left[K[\infty]/K, \widehat{K}^{(p)*}\right]$. *Then*

$$\begin{array}{rccl} \mathrm{RED}: & \mathcal{L}_p & \to & \prod_{\ell\in S} X_0^{\mathrm{ss}}(N)\big(k(\ell)\big)^{\mathcal{R}} \\ & a & \mapsto & \Big(\mathrm{red}_\ell\big(\sigma \cdot H(a)\big)\Big)_{\sigma\in\mathcal{R},\ell\in S} \end{array}$$

is surjective.

We refer the reader to the Introduction for an overview of the proof. With $\mathcal{R} = \{1\}$, the theorem implies:

Corollary 3.2 *Let $\mathcal{I}$ be the set of all rational primes $\ell \nmid pN$ inert in K, choose for each ℓ a place v_ℓ of $K[\infty]$ above ℓ and let $k(\ell)$ be the residue field. Then the image of the map*

$$a \in \mathcal{L}_p \mapsto \Big(\mathrm{red}_\ell\big(H(a)\big)\Big)_{\ell\in\mathcal{I}} \in \prod_{\ell\in\mathcal{I}} X_0^{\mathrm{ss}}(N)\big(k(\ell)\big)$$

is dense (with respect to the product of the discrete topologies).

3.2 Preliminary normalizations

3.2.1 Fields of definition

In view of Proposition 1.2, we first *may and do assume* that E is defined over a finite extension $F \subset K[\infty]$ of K, that $E_{/F}$ has good reduction at all places above S, and is furthermore F-isogenous to an elliptic curve with complex multiplication by $O_{c'}$, with c' prime to S and $O_{c'}^* = \{\pm 1\}$ (the latter is an empty condition if $d_K \neq -3, -4$).

If $e, e' \in \mathcal{L}$ correspond respectively to the subgroups 0 and C of $E(\overline{F})$, then for each $a \in \mathcal{L}'$, E/X_a has CM by $O_{c(a)}$ and $E/(X_a \oplus C)$ has CM by $O_{c'(a)}$, where $c'(a) = c(a) \times c(e)/c(e')$. Propositions 1.1 and 1.2 imply:

- $g_a : E \to E/X_a$ is defined over $F[c(a)]$,
- $h_a : E/X_a \to E/(X_a \oplus C)$ is defined over $F[\mathrm{lcm}(c(a), c'(a))]$,
- $H(a) = [E/X_a \to E/(X_a \oplus C)]$ belongs to $X_0(N)\big(K[\mathrm{lcm}(c(a), c'(a))]\big)$.

3.2.2 Good reduction

Let v be a place of $K[\infty]$ with residue field $k(\ell)$ of characteristic ℓ *inert* in K. Let $F_1 \subset F_2$ be two finite subextensions of $K[\infty]/K$, with valuation rings $O_{v_1} \subset O_{v_2}$ at v. Let $A_{/F_1}$ be an abelian variety with good reduction at v, so that its Néron model $A_{/O_{v_1}}$ is an abelian scheme. The base change of this Néron model to O_{v_2} is also an abelian scheme, hence the Néron model of its generic fiber $A_{/F_2}$, which is the base change of $A_{/F_1}$ to F_2. Since the residue fields of O_{v_1} and O_{v_2} are both equal to $k(\ell)$ (ℓ being inert in K), we can simply identify the special fibers of the Néron models of $A_{/F_1}$ and $A_{/F_2}$. We will refer to this special fiber $\widetilde{A}_{/k(\ell)}$ as the "reduction of A at v", disregarding the subextension F of $K[\infty]/K$ where we need to consider A.

Since $E_{/F}$ has good reduction at all places above $\ell \in S$, this applies to the elliptic curves that we shall consider below, these being isogenous to E over finite subextensions of $K[p^\infty]/F$. We can thus refer to their reduction at v_ℓ.

3.2.3 Normalizing data

The computations below involve a few normalizations with respect to our base point e, ultimately reducing to the choice of an isomorphism:

$$\xi : T_p(E) \xrightarrow{\sim} \mathbb{Z}_p^2.$$

It extends to an isomorphism $\xi : V_p(E) \xrightarrow{\sim} \mathbb{Q}_p^2$.

Let $\mathcal{T}_p = GL_2(\mathbb{Z}_p)\mathbb{Q}_p^* \setminus GL_2(\mathbb{Q}_p)$ be the Bruhat-Tits tree of $PGL_2(\mathbb{Q}_p)$. For each $a \in \mathcal{L}_p$, *we choose* $\tau_a \in GL_2(\mathbb{Q}_p)$ such that $\tau_a \cdot \mathbb{Z}_p^2 = \xi(T_p(a)) \subset \mathbb{Q}_p^2$. This yields a bijection:

$$\begin{array}{rccc} \phi_1 : & \mathcal{L}_p & \xrightarrow{\sim} & \mathcal{T}_p \\ & a & \longmapsto & [\tau_a^{-1}] \end{array}$$

For each $\ell \in S$, let $\widetilde{E}_{/k(\ell)}$ be the reduction of E at v_ℓ, $R(\ell) = \mathrm{End}_{k(\ell)}(\widetilde{E})$ and $B(\ell) = \mathrm{End}^0_{k(\ell)}(\widetilde{E})$. Our assumptions on E, F and S imply that $R(\ell) = \mathrm{End}_{\overline{k(\ell)}}(\widetilde{E})$, so that $R(\ell)$ is a maximal order in $B(\ell)$, a quaternion algebra that ramifies precisely at ℓ and ∞. According to Lemmas 2.2 and 2.3, the reduction of $h : E \to E/C$ at v_ℓ is a (separable) cyclic N-isogeny with kernel $\widetilde{C}$, which identifies with the isogeny $\widetilde{E} \to \widetilde{E}^{I(\ell)}$ induced by $I(\ell) \subset_{N,N} R(\ell)$, where

$$I(\ell) = \left\{ x \in R(\ell) \mid x \cdot \widetilde{C} = 0 \right\}.$$

Using $\widetilde{E}_{/k(\ell)}$ and this inclusion of left $R(\ell)$-ideals to normalize the description of $X_0^{\mathrm{ss}}(N)(k(\ell))$ in section 2, we thus obtain:

$$\begin{array}{rcl} R(\ell)_p^* \mathbb{Q}_p^* \setminus B(\ell)_p^* / \Gamma(\ell) & \xrightarrow{\sim} & X_0^{\mathrm{ss}}(N)(k(\ell)) \\ {[b \in B(\ell)_p^*]} & \longmapsto & [\widetilde{E}^{R(\ell)\cdot b} \to \widetilde{E}^{I(\ell)\cdot b}] \end{array}$$

where $\Gamma(\ell) = R'(\ell)[1/p]^* \subset B(\ell)_p^*$, with $R'(\ell) = R(\ell) \cap O_r(I(\ell))$ (observe that $R'(\ell)_p = R(\ell)_p$ since p does not divide N).

The reduction at v_ℓ however yields an isomorphism $x \in T_p(E) \mapsto \widetilde{x} \in T_p(\widetilde{E})$, which together with ξ gives an isomorphism $\widetilde{\xi} : T_p(\widetilde{E}) \to \mathbb{Z}_p^2$. Using the action of $R(\ell)_p$ on $T_p(\widetilde{E})$, we thus obtain an isomorphism $\theta_\ell : B(\ell)_p \to M_2(\mathbb{Q}_p)$ mapping $R(\ell)_p$ onto $M_2(\mathbb{Z}_p)$, and characterized by $\theta_\ell(\alpha) \cdot \xi(x) = \widetilde{\xi}(\alpha \cdot \widetilde{x})$ for all $\alpha \in R(\ell)$, $x \in T_p(E)$. If $i_\ell : K \to B(\ell)$ is the natural embedding given by the reduction of endomorphisms, then the composite map $\theta_\ell \circ i_\ell : K_p \to M_2(\mathbb{Q}_p)$ does *not* depend on $\ell \in S$.

Using θ_ℓ, we can now rewrite our description of $X_0^{\mathrm{ss}}(N)(k(\ell))$ as a bijection:

$$\begin{array}{rcl} \mathcal{T}_p/\theta_\ell(\Gamma(\ell)) & \xrightarrow{\sim} & X_0^{\mathrm{ss}}(N)(k(\ell)) \\ [\theta_\ell(b)] & \longmapsto & [\widetilde{E}^{R(\ell)\cdot b} \to \widetilde{E}^{I(\ell)\cdot b}] \end{array}$$

(for $b \in B(\ell)_p^*$). Let δ_ℓ be the inverse map.

Finally, we choose for each $\sigma \in \mathcal{R}$ a finite idele $\widehat{\lambda}_\sigma \in \widehat{K}^*$ such that

$$\left[K[\infty]/K, \widehat{\lambda}_\sigma\right] = \sigma \in \mathrm{Gal}(K[\infty]/K).$$

3.3 Computation of $\mathrm{red}_\ell(\sigma \cdot H(a))$

We first compute the (ℓ,σ)-component of RED ($\ell \in S$, $\sigma \in \mathcal{R}$), and drop the fixed ℓ from all the above notations: $R = R(\ell)$, $B = B(\ell)$, $\theta = \theta_\ell$ and so on.

3.3.1 Step 1

Pick $a \in \mathcal{L}'$ and start with

$$H(a) = \big[h_a : E/X_a \to E/X_a \oplus C\big] \in X_0(N)\big(K\big[\mathrm{lcm}(c(a), c'(a))\big]\big).$$

Let $d = \mathrm{lcm}(c(a), c'(a), c(e))$ and $Q = O_d \cdot \hat{\lambda}_\sigma \subset K$. Then Q is a proper O_d-ideal and $\sigma\mid_{K[d]} = \left(\frac{K[d]/K}{Q}\right) \in \mathrm{Gal}(K[d]/K)$, hence by proposition 1.3:

$$\sigma \cdot H(a) = \left[h_a^Q : (E/X_a)^Q \to (E/X_a \oplus C)^Q\right] \in X_0(N)\big(K[d]\big),$$

where we use the action of $O_d \subset O_{c(a)}, O_{c'(a)}$ on the elliptic curves to define their transforms. Reducing at v_ℓ we find

$$\begin{array}{rcl} \mathrm{red}_\ell\big(\sigma \cdot H(a)\big) & = & \left[\Big((E/X_a)^Q\Big)^\sim \to \Big((E/X_a \oplus C)^Q\Big)^\sim\right] \\ & = & \left[((E/X_a)^\sim)^Q \to ((E/X_a \oplus C)^\sim)^Q\right]. \end{array}$$

Let $J_a = \{x \in R \mid x \cdot (X_a)^\sim = 0\}$ and $I_a = \{x \in R \mid x \cdot (X_a \oplus C)^\sim = 0\}$. Thus $J_e = R$ and $I_e = I$. According to the lemmas 2.2 and 2.3, $I_a \subset_{N,N} J_a$, $[R : J_a] = [I : I_a] = d(a)^2$ and there exists a commutative diagram

$$\begin{array}{ccc} \widetilde{E}^{J_a} & \xrightarrow{\sim} & (E/X_a)^\sim \\ \downarrow & & \downarrow \\ \widetilde{E}^{I_a} & \xrightarrow{\sim} & (E/X_a \oplus C)^\sim . \end{array}$$

By *transport de structure*, our point can thus be written:

$$\mathrm{red}_\ell\big(\sigma\cdot H(a)\big)=\left[\left(\widetilde{E}^{J_a}\right)^Q\to\left(\widetilde{E}^{I_a}\right)^Q\right]\in X_0^{\mathrm{ss}}(N)\big(k(\ell)\big).$$

However, we have to know how O_d acts on $\widetilde{E}^{J_a}$ and $\widetilde{E}^{I_a}$. Unwinding the definitions, we find that for any $k(\ell)$-scheme T, in the formula

$$\left(\widetilde{E}^{J_a}\right)^Q(T)=\mathrm{Hom}_{O_d}\left(Q,\mathrm{Hom}_R\left(J_a,\widetilde{E}(T)\right)\right),$$

$x\in O_d$ acts on $\mathrm{Hom}_R\left(J_a,\widetilde{E}(T)\right)$ by right multiplication by $i(x)$ on J_a (and $i(O_d)\subset O_r(J_a)$): this follows from the fact that the isogenies that we are reducing are K-linear. Since Q is O_d-projective, we obtain:

$$\begin{aligned}\left(\widetilde{E}^{J_a}\right)^Q(T)&=\mathrm{Hom}_R\left(J_a\otimes_{i(O_d)}i(Q),\widetilde{E}(T)\right)\\&=\mathrm{Hom}_R\left(J_ai(Q),\widetilde{E}(T)\right)\\&=\widetilde{E}^{J_ai(Q)}(T).\end{aligned}$$

But $J_ai(Q)=J_ai(O_d\widehat{\lambda}_\sigma)=J_a\cdot i(\widehat{\lambda}_\sigma)$, so that

$$\mathrm{red}_\ell\big(\sigma\cdot H(a)\big)=\left[\widetilde{E}^{J_a\cdot i(\widehat{\lambda}_\sigma)}\to\widetilde{E}^{I_a\cdot i(\widehat{\lambda}_\sigma)}\right]\in X_0^{\mathrm{ss}}(N)\big(k(\ell)\big).$$

where we now use the action of R on $\widetilde{E}$ to construct the indicated isogeny.

3.3.2 Step 2

Assume from now on that a belongs to $\mathcal{L}_p$, let $d(a)=p^n$ and define $x_a\in B_p^*$ by $\theta(x_a)=\tau_a^{-1}$. Then, viewing x_a as an element of $\widehat{B}^*$ we have:

Lemma 3.3 *$J_a=R\cdot x_a$ and $I_a=I\cdot x_a$.*

Proof: Both sides of the first equality do not differ from R outside p, so we just need to check that they are also equal at p. Reducing the commutative diagram

$$\begin{array}{ccc}T_p(a)/T_p(E)&\xrightarrow{\sim}&X_a\\ \cap&&\cap\\ V_p(E)/T_p(E)&\xrightarrow{\sim}&E(\overline{F})_{p-\mathrm{tors}}\end{array}$$

we find that

$$\begin{aligned}(J_a)_p&=\left\{x\in B_p\mid x\cdot\big(T_p(a)\big)^\sim\subset T_p(\widetilde{E})\right\}\\&=\left\{x\in B_p\mid \widetilde{\xi}\big(x\cdot\big(T_p(a)\big)^\sim\big)\subset\widetilde{\xi}\big(T_p(\widetilde{E})\big)\right\}\\&=\left\{x\in B_p\mid\theta(x)\cdot\tau_a\cdot\mathbb{Z}_p^2\subset\mathbb{Z}_p^2\right\}\\&=\left\{x\in B_p\mid\theta(x)\in M_2(\mathbb{Z}_p)\tau_a^{-1}\right\}\end{aligned}$$

since $\widetilde{\xi}\,((T_p(a))^{\sim}) = \tau_a \cdot \mathbb{Z}_p^2$ and $\widetilde{\xi}\,(x \cdot t) = \theta(x) \cdot \widetilde{\xi}\,(t)$ for $x \in B_p$ and $t \in V_p(\widetilde{E})$. But $M_2(\mathbb{Z}_p) = \theta(R_p)$, so that $(J_a)_p = R_p x_a$ as was to be shown.

The second equality may be proven similarly, and follows anyway from the first one since p is prime to N. $\square$

Our point thus becomes:

$$\mathrm{red}_\ell\big(\sigma \cdot H(a)\big) = \Big[\widetilde{E}^{R\cdot\left(x_a i(\widehat{\lambda}_\sigma)\right)} \to \widetilde{E}^{I\cdot\left(x_a i(\widehat{\lambda}_\sigma)\right)}\Big] \in X_0^{\mathrm{ss}}(N)\big(k(\ell)\big).$$

3.3.3 Step 3

The strong approximation theorem (section 2.3) implies that there exists an element $b \in B^*$ such that for all prime $q \neq p$:

$$\Big(\Big(I \cdot i(\widehat{\lambda}_\sigma) \subset_{N,N} R \cdot i(\widehat{\lambda}_\sigma)\Big) \times b\Big)_q = \big(I \subset_{N,N} R\big)_q.$$

Since $x_a \in B_p^*$, we then also have:

$$\Big(\Big(I \cdot \big(x_a i(\widehat{\lambda}_\sigma)\big) \subset_{N,N} R \cdot \big(x_a i(\widehat{\lambda}_\sigma)\big)\Big) \times b\Big)_q = \big(I \subset_{N,N} R\big)_q.$$

The inclusion $\Big(I \cdot \big(x_a i(\widehat{\lambda}_\sigma)\big) \subset R \cdot \big(x_a i(\widehat{\lambda}_\sigma)\big)\Big) \times b$ can therefore be computed using *only the p-component* of $\big(x_a i(\widehat{\lambda}_\sigma)\big) \times b$, and our point thus becomes:

$$\mathrm{red}_\ell\big(\sigma \cdot H(a)\big) = \Big[\widetilde{E}^{R\cdot\left(x_a i(\widehat{\lambda}_{\sigma,p})b\right)} \to \widetilde{E}^{I\cdot\left(x_a i(\widehat{\lambda}_{\sigma,p})b\right)}\Big] \in X_0^{\mathrm{ss}}(N)\big(k(\ell)\big),$$

where we now consider b *as an element of* $B_p^* \subset \widehat{B}^*$. In other words:

$$\delta_\ell\Big(\mathrm{red}_\ell\big(\sigma \cdot H(a)\big)\Big) = \Big[\tau_a^{-1}\theta\big(i(\widehat{\lambda}_{\sigma,p})b\big)\Big] \in \mathcal{T}_p/\theta(\Gamma).$$

3.4 Enters topology

We have just proven that $\forall(\ell,\sigma) \in S \times \mathcal{R}$, there exists $b_{\ell,\sigma} \in B(\ell)^*$ such that:

$$\forall a \in \mathcal{L}_p : \quad \delta_\ell\Big(\mathrm{red}_\ell\big(\sigma \cdot H(a)\big)\Big) = \Big[\tau_a^{-1}\theta_\ell\big(i_\ell(\widehat{\lambda}_{\sigma,p})b_{\ell,\sigma}\big)\Big] \in \mathcal{T}_p/\theta_\ell\big(\Gamma(\ell)\big).$$

Multiplication on the right by $z_{\ell,\sigma} = \theta_\ell\big(i_\ell(\widehat{\lambda}_{\sigma,p})b_{\ell,\sigma}\big)^{-1} \in GL_2(\mathbb{Q}_p)$ yields a bijection $\mathcal{T}_p/\theta_\ell\big(\Gamma(\ell)\big) \xrightarrow{\sim} \mathcal{T}_p/\Gamma_{\ell,\sigma}$, where $\Gamma_{\ell,\sigma} = z_{\ell,\sigma}^{-1}\theta_\ell\big(\Gamma(\ell)\big)z_{\ell,\sigma}$. Composing it with δ_ℓ, we obtain a bijection:

$$\delta_{\ell,\sigma} : X_0^{\mathrm{ss}}(N)\big(k(\ell)\big) \xrightarrow{\sim} \mathcal{T}_p/\Gamma_{\ell,\sigma},$$

and $\delta_{\ell,\sigma}\Big(\mathrm{red}_\ell\big(\sigma \cdot H(a)\big)\Big) = [\tau_a^{-1}]$ is the class of $\phi_1(a) \in \mathcal{T}_p$.

We have thus constructed a *commutative diagram*:

$$\begin{array}{rccc} \mathrm{RED}: & \mathcal{L}_p & \to & \prod_{\ell \in S}\Big(X_0^{\mathrm{ss}}(N)\big(k(\ell)\big)\Big)^{\mathcal{R}} \\ & \phi_1 \downarrow \simeq & & \simeq \downarrow \phi_2 \\ \mathrm{DIAG}: & \mathcal{T}_p & \to & \prod_{\ell \in S, \sigma \in \mathcal{R}} \mathcal{T}_p/\Gamma_{\ell,\sigma} \end{array}$$

where DIAG is the "diagonal map" and $\phi_2 = (\delta_{\ell,\sigma})_{\ell\in S,\sigma\in\mathcal{R}}$. Theorem 3.1 is therefore equivalent to the surjectivity of:

$$\begin{array}{ccc} PGL_2(\mathbb{Q}_p) & \to & \prod_{\ell,\sigma} PGL_2(\mathbb{Z}_p) \setminus PGL_2(\mathbb{Q}_p)/\Gamma_{\ell,\sigma} \\ v & \mapsto & ([v],\cdots,[v]) \end{array}$$

In fact, we can work with $PSL_2(\mathbb{Q}_p)$ instead of $PGL_2(\mathbb{Q}_p)$. Indeed:

Proposition 3.4 *$PSL_2(\mathbb{Q}_p) \hookrightarrow PGL_2(\mathbb{Q}_p)$ induces a bijection:*

$$PSL_2(\mathbb{Z}_p) \setminus PSL_2(\mathbb{Q}_p)/\Gamma^1_{\ell,\sigma} \xrightarrow{\sim} PGL_2(\mathbb{Z}_p) \setminus PGL_2(\mathbb{Q}_p)/\Gamma_{\ell,\sigma},$$

where $\Gamma^1_{\ell,\sigma}$ is the intersection in $PGL_2(\mathbb{Q}_p)$ of $PSL_2(\mathbb{Q}_p)$ with the image of $\Gamma_{\ell,\sigma} \subset GL_2(\mathbb{Q}_p)$.

This is a straightforward corollary of the following:

Lemma 3.5 *$\pm p^{\mathbb{Z}} \subset \Gamma_{\ell,\sigma}$ and $\det(\Gamma_{\ell,\sigma}) = p^{\mathbb{Z}}$ for all $\ell \in S$, $\sigma \in \mathcal{R}$.*

Proof: Since $\Gamma_{\ell,\sigma} = z^{-1}_{\ell,\sigma}\theta_\ell\big(\Gamma(\ell)\big)z_{\ell,\sigma}$, we must show that $\pm p^{\mathbb{Z}} \subset \Gamma(\ell)$ and that the reduced norm of $\Gamma(\ell)$ equals $p^{\mathbb{Z}}$. Since $\Gamma(\ell) = R'(\ell)[1/p]^*$, the first statement is obvious, and the second follows from [21, p. 90]. $\square$

So let $G = PSL_2(\mathbb{Q}_p)$, $U = PSL_2(\mathbb{Z}_p)$), call $\Delta : G \to G^{S\times\mathcal{R}}$ the diagonal and put $\Gamma^1 = \prod_{\ell,\sigma}\Gamma^1_{\ell,\sigma} \subset G^{S\times\mathcal{R}}$. The $\Gamma^1_{\ell,\sigma}$'s are discrete and cocompact subgroups of G [21, p. 104], and U is an open compact subgroup. Theorem 3.1 is then equivalent to the statement that the "diagonal" map

$$G \to U^{S\times\mathcal{R}} \setminus G^{S\times\mathcal{R}}/\Gamma^1$$

is surjective. Since $U^{S\times\mathcal{R}}$ is an open subgroup of $G^{S\times\mathcal{R}}$, this follows from:

Proposition 3.6 *$\Delta(G)\Gamma^1$ is dense in $G^{S\times\mathcal{R}}$.*

We prove this proposition in the next three paragraphs, essentially following Vatsal ([19] and [20]).

3.5 Commensurability

We say that two subgroups H_1 and H_2 of G are commensurable, and write $H_1 \sim H_2$, if $H_{12} = H_1 \cap H_2$ has finite index in H_1 and H_2. For a subgroup H of G, the commensurator of H is $\mathrm{Com}(H,G) = \{x \in G \mid x^{-1}Hx \sim H\}$. If $H_1 \sim H_2$, then $\mathrm{Com}(H_1,G) = \mathrm{Com}(H_2,G)$. Our assumption in Theorem 3.1 is precisely meant for the following:

Proposition 3.7 *If $(\ell,\sigma) \neq (\ell',\sigma') \in (S\times\mathcal{R})^2$, then $\Gamma^1_{\ell,\sigma}$ and $\Gamma^1_{\ell',\sigma'}$ are not commensurable in G.*

Proof: First recall that $\Gamma^1_{\ell,\sigma}$ is the intersection in $PGL_2(\mathbb{Q}_p)$ of $PSL_2(\mathbb{Q}_p)$ with the image of $\Gamma_{\ell,\sigma} \subset GL_2(\mathbb{Q}_p)$. For this step, we have:

Lemma 3.8 *Let Γ_1 and Γ_2 be subgroups of $GL_2(\mathbb{Q}_p)$ such that $\det(\Gamma_i) = p^{\mathbb{Z}}$ and $\pm p^{\mathbb{Z}} \subset \Gamma_i$ for $i = 1, 2$. Let Γ_i^1 be the intersection in $PGL_2(\mathbb{Q}_p)$ of $PSL_2(\mathbb{Q}_p)$ with the image of Γ_i, $i = 1, 2$. Then $\Gamma_1^1 \sim \Gamma_2^1 \Leftrightarrow \Gamma_1 \sim \Gamma_2$.*

By lemma 3.5, the proposition is therefore equivalent to a similar statement about the $\Gamma_{\ell,\sigma}$'s. The commensurator of $\Gamma(\ell)$ is known; we just quote the result from [21, p. 106] using our notations.

Proposition. $\mathrm{Com}\left(\Gamma(\ell), B(\ell)_p^*\right) = \mathbb{Q}_p^* B(\ell)^*$.

The commensurator of $\Gamma_{\ell,\sigma} = z_{\ell,\sigma}^{-1}\theta_\ell\big(\Gamma(\ell)\big)z_{\ell,\sigma}$ thus equals $z_{\ell,\sigma}^{-1}\theta_\ell\left(\mathbb{Q}_p^* B(\ell)^*\right) z_{\ell,\sigma}$.

First consider the case of a couple $\big((\ell,\sigma),(\ell',\sigma')\big) \in (S \times \mathcal{R})^2$ with $\ell \neq \ell'$. Then $\Gamma_{\ell,\sigma}$ and $\Gamma_{\ell',\sigma'}$ are not commensurable since they simply do not have the same commensurator:

Proposition 3.9 *Let B and B' be two* non-isomorphic *quaternion algebras splitting at p, and choose identifications of B_p and B'_p with $M_2(\mathbb{Q}_p)$. Then:*

$$\mathbb{Q}_p^* B^* \neq \mathbb{Q}_p^* B'^* \quad \text{in} \quad GL_2(\mathbb{Q}_p).$$

Proof: Suppose that $\mathbb{Q}_p^* B^* = \mathbb{Q}_p^* B'^*$, hence $B \subset \mathbb{Q}_p B'$. For $b \in B$, write $b = \lambda b'$ with $\lambda \in \mathbb{Q}_p$ and $b' \in B'$, so that $\mathrm{tr}(b) = \lambda \mathrm{tr}(b')$. If $\mathrm{tr}(b) \neq 0$, then $\mathrm{tr}(b') \neq 0$ hence $\lambda = \mathrm{tr}(b)/\mathrm{tr}(b') \in \mathbb{Q}$, so that $b \in B'$. If $\mathrm{tr}(b) = 0$, then $\mathrm{tr}(b-1) \neq 0$, hence $b - 1 \in B'$ and $b \in B'$. Thus $B \subset B'$; by symmetry $B = B'$, a contradiction. □

Consider then the case $\ell = \ell'$, and suppose that $\Gamma_{\ell,\sigma} \sim \Gamma_{\ell,\sigma'}$, i.e. that

$$z_{\ell,\sigma} z_{\ell,\sigma'}^{-1} \in \mathrm{Com}\Big(\theta_\ell\big(\Gamma(\ell)\big), GL_2(\mathbb{Q}_p)\Big) = \mathbb{Q}_p^* \theta_\ell\big(B(\ell)^*\big).$$

Since $z_{\ell,\sigma} = \theta_\ell\big(i_\ell(\widehat{\lambda}_{\sigma,p}) b_{\ell,\sigma}\big)^{-1}$ with $b_{\ell,\sigma} \in B(\ell)^*$, it follows that

$$i_\ell\big(\widehat{\lambda}_{\sigma,p}^{-1}\widehat{\lambda}_{\sigma',p}\big) \in \mathbb{Q}_p^* B(\ell)^* \subset B(\ell)_p^*.$$

Write $i_\ell\big(\widehat{\lambda}_{\sigma,p}^{-1}\widehat{\lambda}_{\sigma',p}\big) = xy$, with $x \in \mathbb{Q}_p^*$ and $y \in B(\ell)^*$. Then y commutes with $i_\ell(K)$, a maximal commutative subring of $B(\ell)$, hence y belongs to $i_\ell(K)$ and

$$\widehat{\lambda}_{\sigma,p}^{-1}\widehat{\lambda}_{\sigma',p} \in \mathbb{Q}_p^* K^* \subset K_p^*.$$

Since $\left[K[\infty]/K, \mathbb{Q}_p^* K^*\right] = 1$, it follows that $\sigma^{-1}\sigma' \in \left[K[\infty]/K, \widehat{K}^{(p)*}\right]$, so that $\sigma = \sigma'$ in view of our assumption in theorem 3.1. □

3.6 A lemma on simple non-commutative groups

Fix a group G, a finite set S, and put $G^S = \prod_{s \in S} G$. For $s \in S$, let $p_s : G^S \to G$ be the projection, and for $S' \subset S$, identify $G^{S'}$ to the corresponding subgroup of G^S: $G^{S'} = \left\{x \in G^S \mid \forall s \in S \setminus S',\ p_s(x) = 1\right\}$. Denote $\Delta^{S'} : G \to G^{S'} \subset G^S$ the diagonal of $G^{S'}$.

We say that a subgroup H of G^S is *a product of diagonals* if there exist a finite set I and *disjoint* subsets $(S_i)_{i\in I}$ of S such that

$$H = \prod_{i\in I} \Delta^{S_i}(G) \subset G^S.$$

These subgroups are normalized by $\Delta^S(G)$. Conversely, we have the following result (a mild generalization of [20, Lemma 5.10]):

Proposition 3.10 *If G is a* simple non-commutative group*, then any subgroup H of G^S which is normalized by $\Delta^S(G)$ is a product of diagonals.*

Proof: 1) We use induction on $n = \#S$. The starting case $n = 1$ is trivial since G is simple. We may thus assume that $n > 1$, and that the result is true for any set S' of order $n' < n$. If $S' \subsetneq S$, $\Delta^S(G)$ normalizes H and $G^{S'}$, hence also $H^{S'} = H \cap G^{S'}$. Then $\Delta^{S'}(G)$ also normalizes $H^{S'}$, which is therefore a product of diagonals in $G^{S'}$ (and in G^S), by induction. Note also that $\forall s \in S$, $p_s(H^{S'})$ being normalized by $p_s\big(\Delta^S(G)\big) = G$, is either $\{1\}$ or G since G is simple.

Pick $s_0 \in S$ and put $S_0 = S \setminus \{s_0\}$, so that H^{S_0} is a product of diagonals. If $p_{s_0}(H) = \{1\}$, then $H = H^{S_0}$ and we are done. So we can assume that $p_{s_0}(H) = G$ and pick a *minimal* subset S_1 of S such that $p_{s_0}(H^{S_1}) = G$. Then $s_0 \in S_1$ and for any $s \in S_1$, $p_{s_0}(H^{S_1\setminus\{s\}}) = 1$.

2) If $S_1 \neq S$, then H^{S_1} is a product of diagonals; the definition of S_1 then implies: $H^{S_1} = \Delta^{S_1}(G)$. Suppose that S_1 intersects the support S_2 of a diagonal $\Delta^{S_2}(G) \subset H^{S_0}$, and put $S_3 = (S_1 \cup S_2) \setminus (S_1 \cap S_2)$. Since $S_1 \cap S_2 \neq \emptyset$, $S_3 \subsetneq S$ and H^{S_3} is a product of diagonals. If $g \neq 1 \in G$, then $z = \Delta^{S_2}(g)\Delta^{S_1}(g^{-1})$ is a nontrivial element of H^{S_3}, so that H^{S_3} contains a nontrivial diagonal $\Delta^{S_4}(G)$. Since $H^{S_1} = \Delta^{S_1}(G)$ and $H^{S_2} = \Delta^{S_2}(G)$, S_4 intersects *both* S_1 and S_2. If $s_1 \in S_1 \cap S_4$ and $s_2 \in S_2 \cap S_4$, then any element in H^{S_3} has the *same* component at s_1 and s_2. In particular, $p_{s_1}(z) = g^{-1} = p_{s_2}(z) = g$, hence $g^2 = 1$ for all $g \in G$. This forces G to be commutative, a contradiction. Thus S_1 does not intersect the support of the diagonals of H^{S_0}; it follows easily that H is indeed a product of diagonals, namely those of H^{S_0}, and $\Delta^{S_1}(G)$.

3) If now $S_1 = S$, $p_{s_0}(H^{S\setminus\{s\}}) = 1$ for all $s \in S$, whereas $p_{s_0}(H) = G$. In particular, $p_s(H) = G$ for all $s \in S$, since otherwise $H = H^{S\setminus\{s\}}$, a contradiction. Moreover, $H^{S_0} = 1$: if H^{S_0} contains a nontrivial diagonal $\Delta^{S_2}(G)$, pick $s \in S_2$, and also $x \in H$ such that $p_{s_0}(x) \neq 1$; then $z = x\Delta^{S_2}\big(p_s(x)^{-1}\big)$ belongs to $H^{S\setminus\{s\}}$ and $p_{s_0}(z) = p_{s_0}(x) \neq 1$, a contradiction. It follows that $p_{s_0} : H \to G$ is a bijection. Let $q : G \to H$ be the inverse map, and put $\theta_s = p_s \circ q$ for $s \in S$, so that θ_s is a surjective homomorphism, and θ_{s_0} is the identity.

For all $x, y \in G$, $\Delta^S(y)^{-1}q(x)\Delta^S(y)$ belongs to H, hence equals $q(z)$ for some $z \in G$. Looking first at the s_0-component, we find that $z = y^{-1}xy$; looking then at the s-component, we find $\theta_s(y^{-1}xy) = y^{-1}\theta_s(x)y$. Since also $\theta_s(y^{-1}xy) = \theta_s(y)^{-1}\theta_s(x)\theta_s(y)$, we obtain: $\theta_s(y)y^{-1}\theta_s(x) = \theta_s(x)\theta_s(y)y^{-1}$, so that $\theta_s(y)y^{-1} \in G$ commutes with all elements of $\theta_s(G) = G$. Since G is simple and non-commutative, $\theta_s(y) = y$, hence $q(y) = \Delta^S(y)$ and $H = q(G) = \Delta^S(G)$ is the full diagonal in G^S. $\square$

Remark: This property characterizes the simple non-commutative groups.

3.7 An application of Ratner's theorem

Proposition 3.11 [20, Lemma 5.10] *Let* $G = PSL_2(\mathbb{Q}_p)$ *and* $X \neq \emptyset$ *be a finite set. Let* $(\Gamma_x)_{x\in X}$ *be a collection of mutually* non-commensurable *discrete and cocompact subgroups of* G*, and put* $\Gamma = \prod_{x\in X}\Gamma_x \subset G^X$*. Then* $\Delta\Gamma$ *is dense in* G^X*, where* Δ *is the diagonal of* G^X*.*

Proof: We use induction on $n = \#X$. If $n = 1$, there is nothing to prove since $\Delta = G$ already. So let us assume that $n > 1$.

By Ratner's Theorem on the closure of unipotent orbits in p-adic Lie groups [14, Theo. 2], there exists a *closed subgroup* $H \subset G^X$ *containing* Δ, such that $\overline{\Delta\Gamma} = H\Gamma$. Since G is simple and non-commutative, and Δ normalizes H, Proposition 3.10 says: H is a product of diagonals. Since $\Delta \subset H$, this means that there exists a *partition* $(X_i)_{i\in I}$ of X such that, in the notations of 3.10, $H = \prod_{i\in I}\Delta^{X_i}(G)$.

Suppose that $\#I = 1$, so that $H = \Delta$ and $\Delta\Gamma$ is already closed in G^X, hence a Baire space since G^X is locally compact. Now Γ is discrete in G^X (and therefore countable), so that Δ is open in $\Delta\Gamma$ and the natural continuous map

$$G/\bigcap_{x\in X}\Gamma_x \to \Delta/\Delta\cap\Gamma \to \Delta\Gamma/\Gamma$$

is a homeomorphism. It follows that $G/\bigcap_{x\in X}\Gamma_x$ is compact since Γ is cocompact in G^X. But then for any $x_0 \in X$, $\Gamma_{x_0}/\bigcap_{x\in X}\Gamma_x$ should be both discrete and compact, hence finite: this contradicts our non-commensurability assumption, since $n > 1$.

Therefore $\#I \neq 1$ and for all $i \in I$, $\#X_i < n$. According to the induction hypothesis, $\Delta^{X_i}(G)\Gamma^{X_i}$ is dense in the closed subgroup G^{X_i} of G^X, so that $G^{X_i} \subset \overline{\Delta\Gamma}$, hence $G^X = \overline{\Delta\Gamma}$. □

In view of Proposition 3.7, this proves Proposition 3.6 and therefore also Theorem 3.1.

4 Mazur's Conjecture

Let $\mathbb{A}_{/\mathbb{Q}}$ be a nonzero *modular* abelian variety, i.e., such that there exists a surjective $\mathbb{Q}$-morphism $\alpha : J_0(N) \to \mathbb{A}$. Define $\pi : X_0(N) \to \mathbb{A}$ to be the composite of α with the usual embedding $X_0(N) \to J_0(N)$ that sends ∞ to 0.

We assume that the *Heegner Hypothesis* holds for N and K (see the introduction), and choose an ideal $\mathcal{N}$ of O_K such that $O_K/\mathcal{N} \simeq \mathbb{Z}/N\mathbb{Z}$. Let furthermore $E_{/\Omega}$ be an elliptic curve with complex multiplication by O_K, and consider the family of *Heegner* points associated to E and $C = E[\mathcal{N}]$ (see section 1):

$$H : a \in \mathcal{L}' \longmapsto H(a) = \left[E/X_a \to E/X_a \oplus C\right] \in X_0(N)(K[\infty]).$$

Let $p \nmid N$ be a prime number and put $G_0 = \mathrm{Gal}(K[p^\infty]/K)_{\mathrm{tors}}$, so that $G_0 = \mathrm{Gal}(K[p^\infty]/H_\infty)$. If R is a ring and $\chi : G_0 \to R^*$ is a character, we write $e_\chi = \sum_{\sigma \in G_0} \chi^{-1}(\sigma)\sigma \in R[G_0]$ for the corresponding "idempotent".

The Heegner point x_{p^n} of the Introduction belongs to the sub-family $H(\mathcal{L}_p)$. Moreover, it is not hard to see — using for instance Proposition 1.3, that

$$H(\mathcal{L}_p) \subset \left\{ \sigma x_{p^n} \mid \sigma \in \mathrm{Gal}(K[p^\infty]/K),\, n \geq 0 \right\} \subset X_0(N)(K[p^\infty]).$$

Mazur's conjecture thus follows (with $\chi = 1$) from the stronger statement:

Theorem A. *For any character $\chi : G_0 \to \mathbb{C}^*$, the $\mathbb{C}$-vector span $\mathcal{H}_\chi$ of*

$$\left\{ e_\chi \left(\pi(H(a)) \otimes 1 \right) \mid a \in \mathcal{L}_p \right\} \subset \mathbb{A}\left(K[p^\infty]\right) \otimes \mathbb{C}$$

has infinite dimension.

We first remark that $\mathbb{A}\left(K[p^\infty]\right)_{\mathrm{tors}}$ is *finite*, since:

Lemma 4.1 *$\mathbb{A}\left(K[\infty]\right)_{\mathrm{tors}}$ is finite.*

Proof: [11] Let v be a place of $K[\infty]$ above $\ell \nmid N$ inert in K. Since $\mathbb{A}_{/\mathbb{Q}}$ has good reduction at ℓ (being a quotient of $J_0(N)_{/\mathbb{Q}}$), reduction at v yields an injective map $\mathbb{A}\left(K[\infty]\right)_{\mathrm{non}-\ell-\mathrm{tors}} \to \mathbb{A}(\mathbb{F}_{\ell^2})$. Using a second place v' above $\ell' \neq \ell$ shows that $\mathbb{A}\left(K[\infty]\right)_{\mathrm{tors}}$ is indeed finite. $\square$

Theorem A is therefore a consequence of:

Theorem B. *If q is a prime number dividing neither $\varphi(Nd_K) = \#(\mathbb{Z}/Nd_K\mathbb{Z})^*$, nor the number η of geometrically connected components of $\ker(\alpha)$, then for any character $\chi : G_0 \to \mathbb{F}_q^*$, the $\mathbb{F}_q$-vector span $\mathcal{H}_\chi$ of*

$$\left\{ e_\chi \left(\pi(H(a)) \otimes 1 \right) \mid a \in \mathcal{L}_p \right\} \subset \mathbb{A}\left(K[p^\infty]\right) \otimes \mathbb{F}_q$$

has infinite dimension.

Indeed, starting with a character $\chi : G_0 \to \mathbb{C}^*$, let O_χ be the ring of integers of $\mathbb{Q}(\chi(G_0))$. For any prime ideal Q such that $O_\chi/Q \simeq \mathbb{F}_q$, $\chi \bmod Q$ is a character of G_0 with values in $\mathbb{F}_q^*$. In view of the lemma, a simple argument shows that if $\dim_{\mathbb{C}}(\mathcal{H}_\chi)$ were finite, then $\dim_{\mathbb{F}_q}(\mathcal{H}_{\chi \bmod Q})$ would also be finite. Since there are infinitely many such Q's, theorem B implies theorem A.

In the spirit of the introduction, we prove theorem B by showing that the set $\left\{ \left(\sigma \cdot \pi(H(a)) \right)_{\sigma \in G_0} \mid a \in \mathcal{L}_p \right\}$ is just as large as it can be, in view of the restriction imposed by the known geometrical relations among the conjugates of the $H(a)$'s. More precisely, there is a subgroup G_1 of G_0 such that G_1 acts "geometrically" on the involved CM points, whereas the action of the remaining part G_0/G_1 is "chaotic".

We start with a prime number $q \nmid \varphi(Nd_K)\eta$ and a character $\chi : G_0 \to \mathbb{F}_q^*$.

4.1 The geometric part

Let

$$G_1 = \left\langle \operatorname{Frob}_Q(K[p^\infty]/K) \middle| \, Q^2 = q'O_K,\, q' \mid d_K,\, q' \neq p \right\rangle \subset G_0$$

be the group generated in $\operatorname{Gal}(K[p^\infty]/K)$ by the Frobeniuses of the ramified primes Q of K that do not divide p. Since these Frobeniuses have order 2, G_1 is indeed a subgroup of G_0, and we can choose a set $\{q_1, \dots, q_g\}$ with $p \neq q_i \mid d_K$, whose corresponding set of Galois elements $\{\operatorname{Frob}_{Q_i}(K[p^\infty]/K);\, i = 1 \dots g\}$ is an $\mathbb{F}_2$-*base* of G_1 (with $Q_i^2 = O_K q_i$). Let $M = q_1 \cdots q_g$, so that M is prime to pN (since all primes dividing N split in K), and put $\tau_d = \prod_{q_i | d} \operatorname{Frob}_{Q_i}(K[p^\infty]/K)$ for $d \mid M$, so that $G_1 = \{\tau_d;\, d \mid M\}$.

There is a ***unique*** cyclic subgroup $C_M \subset E(\mathbb{C})$ of order M which is stable by O_K, namely $C_M = E[Q_1 \cdots Q_g]$. Put $C' = C \oplus C_M$, so that $C' \subset E(\mathbb{C})$ is a cyclic subgroup of order NM. Let H' be the associated family of *Heegner* points (see section 1, especially Proposition 1.2), so that

$$\forall a \in \mathcal{L}_p : \quad H'(a) = \left[E/X_a \to E/X_a \oplus C \oplus C_M\right] \in X_0(NM)(K[p^\infty]).$$

For $d \mid M$, let $\beta_d : X_0(NM) \to X_0(N)$ be the degeneracy map induced by

$$\beta_d\left[\mathcal{E} \to \mathcal{E}/\mathcal{C}\right] = \left[\,(\mathcal{E}/\mathcal{C}[d]) \to (\mathcal{E}/\mathcal{C}[Nd])\,\right],$$

for an elliptic curve $\mathcal{E}$ with a cyclic subgroup $\mathcal{C}$ of order NM.

Lemma 4.2 *For all $a \in \mathcal{L}_p$, $\beta_d\big(H'(a)\big) = \tau_d \cdot H(a) \in X_0(N)(K[p^\infty])$.*

Proof: Let $c(a) = p^n$ and define $Q_d = \prod_{q_i | d} Q_i$ and $Q_{d,n} = Q_d \cap O_{p^n}$. Then $Q_{d,n}$ is a proper O_{p^n}-ideal and $\tau_d \,|_{K[p^n]} = \left(\frac{K[p^n]/K}{Q_{d,n}}\right)$, so that by proposition 1.3:

$$\tau_d \cdot H(a) = \left[(E/X_a)^{Q_{d,n}} \to (E/X_a \oplus C)^{Q_{d,n}}\right].$$

The inclusion $Q_{d,n} \hookrightarrow O_{p^n}$ yields a commutative diagram:

$$\begin{array}{ccccc}
\big(E/X_a\big)[Q_{d,n}] & \hookrightarrow & E/X_a & \twoheadrightarrow & \big(E/X_a\big)^{Q_{d,n}} \\
\downarrow & & \downarrow & & \downarrow \\
\big(E/X_a \oplus C\big)[Q_{d,n}] & \hookrightarrow & E/X_a \oplus C & \twoheadrightarrow & \big(E/X_a \oplus C\big)^{Q_{d,n}}
\end{array}$$

An easy computation shows that

$$\big(E/X_a\big)[Q_{d,n}] = \big(X_a \oplus E[Q_d]\big)/X_a = \big(X_a \oplus C_M[d]\big)/X_a.$$

Similarly, $\big(E/X_a \oplus C\big)[Q_{d,n}] = \big(X_a \oplus C \oplus C_M[d]\big)/\big(X_a \oplus C\big)$. It follows that

$$\tau_d \cdot H(a) = \left[E/\big(X_a \oplus C_M[d]\big) \to E/\big(X_a \oplus C \oplus C_M[d]\big)\right],$$

hence indeed $\tau_d \cdot H(a) = \beta_d\big(H'(a)\big)$. □

The restricted character $\chi : G_1 \to \{\pm 1\} \subset \mathbb{F}_q^*$ lifts to a character with values in $\{\pm 1\} \subset \mathbb{Z}$. We can then define the following $\mathbb{Q}$-morphisms:

- $u : X_0(NM) \to X_0(N)^{2^g}$, given by $u(x) = \big(\beta_d(x)\big)_{d|M}$,
- $s_\chi : \mathbb{A}^{2^g} \to \mathbb{A}$, given by $s_\chi(x_d)_{d|M} = \sum_{d|M} \chi(\tau_d)\, x_d$,
- $\pi_\chi : X_0(NM) \to \mathbb{A}$, given by $\pi_\chi = s_\chi \circ (\pi)^{2^g} \circ u$.

Pick a set of representatives $\{1\} \in \mathcal{R} \subset G_0$ of G_0/G_1. Lemma 4.2 then implies:

$$\begin{aligned} e_\chi\Big(\pi\big(H(a)\big) \otimes 1\Big) &= \sum_{\sigma\in\mathcal{R}} \chi^{-1}(\sigma)\cdot\sigma\cdot\Big(\pi_\chi\big(H'(a)\big)\otimes 1\Big) \\ &= \sum_{\sigma\in\mathcal{R}} \chi^{-1}(\sigma)\cdot\Big(\pi_\chi\big(\sigma\cdot H'(a)\big)\otimes 1\Big). \end{aligned} \tag{1}$$

Since $\beta_d : X_0(NM) \to X_0(N)$ maps the cusp $\infty \in X_0(NM)$ to the cusp $\infty \in X_0(N)$, $(\beta_d)_* : J_0(NM) \to J_0(N)$ commutes with the usual embeddings of the modular curves into their Jacobians. Let $u_* : J_0(NM) \to J_0(N)^{2^g}$ be the product of these maps, and call again $s_\chi : J_0(N)^{2^g} \to J_0(N)$ the map defined by $(x_d)_{d|M} \mapsto \sum_{d|M} \chi(\tau_d)x_d$. Put $\alpha_\chi = \alpha \circ s_\chi \circ u_* : J_0(NM) \to \mathbb{A}$, so that $\alpha_\chi(x - \infty) = \pi_\chi(x)$ for all $x \in X_0(NM)$.

Its dual morphism $\alpha_\chi^{\mathrm{dual}} : \mathbb{A}^{\mathrm{dual}} \to J_0(NM)^{\mathrm{dual}} = J_0(NM)$ decomposes in:

- $\alpha^{\mathrm{dual}} : \mathbb{A}^{\mathrm{dual}} \to J_0(N)$, whose kernel is finite and isomorphic to the $\mathbb{G}_m$-dual of the group of connected components of $\ker(\alpha)$.
- $s_\chi^{\mathrm{dual}} : J_0(N) \to J_0(N)^{2^g}$, which is the embedding $x \mapsto \big(\chi(\tau_d)x\big)_{d|M}$.
- $u^{\mathrm{dual}} : J_0(N)^{2^g} \to J_0(NM)$, given by $(x_d)_{d|M} \mapsto \sum_{d|M} \beta_d^*(x)$.

Lemma 4.3 *The kernel of u^{dual} is finite and its rank divides a power of $\varphi(NM)$.*

Proof: If $g = 0$, there is nothing to prove. If $g \geq 1$, then we can split the morphism u^{dual} into

$$\big(J_0(N)^2 \xrightarrow{v} J_0(Nq_1)\big)^{2^{g-1}} \quad\text{and}\quad J_0(Nq_1)^{2^{g-1}} \xrightarrow{w} J_0(NM),$$

where v is the sum of the two degeneracy maps $J_0(N) \to J_0(Nq_1)$, and w is the analog of u^{dual}, with (N, M) replaced by $(Nq_1, M/q_1)$. According to [15, Theorem 4.3]:

$$\ker(v) = \big\{(x, y) \in \mathrm{Sh}_N \mid x + y = 0\big\},$$

where $\mathrm{Sh}_N = \ker\big(J_0(N) \to J_1(N)\big)$ is the Shimura subgroup of $J_0(N)$. The lemma follows by induction, since the order of Sh_N divides $\varphi(N)$ [9]. $\square$

If C is the connected component of $\ker(\alpha_\chi)$ and $D = J_0(NM)/C$, we thus obtain exact sequences of proper commutative group schemes over $\mathbb{Q}$:

$$0 \to C \xrightarrow{i} J_0(NM) \xrightarrow{b} D \to 0 \quad\text{and}\quad 0 \to Y \to D \xrightarrow{a} \mathbb{A} \to 0 \tag{2}$$

such that $a \circ b = \alpha_\chi$, and Y is the Cartier dual of $\ker(\alpha_\chi^{\mathrm{dual}})$, hence finite of rank r, with r dividing a power of $\varphi(Nd_K)\eta$.

Extending $\alpha_\chi : J_0(NM) \to \mathbb{A}$ to a (surjective) morphism between the Néron models $J_0(NM)_{/\mathbb{Z}[1/NM]} = \mathrm{Pic}^0(X_0(NM)_{/\mathbb{Z}[1/NM]})$ and $\mathbb{A}_{/\mathbb{Z}[1/NM]}$, we have:

Proposition 4.4 *For any rational prime $\ell \nmid 2NM$, let $J_0^{\mathrm{ss}}(NM)(\mathbb{F}_{\ell^2})$ be the subgroup of $J_0(NM)(\mathbb{F}_{\ell^2})$ generated by $(x-y)$, for all $x, y \in X_0^{\mathrm{ss}}(NM)(\mathbb{F}_{\ell^2})$. Then*

$$(\alpha_\chi \otimes 1)\big(J_0^{\mathrm{ss}}(NM)(\mathbb{F}_{\ell^2}) \otimes \mathbb{F}_q\big) = \mathbb{A}(\mathbb{F}_{\ell^2}) \otimes \mathbb{F}_q .$$

Proof: It follows from a theorem of Ihara [7, Corollary 1, p. 169] that the index of the subgroup $J_0^{\mathrm{ss}}(NM)(\mathbb{F}_{\ell^2})$ of $J_0(NM)(\mathbb{F}_{\ell^2})$ equals the order of the Shimura subgroup Sh_{NM} [13, Proposition 3.6], so that in particular

$$J_0^{\mathrm{ss}}(NM)(\mathbb{F}_{\ell^2}) \otimes \mathbb{F}_q \quad = \quad J_0(NM)(\mathbb{F}_{\ell^2}) \otimes \mathbb{F}_q$$

since q does not divide $\varphi(NM)$.

The morphisms i, b and a of (2) extend to morphisms between the Néron models of C, $J_0(NM)$, D and $\mathbb{A}$ over $\mathbb{Z}_\ell$ (which we denote by the same letters); let $Y_{/\mathbb{Z}_\ell}$ be the kernel of the extended a. Since $\ell \nmid NM$, $J_0(NM)$, $\mathbb{A}$, C and D are abelian schemes over $\mathbb{Z}_\ell$; since moreover $\ell \neq 2$, the exact sequences of (2) yield *fppf*-exact sequences of proper commutative group schemes over $\mathbb{Z}_\ell$ [2, Chap. 7], and $Y_{/\mathbb{Z}_\ell}$ is a finite flat commutative group scheme of rank r. From these exact sequences, restricted to the special fiber, we get using Lang's theorem on the triviality of the first Galois cohomology of a connected group over a finite field:

$$J_0(NM)(\mathbb{F}_{\ell^2}) \to D(\mathbb{F}_{\ell^2}) \to 0 \quad \text{and} \quad D(\mathbb{F}_{\ell^2}) \to \mathbb{A}(\mathbb{F}_{\ell^2}) \to \mathrm{H}^1(\mathbb{F}_{\ell^2}, Y) \to 0.$$

Since q does not divide r and r kills $\mathrm{H}^1(\mathbb{F}_{\ell^2}, Y)$, we obtain

$$(\alpha_\chi \otimes 1)\big(J_0(NM)(\mathbb{F}_{\ell^2}) \otimes \mathbb{F}_q\big) \quad = \quad \mathbb{A}(\mathbb{F}_{\ell^2}) \otimes \mathbb{F}_q .$$

The proposition follows. □

4.2 The chaotic part

Lemma 4.5 [19, Prop. 3.7] $\forall (\sigma \neq \sigma') \in \mathcal{R}^2$, $\sigma^{-1}\sigma' \notin \big[K[p^\infty]/K, \widehat{K}^{(p)*}\big]$.

Proof: We must show that if $\widehat{\lambda} = (\widehat{\lambda}_q)_q \in \widehat{K}^{(p)*}$ (i.e. $\widehat{\lambda}_p = 1$), then

$$\big[K[p^\infty]/K, \widehat{\lambda}\big] = \sigma \in G_0 \Longrightarrow \sigma \in G_1 .$$

Since the kernel of $[K[\infty]/K, \star] : \widehat{K}^* \to \mathrm{Gal}(K[\infty]/K)$ contains $\widehat{\mathbb{Q}}^* K^*$, we may also assume that $\widehat{\lambda}_q \in (O_K)_q$ for all q. Then the proper O_{p^n}-ideal $I_n = O_{p^n}\widehat{\lambda}$ is integral, and its index $d = [O_{p^n} : I_n]$ is prime to p and independent of n.

Let r be the order of $\sigma \in G_0$. Since $\sigma|_{K[p^n]} = \left(\frac{K[p^n]/K}{I_n}\right)$, I_n^r is a principal O_{p^n}-ideal, say $I_n^r = O_{p^n} x_n$ with $x_n \in O_{p^n}$. Then $I_0^r = O_K I_n^r = O_K x_n$, so that $(x_n)_{n \geq 0}$ takes only a finite number of values. If $x = x_n$ for infinitely many n, then x is an element of $\bigcap_{n \geq 0} O_{p^n} = \mathbb{Z}$, and $I_n^r = O_{p^n} x$ for all $n \geq 0$ (since $O_{p^n} I_{n'} = I_n$ if $n \leq n'$).

Let d_i, d_s and d_r be the divisors of d that correspond respectively to inert, split and ramified primes. Recall that the unique factorization theorem holds in the group of proper O_{p^n}-ideals whose norm is prime to p. Since $p \nmid d$, we thus have a decomposition of I_n into a product of prime (and proper) O_{p^n}-ideals:

$$I_n = \prod_{Q|q|d} Q^{v_Q(I_n)}.$$

Since $I_n^r = O_{p^n}x$, the unique factorization theorem implies:

$$r \times v_Q(I_n) = r \times v_{\overline{Q}}(I_n) = \begin{cases} v_q(x) & \text{if } q \mid d_i d_s \\ 2 \times v_q(x) & \text{if } q \mid d_r \end{cases}$$

In particular, $v(q) = v_Q(I_n)$ does not depend on n or $Q \mid q$ and

$$I_n = \prod_{q|d_s d_i} q^{v(q)} \prod_{q|d_r} Q^{v(q)}.$$

Therefore,

$$\sigma \mid_{K[p^n]} = \prod_{q|d_r} \left(\frac{K[p^n]/K}{Q^{v(q)}} \right) = \prod_{q|d_r} \mathrm{Frob}_Q(K[p^n]/K)^{v(q)},$$

and σ belongs to G_1. $\square$

In other words, we can apply Theorem 3.1 to H' and $\mathcal{R}$. So let S be a finite set of inert primes $\ell \nmid 2NMp$, and choose for each ℓ a place v_ℓ of $K[p^\infty]$ above ℓ. With notations as in Theorem 3.1, the following map is surjective:

$$\begin{array}{rccc} \mathrm{RED}: & \mathcal{L}_p & \to & \prod_{\ell \in S} X_0^{\mathrm{ss}}(NM)\big(k(\ell)\big)^{\mathcal{R}} \\ & a & \mapsto & \Big(\mathrm{red}_\ell\big(\sigma \cdot H'(a)\big)\Big)_{\sigma \in \mathcal{R}, \ell \in S} \end{array}$$

Consider the $\mathbb{F}_q$-linear map:

$$\begin{array}{rccc} \mathrm{R}_S: & \mathbb{A}(K[p^\infty]) \otimes \mathbb{F}_q & \to & \bigoplus_{\ell \in S} \mathbb{A}(k(\ell)) \otimes \mathbb{F}_q \\ & x \otimes 1 & \mapsto & \oplus_{\ell \in S} \mathrm{red}_\ell(x) \otimes 1 \end{array}$$

For $\ell \in S$ and $x, y \in X_0^{\mathrm{ss}}(NM)(k(\ell))$, pick $a, b \in \mathcal{L}_p$ such that *all* components of $\mathrm{RED}(a)$ coincide with those of $\mathrm{RED}(b)$, *except at* $(\ell, 1) \in S \times \mathcal{R}$ where $\mathrm{red}_\ell\big(H'(a)\big) = x$ and $\mathrm{red}_\ell\big(H'(b)\big) = y$. Using equation (1), we compute:

$$\begin{aligned} &\mathrm{R}_S\Big(e_\chi\big(\pi(H(a)) \otimes 1\big)\Big) - \mathrm{R}_S\Big(e_\chi\big(\pi(H(b)) \otimes 1\big)\Big) \\ &\quad = \big(0, \cdots, 0, (\pi_\chi(x) - \pi_\chi(y)) \otimes 1, 0, \cdots, 0\big) \\ &\quad = \big(0, \cdots, 0, \alpha_\chi(x - y) \otimes 1, 0, \cdots, 0\big). \end{aligned}$$

Proposition 4.4 then implies that R_S is *surjective* on $\mathcal{H}_\chi$. In particular:

$$\dim_{\mathbb{F}_q}(\mathcal{H}_\chi) \geq \sum_{\ell \in S} \dim_{\mathbb{F}_q} \big(\mathbb{A}(k(\ell)) \otimes \mathbb{F}_q\big). \tag{3}$$

To conclude the proof of Theorem B, we must show that it is possible to choose the set S in such a way that the r.h.s of (3) is arbitrarily large.

Put $L = K(\mathbb{A}[q])$. Note that L is Galois over $\mathbb{Q}$, embed it into $\mathbb{C}$ and let $\tau \in \mathrm{Gal}(L/\mathbb{Q})$ be the complex conjugation. Consider the set S_∞ of rational primes ℓ not dividing $2NMd_K q$, and such that

$$\mathrm{Frob}_\ell(L/\mathbb{Q}) = [\tau] \in \mathrm{Gal}(L/\mathbb{Q}).$$

Then S_∞ is *infinite*. Let S be a finite subset of S_∞, and for each $\ell \in S$, pick a prime Q_ℓ of L above ℓ such that $\mathrm{Frob}_{Q_\ell}(L/\mathbb{Q}) = \tau \in \mathrm{Gal}(L/\mathbb{Q})$. Pick also a place v'_ℓ of $K[p^\infty](\mathbb{A}[q])$ above Q_ℓ, let v_ℓ be its restriction to $K[p^\infty]$ and $k(\ell)$ the residue field. Then ℓ is inert in K, and

$$\dim_{\mathbb{F}_q}\left(\mathbb{A}(k(\ell)) \otimes \mathbb{F}_q\right) = 2\dim(\mathbb{A}).$$

Hence $\dim_{\mathbb{F}_q}(\mathcal{H}_\chi) \geq \#S \times 2\dim(\mathbb{A})$ by (3). Taking S arbitrarily large, we obtain $\dim_{\mathbb{F}_q}(\mathcal{H}_\chi) \geq \infty$.

5 The case where p divides N

As before, let $\mathbb{A}_{/\mathbb{Q}}$ be a quotient of $J_0(N)$ and $\pi : X_0(N) \to \mathbb{A}$ the induced morphism. Fix a prime number p, and write $N = N_0 p^\mu$, with $(N_0, p) = 1$. We assume that the *Heegner Hypothesis* holds for N_0 and K, and choose an ideal $\mathcal{N}_0$ of O_K such that $O_K/\mathcal{N}_0 \simeq \mathbb{Z}/N_0\mathbb{Z}$. Let $E_{/\Omega}$ be an elliptic curve with complex multiplication by O_K, and put $C = E[\mathcal{N}_0]$, so that $C \approx \mathbb{Z}/N_0\mathbb{Z}$.

As in section 1, we can "push forward" C through any p^n-isogeny $E \to E'$ to obtain a $\Gamma_0(N_0)$-structure on E'. However, in order to get a point on $X_0(N)$, we need to add some $\Gamma_0(p^\mu)$-structure on E'. With $\mathcal{L}$ as in section 1, let us consider the following indexing set:

$$\mathcal{L}_p = \left\{(a_1, a_2) \in \mathcal{L}^2 \mid \exists n \text{ s.t. } X_{a_1} \approx \mathbb{Z}/p^n\mathbb{Z},\ X_{a_1} \subset X_{a_2},\ X_{a_2}/X_{a_1} \approx \mathbb{Z}/p^\mu\mathbb{Z}\right\}$$

and the associated family of CM-points:

$$a = (a_1, a_2) \in \mathcal{L}_p \longmapsto H(a) = [E/X_{a_1} \to E/X_{a_2} \oplus C] \in X_0(N).$$

Since both E/X_{a_1} and $E/X_{a_2} \oplus C$ have complex multiplication by O_{p^n} for some $n \geq 0$, Proposition 1.2 implies that $H(a) \in X_0(N)(K[p^\infty])$.

We contend that Theorems A and B generalize *mutatis-mutandis* to this setting. Since the proof is essentially the same, we will just indicate the necessary modifications, leaving the details to the reader.

First, Theorem B follows from Theorem A and Theorem A from the surjectivity statement of Theorem 3.1 in exactly the same way as before. The only changes in the proof of the latter are due to the fact that $\mathcal{L}_p$ does not have a tree structure any more. In section 3.2.3 we have to fix a *base point* $e \in \mathcal{L}_p$ (i.e., a $\Gamma_0(p^\mu)$-structure on E), and replace $GL_2(\mathbb{Z}_p)$ by the *ad-hoc* congruence subgroup in the definition of $\mathcal{T}_p$. Our description of $X_0^{\mathrm{ss}}(N)\big(k(\ell)\big)$ in section 2.3

did not assume anything on p relative to N, and the computation of $\mathrm{red}_\ell(\sigma \cdot H_a)$ in section 3.3 remains unchanged, as well as the reduction from PGL_2 to PSL_2 made in Proposition 3.4, once $U = PSL_2(\mathbb{Z}_p)$ has been replaced by a suitable congruence subgroup. Theorem 3.1 thus reduces again to the topological statement of Proposition 3.6, whose proof does not require any more changes.

References

[1] Bertolini M., *Selmer groups and Heegner points in anticyclotomic $\mathbb{Z}_p$-extensions.* Comp. Math., **99** (1995), pp. 153-182.

[2] Bosch S., Lütkebohmert W. and Raynaud M., *Néron Models*, Ergebnisse der Mathematik und ihrer Grenzgebiete, Springer-Verlag (1990).

[3] Cornut C., *Réduction de familles de points CM*, Thesis, Prépublication de l'Institut de Recherche Mathématique Avancée, Strasbourg (2000).

[4] Cox D.A., *Primes of the form $x^2 + ny^2$.* Wiley & Sons (1989).

[5] Gross B.H., *Heights and the special values of L-series, Number Theory* (H. Kisilevsky and J. Labute, eds), CMS Conference Proceedings, vol. **7**, Amer. Math. Soc. (1987), pp. 115-189.

[6] Gross B.H. and Zagier D., *Heegner points and derivatives of L-series.* Invent. Math., **84** (1986), pp. 225-320.

[7] Ihara Y., *On modular curves over finite fields.* Discrete subgroups of Lie groups and applications to moduli, Oxford University Press (1975), pp. 161-202.

[8] Kolyvagin V.A., *Euler Systems.* The Grothendieck Festschrift. Prog. in Math., Boston, Birkhauser (1990).

[9] Ling S. and Oesterlé J., *The Shimura subgroup of $J_0(N)$.* Astérisque **196-197**, Société mathématique de France (1991).

[10] Mazur B., *Modular Curves and Arithmetic.* Proceedings of the International Congress of Mathematicians, Warsaw 1983, PWN (1984), pp. 185-211.

[11] Nekovář J. and Schappacher N., *On the asymptotic behaviour of Heegner points.* Turkish J. Math., **23** (1999), pp. 549-556.

[12] Nekovář J., *On the parity of ranks of Selmer groups II.* Preprint, 2000.

[13] Prasad D., *Ribet's theorem: Shimura-Taniyama-Weil implies Fermat*, in Seminar on Fermat's Last Theorem, 1993-1994 (V.K. Murty ed.). CMS Conference Proceedings, **17**, (1995), pp. 155-177.

[14] Ratner M., *Raghunatan's conjectures for cartesian products of real and p-adic Lie groups.* Duke Math. J., **77 vol. 2** (1995), pp. 275-382.

[15] Ribet K., *Congruence Relations between Modular Forms*, Proccedings of the International Congress of Mathematicians, Warsaw 1983, PWN (1984), pp. 503-514.

[16] Serre J-P., *Complex Multiplication*, in Algebraic Number Theory (J.W.S. Cassels and A. Fröhlich, eds), Academic Press (1967), pp. 292-296.

[17] Serre J-P. and Tate J., *Good reduction of abelian varieties.* Ann. Math. **88** (1968), pp. 492-517.

[18] Silverman J. H., *The Arithmetic of Elliptic Curves*, GTM **106**, Springer-Verlag (1986).

[19] Vatsal V., *Uniform distribution of Heegner points.* Preprint, 2000.

[20] Vatsal V., *Special values of anticylotomic L-functions.* Preprint, 2000.

[21] Vignéras M-F., *Arithmétique des Algèbres de Quaternions.* LNM **800**, Springer-Verlag (1980).