A criterion for local triviality.

by FABRIZIO ANDREATTA

1 Introduction.

The goal of these brief notes is to prove Proposition 6.2 of Gross' paper. Let us fix some notation. Let E be a modular elliptic curve over $\mathbf{Q}$ of conductor N. Let

$$\varphi: X_0(N) \longrightarrow E$$

be a modular parametrization. Let K be the usual imaginary quadratic field. Using Heegner points, we have constructed certain cohomology classes $c(n)$, $d(n)$. We will give a criterion to decide whether they lie in the p-Selmer group (resp. p-Shafarevich group). The main technique is the study of the reduction of E at a place v of K. There is an elementary approach to the problem. Consider the base change E_v of E to the local field K_v. Then one can define a minimal Weierstrass equation of E_v with coefficients in the ring of integers of K_v and define the reduction of E_v at v as the curve defined by reducing this equation modulo v. This works fine if E_v has good reduction, i. e. if v does not divide the conductor N. Instead, if E_v has bad reduction at v, this approach gives some problems. The first is that it does not capture enough arithmetic information about E_v, at least not enough for Kolyvagin's work. The second problem is that we need to reduce the Jacobian $J_0(N)$ of $X_0(N)$ and the map $\varphi_*: J_0(N) \to E$ induced by φ. As already noted in [Cl] the method of the Weierstrass model does not generalize to these situations. The right approach goes via the so called *Néron models.* The plan of the notes is to deal first with the places v where E has good reduction and then to introduce the geometry necessary to deal with the places of bad reduction.

2 The main result.

So far, we have constructed for suitable integers n classes $c(n) \in H^1(K, E_p)$. For each n we get a class $d(n) \in H^1(K, E)_p$ as the image of $c(n)$ via $H^1(K, E_p) \to H^1(K, E)_p$. See [Gr, Section 4] or [Ja]. Consider now the following diagram with exact rows:

$$\begin{tikzcd}
0 \arrow[r] & \mathrm{Sel}(E/K)_p \arrow[r] \arrow[d] & H^1(K, E_p) \arrow[r] \arrow[d] & \Pi_v H^1(K_v, E)_p \arrow[d, equal] \\
0 \arrow[r] & Ш(E/K)_p \arrow[r] & H^1(K, E)_p \arrow[r] & \Pi_v H^1(K_v, E)_p .
\end{tikzcd}$$

The goal of these notes is to give criteria to decide if the classes $c(n)$ (equiv. $d(n)$) are in $\mathrm{Sel}(E/K)_p$ (resp. $(E/K)_p$). In this direction we prove:

2.1 Proposition. (1) *The class $d(n)_v$ is trivial in $H^1(K_v, E)_p$ for all the finite places v not dividing n and for the archimedean place $v = \infty$.*

(2) *If $n = l\, m$ and λ is the unique prime of K dividing l, the class $d(n)_\lambda$ is trivial in $H^1(K_\lambda, E)_p$ if and only if $P_m \in pE(K_{\lambda_m}) = pE(K_\lambda)$ for one (and hence all) places λ_m of K_m dividing λ.*

3 The proof of [Gr, Prop. 6.2 (2)].

Using class field theory, we have proven that λ splits completely in K_m. Moreover, for every prime λ_m of K_m above λ, there is a unique prime λ_n of K_n above λ_m. The prime λ_n is totally ramified of index $l+1$ over K_m. We let G_l be the Galois group of the extension K_n over K_m. It is cyclic of order $l+1$. Hence we can choose a generator σ_l. We denote by F_λ the residue field of K_λ (equivalently of K_{λ_m} or of K_{λ_n}). By construction, the localization $d(n)_\lambda$ of $d(n)$ in $H^1(K_\lambda, E)_p$ lives in $H^1\big(G_l, E(K_{\lambda_n})\big)$. By [Gr, (4.6) and following] or by [Ja, pag. 3], the class $d(n)_\lambda$ is represented by the cocycle:

$$\begin{array}{ccc} G_l & \longrightarrow & E(K_{\lambda_n}) \\ \sigma & \mapsto & -\frac{(\sigma-1)P_n}{p}. \end{array}$$

Here $-\frac{(\sigma-1)P_n}{p}$ is obtained from the *unique* point of $E(K_n)$ whose image by multiplication by p is $-(\sigma-1)P_n$. Since l does not divide N by assumption, we can use [Cl, Thm 2] to conclude that the elliptic curve E over $\mathbf{Q}$ has good reduction at l. This implies the existence of the following cartesian diagram:

$$\begin{tikzcd} \tilde{E} \arrow[r] \arrow[d] & \mathcal{E} \arrow[d] & E \times_{\mathrm{Spec}(\mathbf{Q})} \mathrm{Spec}(\mathbf{Q}_l) \arrow[l] \arrow[d] \\ \mathrm{Spec}(F_l) \arrow[r] & \mathrm{Spec}(\mathbf{Z}_l) & \mathrm{Spec}(\mathbf{Q}_l) \arrow[l] \end{tikzcd}$$

where $E \times_{\mathrm{Spec}(\mathbf{Q})} \mathrm{Spec}(\mathbf{Q}_l)$ is the curve E basechanged from $\mathbf{Q}$ to $\mathbf{Q}_l$, while $\mathcal{E}$ is the "elliptic curve" over $\mathbf{Z}_l$ defined by the minimal Weierstrass model of E at l and $\tilde{E}$ is the reduced curve modulo l. First of all we remark that, by the valuative criterion of properness, we have an isomorphism of G_l-modules

$$\mathcal{E}(O_{\lambda_n}) \xrightarrow{\sim} E(K_{\lambda_n})$$

where we define $\mathcal{E}(O_{\lambda_n}) := \mathrm{Hom}_{\mathrm{Spec}(\mathbf{Z}_l)}\big(\mathrm{Spec}(O_{\lambda_n}), \mathcal{E}\big)$. Here O_{λ_n} is the ring of integers of K_{λ_n}. We denote by $\hat{\mathcal{E}}$ the formal group of E at l. The notation suggests that it is simply the completion of $\mathcal{E}$ along the identity section $0 \in \mathcal{E}(O_{\mathbf{Z}_l})$. Then we have an exact sequence of G_l-modules

$$0 \longrightarrow \hat{\mathcal{E}}(m_{\lambda_n}) \longrightarrow \mathcal{E}(O_{\lambda_n}) \longrightarrow \mathcal{E}(F_\lambda) = \tilde{E}(F_\lambda) \longrightarrow 0$$

where m_{λ_n} is the maximal ideal of O_{λ_n}. This sequence describes the reduction of points on E modulo l. We remark that multiplication by p on $\hat{\mathcal{E}}$ is an isomorphism since p and l are coprime. This is due to the fact that multiplication by p on the tangent space of $\mathcal{E}$ at the identity section 0 is an isomorphism. In particular, we have that $H^1\big(G_l, \hat{\mathcal{E}}(m_{\lambda_n})\big)_p = 0$. Since

$$\mathcal{E}(O_{\lambda_n})^{G_l} = \mathcal{E}(\mathbf{Z}_l) \longrightarrow \tilde{E}(F_l) = \tilde{E}(F_\lambda)^{G_l}$$

is surjective, we conclude that

$$H^1(G_l, E(K_{\lambda_n})_p \hookrightarrow H^1\big(G_l, \tilde{E}(F_\lambda)\big)_p = \mathrm{Hom}_{\mathrm{gr}}\big(G_l, , \tilde{E}(F_\lambda)_p\big).$$

The hooked arrow means injection. The last equality follows since G_l acts trivially on $\tilde{E}(F_\lambda)$. To conclude the proof, it suffices to prove that the point $Q_n := \frac{(\sigma_l-1)P_n}{p}$ has trivial reduction modulo λ_n.

We recall that $P_n := \sum_{\sigma \in S} \sigma\, D_m\, D_l\, y_n$ where S is a set of coset representatives of $G_n = \mathrm{Gal}(K_n/K_1)$ in $\mathcal{G}_n = \mathrm{Gal}(K_n/K)$. By definition of D_l, we have $(\sigma_l - 1)\, D_l = l + 1 - \mathrm{Tr}_l$. For all this, see [Ja, pag. 1]. Hence we have

$$(\sigma_l - 1)P_n = \sum_S \sigma\, D_m \left((l + 1 - \mathrm{Tr}_l) y_n \right).$$

Here we have used the fact that σ_l commutes with D_m. Next we use [Gr, Prop. 3.7(1)] or equivalently [Cl, Prop. 8(1)], which state that $\mathrm{Tr}_l y_n = a_l y_m$. Hence

$$(\sigma_l - 1)P_n = \sum_S \sigma\, D_m \left((l+1) y_n - a_l y_m \right).$$

By [Gr, (3.3)] the integers $l+1$ and a_l are divisible by p, hence

$$Q_n = \sum_S \sigma\, D_m \left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right).$$

By [Gr, Prop. 3.7(2)] or equivalently [Cl, Prop. 8(2)], we know that $y_n \equiv \mathrm{Forb}(\lambda_m)(y_m)$ modulo λ_n. Hence we conclude that

$$\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \equiv \left(\frac{l+1}{p} \mathrm{Frob}(\lambda_m) - \frac{a_l}{p} \right) y_m \pmod{\lambda_n}$$

for all primes λ_n of K_n above λ. For $\sigma \in \mathrm{Gal}(K_n/K)$ we conjugate this congruence modulo $\sigma^{-1}\lambda_n$ by σ to obtain:

$$\begin{aligned} \sigma\left(\frac{l+1}{p} y_n - \frac{a_l}{p} y_m \right) &\equiv \sigma\left(\frac{l+1}{p} \mathrm{Frob}(\sigma^{-1}\lambda_m) - \frac{a_l}{p} \right) y_m \pmod{\lambda_n} \\ &\equiv \left(\frac{l+1}{p} \mathrm{Frob}(\lambda_m) - \frac{a_l}{p} \right) \sigma(y_m) \pmod{\lambda_n}. \end{aligned}$$

Hence

$$Q_n \equiv \left(\frac{l+1}{p} \mathrm{Frob}(\lambda_m) - \frac{a_l}{p} \right) P_m \pmod{\lambda_n}.$$

We remark that

$$\mathrm{Gal}(F_\lambda/F_l) = \langle 1, \tau \rangle = \langle \mathrm{Frob}(\lambda_m) \rangle = \langle \mathrm{Frob}(l) \rangle$$

where τ is complex conjugation and $\mathrm{Frob}(l) = \mathrm{Frob}(\lambda_m)$ is Frobenius at l. Due to [Gross, Prop. 5.4(1)] or equivalently [Ro, Prop. 2(a)], the reduction of P_m modulo λ_m lies in the ϵ_m eigenspace of $\tilde{E}(F_\lambda)/p\tilde{E}(F_\lambda)$ for the action of τ. Consider the eigenspaces

$$\tilde{E}(F_\lambda)^+, \tilde{E}(F_\lambda)^- \subset \tilde{E}(F_\lambda)$$

with respect to $\tau = \mathrm{Frob}(l)$. On the eigenspace $\tilde{E}(F_\lambda)^+$ the automorphism $\mathrm{Frob}(l)$ acts as the identity. Hence $(l+1)\mathrm{Frob}(\lambda_m) - a_l$ acts as multiplication by $l+1-a_l$. This integer is the order of $\tilde{E}(F_\lambda)^+$ being the degree of $\mathrm{Id} - \mathrm{Frob}(l)$. On the eigenspace $\tilde{E}(F_\lambda)^-$ the automorphism $\mathrm{Frob}(l)$ acts as minus the identity. Hence $(l+1)\mathrm{Frob}(\lambda_m) - a_l$ acts as multiplication by $-l-1-a_l$. The inverse of this integer is the order of $\tilde{E}(F_\lambda)^-$. In any case we conclude that $(l+1)\mathrm{Frob}(l) - a_l$ kills $\tilde{E}(F_\lambda)$. We have also an exact sequence

$$0 \longrightarrow \tilde{E}(F_\lambda)_p^{\epsilon_m} \longrightarrow \tilde{E}(F_\lambda)^{\epsilon_m} \xrightarrow{p} \tilde{E}(F_\lambda)^{\epsilon_m} \longrightarrow \left(\tilde{E}(F_\lambda)/p\tilde{E}(F_\lambda) \right)^{\epsilon_m} \longrightarrow 0.$$

Let α be the endomorphism $\frac{l+1}{p}\mathrm{Frob}(\lambda_m) - \frac{a_l}{p} = \frac{l+1}{p}\epsilon_m - \frac{a_l}{p}$ of $\tilde{E}(F_\lambda)^{\epsilon_m}$. We remark that $\tilde{E}(F_\lambda)^{\epsilon_m}$ is cyclic since $\tilde{E}(\mathbf{C})^{\epsilon_m}$ is. Hence α is not the zero endomorphism. By [Gross, (3.4)] we have that $\tilde{E}(F_\lambda)_p^{\epsilon_m} \cong \mathbf{Z}/p\mathbf{Z}$. In particular, α is an automorphism on $\tilde{E}(F_\lambda)_p^{\epsilon_m}$. Hence the kernel of α in $\tilde{E}(F_\lambda)$ is precisely $p\tilde{E}(F_\lambda)$. Finally, we conclude that the reduction $\tilde{Q}_n$ of Q_n is zero in $\tilde{E}(F_\lambda)_p$ if and only if the image via α of the reduction $\tilde{P}_n$ of P_n is zero in $\tilde{E}(F_\lambda)$. This is equivalent to require that $\tilde{P}_n \in p\tilde{E}(F_\lambda)$. Since multiplication by p is an isomorphism on $\hat{\mathcal{E}}(O_{\lambda_n})$, we conclude that the last condition is equivalent to require that $P_n \in pE(K_{\lambda_n})$ as claimed.

4 The proof of [Gr, Prop. 6.2 (1)] for v prime to n and N.

Let us fix a place v which is either archimedean or finite, but not dividing nN. If v is the infinite place, then $K_v = \mathbf{C}$ ant $H^1(K_v, E)_p$ is trivial. Suppose that v is finite. In this case the local class $d(n)_v \in H^1(K_v, E)_p$ is in the image of $H^1(K_v^{\mathrm{un}}, E)_p$ via the inflation map. Here K_v^{un} is the maximal unramified extension of K_v. Infact, the Heegner point P_n is defined over an extension K_n of K which is unramified at v. By assumption, the elliptic curve E has good reduction at the prime l of $\mathbf{Z}$ below v. As in the previous section we can define the Weierstrass model $\mathcal{E} \to \mathrm{Spec}(\mathbf{Z}_l)$ of $E \times_{\mathrm{Spec}(\mathbf{Q})} \mathrm{Spec}(\mathbf{Q}_l)$. As before we get an injection

$$0 \longrightarrow H^1(K_v^{\mathrm{un}}/K_v, E)_p \longrightarrow H^1(F_v^{\mathrm{sep}}/F_v, \tilde{E})_p$$

where F_v^{sep} is a separable (= algebraic) closure of the residue field F_v of K_v. We conclude the proof using the following theorem of Lang:

4.1 Theorem. *Any torsor under $\tilde{E}$ defined over F_v admits an F_v-valued point and hence it is trivial. In particular, $H^1(F_v^{\mathrm{sep}}/F_v, \tilde{E}) = 0$.*

5 Néron models.

5.1 Definition. *Let L be the fraction field of a Dedekind domain O_L. Let A be an abelian variety over L. The Néron model of A over $\mathrm{Spec}(O_L)$ is a scheme, smooth and separated over $\mathrm{Spec}(O_L)$*

$$\mathcal{A} \longrightarrow \mathrm{Spec}(O_L)$$

such that

1. *Its generic fiber is $A \to \mathrm{Spec}(L)$, i. e. we have a cartesian diagram:*

$$\begin{tikzcd} A \cong \mathcal{A} \times_{\mathrm{Spec}(O_L)} \mathrm{Spec}(L) \arrow[r] \arrow[d] & \mathcal{A} \arrow[d] \\ \mathrm{Spec}(O_L) \arrow[r] & \mathrm{Spec}(L). \end{tikzcd}$$

2. *The scheme $\mathcal{A} \to \mathrm{Spec}(O_L)$ has the following universal property. For any scheme $X \to \mathrm{Spec}(O_L)$ smooth over $\mathrm{Spec}(O_L)$ and any morphism*

$$\psi_L \colon X \underset{\mathrm{Spec}(O_L)}{\times} \mathrm{Spec}(L) \longrightarrow A$$

there is a unique morphism

$$\psi \colon X \longrightarrow \mathcal{A}$$

such that

$$\psi \underset{\mathrm{Spec}(O_L)}{\times} \mathrm{Spec}(L) = \psi_L,$$

i. e. such that the following diagram is commutative:

$$\begin{tikzcd} X \times_{\mathrm{Spec}(O_L)} \mathrm{Spec}(L) \arrow[r] \arrow[d, "\psi_L"] & X \arrow[d, "\psi"] \\ A \cong \mathcal{A} \times_{\mathrm{Spec}(O_L)} \mathrm{Spec}(L) \arrow[r] & \mathcal{A}. \end{tikzcd}$$

5.2 Theorem. *The notation is as in the definition. The Néron model of A over* $\mathrm{Spec}(O_L)$ *exists.*

Proof: This was proven by Néron. For modern proofs see [Ar] and [Ne]. The case of elliptic curves is discussed in [Sil].

5.3 Remark. The definition might seem a bit abstract. See [Sil] for a more intuitive description both of the terms used above (smooth, separated ecc.) and for the property (2). Let see it in action.

5.4 Proposition. *The notation is as in the definition. Then the Néron model*

$$\mathcal{A} \longrightarrow \mathrm{Spec}(O_L)$$

of A over $\mathrm{Spec}(O_L)$ *is unique up to unique isomorphism. Moreover, it has a unique group scheme structure over* $\mathrm{Spec}(O_L)$ *extending the group variety structure on A.*

Proof: Use the universal property.
The first example is the case of good reduction:

5.5 Proposition. *The notation is as usual. Let $\mathcal{A} \to$* $\mathrm{Spec}(O_L)$ *be an abelian scheme, i. e. a group scheme proper and smooth over* $\mathrm{Spec}(O_L)$ *(a family of abelian varieties!). Then $\mathcal{A} \to$* $\mathrm{Spec}(O_L)$ *is the Néron model of its generic fiber $A := \mathcal{A} \times_{\mathrm{Spec}(O_L)} \mathrm{Spec}(L)$.*

Proof: The proof boils down to the valuative criterion of properness. See [Ar, Prop. (1.3)].

5.6 Remark. In the case that A is an elliptic curve, L is a local field and A has good reduction, then the Weierstrass model $\mathcal{A}$ of A over $\mathrm{Spec}(O_L)$ satisfies the conditions of the proposition.

5.7 Remark. Suppose that A is an elliptic curve, L is a local field and A has bad reduction. Let F be the residue field of O_L. By the universal property of the Néron model there is always a morphism from the Weierstrass model (with the singularity removed) to the Néron model. But while the special fiber (=reduction to F) of the Weierstrass model is an irreducible cubic curve, the special fiber of the Néron model might be not connected. Hence, in general, the two concepts are quite different. For example, consider the elliptic curve over $\mathbf{Q}$ defined by the equation $y^2 = (x-p)(x+p)(x-1)$ with p a prime. This equation is also the minimal Weierstrass equation. Let us work over $\mathbf{Q}_p$. The reduction of the curve modulo p is $y^2 = x^2(x-1)$. Hence we have multiplicative reduction. The Weierstrass model with the point $(0,0)$ in char p removed is smooth and separated, but does not satisfy the universal property which characterizes the Néron model of the elliptic curve. Infact, the section $x = 0, y = p$ defines an integral point on the Weierstrass model which goes through the point $(0,0)$ in char. p. Contradicting the following proposition.

5.8 Remark. We also remark that the Néron model changes, in general, with respect to extensions of the ground field. More precisely. Let $O_L \subset O_M$ be an extension of Dedekind domains with fraction fields L and M. Let A be an abelian variety over L. Let $\mathcal{A}^L$ be the Néron model of A over $\mathrm{Spec}(O_L)$. Let $\mathcal{A}^M$ be the Néron model of $A \times_{\mathrm{Spec}(L)} \mathrm{Spec}(M)$ over $\mathrm{Spec}(O_M)$. By the universal property, we have a morphism $\mathcal{A}^L \times_{\mathrm{Spec}(O_L)} \mathrm{Spec}(O_M) \to \mathcal{A}^M$. Then it is not true, in general, that this morphism is an isomorphism. In some cases this holds. For example, in the case of good reduction, i. e. when $\mathcal{A}^L$ is an abelian scheme over $\mathrm{Spec}(O_L)$. Or, by the universal property, when $O_L \subset O_M$ is unramified. For counterexamples, remember that there are examples of elliptic curves over a local field L having bad reduction, but having good reduction over an extension M of L. In this case the Néron model of the elliptic curve over $\mathrm{Spec}(O_L)$ is not an abelian scheme, i. e. its reduction to the residue field is not an abelian variety, but the Néron model over $\mathrm{Spec}(O_M)$ is an abelian scheme!

What mainly interests us, is the following:

5.9 Proposition. *The notation is as in the definition. Let L^{un} be the maximal unramified extension of L. Let O_L^{un} be the normalization of O_L in L^{un}. Define*

$$\mathcal{A}(O_L^{\mathrm{un}}) := \mathrm{Hom}_{\mathrm{Spec}(O_L)}\big(\mathrm{Spec}(O_L^{\mathrm{un}}), \mathcal{A}\big) \qquad \text{and} \qquad A(L^{\mathrm{un}}) := \mathrm{Hom}_{\mathrm{Spec}(L)}\big(\mathrm{Spec}(L^{\mathrm{un}}), A\big).$$

Then the map

$$\mathcal{A}(O_L^{\mathrm{un}}) \longrightarrow A(L^{\mathrm{un}})$$

is a bijection.

5 First reductions in the proof of [Gr, Prop. 6.2(2)] for bad reduction.

From now on we focus on the case that L is the local field K_v where v is a finite place dividing the conductor N. We let F_v be the residue field of the ring of integers O_v of K_v. Finally, we let m_v be the maximal ideal of O_v. We let

$$A := E \underset{\mathrm{Spec}(\mathbf{Q})}{\times} \mathrm{Spec}(K_v) \qquad \text{and} \qquad \mathcal{E} := \mathcal{A} \to \mathrm{Spec}(O_v).$$

5.10 Proposition. *Let $\mathcal{E}_{F_v}$ be $\mathcal{E} \times_{\mathrm{Spec}(O_v)} \mathrm{Spec}(F_v)$, i. e. the reduction of $\mathcal{E}$ at F_v. We have natural morphisms of* $\mathrm{Gal}(K_v^{\mathrm{un}}/K_v)$*-modules:*

$$\mathcal{E}_{F_v}\big(F_v^{\mathrm{sep}}\big) \longleftarrow \mathcal{E}\big(O_v^{\mathrm{un}}\big) \xrightarrow{\sim} E\big(K_v^{\mathrm{un}}\big).$$

This means that we can reduce points of E defined over an unramified extension of K_v. What is relevant to us, is that it allows to reduce the study of Galois cohomology groups of $E(K_v^{\mathrm{un}})$ to the study of the Galois cohomology groups of the reduction $\mathcal{E}_{F_v}(F_v^{\mathrm{sep}})$. The following proposition is the first step in the proof of [Gr, Prop. 6.2 (1)] for finite places v of bad reduction.

5.11 Proposition. *The following natural morphism is injective:*

$$H^1(K_v^{\mathrm{un}}/K_v, E)_p \longrightarrow H^1(F_v^{\mathrm{sep}}/F_v, \mathcal{E}_{F_v})_p.$$

Proof: Let $\hat{\mathcal{E}}$ be the formal group associated to $\mathcal{E}$. We have an exact sequence:

$$0 \longrightarrow \hat{\mathcal{E}}(m_v^{\mathrm{un}}) \longrightarrow \mathcal{E}(O_v^{\mathrm{un}}) \longrightarrow \mathcal{E}(F_v^{\mathrm{sep}}) \longrightarrow 0$$

where m_v^{un} is the maximal ideal of O_v^{un}. Since p is chosen coprime to N, we have that multiplication by p is an isomorphism on $\hat{\mathcal{E}}(m_v^{\mathrm{un}})$. In particular, $H^1(K_v^{\mathrm{un}}/K_v, \hat{\mathcal{E}}(m_v^{\mathrm{un}}))_p = 0$. This, together with the remark that $\mathcal{E}(O_v) \longrightarrow \mathcal{E}(F_v)$ is surjective, implies the claim.

5.12 Remark. In the case of good reduction we have already seen this proof!

5.13 Definition. *We define*

$$\mathcal{E}^0_{F_v} \longrightarrow \mathrm{Spec}(F_v) \qquad \text{and} \qquad \Theta_v = \mathcal{E}_{F_v}/\mathcal{E}^0_{F_v}$$

as the connected component of $\mathcal{E}_{F_v}$ and the group of connected components respectively.

5.14 Theorem. *Any torsor under $\mathcal{E}^0_{F_v}$ defined over F_v admits an F_v-valued point. In particular, it is trivial. Hence $H^1(F_v^{\mathrm{sep}}/F_v, \mathcal{E}^0_{F_v}) = 0$.*

Proof: This is once more an application of Lang's theorem. See [Bo, Cor. 16.5(i)] for a proof.

5.15 Corollary. *We have an injection:*

$$0 \longrightarrow H^1(F_v^{\mathrm{sep}}/F_v, \mathcal{E}_{F_v})_p \longrightarrow H^1(F_v^{\mathrm{sep}}/F_v, \Theta_v)_p.$$

Hence to finish the proof of the proposition we need to check that $d(n)_v$ is trivial in the cohomoly group $H^1(F_v^{\mathrm{sep}}/F_v, \Theta_v)_p$. Let w be a place of K_n over v. We recall that $d(n)_v$ is represented by the cocycle

$$\begin{array}{ccc} \mathrm{Gal}(K_w/K_v) & \longrightarrow & E(K_w) \\ \gamma & \mapsto & -\frac{(\gamma-1)P_n}{p}. \end{array}$$

Using the definition of $P_n = \sum_S \sigma(\times_l D_l) y_n$, the equalities $\sigma_l D_l = l+1-\mathrm{Tr}_l$ and $\mathrm{Tr}_l(y_n) = a_l y_{\frac{n}{l}}$ and the fact that $a_l \equiv l+1 \equiv 0 \pmod{p}$, we conclude that $-\frac{(\gamma-1)P_n}{p}$ is a combination of the elements y_d where d ranges among the divisors of n. To prove the triviality of $d(n)_v$, which is killed by p, we claim:

5.16 Lemma. *For each divisor d of n the image in Θ_v of the reduction of y_d at v lies in a subgroup of order prime to p.*

6 Modular curves over Z.

The goal of this section is to prove the lemma. We can clearly suppose $d = n$. To prove the lemma we need some information about the specialization of y_n. Since y_n is the image of the Heegner point $x_n \in X_0(N)(K_n)$ via the modular parametrization, it is not surprising that we need to study the specialization of Heegner points and the reduction of $X_0(N)$ at the given place v of K.

6.1 *The reduction of y_n and $w_N(y_n)$.* By assumption n and N are coprime. We let l be the prime of $\mathbf{Z}$ below v. The Heegner point y_n is defined by N-isogeny

$$\beta\colon \mathbf{C}/O_n \longrightarrow \mathbf{C}/\mathcal{N}^{-1},$$

where $O_n = \mathbf{Z} + nO_K$ is the order of conductor n and $\mathcal{N}$ is an ideal of O_n of norm N. Let $\bar{\mathcal{N}}$ be the complex conjugate of $\mathcal{N}$. Then

$$\beta^\vee\colon \mathbf{C}/\mathcal{N}^{-1} \longrightarrow \mathbf{C}/\bar{\mathcal{N}}^{-1}\mathcal{N}^{-1} \cong \mathbf{C}/NO_n \cong \mathbf{C}/O_n$$

is the image $w_N(y_n)$ of y_n via the Fricke involution on $X_0(N)$. Since $\mathcal{N}\bar{\mathcal{N}} = N$ and, by assumption, l splits in K we remark that either v divides $\mathcal{N}$, but not $\bar{\mathcal{N}}$ or v divides $\bar{\mathcal{N}}$, but nor $\mathcal{N}$. We recall that the elliptic curves $\mathbf{C}/\mathcal{N}^{-1}$ and $\mathbf{C}/\bar{\mathcal{N}}^{-1}$ can be defined over K_n and have *potentially good reduction* at w. Our discussion implies that either β or β^vee is separable in char l (check it on tangent spaces).

6.2 *A moduli definition of (an open of)* $X_0(N)$. We want to study the reduction of y_n and/or $w_N(y_n)$ at the place v. We need to define a model of $X_0(N)$ over $\mathbf{Z}$. To do this, we use the moduli definition of $X_0(N)$ as in [Gh] instead of the more direct, but less workable definition using the modular polynomial as in [Cl, Section 3]. We recall that over $\mathbf{C}$ the curve $Y_0(N)$ (=$X_0(N)$ minus the cusps) was defined as the moduli space (coarsely) representing the moduli functor which associates to a scheme S over $\mathbf{C}$ isomorphism classes of triples (A, A', τ), where A and A' are elliptic curves over S and $\tau\colon A \to A'$ is a *cyclic* isogeny. The word cyclic means that the kernel of τ is, locally on S, isomorphic to $\mathbf{Z}/N\mathbf{Z}$. See [Gh, Section 4]. Let us try to extend this definition to $\mathbf{Z}$.

6.2 Definition. *We define*

$$\mathcal{F}_0^{\text{et}}(N)\colon \text{Schemes} \longrightarrow \text{Sets}$$

to be the functor which associates to a scheme S isomorphism classes of triples (A, A', τ). Here A and A' are curves over S with smooth sections 0 and $0'$. By curves we mean proper and flat morphisms with one domensional fibers. Moreover, $\tau\colon A \to A'$ is a morphism such that $\tau(0) = 0'$. We require that the following properties hold. For any point $s \in S$, let $\overline{k(s)}$ be an algebraic closure of the residue field $k(s)$ of s and let $\bar{s} = \operatorname{Spec}\bigl(\overline{k(s)}\bigr)$. For any scheme T over S, denote by $T_{\bar{s}}$ the base change of T from S to $\bar{s}$. Then:

a) *either $(A_{\bar{s}}, O_{\bar{s}})$ and $(A'_{\bar{s}}, 0'_{\bar{s}})$ are elliptic curves and the induced homomorphism of elliptic curves over $\operatorname{Spec}\bigl(\overline{k(s)}\bigr)$*

$$\tau_{\bar{s}}\colon A_{\bar{s}} \to A'_{\bar{s}}$$

is an isogeny with kernel isomorphic to $\mathbf{Z}/N\mathbf{Z}$;

b) *or $A_{\bar{s}}$ is an N-gone of $\mathbf{P}^1_{\bar{s}}$'s, i. e. the normalization of $A_{\bar{s}}$ is isomorphic to $\mathbf{P}^1_{\bar{s}} \times \mathbf{Z}/N\mathbf{Z}$ and $A_{\bar{s}}$ is obtained by glueing the infinity section of the ith copy of $\mathbf{P}^1_{\bar{s}}$ to the zero section of the $i+1$th copy of $\mathbf{P}^1_{\bar{s}}$, while $A'_{\bar{s}}$ is $\mathbf{P}^1_{\bar{s}}$ with the sections 0 and ∞ glued tranversally and τ is the natural morphism identifying $A'_{\bar{s}}$ with $A_{\bar{s}}/(\mathbf{Z}/N\mathbf{Z})$.*

The result, which we take for granted from Katz-Mazur's book, is

6.2 Theorem. *The functor $\mathcal{F}_0^{\text{et}}(N)$ is coarsely represented by a smooth and geometrically irreducible scheme $Z_0^{\text{et}}(N) \to \operatorname{Spec}(\mathbf{Z})$.*

6.4 Remark. First of all you may wonder why we added those funny curves, called generalized elliptic curves, satisfying condition b). The point is that the curve $Z_0^{\text{et}}(N)_{\mathbf{Q}}$ is the curve $Y_0(N)_{\mathbf{Q}}$ parametrizing elliptic curves plus the cusp 0. Infact such cusp extend to a section

$$0\colon \operatorname{Spec}(\mathbf{Z}) \longrightarrow Z_0^{\text{et}}(N).$$

We will not go into this. It follows from the theory of the Tate curve. See Katz-Mazur for more on this. The theory of Néron models should convince you that such objects appear as degenerations of elliptic curves with a N-isogeny.

6.5 Remark. You may wonder about the superscript et in the definition above. Consider the case $S = \mathrm{Spec}(\bar{F_l})$, where l divides N. Let A and A' be elliptic curves. Insisting that $\mathrm{Ker}(\tau) \cong \mathbf{Z}/N\mathbf{Z}$ forces the isogeny τ to be separable (=étale in this case). This excludes all inseparable isogenies. This results in a definition of a moduli space where some pieces in char l are missing. The problem is to find a good notion of cyclic isogenies in char l. This is extensively studied in Katz-Mazur via the notion of a Drienfeld basis. Don't worry. We do not need that!

6.6 Remark. The curve resulting from our definition " misses" some pieces in the characteristics dividing N and all, but one, of the cusps. Still it will suffice for our purposes!

6.7 *Some special features of char. l, with l dividing N.* Let k be the biggest integer such that l^k divides N. Let $M := N/l^k$. We remark that M is coprime to l and hence $Y_0(M)_{F_l}$ is defined without "too much trouble". We have the following diagram:

$$Z_0^{\mathrm{et}}(M)_{F_l} \longrightarrow Z_0^{\mathrm{et}}(N)_{F_l} \longrightarrow Z_0^{\mathrm{et}}(M)_{F_l},$$

where on $\bar{F_l}$-valued points the maps are defined as follows. Let $\tau\colon A \to A'$ be a point of $Z_0^{\mathrm{et}}(M)_{F_l}$, i. e. a cyclic isogeny of degree M between ordinary (generalized) elliptic curves. Then its image via the map on the left is $A^{\left(l^k\right)} \xrightarrow{V^k} A \xrightarrow{\tau} A'$ where $V^k\colon A^{\left(l^k\right)} \to A$ is the dual of the kth power of Frobenius. We recall that $A^{\left(l^k\right)}$ is $A \times_{\mathrm{Spec}(\bar{F_l})} \mathrm{Spec}(\bar{F_l})$ via the kth power of Frobenius acting on $\bar{F_l}$. Let $A \to A'$ be an $\bar{F_l}$-valued point of $Z_0^{\mathrm{et}}(N)_{F_l}$. Then, its image via the map on the right is $A/\mathrm{Ker}(V^k) \to A'$. In particular, the morphism $Z_0^{\mathrm{et}}(M)_{F_l} \to Z_0^{\mathrm{et}}(M)_{F_l}$ induced by composing the two is the identity. If you accept the existence of $Z_0^{\mathrm{et}}(M)_{F_l}$ this proves the existence of $Z_0^{\mathrm{et}}(N)_{F_p}$. This reduces the question of the smoothness of $Z_0^{\mathrm{et}}(N)_{F_l}$ over $\mathrm{Spec}(F_l)$ and its irreducibility to the smoothness of $Z_0^{\mathrm{et}}(M)_{F_l}$ over $\mathrm{Spec}(F_l)$ and its irreducibility. Since l does not divide M this is easier.

6.8 *The end of the proof.* First of all we notice that either y_n or $w_N(y_n)$ define O_w-valued points of $Z_0^{\mathrm{et}}(N)$. Here O_w is the ring of integers of K_w. To prove this we use the modular interpretation of $Z_0^{\mathrm{et}}(N)$ and 6.1. Second we remark that, by the universal property of the Néron models, there exists a map

$$Z_0^{\mathrm{et}}(N)_{O_v} \longrightarrow \mathcal{E}_v,$$

where $\mathcal{E}_v$ is the Néron model of E over O_v and its basechange to K_v is induced from the modular parametrization

$$Z_0^{\mathrm{et}}(N)_{O_v} \hookrightarrow X_0(N)_{K_v} \xrightarrow{\varphi \times K_v} E_{K_v}.$$

The modular parametriztion sends the cusp ∞ to the 0-section of E. We conclude that the images of the specialization at v of y_n (or $w_N(y_n)$) and 0 lie in the same conneced component of the special fiber $\mathcal{E}_{F_v}$ of the Néron model. Hence the specialization of x_n lie in the identity component of $\mathcal{E}_{F_v}$ *up to* translation by the specialization of $\pm\big(\varphi(0) - \varphi(\infty)\big)$. But $\varphi(0) - \varphi(\infty)$ belong to $E(\mathbf{Q})$, it is a torsion point and $E(\mathbf{Q})_p = 0$. Hence the conclusion.

References.

[Ar] M. Artin: Néron Models, in *Arithemtic Geometry*, G. Cornell, J.H. Silverman editors. Springer-Verlag, 1985.

[Bo] A. Borel: Linear Algebraic Groups. Second Enlarged Edition. Springer-Verlag, 1991.

[Ne] S. Bosch, W. Lütkebohmert, M. Raynaud: Néron Models. Ergebnisse der Mathematik und ihrer Grenzebiete, 3.Folge, Band 21, Springer-Verlag, 1990.

[Cl] P. Clark: Lectures Notes on Eichler-Shimura Theory. Notes for the seminar.

[Gh] A. Ghitza: Modular Curves and Heegner Points. Notes for the seminar.

[Gr] B. Gross: Kolyvagin's Work on Modular Elliptic curves, in *L-Lunctions and Arithmetic*, LMS Lecture Notes 153, London Mathematical Society, 1991, pp. 235-256.

[Ja] D. Jao: Kolyvagin's construction of cohomology classes. Notes for the seminar.

[Po] A.-A. Popa: Galois action on torsion points of elliptic curves. Notes for the seminar.

[Ro] N. Rogers: The Eigenspaces of Complex Conjugation. Notes for the seminar.

[Sil] J. Silverman: Advanced Topics in the Arithmetic of Elliptic curves. Springer-Verlag, 1994.