Théorie des nombres/*Number Theory*

On invisible elements of the Tate-Shafarevich group

Amod AGASHÉ

Department of Mathematics, 940 Evans Hall, University of California, Berkeley, CA 94720, U.S.A.
Email: amod@math.berkeley.edu

Abstract. Mazur [8] has introduced the concept of visible elements in the Tate-Shafarevich group of optimal modular elliptic curves. We generalized the notion to arbitrary abelian subvarieties of abelian varieties and found, based on calculations that assume the Birch-Swinnerton-Dyer conjecture, that there are elements of the Tate-Shafarevich group of certain sub-abelian varieties of $J_0(p)$ and $J_1(p)$ that are not visible.

1. Introduction and definitions

Let J be an abelian variety and A be any abelian subvariety of J, both defined over $\mathbf{Q}$. The group $H^1(\mathbf{Q}, A)$ is isomorphic to the group of principal homogeneous spaces, or torsors, of A. An A-torsor V is said to be *visible* in J if it is isomorphic over $\mathbf{Q}$ to a sub variety of J. An element of the Tate-Shafarevich of A group is said to be visible (in J) if the corresponding torsor is visible. We say that an element is *invisible* if it is not visible.

Mazur [8] introduced the concept of visible elements in the Tate-Shafarevich groups of optimal modular elliptic curves. Adam Logan, based on Cremona's tables, studied instances of non-trivial Tate-Shafarevich groups for modular elliptic curves of square-free conductor < 3000. The order of the visible elements of the Tate-Shafarevich group divides the modular degree and thus by comparing the order of the Tate-Shafarevich group (as predicted by the Birch-Swinnerton-Dyer conjecture) with the modular degrees, they tried to detect invisible elements. The only instance of an invisible element they could convincingly detect was for the level $N = 2849$, which was not visible in $J_0(N)$; but they could not test whether this element becomes visible in $J_1(N)$ or not.

Next we define the winding quotient. Let p be a prime and let $X_0(p)$ denote the usual modular curve of level p. Let $\{0, i\infty\}$ denote the projection of the geodesic path from 0 to $i\infty$ in $\mathcal{H} \cup \mathbf{P}^1(\mathbf{Q})$ to $X_0(p)(\mathbf{C})$ where $\mathcal{H}$ is the complex upper half plane. We have an isomorphism $H_1(X_0(p), \mathbf{Z}) \otimes \mathbf{R} \xrightarrow{\simeq} \mathrm{Hom}_{\mathbf{C}}(H^0(X_0(p), \Omega^1), \mathbf{C})$. Let $e \in H_1(X_0(p), \mathbf{Z}) \otimes \mathbf{R}$ correspond to the map $\omega \mapsto -\int_{\{0,i\infty\}} \omega$ under this isomorphism. It is called the *winding element*. Let $\mathbf{T}$ denote the sub-ring of endomorphisms of $J_0(p)$ generated by the Hecke-operators and the Atkin-Lehner involution. It is called the *Hecke algebra*. We have an action of $\mathbf{T}$ on $H_1(X_0(p), \mathbf{Z}) \otimes \mathbf{R}$. Let I_e be the annihilator of e with respect to this action. It is an ideal of $\mathbf{T}$. We consider the quotient abelian variety $J_e = J_0(p)/I_e J_0(p)$ over $\mathbf{Q}$. It is called the *winding quotient* of $J_0(p)$.

If B is an abelian variety, let $\hat{B}$ denote the dual of B. Using the fact that the kernel of $J_0(p) \to J_e$ is connected, one can show that the dual map $\hat{J_e} \to \hat{J_0(p)} = J_0(p)$ is an injection. Thus we can view $\hat{J_e}$ as a subvariety of $J_0(p)$ and talk about the visibility of its torsors in $J_0(p)$. We have a map $J_0(p) \xrightarrow{\pi^*} J_1(p)$ obtained via Picard functoriality from the map $\pi : X_1(p) \to X_0(p)$. It has a finite kernel. Let $\hat{J_e}'$ denote the image of $\hat{J_e}$ in $J_1(p)$ under this map.

If B is an abelian variety defined over $\mathbf{Q}$, let Ш_B denote its Tate-Shafarevich group. Based on calculations concerning the order of Ш_{J_e} as predicted by the Birch-Swinnerton-Dyer conjecture, we discovered (Thm. 1 in §3), for $p = 1091$, an element of $\text{Ш}_{\hat{J_e}}$ that is not visible in $J_0(p)$ and whose image in $\text{Ш}_{\hat{J_e}'}$ is not visible in $J_1(p)$. The existence of visible elements is closely related to congruences between modular forms of analytic rank 0 and analytic rank greater than 0.

2. A formula for $|Ш_{J_e}|$

One can easily check that $L(J_e,1) \neq 0$ and hence by work of Kolyvagin and Logachev, $J_e(\mathbf{Q})$ is finite; so the first part of the Birch-Swinnerton-Dyer conjecture is valid in this case. See [9, §1] for details. Also, by [4], the order of the Tate-Shafarevich group, $Ш_{J_e}$ is finite.

The second part of the Birch-Swinnerton-Dyer conjecture (as generalized by Tate and Gross) gives the formula (see [5, III, §5]):

$$L(J_e,1) = \frac{|Ш_{J_e}|\ c_p c_{\mathbf{R}}}{|J_e(\mathbf{Q})_{tor}||\hat{J}_e(\mathbf{Q})_{tor}|} \tag{1}$$

where c_p is the number of connected components of the special fibre of the Néron model of J_e at p and $c_{\mathbf{R}}$ is related to the real period as follows: Let W be the $\mathbf{Z}$-module of invariant differentials on the Néron model of J_e. Then $\mathrm{rank}(W) = d$ where $d = \dim(J_e)$ and $\wedge^d W$ is a free $\mathbf{Z}$-module of rank 1 contained in $H^0(J_e, \Omega^d_{J_e/\mathbf{Q}})$. Let Ω be a generator of $\wedge^d W$. Let $\{\omega_1, ..., \omega_d\}$ be any $\mathbf{Q}$-basis of $H^0(J_e, \Omega_{J_e/\mathbf{Q}})$. Then $\Omega = c \wedge_j \omega_j$ for some $c \in \mathbf{Q}$. Let $\{\gamma_1, ..., \gamma_d\}$ be a basis of $H_1(J_e, \mathbf{Z})^+$ where $+$ denotes the group of elements invariant under the action of complex conjugation. Let c_∞ be the number of connected components of $J_e(\mathbf{R})$. Then define $c_{\mathbf{R}} = c_\infty c \det(\int_{\gamma_i} \omega_j)$. It is independent of the choice of the basis $\{\omega_j\}$.

For any ring R, let $S_2(\Gamma_0(p), R)$ denote the R-module of cusp forms over $\Gamma_0(p)$ with coefficients in R. When R is flat over $\mathbf{Z}$, pulling back differentials along $X_0(p) \to J_0(p)$, one gets an isomorphism between the R-modules $H^0(J_0(p), \Omega_{J_0(p)/R})$ and $S_2(\Gamma_0(p), R)$, where if $f \in S_2(\Gamma_0(p), R)$, then the corresponding differential on $X_0(p)$ is given by $\omega_f = 2\pi i f(z) dz$. One can show that a $\mathbf{Q}$-basis for $H^0(J_e, \Omega_{J_e/\mathbf{Q}})$ is given by the differentials corresponding the set of generators of $S_e = \{f \in S_2(\Gamma_0(p), \mathbf{Z}) : I_e f = 0\}$. If we use this for the basis $\{\omega_j\}$ in the paragraph above, the constant c will be denoted c_M. It is a generalized Manin constant, in the sense that if we look at the analogous definition for elliptic quotients of $J_0(p)$ and figure out c in a similar fashion, it turns out to be precisely the Manin constant.

We next analyze the terms in formula (1) and, by cancelling the transcendental parts on each side, put it in the form given in the following proposition:

Proposition 2.1. *Assuming the Birch-Swinnerton-Dyer formula (1), we have*

$$|Ш_{J_e}|\ c_p c_M n = |J_e(\mathbf{Q})_{tor}||\hat{J}_e(\mathbf{Q})_{tor}|\left|\frac{H^+}{\hat{H_e}^+ + H_e^+}\right|\left|\frac{H_e^+}{\Im e}\right| \tag{2}$$

where $n = \mathrm{numr}((p-1)/12)$, $H = H_1(X_0(p), \mathbf{Z})$, $H_e = \{x \in H : I_e x = 0\}$, $\hat{H}_e$ *is the smallest subgroup of* H *containing* $\hat{H}_e$ *such that* $H/\hat{H}_e$ *is torsion-free,* $\Im$ *is the Eisenstein ideal of* $\mathbf{T}$ *(as in* [6]*) and the rest of the terms are as described just above.*

Proof. We have the pairing $(H^+ \otimes \mathbf{C}) \times S_2(\Gamma_0(p); \mathbf{C}) \to \mathbf{C}$ given by $(\gamma, f) \mapsto <\gamma, f> = \int_\gamma \omega_f$. In the following, at various points, we will be considering pairings between two $\mathbf{Z}$-modules; each such pairing is obtained in a natural way from this pairing.

Using the fact that $J_e = J_0(p)/I_e J_0(p)$, one can show that $H_1(J_e, \mathbf{Z}) \cong H/\hat{H}_e$. Using this and the remark about c_M made just before the statement of the proposition, we get

$$c_{\mathbf{R}} = c_\infty c_M \mathrm{disc}((H/\hat{H}_e)^+ \times S_e \to \mathbf{C})$$

where disc always denotes the discriminant of the pairing of $\mathbf{Z}$-modules.

Next, $L(J_e, 1) = \prod L(f, 1) = \prod <e, f>$, where the product (henceforth) is over all elements f belonging to the normalized eigenform basis for $\{f \in S_2(\Gamma_0(p), \mathbf{C}) : I_e f = 0\}$. Recall that $<e, f> = -\int_{\{0, i\infty\}} \omega_f$.

Putting all this in (1), we get

$$|\text{Ш}_{J_e}|\ c_p c_M c_\infty = |J_e(\mathbf{Q})_{tor}||\hat{J}_e(\mathbf{Q})_{tor}|\ \frac{\prod < e, f >}{\text{disc}((H/\hat{H}_e)^+ \times S_e \to \mathbf{C})}. \tag{3}$$

Next we perform some change of lattices:

$$\frac{\prod <e,f>}{\text{disc}((H/\hat{H}_e)^+ \times S_e \to \mathbf{C})} = \frac{\prod <e,f>}{\text{disc}(H_e^+ \times S_e \to \mathbf{C})}\ |\frac{(H/\hat{H}_e)^+}{H^+/\hat{H}_e{}^+}||\frac{H^+}{\hat{H}_e{}^+ + H_e^+}| = \frac{\prod <e,f>}{\text{disc}(\Im e \times S_e \to \mathbf{C})} c_\infty\ |\frac{H^+}{\hat{H}_e{}^+ + H_e^+}||\frac{H_e^+}{\Im e}|$$
$$= \frac{\prod <e,f>}{\text{disc}(\mathbf{T}e \times S_e \to \mathbf{C})} c_\infty\ |\frac{H^+}{\hat{H}_e{}^+ + H_e^+}||\frac{H_e^+}{\Im e}|\ /\ |\frac{\mathbf{T}e}{\Im e}|,$$

where we used the fact that $|\frac{(H/\hat{H}_e)^+}{H^+/\hat{H}_e{}^+}| = c_\infty$. Note that $|\frac{\mathbf{T}e}{\Im e}| = |\frac{\mathbf{T}}{\Im}| = n$ where the latter equality is from [6, II 9.7]. Next we claim that $\frac{\prod <e,f>}{\text{disc}(\mathbf{T}e \times S_e \to \mathbf{C})} = 1$.

Proof. There is a perfect pairing $\mathbf{T}/I_e \times S_e \to \mathbf{Z}$ which associates to (t, f) the first Fourier coefficient $a_1(tf)$ of the modular form tf. This defines $t_e \in \mathbf{T}/I_e \otimes \mathbf{C}$ characterized by $< e, f >= a_1(t_e f)$ $(f \in S_e)$. On the other hand our product taken over newforms $f \in S_e$ becomes

$$\prod < e, f >= \prod a_1(t_e f) = (\det_{S_e \otimes \mathbf{C}} t_e) \prod a_1(f) = \det_{\mathbf{T}/I_e \otimes \mathbf{C}} t_e.$$

On the other hand, the discriminant of the pairing $\mathbf{T}e \times S_e \to \mathbf{C}$ which associates to (te, f) the complex number $< te, f >$ coincides, via the identification above and the canonical isomorphism $\mathbf{T}e \cong \mathbf{T}/I_e$, with the discriminant of the pairing $\mathbf{T}/I_e \times \text{Hom}(\mathbf{T}/I_e, \mathbf{Z}) \to \mathbf{C}$ which associates to (t, ψ) the complex number $\psi(t_e t)$ (obtained by extending ψ by $\mathbf{C}$-linearity). The latter discriminant is equal to $\det_{\mathbf{T}/I_e \otimes \mathbf{C}} t_e$. □

Putting all these results in (3) finishes the proof of Proposition 2.1. □

With the idea of studying the conjectured Birch-Swinnerton-Dyer formula, we did computations (with the help of a computer) to calculate $|\frac{H^+}{\hat{H}_e{}^+ + H_e^+}|$ and $|\frac{H_e^+}{\Im e}|$ in formula (2) for various primes p. For the first, calculations were done upto $p = 397$ and for the latter, upto $p = 1447$. The computations were done using the theory of modular symbols.

3. Discovery of invisible elements

We shall use the following lemma, which is a generalization of the results that appear in [8]:

Lemma 3.1. *Let* $A = \hat{J}_e$ (or $\hat{J}_e{}'$) *and* $J = J_0(p)$ (or $J_1(p)$ respectively). *Let* V *be an* A*-torsor visible in* J*, considered as an element of* $H^1(\mathbf{Q}, A)$*. Consider the natural map* $\tilde{i} : H^1(\mathbf{Q}, A) \to H^1(\mathbf{Q}, J)$ *obtained via the embedding* i *of* A *in* J*. Then there exists an automorphism* ϕ *of* A *(defined over* $\mathbf{Q}$*) such that* $\tilde{i}(\tilde{\phi}(V))$ *is trivial, where* $\tilde{\phi}$ *is the automorphism of* $H^1(\mathbf{Q}, A)$ *induced by* ϕ*.*

Proof. We first prove that the pair $A = \hat{J}_e$ (or $\hat{J}_e{}'$) and $J = J_0(p)$ (or $J_1(p)$ respectively) satisfy
(∗) if $J \sim A \times B$ is any isogeny over $\overline{\mathbf{Q}}$, then no simple factor (over $\overline{\mathbf{Q}}$) of A is isogenous (over $\overline{\mathbf{Q}}$) to a simple factor (over $\overline{\mathbf{Q}}$) of B.

First the case of $J_0(p)$: this follows because in a decomposition of $J_0(p)$ upto isogeny, no two simple factors can be isogenous over $\mathbf{Q}$ by the multiplicity one theorem and not even over $\overline{\mathbf{Q}}$ because p is squarefree (using [10, Prop. 3.1]). Next the case of $J_1(p)$: let $J_0(p)'$ denote the image of $J_0(p)$ in $J_1(p)$. Then no simple factor of $\hat{J}_e{}'$ can be isogenous to another simple factor of $J_0(p)'$ (by the same argument above). Suppose A' is a simple factor of $\hat{J}_e{}'$ isogenous to a simple factor of $J_1(p)/J_0(p)'$.

Now $J_1(p)/J_0(p)'$ has everywhere good reduction over some extension of $\mathbf{Q}$ (this follows from [3, §5, Ex 3.7(i)]), hence so does A'. But $J_0(p)$ has purely multiplicative reduction at p by [3, §5, Th. 6.9], so it can't have a factor with good reduction even after a base extension. This proves $(*)$.

Suppose V is an A-torsor visible in J and let V' be the subvariety of $J_0(p)$ isomorphic to V over $\mathbf{Q}$ (given by the definition of visibility). Since it is an A-torsor, we have $A \cong V \cong V'$ (over $\overline{\mathbf{Q}}$). Consider the map $A \stackrel{\simeq}{\to} V' \to J/A$ defined over $\overline{\mathbf{Q}}$. Upto translation, it is a homomorphism of abelian varieties. Its image has to be a point because otherwise it would violate $(*)$. Hence the image of $V' \to J/A$ is also a point. Thus V' is a translate of A (over $\overline{\mathbf{Q}}$) and hence has an action of A by translation. As a torsor in $H^1(\mathbf{Q}, A)$ it is given by $\sigma \mapsto \sigma(Q) - Q$ for any $Q \in V'(\overline{\mathbf{Q}})$, where the subtraction is the usual subtraction in J. But this is the zero element in $H^1(\mathbf{Q}, J)$ (under $\tilde{i}$) since $Q \in V'(\overline{\mathbf{Q}}) \subseteq J(\overline{\mathbf{Q}})$. Next, let $P \in V(\overline{\mathbf{Q}})$. Then the element of $H^1(\mathbf{Q}, A)$ corresponding to V is $\sigma \mapsto \sigma(P) -_V P$ where we will be using subscripts to distinguish different actions of A. Let $\iota : V \to V'$ be the isomorphism between V and V' (over $\mathbf{Q}$). Then the element of $H^1(\mathbf{Q}, A)$ corresponding to V' is given by $\sigma \mapsto \sigma(\iota(P)) -_{V'} \iota(P)$. Consider the map $\phi : A \to A$ given by $a \mapsto \iota(P +_V a) -_{V'} \iota(P)$. It is defined over $\mathbf{Q}$ and it is a homomorphism of abelian varieties since it takes the identity element of A to itself. It takes the torsor V to V' and thus $\tilde{i}(\tilde{\phi}(V)) = \tilde{i}(V') = 0$. It is an automorphism since it has an inverse given by $a \mapsto \iota^{-1}(\iota(P) +_{V'} a) -_V P$. □

Theorem 1. *Assuming the Birch-Swinnerton-Dyer formula (1), for the prime $p = 1091$, $Ш_{\hat{J}_e}$ has an element that is not visible in $J_0(p)$ and the image of this element in $Ш_{\hat{J}_e{}'}$ is not visible in $J_1(p)$.*

Proof. For ease of notation, let J_0 denote $J_0(p)$. In what follows, $p = 1091$ unless mentioned otherwise. In this case, what happens is that $J_e = J_0^-$ where $J_0^- = J_0/(1 + W_p)J_0$ and W_p is the Atkin-Lehner involution (this was checked by a calculation and also follows from [2, §8]). By combining the exact sequence defining J_e and the dual exact sequence, we get the map $\hat{J}_e \to \hat{J}_0 \stackrel{\simeq}{\to} J_0 \to J_e$. Call the composite f. It is an isogeny; let N denote its kernel. N is the intersection of $\hat{J}_e$ and $(1 + W_p)J_0$. On the former group, W_p acts as -1 and on the latter group as $+1$. We conclude that N is killed by multiplication by 2, i.e. the order of N is a 2-power.

Now there is an isogeny $g : J_e \to \hat{J}_e$ such that $g \circ f =$ multiplication by $|N|$. So we have $\hat{J}_e \to J_0 \to J_e \stackrel{g}{\to} \hat{J}_e$ which is multiplication by $|N|$. Suppose V is a visible element of $Ш_{\hat{J}_e}$. Apply Lemma 3.1 with $A = \hat{J}_e$ and let ϕ be the automorphism of $\hat{J}_e$ as given by the lemma. Consider $\hat{J}_e \stackrel{\phi}{\to} \hat{J}_e \to J_0 \to J_e \to \hat{J}_e \stackrel{\phi^{-1}}{\to} \hat{J}_e$ which is again multiplication by $|N|$. This gives $Ш_{\hat{J}_e} \stackrel{\tilde{\phi}}{\to} Ш_{\hat{J}_e} \to Ш_{J_0} \to Ш_{J_e} \to Ш_{\hat{J}_e} \stackrel{\tilde{\phi}^{-1}}{\to} Ш_{\hat{J}_e}$, which is again multiplication by $|N|$. Consider V as an element of the first $Ш_{\hat{J}_e}$ in this sequence. Then by Lemma 3.1, its image in $Ш_{J_0}$ is trivial, hence it is killed under the composite, i.e. it is killed by multiplication by $|N|$ i.e. by a 2-power. Thus the visible elements of $Ш_{\hat{J}_e}$ have 2-power order.

In the calculations, we found that (for $p = 1091$) 7 divides the factor $|H_e^+/\Im e|$ which appears in the equation (2) given above. Thus 7 divides the right hand side of equation (2). We will check that it does not divide any factor of the left hand side other than $|Ш_{J_e}|$.

First c_p: We apply [1, Prop. 7.5.3] to the exact sequence $0 \to (1 + W_p)J_0 \to J_0 \to J_0/(1 + W_p)J_0 \to 0$ to conclude that a power of 2 kills the cokernel of the map of Néron models $\mathbf{J_0} \to \mathbf{J_e}$. Hence we have that away from 2, c_p divides the number of connected components in the special fiber at p of $\mathbf{J_0}$, which is n by [6, Thm A.1]. But in our case, $n = \text{numr}\,((1091 - 1)/12) = 545$, so 7 does not divide c_p. Next, one can use [7, Prop. 3.1] to show that c_M is a unit in $\mathbf{Z}[1/2]$, so 7 does not divide the numerator of c_M (it should be possible to show that c_M is in fact an integer). Finally 7 does not divide $n = 545$.

So looking at equation (2) (which follows from (1) by Prop. 2.1), one concludes that 7 divides $|Ш_{J_e}|$. Next, one can check using the Cassels-Tate pairing that $|Ш_{\hat{J}_e}|=|Ш_{J_e}|$. Hence 7 divides $|Ш_{\hat{J}_e}|$. Thus $Ш_{\hat{J}_e}$ has a non-trivial element of order 7. This cannot be visible because such elements are killed by a 2-power as was shown before. Thus $Ш_{\hat{J}_e}$ has an element that is not visible in $J_0(p)$.

Next we consider visibility in $J_1 = J_1(p)$. Consider the series of maps $J_0 \xrightarrow{\pi^*} J_1 \xrightarrow{\simeq} J_1 \xrightarrow{\pi_*} J_0$ where the last map is obtained from $\pi : X_1(p) \to X_0(p)$ via the Albanese functoriality. The composite is just multiplication by deg(π)= $(p-1)/2 = 545$. So the map $\hat{J}_e \to J_0 \to J_1 \to J_1 \to J_0 \to J_e$ is an isogeny of a degree such that the only primes dividing it are 2 and those diving 545 i.e. 5 and 109. Using this, one can show that the element of order 7 in $Ш_{\hat{J}_e}$ does not get killed in $Ш_{J_1}$ and hence that there is a nontrivial element of order 7 in $Ш_{\hat{J}_e{}'}$. Call it V and suppose it is visible in J_1. Then by Lemma 3.1 with $A = \hat{J}_e{}'$, there is an automorphism ϕ of $\hat{J}_e{}'$ such that V is killed under the composite $Ш_{\hat{J}'_e} \xrightarrow{\tilde{\phi}} Ш_{\hat{J}_e{}'} \to Ш_{J_1}$. In the isogeny $\hat{J}_e \to \hat{J}_e{}' \to J_1 \to J_0 \to J_e$, the first map $\hat{J}_e \to \hat{J}_e{}'$ is also an isogeny, and its degree divides the order of the kernel of π^*, which is $n = 545$ by [6, II.11.6, II.11.7]. So the map $\hat{J}_e{}' \to J_1 \to J_0 \to J_e$ is also an isogeny. Hence so is the map $\hat{J}_e{}' \xrightarrow{\phi} \hat{J}_e{}' \to J_1 \to J_0 \to J_e$ and the only primes dividing its degree are 2, 5 and 109. So by the familiar argument, the element V of order 7 is not killed under $Ш_{\hat{J}'_e} \xrightarrow{\tilde{\phi}} Ш_{\hat{J}_e{}'} \to Ш_{J_1}$, a contradiction. Hence V is an element of $Ш_{\hat{J}'_e}$ not visible in J_1. □

A similar result of the existence of an invisible element was found for $p = 1429$ where 5 divides $|H_e^+/\Im e|$. Note that as a byproduct, we have that the Tate-Shafarevich groups of $J_0(1091)$ and $J_1(1091)$ are non-trivial (assuming the Birch-Swinnerton-Dyer conjecture).

Acknowledgements. This work is part of my doctoral research under L. Merel and owes a lot to him. I am very grateful to him for sharing his ideas. I would also like to thank B. Mazur and K. Ribet for several useful discussions, the anonymous referee for some useful comments and H. Lenstra for his help. Part of the work was done at the Université de Paris 6 under a grant from the University of California, Berkeley, and I am very grateful to both institutions for their help.

References

[1] Bosch S., Lütkebohmert W., Raynaud M., Néron Models, Ergebnisse der Math. 21, Springer-Verlag, 1990.

[2] Brumer A., The rank of $J_0(N)$, Columbia University Number Theory Seminar (NY 1992), Astérisque, 228 (1995), 3, 41-68.

[3] Deligne P., Rapoport M., Schémas de modules de courbes elliptiques, in P. Deligne, W. Kuyk (eds.), Modular forms of one variable II, Lecture Notes in Mathematics 349, Springer-Verlag, Berlin-Heidelberg-New York, 1973.

[4] Kolyvagin V. A., Logachev D. Yu., Finiteness of the Shafarevich-Tate group and the group of rational points for some modular abelian varieties, Leningrad Math. J. (1990), **5**, 1229-1253.

[5] Lang S., Number theory III: Diophantine geometry, Encyclopaedia of Mathematics, Vol. 60, Springer-Verlag, 1991.

[6] Mazur B., Modular curves and the Eisenstein ideal, Publ. Math. I.H.E.S.**47** (1977), 33-186.

[7] Mazur B., Rational isogenies of prime degree, Inv. Math. **44** (1978), 129-162.

[8] Mazur B., Handout from the 1998 Arizona Winter School, Southwestern Center for Arithmetical Algebraic geometry, Arizona, USA; to appear in Cremona J., Mazur B., Visualizing elements in the Shafarevich-Tate group (preprint).

[9] Merel L., Bornes pour la torsion des courbes elliptiques sur les corps de nombres, Inv. Math. **124** (1996), 437-449.

[10] Ribet K., Endomorphisms of semi-stable Abelian varieties over number fields, Ann. of Math. **101** (1975), 555-562.