KOLYVAGIN'S METHOD FOR SHIMURA VARIETIES: NEW TYPE OF EULER SYSTEMS. I.

D. Yu. Logachev[1]

1. Introduction.

1.1. The purpose of the present paper is to prove some important steps of a natural program of generalization of Kolyvagin's proof of finiteness of Tate-Shafarevich group of a Taniyama-Weil elliptic curve E of analytic rank 0 or 1 ([K1], [K2], referred below as "K-case") to the case of other Shimura varieties. Some intermediate results of the present paper are of its own importance. For example, analogs of Eichler - Shimura relations for Picard modular varieties X (4.4.1 and 4.4.3) apparently were never published. Euler systems constructed in (5.3) are of new type, because of (1.3.1).

This program is the following. Let X be a Shimura variety (a level is fixed) having a sufficiently large family of Shimura subvarieties V_i of codimension r defined over a number field K, $\bar{X}$ a smooth compact model of X and $\mathcal{M}$ an irreducible quotient motive of $H^{2r-1}(\bar{X})$. We denote by $CH^r(\bar{X}\otimes K)_0$ the group of cycles on $\bar{X}$ of codimension r defined over K, homologically equivalent to 0, modulo rational equivalence, and we denote by $E=H^{2r-1}(\mathcal{M}(r),\mathbb{Z}_l)$ the l-adic realization of $\mathcal{M}(r)$, so there exists the Abel-Jacobi map $\mathrm{cl}\,'\colon CH^r(\bar{X}\otimes K)_0\to H^1(K,E)$. We choose a cycle $\phi(V)\in CH^r(\bar{X}\otimes K)_0$ which is a formal linear combination of V_i. An element $\mathrm{cl}\,'(\phi(V))\in H^1(K,E)$ is an analog of a Heegner point $y\in E(K)$ of the K-case, we denote it by y as well. The final goal of the first part of this program is a proof of the following theorem (a rough statement; see (1.6.1) for the exact statement):

Theorem. If $\exists\ V$ described above such that $y\neq 0$ then $SH(K,E)$ is finite and the Selmer group $S_{l^\infty}(K,E)$ is generated by y.

This part was realized for quaternion Shimura curves in [KL].

To complete this program we have to prove an analog of Gross - Zagier theorem [GrZ] for the present case; this will give us a proof of an analog (according to [BK] and [B]) of the Birch - Swinnerton-Dyer conjecture for sub- (or quotient) motives of Shimura varieties.

The realization of this program in whole is a huge task, first of all, because the existence of the main objects, namely motives H^{2r-1} and $\mathcal{M}$, depends on the standard conjectures of Tate and Langlands. Further, the proof of an analog of Gross - Zagier theorem seems now to be out of human force; the only result that we can try to obtain is to prove that for some cases $y\neq 0$ (maybe modulo some

[1]Partially supported by G.Soros Foundation and by an AMS grant

reasonable assumptions), i.e. to give an evidence that the whole program is not vacuous. A method of [B], §3 can be used for this purpose; see also (1.8.3).

Most steps of the first part of this program are realized in the present paper for one type of Shimura varieties, namely Picard modular threefolds (see (1.5), (4.1) for the definition), denoted by X_P. Some of these steps are valid without any significant change for other types of Shimura varieties. Remaining steps of the proof are of purely technical nature and do not contain serious obstacles. We consider for simplicity only the case of rank 0 ([K1]), although a construction of Euler systems of order 2 is given in (5.5).

Section 1.2 below contains the plan of the present paper together with the plan of realization of the first part of the program. For each step of this plan it is indicated is the obtained proof complete or partial, and can it be applied to other types of Shimura varieties, or not.

In Section 1.3 we indicate some main obstacles that do not exist in K-case and which are got over in the present paper. Section 1.4 contains a list of parallel notations of the present paper and [Gr] which is apparently the best survey of K-case. In 1.5 we give more details on conjectures of Langlands and Serre which are used in the proof. 1.6 contains an exact statement of the theorem, in 1.7 it is explained why namely X_P is chosen for the realization of this program, in 1.8 we describe some possibilities of further research and interesting unsolved questions.

1.2. The whole method of the present paper can be apparently applied to all Shimura varieties satisfying the following condition:

(1.2.1) X contains a family of subvarieties V_i of codimension r such that the reflex field of V_i is not contained or equal to the one of X.

Although throughout the whole paper we work mainly with X_P, proofs for some steps are valid for some others types of Shimura varieties practically without any change. There are 3 cases:

(A) A proof can be obtained for all Shimura varieties satisfying (1.2.1) but each type of these varieties claims its own calculations of growing volume;

(B) The proof is valid for all odd-dimensional Picard modular varieties; for other types of Shimura varieties we have case (A);

(C) The proof is valid for all types of Shimura varieties satisfying (1.2.1).

In Section 2 we remember the definition of Selmer and Tate - Shafarevich group of Galois modules and the definition of Abel-Jacobi map ([BK], [Fl], [J]).

Section 3 contains some information about Shimura varieties of PEL-type ([Sh1], [D]) that is necessary for us.

Step 1. It is shown by explicit construction of subvarieties that Picard modular varieties satisfy (1.2.1). Case B. Namely, in Section 4 we consider properties of a threefold $X = X_P$ and curves $V \subset X$. In (4.1) we define a curve $V = V_d \subset X$ which is an analog of a Heegner point in K-case ($d \in \mathbb{Z}$ is a non-essential parameter).

Step 2. Let $\mathbb{T}_p$ be the p-Hecke algebra of X. We choose an element $T_p \in \mathbb{T}_p$ and we consider it as a correspondence on X. The problem is to study the Galois action on irreducible components of $T_p(V)$, these are analogs of Kolyvagin's "trace relations"((4.3.4), (4.3.6), (5.3.8) (1), (2)). Case A.

The proof of this result (proposition 4.3.2) is highly calculational and claims consideration of many cases. Not all cases are considered in the present paper, by only reason of voluminous calculation (there is no obstacles of principle). By analogy with [L] where similar calculations were completed for Siegel threefolds, we can conjecture the result. Moreover, we have to use this result for a product of 2 Hecke correspondences T_p, T_q (because of (1.3.3) below). We conjecture the desired result for this situation (Proposition 4.3.6) by analogy with the situation of one Hecke correspondence.

Further, we have

1.2.2. Conjecture. For all types of Shimura varieties (1.2.1) implies that the above Galois action is non-trivial.

We check this conjecture for $X = X_P$ by proving in (4.3.3) that an irreducible component of $T_p(V)$ is defined over the ring class field K^p. The fact that this implies the non-triviality of Galois action, although obvious, claims a proof; it is omitted.

Non-triviality of Galois action on irreducible components of $T_p(V)$ is necessary for the construction of Euler systems using Kolyvagin's derivative operator. (See (1.7); this observation was indicated me by J.Nekovář).

Step 3. Finding of reductions of Hecke operators on X (analogs of Eichler - Shimura formula $\tilde{T}_p = \mathrm{fr}_{\ p} + \mathrm{fr}_{\ p}'$) and calculation of the characteristic polynomial (CHP) of Frobenius at p on E. Case B. Calculation of CHP is made by 2 ways (4.2; 4.4.1); both these ways of proof depend on a Langlands conjecture describing zeta function of E.

Step 4. Finding of relations between reductions of V and of irreducible components of $T_p(V)$ at p (4.4.11). Case A. Here we use without proofs 2 technical lemmas (5.3.5), (5.3.7) showing that Abel-Jacobi map commutes with bad reduction, hence the result is obtained up to a calculation of multiplicity of a cycle (c of Lemma 5.3.7; $C_{p,i}$ of Proposition 4.3.5), that is not essential for the sequel (see Step 6 below).

Step 5. We consider formal linear combinations $\phi(V)$, $\phi(V_p)$ of irreducible components of $T_\bullet(V)$ such that $\phi(V_p) \in CH^r(\bar{X} \otimes K^p)_0$ where K^p is a ring class field extension of K, Section 4.5. Elements $y_p = \mathrm{cl}'(\phi(V_p)) \in H^1(K^p, E)$ are used to construct Euler system. Case C; this result is complete. Really here and below we use 2 primes p, q but not one because of (1.3.3).

The final part of the proof is given in Section 5. In 5.1 we discuss a condition of existence of $\mathbb{Q}$-structure on E.

Step 6. The same procedure like in K-case applied to y_p will give us elements of Euler system $c_p \in H^1(K, E)$ (5.3.10). Case C. A calculation to prove the main property of these systems is given in (5.3.17). Propositions (5.3.13) - (5.3.14) (resp. (5.3.22)) show how to get over an obstacle (1.3.3) (resp. (1.3.1)). In (5.3) the theorem is proved modulo a congruence (5.3.19) that most likely is true, although must be checked (it depends on calculations of multiplicities in Step 4 which are not made). Nevertheless, it is not essential. It is shown in (5.4) how to prove the theorem if (5.3.19) is not true.

This result is complete modulo a number theoretic conjecture on units in real quadratic fields (3.7.2); most likely it will be possible to prove the theorem without using this conjecture.

Step 7. In (5.2) it is shown that the existence of these c_p implies the theorem, an obstacle 1.3.2 is got over. Case C. Here we use for a reader's convenience the following assumption:

(1.2.3) E is the first cohomology motive of an abelian surface

This surface is denoted by E as well. (1.2.3) is certainly always false but permits to make the proof more transparent, because under this assumption we can consider y as an element of $E(K)$ as well, but not only of $H^1(K,E)$ where it really lives. A proof for the real situation can be obtained practically by a mechanical change of notations; lemmas (5.6.1), (5.6.2) show how to do it. See also [N] where the analogous problem is got over.

The proof uses also Serre conjecture about image of Galois representation for E, see (1.5.2).

In (5.5) a sketch of the definition and the proof of the main property of Euler systems of order 2 is given.

1.2′. Throughout the whole paper we neglect the problems related to the level structure on X_P, and problems related to the boundary components of $\bar{X}_P$. By analogy with cases of curves we can expect that solution of these problems does not contain difficulties of principle. At last, we assume for simplicity that (a) the coefficient field of $\mathcal{M}$ is $\mathbb{Q}$; (b) $l\neq 2$; moreover once we assume that l is sufficiently large; (c) y is not divisible by l; (d) quadratic fields K and Y both are of class number 1, in order to avoid difficulties related to non-connectedness of Shimura varieties.

1.3. Here is a list of main obstacles that are got over in the present paper.

1.3.1. Step 6. A construction of Euler systems in K-case uses essentially that CHP(E) has degree 2 and moreover is equal to X^2-a_pX+p where X is an independent variable, a_p is the eigenvalue of T_p on E. For general E CHP(E) has a higher degree so the Euler systems constructed in the present paper are of a new type, their main property is weaker than the one of Euler systems of K-case. Nevertheless, this weakened main property is sufficient for our purpose.

1.3.2. Step 7. Its proof in K-case uses essentially that dim $E=2$. Really, Kolyvagin considers: (a) a decomposition $E/l=E/l^+\oplus E/l^-$ with respect to the action of complex conjugation on E/l; (b) elements $y^+\in E/l^+$, $y^-\in E/l^-$ which are images of any element s of Selmer group $S_l(\mathbb{Q},E)$ and of y respectively. Further, he shows (roughly speaking):

1) $[y_+,y_-]=1$ where $[.,.]$ is the Weil pairing;

2) $y\neq 0$ implies $y_-\neq 0$, and $s\neq 0$ implies $y_+\neq 0$.

One-dimensionality of both E/l^+, E/l^-, non-degeneracy of the Weil pairing and a condition $y\neq 0$ imply immediately that $s=0$.

Since for a "general" E we have dim $E=\deg(\text{CHP}(E))$ and for most cases this degree is >2, the arguments above must be changed. This is made in (5.2).

1.3.3. Step 6. For $X=X_P$ the field K is a real quadratic field but not the imaginary one like in K-case. Since ring class field extensions of real quadratic fields are "smaller" than the ones of imaginary quadratic fields we have to use 2 primes p,q in Step 2 instead of one prime p used in [K1], to consider elements $c_{p,q}$ instead of elements c_p (and hence to use new arguments in Step 6) etc. (The existence of this obstacle was indicated me by B.H.Gross by pointing out my attention to a necessity to use 2 primes because of a "small" ring class field extension).

1.4. Table of correspondence of notations and propositions of [Gr] and the present paper.

Present paper	[Gr]
X Picard threefold	$X_0(N)$ elliptic curve
$E \subset H^3(\bar{X} \otimes \bar{\mathbb{Q}}, \mathbb{Z}_l(2))$, dim $E = 4$	$T_p(E)$, E Weil elliptic curve, dim $T_p(E) = 2$
K real quadratic field	K imaginary quadratic field
Y imaginary quadratic field	$\mathbb{Q}$
$p = \mathfrak{p}\bar{\mathfrak{p}}$ in Y, p inert in K	l inert in K
l (resp. n, M); $M = l^n$	p (resp. 1, p)
V quaternion Shimura curve, $V \subset X$	$x_1 \in X_0(N)$ Heegner point
$y = y_2 \in H^1(K, E)$	$y_K \in E(K)$
$c_{p,q} \in H^1(K, E/M)$	$c_l \in H^1(K, E_M)$ elements of Euler system
(5.3.2.1)	(3.2) choice of l
(5.3.4)	(3.3) congruence relations
(4.3.4), (4.3.6), (5.3.8) (1), (2)	(3.7) (1) trace relation
(4.4.11), (5.3.8) (3)	(3.7) (2) relations for reductions of Heegner points

1.5. From here and throughout the whole paper we consider only a Picard modular threefold $X = X_0(N)$ which is the moduli space of abelian fourfolds with multiplication by an imaginary quadratic field Y endowed by some level structure (an isogeny of order N). See (4.1) for the exact definition. Let G be a reductive group that corresponds to X; it is of type $GU(3,1)$. The reflex field of X is Y, hence $\mathcal{M}$ is defined over Y. We assume that the following standard conjectures (1.5.1), (1.5.2) are true:

1.5.1. $L_{\mathfrak{p}}(\mathcal{M}, s)$ at almost all places $\mathfrak{p}$ of Y is the same as it is predicted by a Langlands' conjecture.

Let $\mathcal{M}_{\mathbb{Q}} = \text{Ind}\,_{\mathbb{Q}}^{Y}(\mathcal{M})$. A more exact form of (1.5.1) is the following:

(1.5.1.1) $\mathcal{M}_{\mathbb{Q}}$ is associated by a Langlands correspondence to a pair $(\pi, r_{\mathbb{Q}})$ where π is a cuspidal automorphic representation of $G(\mathbb{A}_{\mathbb{Q}})$, $r_Y : {}^LG_Y \to GL(W)$ is the finite-dimensional representation associated to X according [La] and $r_{\mathbb{Q}} : {}^LG_{\mathbb{Q}} \to GL(W_{\mathbb{Q}})$, $r_{\mathbb{Q}} = \text{Ind}\,_{\mathbb{Q}}^{Y}(r_Y)$ is the induced representation.

For our case ([BlR], p.550, (b)) ${}^LG_Y = GL_4(\mathbb{C}) \times \text{Gal}\,(Y)$, r_Y is the standard representation of $GL_4(\mathbb{C})$ and is trivial on Gal (Y), hence

$$\dim W = 4, \ \dim W_{\mathbb{Q}} = 8 \tag{1.5.1.2}$$

Let U be the field of coefficients of $\mathcal{M}$ (we assume usually that $U = \mathbb{Q}$). For a fixed prime $\lambda | l$ of U we denote by $\mathcal{E}$ (resp. $\mathcal{E}_{\mathbb{Q}}$) the λ-adic realization of $\mathcal{M}$ (resp. $\mathcal{M}_{\mathbb{Q}}$) with integer coefficients and by ρ_λ (resp. $\rho_{\lambda,\mathbb{Q}} = \text{Ind}\,_{\mathbb{Q}}^{Y}(\rho_\lambda)$) its λ-adic representation Gal $(Y) \to GL(\mathcal{E})$ (resp. Gal $(\mathbb{Q}) \to GL(\mathcal{E}_{\mathbb{Q}})$). (1.5.1.1) means that we have the equality of local zeta-functions at a place $\mathfrak{p}$ of Y (resp. a prime p of $\mathbb{Q}$):

$$\mathcal{Z}_{\mathfrak{p}}(\pi, r, T) = \kappa(\mathcal{Z}_{\mathfrak{p}}(\rho, \mathcal{E}, U, T)), \text{ resp. } \mathcal{Z}_p(\pi, r_{\mathbb{Q}}, T) = \kappa(\mathcal{Z}_p(\rho_{\mathbb{Q}}, \mathcal{E}_{\mathbb{Q}}, U, T)) \quad (1.5.1.3)$$

where $T = p^{-s}$ is an independent variable, $\mathcal{Z}_{\mathfrak{p}}(\pi, r, T)$ is the standard zeta function associated to (π, r) (see 4.2.1.1 below for more details), $\mathcal{Z}_{\mathfrak{p}}(\rho, \mathcal{E}, U, T)$ is the zeta function of ρ respectively multiplication by U and an inclusion $\kappa : U \to \mathbb{C}$ is defined by Hecke action (see (4.2.3) for the exact definition).

Since $E = \mathcal{E}(2)$, (1.5.1.3) gives us immediately the characteristic polynomial of Frobenius on E, see (4.2.3.5) and (4.4.3). Later we shall work mainly with E without using $\mathcal{M}$.

Equalities (1.5.1.2), (1.5.1.3) imply that dim $(E \otimes \mathbb{Q}_l) = 4$.

1.5.2. Serre's conjecture is true for $\mathcal{M}$, i.e. the image of the l-adic representation of $\mathcal{M}$ is an open subgroup of $G(\mathbb{Z}_l)$ and is equal to $G(\mathbb{Z}_l)$ for almost all l, where $G = GSp_4$ if the restriction on $\mathcal{E}$ of the pairing in $H^3(\bar{X} \otimes \bar{\mathbb{Q}}, \mathbb{Z}_l)$ is non-degenerate, and $G = GL_4(\mathbb{Z}_l)$ if it is 0.

1.5.2.1. Not only the knowledge of im ρ_l that is given by Serre's conjecture (1.5.2) is necessary for us, but also the knowledge of im $\rho_{l,\mathbb{Q}} = \text{Ind}\,{}_{\mathbb{Q}}^{Y}(\rho_l)$. The existence of a $\mathbb{Q}$-structure on E which is a consequence of (5.1.4) makes groups $S(\mathbb{Q}, E)$, $SH(\mathbb{Q}, E)$ meaningful.

1.5.2.2. If X is any Shimura variety and E is an irreducible subspace in the middle cohomology of X then the restriction on E of the pairing P in this middle cohomology space can be either non-degenerate or 0. Since the method of the present paper can be applied to other types of Shimura varieties we consider both of these cases, without precising what of these 2 cases is realized in the present situation.

In the most part of the paper we consider the first case (P is non-degenerate on E). To formulate and prove the theorem when P is 0 on E we must replace E by $E \oplus E'$ throughout the whole paper, here E' is a subspace in the middle cohomology which is orthogonal to E. Details are considered in Sections 5.3$'$, 5.4$'$.

1.6. For a given Picard modular threefold X we have $r = 2$, curves V_i are quaternion Shimura curves $V_{B,K} \subset X$ which are parametrized by pairs (B, K) where K is a real quadratic field and B is a quaternion algebra over K. $V_{B,K} = \Gamma \backslash \mathfrak{H}$ where $\Gamma \subset O_B^*$ is a congruence subgroup. $V_{B,K}$ is defined over (an extension of) K (4.1.4); points of $V_{B,K}$ parametrize abelian fourfolds with some auxiliary multiplications. If B and K are fixed we denote $V_{B,K}$ simply by V.

A cycle $\phi(V) = \phi_m(V)$ (m is a non-essential parameter) is defined in (4.5). We denote by σ (resp. τ) the non-trivial element of Gal $(K/\mathbb{Q})$ (resp. Gal $(Y/\mathbb{Q})$).

Under these assumptions the statement of the theorem is:

1.6.1. Let there exist a real quadratic field K and a quaternion algebra B over K such that $V = V_{B,K}$ is defined and such that $y = \text{cl}'(\phi_m(V))$ is not of torsion over the algebra generated by Hecke operators (conjecturally, this condition does not depend on l if π and hence $\mathcal{M}$ are fixed) and $\sigma(y) = -y$, $\tau(y) = y$. Then $SH_{l^\infty}(\mathbb{Q}, E)$ and $S_{l_\infty}(\mathbb{Q}, E)$ are finite and $= 0$ for almost all l.

1.7. Why namely this X?

Condition (1.2.1) is essential to obtain a property of elements c_p of Euler system to be ramified at p. Really, applying the Abel-Jacobi map to an element of $CH^2(X)_0(K')$ we get an element of $H^1(K', E)$ which is non-ramified at all places of K'; only considering its inverse image under a map Res of [Gr], (4.2) we get an element of $H^1(K, E)$ which is ramified at ramification places of K'/K.

For example, we cannot apply the method of the present paper to a Siegel modular threefold X_S, because a non-trivial Shimura curve V on X_S (studied in [Ko]) is a quaternion curve over $\mathbb{Q}$; an analog of Kolyvagin's norm relations for V was obtained in [L], and in this case curves $V_{p,i}$ are defined over $\mathbb{Q}$ as well. Moreover, looking at the table of Shimura curves and threefolds which are moduli spaces of abelian varieties of PEL-type we see that V, X represent the simplest type of them satisfying condition (1.2.1) (I omit those types of Shimura threefolds for which the realization of the program will give us finiteness of SH of the same (conjecturally) objects for which it was proved in [KL]).

1.8. Possibilities of further investigation.

1.8.1. It is natural to prove (1.2.2), to find a better way of proving of theorems of Step 2 and to find a general statement of these theorems (valid for all types of Shimura varieties).

1.8.2. π and E considered in the present paper are "of general type". It is interesting to consider an "exceptional" E, i.e. the one corresponding to a representation π' of an endoscopic group H of G. Typical example: a group $H = \{(h_1, h_2) | h_1 \in GU(2,0), h_2 \in GU(1,1), \lambda(h_1) = \lambda(h_2)\}$ is endoscopic (see ([BlR], (5.4) for example). Let $\pi = \pi_1 \otimes \pi_2$ where π_1 (resp. π_2) is an automorphic representation of $GU(2,0)$ (resp. $GU(1,1)$). Let $\mathcal{M}_i$ be motives that correspond to π_i; then (most likely) $\mathcal{M} = \mathcal{M}_1 \oplus \mathcal{M}_2$. It can happen that one of $\mathcal{M}_i$ is a motive of an elliptic curve A defined over $\mathbb{Q}$. For example, it is so if X is a Siegel modular threefold ([W]). In this case the method of the present paper can be applied to A. Particularly, we shall be able to construct Heegner points on $A(K)$ for a real quadratic field K.

Certainly the same idea of consideration of "exceptional" E cam be applied to other Shimura varieties satisfied (1.2.1): we shall be able to prove the theorem for analogs of motives $\mathcal{M}_i$ above. What kinds of motives can be obtained by this way?

1.8.3. Let us consider the K-case, $K = \mathbb{Q}(\sqrt{-\Delta})$ is an imaginary quadratic field. There is a following condition on N, Δ:

$$\exists a \in \mathbb{Z} \text{ such that } \Delta \equiv a^2 \pmod{4N} \tag{1.8.3.1}$$

For K-case it is known that :

1. (1.8.3.1) is equivalent to a condition of existence of a Heegner point attached to K on a modular curve $X_0(N)$.
2. (1.8.3.1) implies (modulo WBSDC = weak form of the Birch - Swinnerton-Dyer conjecture) that $\operatorname{rk}_K(E)$ is odd, here E is a Weil elliptic curve of conductor N.

3. Let (1.8.3.1) be fulfilled and $y \in E(K)$ the corresponding Heegner point. We have: $\mathrm{rk}_{\mathbb{Q}}(E)$ is odd (resp. even) implies that $\tau(y) = y$ (resp. $\tau(y) = -y$) where τ is the complex conjugation, again modulo WBSDC.

A consideration of the Fricke involution on modular forms permits us to formulate the propositions above without mentioning of WBSDC.

It is reasonable to prove an analog of propositions above for the case of the present paper, as well as to relate the sign of the functional equation of $L(E,s)$ and the eigenvalue of Fricke involution. The same question has a sense for $\mathcal{M}_i$ of 1.8.2. The truth of analogs of (1), (2) above will suggest that namely the Abel - Jacobi image of an (existing) Heegner curve gives us a non-trivial element in $S_{l^\infty}(K,E)$, existing according to WBSDC. This will give us some evidence that y can be really non-zero.

1.8.4. According to Remark 4.5.2, it is reasonable to find the order of growth of eigenvalues of Hecke operators T_p on E.

1.9.Thanks. During preparation of this paper I visited universities of Heidelberg, Paris-Sud, Grenoble, Paris-Nord, Bielefeld, Rennes, Münster. I want to thank M.Flach, E.Freitag, L.Clozel, L. Illusie, R.Gillard, J.Tilouine, Th.Zink, B.Edixhoven, P.Schneider for their kind hospitality and discussions on the subject of the present paper. I am grateful to D.Blasius, B.Gross, S.Kudla, J.Nekovář, R.Taylor, R.Weissauer for some important remarks.

2. Some definitions.

We fix a power $M = l^n$ of l (which is assumed to be large enough). The l^∞-part of Selmer and Tate-Shafarevich group of E is defined in [BK] (see also [Fl]). For a prime number r and a place $\mathfrak{r}|r$ of Y such that $r \neq l$ and E has a good reduction at $\mathfrak{r}$ we let

$$H^1_f(Y_\mathfrak{r}, E/M) \overset{\mathrm{def}}{=} H^1(Y_\mathfrak{r}^{\mathrm{nr}}/Y_\mathfrak{r}, E/M)$$

where $Y_\mathfrak{r}^{\mathrm{nr}}$ is the maximal non-ramified extension of $Y_\mathfrak{r}$. The definition of $H^1_f(Y_\mathfrak{r}, E/M)$ for other $\mathfrak{r}$ is given in [BK]. Now we can define

$$S_M(Y,E) \overset{\mathrm{def}}{=} \{s \in H^1(Y, E/M) | \forall \mathfrak{r}\ \mathrm{loc}_{\mathfrak{r}}(s) \in H^1_f(Y_\mathfrak{r}, E/M)\}$$

where $\mathrm{loc}_{\mathfrak{r}} : H^1(Y,E/M) \to H^1(Y_\mathfrak{r}, E/M)$ is the localization map.

Further, $S_{l^\infty}(Y,E) \overset{\mathrm{def}}{=} \varinjlim_M S_M(Y,E)$ where $\varinjlim$ is taken with respect to maps $E/M \to E/Ml$ induced by multiplication by l.

Let us remember now the definition of $\mathrm{SH}(Y,E)$. We let $E_\mathbb{Q} = E \otimes \mathbb{Q}_l$ and $E_a = \varinjlim_M E/M$ so there is an exact sequence

$$0 \to E \to E_\mathbb{Q} \to E_a \to 0$$

Groups $H^1_f(Y_\mathfrak{r}, E_\mathbb{Q})$ and $H^1_f(Y, E_\mathbb{Q})$ are defined analogously. For example,

$$H^1_f(Y, E_\mathbb{Q}) = \{s \in H^1(Y, E_\mathbb{Q}) | \forall \mathfrak{r}\ \mathrm{loc}_{\mathfrak{r}}(s) \in H^1_f(Y_\mathfrak{r}, E_\mathbb{Q})\}$$

SH(Y, E) is defined via the following exact sequence ([Fl]):

$$H^1_f(Y, E_{\mathbb{Q}}) \xrightarrow{\alpha} S_{l^\infty}(Y, E) \to SH_{l^\infty}(Y, E) \to 0$$

To construct elements of Euler systems, we use the Abel-Jacobi map (see, for example, [J]). For a number field k let $CH^2(X \otimes k)$ be the group of codimension 2 cycles on X modulo rational equivalence defined over k,

$$\mathrm{cl}\ : CH^2(X \otimes k) \to H^0(k, H^4_{\text{et}}(X \otimes \bar{\mathbb{Q}}, \mathbb{Z}_l(2)))$$

the class map and $CH^2(X \otimes k)_0$ its kernel; then there exists the Abel-Jacobi map

$$\mathrm{cl}\ ' : CH^2(X \otimes k)_0 \to H^1(k, H^3_{\text{et}}(X \otimes \bar{\mathbb{Q}}, \mathbb{Z}_l(2)))$$

The existence of a non-degenerate pairing on $H^3_{\text{et}}(X \otimes \bar{\mathbb{Q}}, \mathbb{Z}_l(2))$ implies the existence of a canonical projection $H^3_{\text{et}}(X \otimes \bar{\mathbb{Q}}, \mathbb{Z}_l(2)) \to E$ hence we can define maps

$$\mathrm{cl}\ '_E : CH^2(X \otimes k)_0 \to H^1(k, E); \quad \mathrm{cl}\ '_{E,M} : CH^2(X \otimes k)_0 \to H^1(k, E/M)$$

It is conjectured that im $\mathrm{cl}\ '_{E,M} \subset S_M(k, E)$ and, moreover, that im $\mathrm{cl}\ '_E \subset$ im (α). At the local level (for primes $\mathfrak{p}$ of k such that $\mathfrak{p}$ does not divide l and E has a good reduction at $\mathfrak{p}$) this conjecture is proved.

3. Shimura varieties.

In this section X is an arbitrary Shimura variety of PEL-type. We remember a way of construction and some properties of X ([Sh1], [D]).

Let X be the moduli space of abelian varieties A_t $(t \in X)$. We let $A_t = \mathbb{C}^n/D$, D is a lattice in $\mathbb{C}^n$, and we denote by $T_0(A_t) = \mathbb{C}^n$ the tangent space of A_t in 0.

3.1. To define X we must fix the following objects:

3.1.1) An endomorphism algebra L with a positive involution: $L \subset \mathrm{End}(A_t) \otimes \mathbb{Q}$ $\forall t \in X$.

We denote $m = \dim_L(D \otimes \mathbb{Q})$

3.1.2) A representation $\Phi : L \to \mathrm{End}(T_0(A_t))$;

3.1.3) A polarization matrix T (defined in (3.3));

3.1.4) A $\mathbb{Z}$-lattice $\mathfrak{M} \subset L^m$.

These objects are called Shimura data that define X.

We shall consider only the case when L is a CM-field (case IV, $q = 1$ of [Sh1], p.155). Let dim $L = 2g, L \supset F$ where F is a totally real number field, dim $F = g$. The positive involution of L is the complex conjugation, it is denoted by bar. Throughout the whole paper we denote by $\chi_j : F \to \mathbb{R}$ $(j = 1, .., g)$ the real points of F and by $\chi_j, \bar{\chi_j} : L \to \mathbb{C}$ the corresponding complex points of L. It is known ([Sh1], (8), p. 156) that $\exists\ r_j, s_j$ such that $\forall j\ r_j + s_j = m$ and

$$\Phi = \sum_{j=1}^{g} r_j \chi_j + s_j \bar{\chi}_j$$

We choose complex coordinates in $T_0(A_t)$ such that $\forall a \in L$ the matrix of $\Phi(a)$ in these coordinates is

$$\mathrm{diag}(\underbrace{\chi_1(a), ..., \chi_1(a)}_{r_1 \text{ times}}, \dots, \underbrace{\chi_g(a), ..., \chi_g(a)}_{r_g \text{ times}}, \underbrace{\bar\chi_1(a), ..., \bar\chi_1(a)}_{s_1 \text{ times}}, \dots, \underbrace{\bar\chi_g(a), ..., \bar\chi_g(a)}_{s_g \text{ times}})$$

We shall identify $T_0(A_t)$ with $\mathbb{C}^n$ and omit Φ considering action of L.

3.2. For a given sequence of vectors $x = (x_1, \dots x_m)$ $(x_j \in \mathbb{C}^n)$ we consider a map $\beta_x : L^m \to \mathbb{C}^n$ defined by $(l_1, \dots l_m) \mapsto \sum_{j=1}^m l_j x_j$. A problem of definition of $A_t = \mathbb{C}^n/D$ is a problem of finding of a sequence $x = (x_1, \dots x_m)$ such that $D = \beta_x(\mathfrak{M})$.

3.3. Let E be the imaginary part of the polarization form on A_t. There exists a matrix $T = (t_{jk}) \in M_m(L)$ such that $\forall a, b \in L$

$$E(ax_j, bx_k) = \mathrm{Tr}_{L/\mathbb{Q}}(at_{jk}\bar b) \tag{3.3.1}$$

([Sh1], p.157, (11)).

T must satisfy the properties:

3.3.2) $\bar T^t = -T$ (^{t} means the transpose) ([Sh1], p. 157, (12)).

3.3.3) $\forall j = 1, \dots g$ the signature of $i\chi_j(T^{-1})$ is (r_j, s_j) ([Sh1], p. 160, (25)).

Let Φ and T are fixed. It is natural to ask for which $x = (x_1, \dots x_m)$ the following proposition (3.3.4) is true:

(3.3.4) $\beta_x(L^m)$ is a $\mathbb{Q}$-lattice in $\mathbb{C}^n$ such that $\mathbb{C}^n/\beta_x(\mathfrak{M})$ is an abelian variety and (3.3.1) defines the imaginary part of a Riemann form on it.

(3.3.5). The answer is given in ([Sh1], p. 161, (30)). Firstly, we define matrices $X_\nu \in M_m(\mathbb{C})$ $(\nu = 1, \dots g)$ whose entries are permuted and (partly) conjugated coordinates of $x_1, \dots x_m$ ([Sh1], p. 159, (20)). Further, let W_ν $(\nu = 1, \dots g)$ satisfy $\forall \nu$

$$W_\nu i\chi_\nu(T)^{-1}\bar W_\nu^t = \mathrm{diag}(\underbrace{1, \dots 1}_{r_\nu \text{ times}} \underbrace{-1, \dots -1}_{s_\nu \text{ times}}) \tag{3.3.6}$$

and we let

$$X_\nu \bar W_\nu^{-1} = \begin{pmatrix} \mathfrak{U}_\nu & \mathfrak{V}_\nu \\ \mathfrak{W}_\nu & \mathfrak{Y}_\nu \end{pmatrix} \tag{3.3.7}$$

where $\mathfrak{U}_\nu, \mathfrak{V}_\nu, \mathfrak{W}_\nu, \mathfrak{Y}_\nu$ are respectively $r_\nu \times r_\nu$, $s_\nu \times r_\nu$, $r_\nu \times s_\nu$, $s_\nu \times s_\nu$-matrices. Then (3.3.4) is equivalent to the following conditions:

$$\bar{\mathfrak{U}}_\nu \mathfrak{W}_\nu^t = \bar{\mathfrak{V}}_\nu \mathfrak{Y}_\nu^t;$$

$$\bar{\mathfrak{U}}_\nu \mathfrak{U}_\nu^t - \bar{\mathfrak{V}}_\nu \mathfrak{V}_\nu^t \text{ and } \bar{\mathfrak{Y}}_\nu \mathfrak{Y}_\nu^t - \bar{\mathfrak{W}}_\nu \mathfrak{W}_\nu^t$$

are positive hermitian.

If x satisfies these conditions then we denote by $\gamma(x)$ a point $t \in X$ such that $A_t = \mathbb{C}^n/\beta_x(\mathfrak{M})$. γ is an epimorphism (by definition), and for $t \in X$ any 2 elements of $\gamma^{-1}(t)$ differ by an element of $GL(\mathbb{C}^n) \times \Gamma$, Γ is defined below.

3.4. According [D], there exists an algebraic group G over $\mathbb{Q}$ and a subgroup $\mathcal{K}_f \subset G(\mathbb{A}_f)$ such that X is a connected component of a non-connected Shimura variety

$$X_{nc} = \mathcal{K}_f \times \mathcal{K}_\infty \backslash G(\mathbb{A})/G(\mathbb{Q})$$

(exact definitions are given in [D]). We have also $X = \Gamma\backslash\mathfrak{D}$ where $\mathfrak{D} = \mathcal{K}_\infty\backslash G(\mathbb{R})$ is an Hermitian symmetric domain and $\Gamma \subset G(\mathbb{Q})$ is a congruence subgroup.

If X is defined by Shimura data (3.1.1) - (3.1.4) then $\mathfrak{D}$ is defined by formulas ([Sh1], p. 162, (36)) and G is defined by the following way. Firstly, formulas ([Sh1], p.164, (38)) define us a group $\bar{G}(\mathbb{Q})$:

$$\bar{G}(\mathbb{Q}) = \{U \in M_m(L) | UT\bar{U}^t = \lambda T\} \tag{3.4.1}$$

There exists an action of $\bar{G}$ on $\mathfrak{D}$ ([Sh1], p. 164, lines below (38)). Let $\bar{G}_0 \subset G$ be a subgroup of elements that act trivially on $\mathfrak{D}$, then $G = \bar{G}/\bar{G}_0$, with the natural projection $\beta : \bar{G} \to G$.

Further,

$$\bar{\Gamma} = \{U \in M_m(L) | UT\bar{U}^t = T,\ \mathfrak{M}U = \mathfrak{M}\}$$

and $\Gamma = \beta(\bar{\Gamma})$. At last, $\mathcal{K}_f = \prod_{p \text{ prime}} \mathcal{K}_p$ and

$$\mathcal{K}_p = \{U \in M_m(L \otimes \mathbb{Q}_p) | UT\bar{U}^t = T,\ \mathfrak{M}U = \mathfrak{M}\} \tag{3.4.2}$$

Let $S = \mathrm{Res}_{\mathbb{C}/\mathbb{R}}(G_m)$. A map $h : S(\mathbb{R}) \to G(\mathbb{R})$ (depending on $x \in X$) is defined as follows. We have $G(\mathbb{R}) = \{U \in M_m(L \underset{\mathbb{Q}}{\otimes} \mathbb{R}) | UT\bar{U}^t = \lambda T\}$ and $S(\mathbb{R}) = \mathbb{C}^*$. For $z \in \mathbb{C}^* = S(\mathbb{R})$ we have $h(z)$ is the matrix of multiplication by z in $\mathbb{C}^n$ considered as a $L \underset{\mathbb{Q}}{\otimes} \mathbb{R}$–space, they are indentified by the basis $x_1, \dots, x_m$.

3.5. Shimura curves are either modular or quaternionic. A quaternionic Shimura curve over a real quadratic field F can be described as follows. Let B be a quaternion algebra over F which is ramified at χ_1 and non-ramified at χ_2. Fixing an isomorphism $B \underset{F}{\otimes} \mathbb{R} = M_2(\mathbb{R})$ ($F \overset{\chi_2}{\hookrightarrow} \mathbb{R}$) we get an inclusion $B^* \hookrightarrow GL_2(\mathbb{R})$ and hence an action of B^* on $\mathfrak{H}$. Let $\Gamma \subset O_B^*$ be a subgroup, then $V = \Gamma\backslash\mathfrak{H}$ is a quaternionic Shimura curve.

A way to represent V using Shimura data (3.1.1) - (3.1.4) is the following. B can be represented as a matrix algebra

$$\{\begin{pmatrix} x & y \\ a\bar{y} & \bar{x} \end{pmatrix}\} \tag{3.5.1}$$

where $x, y \in L$, L is a fixed CM-extension of F and $a \in F$ is fixed. We let $n = 4$, $m = 2$, $\Phi = 2\chi_1 + \chi_2 + \bar{\chi}_2$, $T = \begin{pmatrix} b & 0 \\ 0 & -ab \end{pmatrix}$ for some appropriate $b \in L$.

If $U = \begin{pmatrix} l_{11} & l_{12} \\ l_{21} & l_{22} \end{pmatrix} \in \bar{G}(\mathbb{Q})$ ($l_{jk} \in L$) then (3.4.1) shows that $l_{11}\bar{l}_{11} = l_{22}\bar{l}_{22}$ and $l_{11}\bar{l}_{21} = al_{12}\bar{l}_{22}$. This means that matrices (3.5.1) define an inclusion $B^* \hookrightarrow \bar{G}(\mathbb{Q}) \subset GL_2(L)$ that is a section of β.

At last, if we represent V according [D] then $G(\mathbb{Q}) = B^*, G(\mathbb{A}_{\mathbb{Q}}) = (B \underset{F}{\otimes} \mathbb{A}_F)^*$ and $V_{nc} = \mathcal{K}_\infty \times \mathcal{K}_f \backslash G(\mathbb{A}_{\mathbb{Q}})/B^*$ for some $\mathcal{K}_f \subset (B \underset{F}{\otimes} \mathbb{A}_F^f)^*$. The field of definition of V is an abelian extension of F that corresponds to $N(\mathcal{K}_f)$ where $N : B^* \to F^*$ is the reduced norm. As usual we shall consider only cases when $\mathcal{K}_f = \mathcal{K}^p \times \mathcal{K}_p$, $\mathcal{K}_p \subset G(\mathbb{Q}_p) = GL_2(F_p)$, $\mathcal{K}^p \subset \prod_{l \neq p} G(\mathbb{Q}_l)$.

3.6. Let us remember the definition of the ring class field extension. Let K be a quadratic field, p a prime inert in K, $\beta : O^*_{K_p} \to \mathbb{F}^*_{p^2}$ the projection to the residue field and $\mathbb{F}^*_p \to \mathbb{F}^*_{p^2}$ the natural inclusion. We denote by $O^{p\text{-ring}}_{K_p}$ the subgroup $\beta^{-1}(\mathbb{F}^*_p)$ of $O^*_{K_p}$. Analogously we can define a subgroup $O^{p^n\text{-ring}}_{K_p}$ for $n > 1$.

For primes $p_1, \dots, p_k$ inert in K we consider the following subgroup $I^{p_1,\dots,p_k}_K \subset I_K$:

$$I^{p_1,\dots,p_k}_K = \prod_{\lambda \text{ arch.}} K^*_\lambda \times \prod_{\lambda \neq p_1,\dots,p_k} O^*_{K_\lambda} \times \prod_{j=1,\dots,k} O^{p_j\text{-ring}}_{K_{p_j}}$$

Now we define the ring class field extension $K^{p_1,\dots,p_k}/K$ as an abelian extension that corresponds to the subgroup $I^{p_1,\dots,p_k}_K \times K^*$. For a real quadratic field K we have

$$\text{Gal } (K^{p_1,\dots,p_k}/K) = \{\oplus_{j=1,\dots,k} \mathbb{Z}/(p_j+1)\}/\text{im } O^*_K$$

where O^*_K is the group of units. Here $\mathbb{Z}/(p_j+1) = \mathbb{F}^*_{p^2}/\mathbb{F}^*_p$, O^*_K is mapped to $\mathbb{Z}/(p_j+1)$ via β.

3.7. We shall consider below primes p, q such that $(p+1)|(q+1)$, p is inert in K and splits in Y, and for d corresponding to (B, K) of the statement of the Theorem we have

$$(d+1, p+1) = (d+1, q+1) = 1 \tag{3.7.1}$$

i.e. particularly d must be even. Further, we assume:

3.7.2. The order of the image of a generator of O^*_K in $\mathbb{Z}/(p+1) \oplus \mathbb{Z}/(q+1) \oplus \mathbb{Z}/(d+1)$ is the maximal possible, namely $(d+1)(q+1)$.

This means that $K^{d,p} = K^{d,q} = K$ and Gal $(K^{d,p,q}/K) = \mathbb{Z}/(p+1)$. This is a reason why we consider 2 primes.

Remark 3.7.3. An analog of (3.7.2) for $\mathbb{Q}$ is an old number-theoretic open question: let $a \in \mathbb{Z}$ be given; to characterize a set of primes p such that im a in $\mathbb{F}^*_p$ is a generator of this group. Most likely it is possible to prove the theorem without using restrictions (3.7.1), (3.7.2), but this will claim a more careful consideration of Galois groups Gal $(K^{d,p,q}/K)$ and will give more cases in Proposition 4.3.6 below.

4. Threefold X and curves V_d.

4.1. In this subsection we apply the above definitions and results to define a threefold X which is the main object of the present paper (we omit the definition of level N structure, i.e. strictly speaking we define only $X_0(1)$. All the following results are valid also for $X = X_0(N)$). We define here inclusions of curves $V_{B,K} \hookrightarrow X$ as well. Since K will be fixed and algebras B/K will be parametrized by numbers

$d > 0$ we denote these curves by V_d. Notations related to V_d (resp. X) will have a subscript d (resp. will be without subscript).

Let us fix an imaginary quadratic field $Y = \mathbb{Q}(\sqrt{-\Delta})$ and a real quadratic field $K = \mathbb{Q}(\sqrt{f})$; we denote subrings of Y (resp. K, YK) generated by $1, \sqrt{-\Delta}, \sqrt{f}, \sqrt{-f\Delta}$ by $O(Y)$ (resp. $O(K)$, $O(YK)$) (i.e. they are not always the rings of integers, although sometimes we neglect it). We assume for simplicity that $h(Y) = h(K) = 1$, this is not essential.

We let $F_d = K, L_d = YK, F = \mathbb{Q}, L = Y, n_d = n = 4$ (hence $m_d = 2, m = 4$), $r_{1d} = 2, s_{1d} = 0, r_{2d} = s_{2d} = 1, r = 3, s = 1$ (hence $\Phi_d = 2\chi_1 + \chi_2 + \bar{\chi}_2, \Phi = 3\chi_1 + \bar{\chi}_1$),

$$T_d = \sqrt{-\Delta}\begin{pmatrix} 1 & 0 \\ 0 & d\sqrt{f} \end{pmatrix}, \quad T = 2\sqrt{-\Delta}\begin{pmatrix} 1 & 0 & 0 & 0 \\ 0 & f & 0 & 0 \\ 0 & 0 & 0 & f \\ 0 & 0 & f & 0 \end{pmatrix} \tag{4.1.1}$$

$\mathfrak{M}_d \subset (YK)^2$ is generated by vectors $y_j; \sqrt{-\Delta}y_j$ for $j = 1, \ldots 4$ where $y_1 = (1, 0); y_2 = (\sqrt{f}, 0); y_3 = (0, \frac{1}{d}); y_4 = (0, \sqrt{f})$ and $\mathfrak{M} \subset Y^4$ is generated by $e_j, \sqrt{-\Delta}e_j$ where e_j $(j = 1, \ldots 4)$ are coordinate vectors.

Since T_d, T satisfy the properties (3.3.2), (3.3.3) we get that $L_d, \Phi_d, T_d, \mathfrak{M}_d$ (resp. $L, \Phi, T, \mathfrak{M}$) define a Shimura curve V_d (resp. a Shimura threefold X).

Let $t \in V_d$ and $x \in \gamma_d^{-1}(t)$, $x = (x_1, x_2)$, $x_1, x_2 \in \mathbb{C}^4$. We consider a sequence

$$y = (x_1, \sqrt{f}x_1, \frac{1}{d}x_2, \sqrt{f}x_2) \tag{4.1.2}$$

It is obvious that $\beta_x(\mathfrak{M}_d) = \beta_y(\mathfrak{M})$ and an elementary calculation (which uses (3.3.1)) shows that skew symmetric forms E_d and E (defined by matrices T_d and T) on $\beta_x(\mathfrak{M}_d) = \beta_y(\mathfrak{M})$ coincide; this means that we get an inclusion $V_d \hookrightarrow X : t \mapsto \gamma(y)$.

Remarks. 4.1.3. Quaternion algebras B_d that correspond to curves V_d are different for different d, hence a curve V_d is not an image of another curve of this family under an action of a Hecke operator.

4.1.4. It is possible to show (like in 4.3.3) that the field of definition of V_d is K^d.

4.1.5. The Hermitian symmetric domain $\mathfrak{D}$ for X is the complex ball B_3 and the one of V_d is the unit disk B_1, the inclusion $V_d \subset X$ is induced by an inclusion $B_1 \subset B_3$. We denote the image of this inclusion by $B_1(d)$; the explicit equation of $B_1(d)$ is found in (6.1). We denote by ι the canonical projection $B_3 \to X$.

4.1.6. The reflex field of X is Y (see, for example, [BlR], (5.1), examples).

4.2. This subsection contains a sketch of calculations to find the characteristic polynomial of Frobenius of the λ-adic representation of E, with coefficients in Hecke algebra (formulas (4.2.3.4), (4.2.3.5)).

4.2.1. Let us give some definitions. For an arbitrary reductive group G over $\mathbb{Q}$ and an automorphic representation $\pi : G(\mathbb{A}_{\mathbb{Q}}) \to GL(\mathcal{V})$ we have $\pi = \otimes_p \pi_p$, $\pi_p : G(\mathbb{Q}_p) \to GL(\mathcal{V}_p)$. For a prime p such that π_p is non-ramified there is a 1-dimensional $G(\mathbb{Z}_p)$-stable subspace $L \subset \mathcal{V}_p$. The Hecke algebra $\mathbb{T}_p$ acts on

L, this action gives a map $j = j(\pi_p) : \mathbb{T}_p \to \mathbb{C}$. Let $r : {}^LG \to GL(W)$ be a finite-dimensional representation, $\phi_{\pi_p} \in {}^LG$ a Langlands parameter of π_p and $P_L(\pi_p, r, Z) = \det\,(Z - r(\phi_{\pi_p})) \in \mathbb{C}[Z]$ the characteristic polynomial of $r(\phi_{\pi_p})$, Z here and below is an independent variable. By definition,

$$P_L(\pi_p, r, Z) = \mathcal{Z}_p(\pi, r, T)T^{-\dim\, W},\ T = Z^{-1} = p^{-s} \tag{4.2.1.1}$$

where $\mathcal{Z}_p$ is the zeta function. It is well-known that there exists a polynomial $P_{\mathbb{T}}(G, r, p, Z) \in \mathbb{T}_p[Z]$ which does not depend on π such that

$$j(\pi_p)(P_{\mathbb{T}}(G, r, p, Z)) = P_L(\pi_p, r, Z) \tag{4.2.1.2}$$

4.2.2. $P_{\mathbb{T}}(G, r, p, Z)$ can be easily calculated for each given G, r. For example, for $G = GL_n$, $r = r_{st}$ the standard n-dimensional representation of G a (well-known) way to find $P_{\mathbb{T}}(GL_n, r_{st}, p, Z)$ is the following. Let $T \subset B \subset GL_n$ be the standard Borel pair, i.e. T the group of diagonal matrices and B of upper triangular ones. Let $\chi : T(\mathbb{Q}_p) \to \mathbb{C}^*$ be a non-ramified character; we denote by $\omega_k(p) \in T(\mathbb{Q}_p)$ the matrix whose k-th entry is p and other diagonal entries are 1, and we denote $\chi(\omega_k(p)) = b_k$. Let $\pi(\chi) : GL_n(\mathbb{Q}_p) \to GL(\mathcal{V}(\chi))$ be the Borel induced of π.

The Hecke algebra of $GL_n(\mathbb{Q}_p)$ is generated by elements $T_{p,k}$ which are double cosets $\Gamma\ \mathrm{diag}(\underbrace{1, \dots, 1}_{n-k \text{ times}}, \underbrace{p, \dots, p}_{k \text{ times}})\Gamma$, $\Gamma = GL_n(\mathbb{Z}_p)$, $k = 1, \dots, n$. Using the decomposition of double cosets $T_{p,k}$ as a union of left cosets it is easy to check that

$$j(\pi(\chi))(T_{p,k}) = p^{\frac{k(k-1)}{2}}\sigma_k(b_1, pb_2, \dots, p^{n-1}b_n),$$

where σ_k is the symmetric polynomial of degree k. At last, $\phi_{\pi(\chi)}$ is the conjugate class of $\mathrm{diag}(b_1, pb_2, \dots, p^{n-1}b_n)$, hence

$$P_{\mathbb{T}}(GL_n, r_{st}, p, Z) = \sum_{k=0}^{n}(-1)^k p^{\frac{k(k-1)}{2}} T_{p,k} Z^{n-k}.$$

4.2.3. Now let us consider $G, \pi, \mathcal{M}, \mathcal{E}, \rho_l, U$ etc. introduced in (1.3). An element of $\mathbb{T}_p$ is a correspondence on X, this gives us an action of $\mathbb{T}_p$ on E and $\mathcal{E}$. It acts via multiplication by U, hence we get a map $i : \mathbb{T} \to U$. There exists an inclusion $\kappa : U \to \mathbb{C}$ satisfying $j(\pi_p) = \kappa \circ i$. (1.5.1.3), (4.2.1.1) and (4.2.1.2) imply ($T = Z^{-1}$):

$$i(P_{\mathbb{T}}(G, r_{\mathbb{Q}}, p, Z)) = \mathcal{Z}_p(\rho, \mathcal{E}, U, T)T^{-\dim\, \mathcal{E}} \tag{4.2.3.1}$$

Here and below we consider only the case when p splits in Y: $p = \mathfrak{p}\bar{\mathfrak{p}}$, where $\mathfrak{p}$ and $\bar{\mathfrak{p}}$ are places of Y as well as fixed generators of the corresponding prime ideals, existing because $h(Y) = 1$. (4.2.3.1) implies

$$\mathcal{Z}_p(\rho_{\mathbb{Q}}, \mathcal{E}_{\mathbb{Q}}, U, T) = \mathcal{Z}_{\mathfrak{p}}(\rho, \mathcal{E}, U, T)\mathcal{Z}_{\bar{\mathfrak{p}}}(\rho, \mathcal{E}, U, T) \tag{4.2.3.2}$$

Now let us find $P_{\mathbb{T}}(G, r_{\mathbb{Q}}, p, Z)$. We have an isomorphism $G(Y) \to GL_4(Y) \times GL_1(Y)$ (depending on a choice of $\mathfrak{p}$; I neglect $GL_1(Y)$ below). Furhter, ${}^LG_Y =$

$\hat{G}(\mathbb{C})\times \mathrm{Gal}\ (Y) = GL_4(\mathbb{C})\times \mathrm{Gal}\ (Y)$ and (according [BlR], p.550, (b)) $r_Y : {}^LG_Y \to GL(W)$ is trivial on Gal (Y) and is r_{st} on $GL_4(\mathbb{C})$. The same formulas remain valid if we replace Y by $\mathbb{Q}_p$.

It is easy to check that the image of $T_{p,k} \in \mathbb{T}_p(GL_4(\mathbb{Q}_p))$ under the natural isomorphism $\mathbb{T}(GL_4(\mathbb{Q}_p) \times GL_1(\mathbb{Q}_p)) \to \mathbb{T}_p(G(\mathbb{Q}))$ is a double coset

$$T_{\mathfrak{p},k} := \Gamma\ \mathrm{diag}(\underbrace{\mathfrak{p},\dots,\mathfrak{p}}_{k \text{ times}},\ \underbrace{\bar{\mathfrak{p}},\dots,\bar{\mathfrak{p}}}_{4-k \text{ times}})\Gamma \tag{4.2.3.3}$$

where $\Gamma = G(\mathbb{Z})$.

An inclusion Gal $(\mathbb{Q}_p) \to$ Gal $(\mathbb{Q})$ defines a commutative diagram

$$\begin{array}{ccccccccc} 0 & \to & \hat{G}(\mathbb{C}) & \to & {}^LG_{\mathbb{Q}_p} & \to & \mathrm{Gal}\ (\mathbb{Q}_p) & \to & 0 \\ & & \| & & \downarrow & & \downarrow & & \\ 0 & \to & \hat{G}(\mathbb{C}) & \to & {}^LG_{\mathbb{Q}} & \to & \mathrm{Gal}\ (\mathbb{Q}) & \to & 0 \end{array}$$

(identical on $\hat{G}(\mathbb{C})$) and $\phi_{\pi(\chi)} \in^L G_{\mathbb{Q}}$ is the image of $\phi_{\pi(\chi)} \in^L G_{\mathbb{Q}_p}$.

Let us denote by $w \in \mathrm{Aut}\ (\hat{G}(\mathbb{C}))$ the action of the non-trivial element of Gal $(Y/\mathbb{Q})$; then det $(Z - r_{\mathbb{Q}}(\phi_{\pi(\chi)}))$ = det $(Z - r_{st}(\phi_{\pi(\chi)}))$det $(Z - r_{st}(w(\phi_{\pi(\chi)})))$. It is known that w is the only symmetry of A_3 (the root system of GL_4) and that $w(g) = \begin{pmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}(g^t)^{-1}\begin{pmatrix} 0&0&0&1\\0&0&1&0\\0&1&0&0\\1&0&0&0\end{pmatrix}$ (see, for example, [GSh], p. 27 - 30, where the analogous calculation was made for $U(2,1)$).

Using this formula we can easily find that

$$P_{\mathbb{T}}(G, r_{\mathbb{Q}}, p, Z) = (\sum_{k=0}^{4}(-1)^k p^{\frac{k(k-1)}{2}} T_{\mathfrak{p},k} Z^{4-k})(\sum_{k=0}^{4}(-1)^k p^{\frac{k(k-1)}{2}} T_{\bar{\mathfrak{p}},k} Z^{4-k})$$

This formula together with (4.2.3.1) and (4.2.3.2) implies that the characteristic polynomial of $\rho(\mathrm{fr}\ _{\mathfrak{p}})$ on $\mathcal{E}$ is

$$\sum_{k=0}^{4}(-1)^k p^{\frac{k(k-1)}{2}} i(T_{\mathfrak{p},k}) Z^{4-k} \tag{4.2.3.4}$$

After twisting on 2 we get a formula for the characteristic polynomial of $\rho(\mathrm{fr}\ _{\mathfrak{p}})$ on E:

$$\sum_{k=0}^{4}(-1)^k p^{\frac{k(k-5)}{2}} i(T_{\mathfrak{p},k}) Z^{4-k} \tag{4.2.3.5}$$

4.3. Action of Hecke correspondences on V.

Let $t \in X$ be a point and A_t the corresponding abelian variety. We denote $T_{\mathfrak{p},i}(t) = \{t' \in X | (t,t') \in T_{\mathfrak{p},i}\}$ where $T_{\mathfrak{p},i} \subset X \times X$ is a Hecke correspondence defined by a double coset $T_{\mathfrak{p},i}$ in (4.2.3.3). By definition, $t' \in T_{\mathfrak{p},i}(t)$ means that there exists an isogeny $\alpha = \alpha(t, t') : A_t \to A_{t'}$ of type $(\underbrace{\mathfrak{p}, \dots, \mathfrak{p}}_{i \text{ times}}, \underbrace{\bar{\mathfrak{p}}, \dots, \bar{\mathfrak{p}}}_{4-i \text{ times}})$. This isogeny is defined uniquely by its kernel.

Let $e(\mathfrak{p}) : A_t \to A_t$ be the application of multiplication by $\mathfrak{p} \in Y$. We have Ker $(e(\mathfrak{p})) = (O_Y/\mathfrak{p})^4 = (\mathbb{F}_p)^4$; we denote this space by B. Moreover, 2 spaces $B \cap \text{Ker } (\alpha(t, t'))$ and Ker $e(\bar{\mathfrak{p}}) \cap \text{Ker } (\alpha(t, t'))$ are orthogonal with respect to the Weil pairing, hence α is defined uniquely by one of these spaces. We can consider a space $B \cap \text{Ker } (\alpha(t, t'))$ as an element of the Grassman variety $G(i, B)$ of i-dimensional subspaces of B. It is easy to see that a map $k : T_{\mathfrak{p},i}(t) \to G(i, B)$ given by a formula $k : t' \to B \cap \text{Ker } (\alpha(t, t'))$ is an isomorphism. For $s \in T_{\mathfrak{p},i}(t)$ v_s will mean the subspace $B \cap \text{Ker } (\alpha(t, s))$ that corresponds to $k(s)$.

We have $G(1, B) = P^3 = P(B)$, $G(3, B) = P^3 = P(B^*)$, $G(2, B)$ is a quadric hypersurface in $P^5 = P(\lambda^2 B)$.

If we consider a curve V defined over K as a separate object then a Hecke correspondence $T_{p,V}$ is defined on V and has degree (p^2+1, p^2+1) (remember that p is inert in K). If $t \in V$, A_t is the corresponding abelian fourfold, $t' \in V$ such that $(t, t') \in T_{p,V}$, $\alpha : A_t \to A_{t'}$ is the corresponding isogeny then Ker $\alpha = O_{YK}/\mathfrak{p} \oplus O_{YK}/\bar{\mathfrak{p}}$ as O_{YK}-modules where $\mathfrak{p}, \bar{\mathfrak{p}} \in YK$ are generators of corresponding ideals. Since $O_{YK}/\mathfrak{p} = (O_Y/\mathfrak{p})^2$, $O_{YK}/\bar{\mathfrak{p}} = (O_Y/\bar{\mathfrak{p}})^2$ as O_Y-modules we have $(t, t') \in T_{\mathfrak{p},2}$, i.e. $T_{p,V}(t) \subset T_{\mathfrak{p},2}(t)$. Further, the set of $t' \in V$ such that $(t, t') \in T_{p,V}$ (denoted by $T_{p,V}(t)$) is in 1-1-correspondence with the set of 1-dimensional subspaces in $(O_{YK}/\mathfrak{p})^2$. Forgetting the structure of multiplication by O_K we get an inclusion of this set to $G(2, B)$.

Proposition 4.3.1. There exists a distinguished $P^3 = P^3(V) \subset P^5 = P(\lambda^2(B))$ such that $T_{p,V}(t) = P^3(V) \cap G(2, B)$.

Proof. Straightforward calculation, see Section 6.0. ■

We denote $P^3(V) \cap G(2, B)$ by S_0, it is a quadric hypersurface in $P^3(V)$.

Further we shall work mainly with $T_{\mathfrak{p},2}$, we denote it simply by T_p (because $T_{\mathfrak{p},2} = T_{\bar{\mathfrak{p}},2}$).

Let S be a set of representatives of left cosets in the double coset decomposition: $\Gamma T_p \Gamma = \cup_{s_i \in S} \Gamma s_i$. If $t_B \in \iota^{-1}(t) \subset B_3$ is a lift of t on B_3 ($\iota : B_3 \to X$ is a canonical projection) then $T_p(t) = \{\iota(s_i(t_B))\}$, hence there exists an isomorphism $j : S \to G(2, B)$ (depending on a choice of t_B). Let I_0 be the set of irreducible components of $T_p(V)$:

$$T_p(V) = \bigcup_{i \in I_0} V_{p,i}$$

There is a surjective map $\chi : G(2, B) \to I_0$ defined like in [L]. If $t \in V$, $t_B \in B_1(d)$ then a composite map $\chi \circ j : S \to I_0$ does not depend on a choice of $t_B \in B_1(d)$ but only on a choice of $B_1(d)$ which is not canonical.

Further, we denote by I the set of all projective spaces P^4 such that $P^3(V) \subset P^4 \subset P(\lambda^2(B)) = P^5$ and for $i \in I$ we denote the corresponding space by $P^4(i)$.

Proposition 4.3.2. $I_0 = I \cup \{i_0\}$ where i_0 is one point, $\chi^{-1}(i_0) = S_0$, $\chi^{-1}(i) = P^4(i) \cap G(2, B) - S_0$.

This is an analog of the main result of [L] for X. The proof is completely calculational, it is given in Sections 6.1 - 6.3. ■

Proposition 4.3.3. $\exists i \in I$ such that $V_{p,i}$ is defined over K^p.

Proof. We define a curve V' , we show that there is an embedding $i' : V' \hookrightarrow X$ such that the image of V' is a component of $T_p(V)$ (not equat to V) and that V' is defined over K^p. The objects related to V' will be denoted by prime. For a convenience of calculations we use an isogeny of type diag $(\mathfrak{p}, \bar{\mathfrak{p}}, 1, p)$, since Γ diag $(\mathfrak{p}, \bar{\mathfrak{p}}, 1, p)\Gamma = \Gamma$ diag $(\mathfrak{p}, \mathfrak{p}, \bar{\mathfrak{p}}, \bar{\mathfrak{p}})\Gamma$.

Definition of V'. Shimura data (3.1.1) - (3.1.3) for V' are the same as those for V_1, i.e. $F' = K$, $L' = YK$, $n' = 4$, $m' = 2$, $r_1' = 2$, $s_1' = 0$, $r_2' = s_2' = 1$, $\Phi' = 2\chi_1 + \chi_2 + \bar{\chi}_2$, $T' = \sqrt{-\Delta}\begin{pmatrix} 1 & 0 \\ 0 & d\sqrt{f} \end{pmatrix}$ and $\mathfrak{M}' \subset (YK)^2$ is O_Y-generated by the following vectors: $(\mathfrak{p}, 0)$; $(\bar{\mathfrak{p}}\sqrt{f}, 0)$; $(0, 1)$; $(0, p\sqrt{f})$.

Definition of an embedding $i' : V' \hookrightarrow X$. Let $t \in V'$ and $x \in \gamma'^{-1}(t)$, $x = (x_1, x_2)$, $x_1, x_2 \in \mathbb{C}^4$. We consider a sequence $y = \mathfrak{p}^{-1}(\mathfrak{p}x_1, \bar{\mathfrak{p}}\sqrt{f}x_1, x_2, p\sqrt{f}x_2) = (x_1, \mathfrak{p}^{-1}\bar{\mathfrak{p}}\sqrt{f}x_1, \mathfrak{p}^{-1}x_2, \bar{\mathfrak{p}}\sqrt{f}x_2)$. Then $\beta_y(\mathfrak{M}) = \mathfrak{p}^{-1}\beta_x(\mathfrak{M}')$ and it is seen that (identifying $\beta_x(\mathfrak{M}')$ and $\beta_y(\mathfrak{M})$ via multiplication by $\mathfrak{p}$) the restriction of E' on $\beta_x(\mathfrak{M}')$ coincide with E on $\beta_y(\mathfrak{M})$. This gives us the desired embedding: $i'(t) = \gamma(y)$.

V' is a component of $T_p(V)$. Really, it is clear (comparing $\mathfrak{M}$ and $\mathfrak{M}'$) that for $t \in V$, $x \in \gamma^{-1}(t)$ we have $(i(t), i'(\gamma'(x))) \in T_{p^2}$ (the inclusion $V \hookrightarrow X$ is denoted by i).

Finding of the field of definition of V'. There exist subgroups $\mathcal{K}_{V',\infty} \subset B^*(\mathbb{R})$, $\mathcal{K}_{V',f} \subset B^*(\mathbb{A}^f)$, $\mathcal{K}_{V',f} = \prod_{\mathfrak{p} \text{ place of } K} \mathcal{K}_\mathfrak{p}$, $\mathcal{K}_{V'} = \mathcal{K}_{V',f} \times \mathcal{K}_{V',\infty}$ such that V' is a connected component of a Shimura variety

$$V_{nc} = \mathcal{K}_{V'} \backslash (B \underset{K}{\otimes} \mathbb{A}_K)^* / B^*$$

Let G and $\mathcal{K}_X$ be Deligne data that define X. The embedding i' defines an embedding $i_G : B^* \to G$ such that:

1) $i_G(\mathcal{K}_{V'}) = \mathcal{K}_X$, hence an embedding $i'_{nc} : V_{nc} \to X$ is defined;

2) $i'_{nc}|_{V'} = i'$.

This means that 2 structures of an algebraic variety over a number field on V coincide: the first one is defined by the Deligne data B^*, $\mathcal{K}_{V',*}$, and the second one is the i'-restriction of a structure of an algebraic variety over a number field on X defined by the Deligne data G, $\mathcal{K}_{X,*}$. This means that to prove that V' is defined over K^p we must show that det $(\mathcal{K}_p) = O_{K_p}^{p\text{-ring}}$.

B can be identified with a matrix algebra $\{\begin{pmatrix} x & y \\ a\bar{y} & \bar{x} \end{pmatrix}\}$ where $x, y \in YK$, $a \in K$ is a fixed number (we do not need the exact value of a). Further, $YK \underset{K}{\otimes} K_p$ is an algebra over K_p generated by elements $(1, \delta)$ satisfying $\delta^2 = -\Delta$, hence we have an isomorphism σ from $B \underset{K}{\otimes} K_p$ to a subalgebra of $M_2(YK \underset{K}{\otimes} K_p)$ formed by matrices $\begin{pmatrix} x_1 + \delta x_2 & y_1 + \delta y_2 \\ a(y_1 - \delta y_2) & x_1 - \delta x_2 \end{pmatrix}$, $x_1, x_2, y_1, y_2 \in K_p$.

We have $\mathcal{K}_p \subset (B \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_p)^* = (B \underset{K}{\otimes} K_p)^* = GL_2(K_p)$. An isomorphism

$$\psi : GL_2(K_p) \to \{U \in M_2(YK \underset{\mathbb{Q}}{\otimes} \mathbb{Q}_p) | UT\bar{U}^t = \lambda T\} \tag{4.3.3.1}$$

is constructed as follows. We choose $\alpha \in K_p$ such that $\alpha^2 = -\Delta$; for $\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \in GL_2(K_p)$ we let

$$\psi(\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix}) = Z$$

where $Z = \begin{pmatrix} x_1 + \delta x_2 & y_1 + \delta y_2 \\ a(y_1 - \delta y_2) & x_1 - \delta x_2 \end{pmatrix}$, $x_1, x_2, y_1, y_2 \in K_p$,

$$x_1 = \frac{k_{11} + k_{22}}{2},\ x_2 = \frac{k_{11} - k_{22}}{2\alpha},\ y_1 = \frac{k_{21} + ak_{12}}{2a},\ y_2 = \frac{-k_{21} + ak_{12}}{2a\alpha} \tag{4.2.3}$$

(the entries of Z belong to $YK \underset{K}{\otimes} K_p$). We have $Z \in \sigma(B)$, and formulas of Section 3.5 show that the image of ψ is contained in the right hand side of (4.3.3.1).

Since im $\mathfrak{p}O_Y$ (resp. $\bar{\mathfrak{p}}O_Y$) is $(p\mathbb{Z}_p;\ \delta p\mathbb{Z}_p)$ (resp. $(\mathbb{Z}_p;\ \delta\mathbb{Z}_p)$) up to the interchanging of $\mathfrak{p}$, $\bar{\mathfrak{p}}$, which is not essential, we have that $\mathfrak{M}' \underset{K}{\otimes} O_{K_p}$ is generated by elements $(p, 0)$, $(p\delta, 0)$, $(\sqrt{f}, 0)$, $(\delta\sqrt{f}, 0)$, $(0, 1)$, $(0, \delta)$, $(0, p\sqrt{f})$, $(0, p\delta\sqrt{f})$.

According (3.4.2), we must find

$$\{x \in GL_2(K_p) | (\mathfrak{M}' \underset{K}{\otimes} O_{K_p})\psi(x) = \mathfrak{M}' \underset{K}{\otimes} O_{K_p}\}$$

To do it we consider the action of Z above on an element (0,1) of a basis of $\mathfrak{M}' \underset{K}{\otimes} O_{K_p}$:

$$(0, 1)Z = (ay_1 - ay_2\sqrt{-\Delta};\ x_1 - x_2\sqrt{-\Delta})$$

We denote $x_1 = x_{11} + x_{12}\sqrt{f}$ and analogously for x_2, y_1, y_2, where $x_{ij}, y_{ij} \in \mathbb{Q}_p$. Condition $(0, 1)Z \in \mathfrak{M}' \underset{K}{\otimes} O_{K_p}$ is equivalent (for almost all p) to conditions

$$x_{11}, x_{21}, y_{12}, y_{22} \in \mathbb{Q}_p;\quad x_{12}, x_{22}, y_{11}, y_{21} \in p\mathbb{Q}_p \tag{4.3.3.3}$$

It is easy to check (considering the action of Z on other elements of the basis of $\mathfrak{M}' \underset{K}{\otimes} O_{K_p}$) that if x_1, x_2, y_1, y_2 satisfy (4.3.3.3) then $(\mathfrak{M}' \underset{K}{\otimes} O_{K_p})Z \subset \mathfrak{M}' \underset{K}{\otimes} O_{K_p}$.

Now we find determinants of elements Z whose entries satisfy (4.3.3.3). Formulas (4.3.3.2) show that (again for almost all p) (4.3.3.3) imply $k_{11}, k_{22} \in \mathbb{Z}_p + p\sqrt{f}\mathbb{Z}_p$, $k_{12}, k_{21} \in p\mathbb{Z}_p + \sqrt{f}\mathbb{Z}_p$, hence det $\begin{pmatrix} k_{11} & k_{12} \\ k_{21} & k_{22} \end{pmatrix} \in O_{K_p}^{p\text{-ring}}$. ■

Remark 4.3.4. We have $\#(I) = p + 1$. The formula above can be rewritten as:

$$T_p(V) = V \cup (\bigcup_{i \in I} V_{p,i})$$

According to (3.7.2), all $V_{p,i}$ are defined over YK. We use $T_p = T_{\mathfrak{p},2}$ but not $T_{\mathfrak{p},i}$ $(i = 1, 3)$ because an analog of Proposition 4.3.2. (resp. 4.3.3) for these $T_{\mathfrak{p},i}$ shows that there is only one component of $T_{\mathfrak{p},i}(V)$ (resp. that a component of $T_{\mathfrak{p},i}(V)$ is defined over K but not over K^p).

Proposition 4.3.5 below will be used only in (5.3.19). Let us consider $i \in I_0$, a restriction of T_p on $V \times V_{p,i}$, and let $C_{p,i}$ be the degree of the projection $\Gamma_i \to V_{p,i}$ where Γ_i is the graph of T_p restricted on $V \times V_{p,i}$. Here we shall find $C_{p,i}$.

Let $\Gamma T_p \Gamma = \cup c_i \Gamma$ be a representation of the double coset as a union of right cosets, for our case we can take $c_i = s_i^t$. Let G_V be a reductive group that corresponds to V.

Proposition 4.3.5. Let $s \in (\chi \circ j)^{-1}(i)$. Then $C_{p,i} = \{\# c_i | \Gamma c_i^{-1} s \cap G_V \neq \emptyset\}$.

Proof. Let $y \in X$ and $y_B \in \iota^{-1}(y)$ be its lift on B_3. We have $T_p^{-1}(y) = \{\iota(c_i^{-1}(y_B))\}$. If, moreover, $y \in V_{p,i}$, $t \in V$ such that $y \in T_p(t)$ then $\exists t_B \in \iota^{-1}(t) \cap B_1$ and $y_B \in \iota^{-1}(y)$ such that $y_B = s(t_B)$. We have $C_{p,i} = \{\# c_i | \iota(c_i^{-1}(y_B)) \in V\}$. Further, $\iota(c_i^{-1}(y_B)) \in V \iff \exists \gamma \in \Gamma$ such that $\gamma c_i^{-1}(y_B) = \gamma c_i^{-1} s(t_B) \in B_1$. Since G_V acts transitively on B_1, $\exists g \in G_V$ such that $\gamma c_i^{-1} s(t_B) = g(t_B)$. We see that g does not depend on t, because γ, c_i and s belong to discrete sets. This gives us a desired equality $\gamma c_i^{-1} s = g$. ■

Remark. Using an explicit description of a set S we can find $C_{p,i}$ for all $i \neq i_0$ (it is clear that $C_{p,i_0} = p^2 + 1$). A preliminary calculation gives (a) $\forall i, j \neq i_0$ $C_{p,i} = C_{p,j}$; (b) moreover $\forall i \neq i_0$ $C_{p,i} = 1$. We shall assume below the truth of (a), and we denote $C_{p,i}$ simply by C_p, but not necessarily of (b), because the exact value of C_p is not essential, see (5.3.19), (5.4).

Now we shall consider 2 primes p, q of (3.7). The set I for the primes p, q is denoted respectively by I_p, I_q.

Proposition 4.3.6. $\forall j \in I_q$ there exists a curve $V_{p,q,j}$ defined over $K^{p,q}$ such that

$$T_p(V_{q,j}) = V_{q,j} \cup \Big(\bigcup_{\gamma \in \mathrm{Gal}\,(K^{p,q}/K)} \gamma(V_{p,q,j}) \Big) \tag{4.3.6.1}$$

Idea of the proof. Let $V_{p,q,j}$ be a component of $T_p(V_{q,j})$. Since Hecke operators T_p, T_q are independent we get like in (4.3.3) that for $\mathcal{K} = \mathcal{K}_{V_{p,q,j}}$ we have

$$\det \mathcal{K}_p = O_{K_p}^{p\text{-ring}}; \quad \det \mathcal{K}_q = O_{K_q}^{q\text{-ring}}$$

hence $V_{p,q,j}$ is defined over $K^{p,q}$. Further, T_p is defined over Y, $\#\mathrm{Gal}\,(K^{p,q}/K) = p+1$ and by analogy with (4.3.2) we can conclude that the number of irreducible components of $T_p(V_{q,j})$ (which are not equal to $V_{q,j}$ itself) is $p+1$ as well. This means that all components of $T_p(V_{q,j})$ are: (a) Galois-conjugate of $V_{p,q,j}$; (b) $V_{q,j}$ itself. ■

Remark 4.3.7. Although it is not necessary for us we can mention that there exists a map $\psi : I_q \to I_p$ such that $\forall j \in I_p$ $\#\psi^{-1}(j) = \frac{q+1}{p+1}$ and

$$T_q(V_{p,j}) = V_{p,j} \cup \left(\bigcup_{i \in \psi^{-1}(j)} \bigcup_{\gamma \in \mathrm{Gal}\,(K^{p,q}/K)} \gamma(V_{p,q,i}) \right)$$

It follows immediately from commutativity of T_p and T_q. This formula can be useful for a proof of an analog of Kolyvagin's rank 1 case, see 5.5.

Remark 4.3.8. An analog of (4.3.2) for a Siegel modular threefold X_S is proved in [L] by a straightforward calculation. May be this is not the best way. In a forthcoming paper of S.Kudla a general result about the action of Hecke algebra on Shimura subvarieties of a Shimura variety is proved.

4.4. Reductions of Hecke correspondences.

Let us assume now that A_t is defined over a number field $L \supset Y$ and $\mathfrak{p}'$ a place of L over $\mathfrak{p}$. We assume that A_t has a good ordinary reduction at $\mathfrak{p}'$; tilde will mean this reduction. Let $\tilde{e}(\mathfrak{p}) : \tilde{A}_t \to \tilde{A}_t$ be the reduction of $e(\mathfrak{p})$ ($e(\mathfrak{p})$ is defined in the beginning of (4.3)) and $\tilde{A}_t \overset{\tilde{e}(\mathfrak{p})_n}{\to} \tilde{A}_t' \overset{\tilde{e}(\mathfrak{p})_s}{\to} \tilde{A}_t$ its decomposition on purely non-separable and separable parts. Since the action of $e(\mathfrak{p})$ on $T_0(A_t)$ is given by a matrix diag $(\mathfrak{p}, \mathfrak{p}, \mathfrak{p}, \bar{\mathfrak{p}})$ we see that dim Ker $T_0(\tilde{e}(\mathfrak{p})) = 3$ and hence dim Ker $\tilde{e}(\mathfrak{p})_n = 3$. This means that there exists a distinguished subspace $F \subset B$, dim $F = 3$ such that $\tilde{F} =$ Ker $\tilde{e}(\mathfrak{p})_n$ in the obvious sense. (I am grateful to B.Edixhoven for an explanation of ideas above).

This means that we have the following formulas for reductions of $T_{\mathfrak{p},i}$:

$$\tilde{T}_{\mathfrak{p},i} = \Phi_{i,1} + \Phi_{i,2} \tag{4.4.1}$$

where $\Phi_{i,j}$ are defined as follows:

$$\Phi_{i,1}(\tilde{t}) = \{s \in \tilde{T}_{\mathfrak{p},i}(\tilde{t}) | \text{dim } (v_s \cap F) = i-1\};$$

$$\Phi_{i,2}(\tilde{t}) = \{s \in \tilde{T}_{\mathfrak{p},i}(\tilde{t}) | \text{dim } (v_s \cap F) = i\} \text{ (i.e. } v_s \subset F)$$

Particular cases: $\Phi_{3,2}(\tilde{t}) = \text{fr } (\tilde{t})$, i.e. $\Phi_{3,2}$ is the Frobenius map (considered as a correspondence). Analogously, $\Phi_{1,1}$ is the dual correspondence fr $'$. Analogs of formulas (4.4.1) and (4.4.2) below for a Siegel modular threefold are given in [Sh2], Theorem 6.

We have the following table of degrees of these correspondences:

i	$\Phi_{i,1}$	$\Phi_{i,2}$
1	$(p^3, \ 1)$	$(p^2+p+1, \ p(p^2+p+1))$
2	$(p^2(p^2+p+1), \ p^2+p+1)$	$(p^2+p+1, \ p^2(p^2+p+1))$
3	$(p(p^2+p+1), \ p^2+p+1)$	$(1, \ p^3)$

(2 numbers are degrees of 2 projections of $\Gamma(\Phi_{i,j})$ on $\tilde{X}$). In all cases the p-power multiplier is the degree of the non-separable part of the correspondence, and the non-p-power multiplier is the one of its separable part.

Considering cosets that correspond to $\Phi_{i,j}$ it is easy to find the following relations between $\Phi_{i,j}$:

$$\Phi_{1,1}\Phi_{i,2} = p^i \Phi_{i+1,1} \quad (i < 3); \quad \Phi_{1,1}\Phi_{3,2} = p^3 \tag{4.4.2}$$

Remark 4.4.3. When we consider $\tilde{T}_{\mathfrak{p},i}$ in (4.4.1) as known variables and $\Phi_{i,j}$ as unknown ones then (together with (4.4.2)) we get 6 equations with 6 unknowns;

a formal solution gives us certainly the equation (4.2.3.4) for Frobenius. Analogs of formulas (4.4.1) and (4.4.2) and equality of polynomials are true for Picard modular varieties of any dimension. A similar way of finding polynomial satisfied by Frobenius over the ring generated by Hecke correspondences for Siegel modular varieties of any genus is given in [FCh], Ch.7.

Let us give a geometric description of the partition $\tilde{T}_{\mathfrak{p},i}(\tilde{t}) = \Phi_{i,1}(\tilde{t}) \cup \Phi_{i,2}(\tilde{t})$ for $i = 2$. A quadric fourfold $G(2,B)$ contains 2 families of projective planes that we denote by D_1 and D_2. If $A_1, A_2 \subset G(2,B)$ are 2 projective planes belonging to the same family then either $A_1 = A_2$ or $A_1 \cap A_2$ is one point; if A_1, A_2 belong to the different families then either $A_1 \cap A_2$ is a projective line or $A_1 \cap A_2$ is the empty set.

We have:

1) $\Phi_{2,2}(\tilde{t})$ is a projective plane belonging to D_1;

2) $\Phi_{2,1}(\tilde{t}) = \bigcup_{c \subset \Phi_{2,2}(\tilde{t})} (A_c - c)$ where c runs over the set of all projective lines in $\Phi_{2,2}(\tilde{t})$ (there is p^2+p+1 such lines) and A_c is the only projective plane of family D_2 such that $A_c \cap \Phi_{2,2}(\tilde{t}) = c$, hence $\#(A_c - c) = p^2$. At last,

(4.4.4) For $s \in (A_c - c)$ $\tilde{k}^{-1}(s)$ does not depend on s but only on c.

We have the Eichler-Shimura formula for V: $\tilde{T}_{p,V} = \text{fr}_{\ K} + \text{fr}\,'_{K}$. Since $\text{fr}_{\ K} = \text{fr}^{\ 2}_{\ \mathbb{Q}}$ we see that $\exists s_0 \in S_0$ (S_0 is defined in (4.3.1)) such that $\tilde{k}^{-1}(s_0) = \text{fr}^{\ 2}(\tilde{t})$, and

$$\forall s \in S_0 - s_0 \;\; \tilde{k}^{-1}(s) = \text{fr}^{\ -2}(\tilde{t}) \tag{4.4.5}$$

Since $\deg \text{fr}\,' = p^2$ we see that $\#S_0 = p^2 + 1$, i.e. S_0 is an ellipsoid.

Further, it is easy to see that $\Phi_{2,2}(\tilde{t}) \cap P^3 = s_0$ (comparing Ker $\alpha(T_0(\tilde{A}_t))$). For any projective line $c \subset \Phi_{2,2}(\tilde{t})$ we have: $A_c \cap P^3$ is one point. Really, $A_c \cap P^3 \subset S_0$ but S_0 does not contain lines.

If $c \not\ni s_0$ then $A_c \cap P^3 \neq s_0$ and $(A_c - c) \cap (S_0 - \{s_0\}) \neq \emptyset$, hence, according (4.4.4) and (4.4.5) we have

$$\forall s \in A_c - c \;\; \tilde{k}^{-1}(s) = \text{fr}^{\ -2}(\tilde{t}) \tag{4.4.6}$$

Lemma 4.4.7. $\forall i \in I \;\; \exists s \in \chi^{-1}(i)$ such that

$$\tilde{k}^{-1}(s) = \text{fr}^{\ -2}(\tilde{t}) \tag{4.4.8}$$

Proof. Let us take an arbitrary $c \subset \Phi_{2,2}(\tilde{t})$ such that $c \not\ni s_0$, and let us consider a line l joining points $c \cap P^4(i)$, $A_c \cap P^3$ (they are different, because $c \cap P^3 = \emptyset$). All points of l but $c \cap P^4(i)$, $A_c \cap P^3$ are in $\chi^{-1}(i) \cap (A_c - c)$ hence (4.4.6) implies (4.4.8) for them. ■

Lemma 4.4.9. $\forall i \in I$, $\forall s \in \chi^{-1}(i)$, $\forall t \in V_{p,i}$ $\exists h \in B_1(d)$ such that $t = \iota(s(h))$.

Proof. By definition of χ, $\forall i \in I$, $\forall t \in V_{p,i}$ $\exists s_0 \in \chi^{-1}(i)$ such that $t = \iota(s_0(h))$. According (4.4.4), $\exists g \in G_V$, $\gamma \in \Gamma$ such that $sgs_0^{-1} = \gamma$. Then $\gamma(s_0(h)) = s(g(h))$ and hence $t = \iota(s(g(h)))$, $g(h) \in B_1(d)$. ■

Further we assume that p is sufficiently large so V and X have a good reduction at all $\mathfrak{p}, \bar{\mathfrak{p}}$. We denote the reduction modulo $\mathfrak{p}$ by $\text{red}_{\,p}$ or by tilde if the place is clear. Curves $V_{p,q,j}$ have a bad reduction at $\mathfrak{p}$, and $\tilde{V}_*$ or $\text{red}_{\,p}(V_*)$ ($* = \emptyset$, (p,j) or (p,q,j)) will mean below the set of points $\tilde{t} \in \tilde{X}$ for all $t \in V_*$.

Corollary 4.4.10. $\forall t \in V_{p,i}$ $\exists t' \in V$ such that $\tilde{t} = \text{fr}^{\,-2}(\tilde{t}')$, and hence $\forall i \in I$ $\tilde{V}_{p,i} = \tilde{V}$ ■

Proposition 4.4.11. $\forall j \in I_q$ $\text{red}_{\,p}(V_{p,q,j}) = \text{red}_{\,p}(V_{q,j})$

Proof. Follows immediately from Corollary 4.4.10. ■

Remark 4.4.12. We have also $\forall j \in I_p, \forall i \in \psi^{-1}(j)$ $\text{red}_{\,q}(V_{p,q,i}) = \text{red}_{\,q}(V_{p,j})$; this follows from 4.3.7. ■

4.5. How to transform Heegner curves into cycles in $C^2(X)_0$.

To construct an analog of Euler systems for X, we must apply the Abel-Jacobi map to cycles in $CH^2(X \otimes K^\bullet)_0$ with supports in Heegner curves and (may be) curves at infinity. A way to construct an element of $CH^2(X \otimes K^\bullet)_0$ such that its Abel-Jacobi image is defined canonically up to a scalar multiplier starting from Heegner curves is the following (the similar way was used in [KL]). We denote $r = \text{rank}(CH^2(X)/CH^2(X)_0)$. Let m be a place of Y, T_m the Hecke operator on X and $Q_m(Z) = \sum_{j=0}^r b_{m,j} Z^j$ the characteristic polynomial of the action of T_m on $CH^2(X)/CH^2(X)_0$, Z is an independent variable. We denote

$$\phi_m(V) \stackrel{\text{def}}{=} \sum_{j=0}^r b_{m,j} T_m^j(V)$$

Then $\phi_m(V) \in CH^2(X \otimes YK)_0$ and $\text{cl}'_E(\phi_m(V)) \in H^1(YK, E)$ is defined. We denote the eigenvalue of T_m on E by a_m, i.e. $a_m = i(T_m)$.

Lemma 4.5.1. For different m $\text{cl}'_E(\phi_m(V))$ are proportional.

Proof. We calculate the double sum in 2 different orders:

$$\text{cl}'_E(\sum_{j_1,j_2=0}^r b_{m_1,j_1} b_{m_2,j_2} T_{m_1}^{j_1} T_{m_2}^{j_2}(V)) = (\sum_{j=0}^r b_{m_1,j} a_{m_1}^j)\text{cl}'_E(\phi_{m_2}(V));$$

$$\text{cl}'_E(\sum_{j_1,j_2=0}^r b_{m_1,j_1} b_{m_2,j_2} T_{m_1}^{j_1} T_{m_2}^{j_2}(V)) = (\sum_{j=0}^r b_{m_2,j} a_{m_2}^j)\text{cl}'_E(\phi_{m_1}(V)) \text{ ■}$$

Analogously, we define

$$\phi_m(V_\bullet) \stackrel{\text{def}}{=} \sum_{j=0}^r b_{m,j} T_m^j(V_\bullet)$$

At last, we denote

$$y = \text{cl}\,'_{E,M}(\phi_m(V)) \in H^1(YK, E/M);$$

$$y_{q,j} = \text{cl}\,'_{E,M}(\phi_m(V_{q,j})) \in H^1(YK, E/M);$$

$$y_{p,q,j} = \text{ cl }'_{E,M}(\phi_m(V_{p,q,j})) \in H^1(YK^{p,q}, E/M)$$

Remark 4.5.2. For the case of ordinary modular curves we have $r=1$, $Q_m(Z) = Z-(m+1)$ and $\phi_m(z) = (a_m-(m+1))y$. Since orders of growth of a_m and $m+1$ are different we see that for the case of curves $\phi_m(z)$ is not 0 if y is not of torsion. This example shows that the construction above is reasonable. Moreover, it is assumed that

(4.5.3) The order of growth of $b_{m,j}$ and a_m is such that $\sum_{j=0}^r b_{m,j}a_m^j$ tends to infinity.

If so then we have the following elementary

Lemma 4.5.4. Let $V_0 = \sum_{i\in I} c_i V_i \in CH^2(X)_0$ be a linear combination of Shimura curves on X such that $\text{cl}'_E(V_0)\neq 0$. Then $\exists i\in I$ such that $\text{cl}'_E(\phi_m(V_i))\neq 0$.

Proof. $\sum_{i\in I} c_i \text{ cl }'_E(\phi_m(V_i)) = (\sum_{j=0}^r b_{m,j}a_m^j) \text{ cl }'_E(V_0)$. ■

This means that the ϕ_m-construction of cycles that are homologically equivalent to 0 is not worse than any other one.

5. The proof.

5.1. Image of $\rho_{\mathbb{Q}}$ and a $\mathbb{Q}$-structure on E.

The pairing in etale cohomology groups induces the Weil pairing

$$P(.,.) = [.,.] : E/M \otimes E/M \to \mathbb{Z}/M(1) \tag{5.1.1}$$

As it was mentioned in (1.5.2.2), we give a detailed proof for the case when P is non-degenerate on E. The case when P is 0 on E is considered in Sections 5.3′, 5.4′; changements of the proof for this case are non-significant.

Pairing P defines a group $GSp(E) = GSp_4(\mathbb{Z}_l)$. According the assumption (1.5.2), the image of the Galois representation $\rho_l : \text{Gal }(YK) \to GSp_4(\mathbb{Z}_l)$ is an open subgroup in $GSp_4(\mathbb{Z}_l)$ and is equal to this group for almost all l.

Let $\lambda = \{\lambda_1, .., \lambda_4\}$ be eigenvalues of $\rho_l(\text{fr }(\mathfrak{p}))$, i.e. $p^{\frac{k(k-5)}{2}} a_{\mathfrak{p},k} = s_i(\lambda)$, where s_i is the i-th symmetric polynomial. We have $\lambda_i\lambda_{2+i} = p^{-1}$, because of (5.1.1), hence $a_{\mathfrak{p},1} = a_{\mathfrak{p},3}$ (a is the eigenvalue of Hecke operator on E). But $T_{\mathfrak{p},k} = T_{\bar{\mathfrak{p}},n-k}$, hence

$$CHP(\text{fr }(\mathfrak{p})) = CHP(\text{fr }(\bar{\mathfrak{p}})) \tag{5.1.2}$$

(CHP is the characteristic polynomial).

Let X^τ, E^τ be the conjugate objects, τ is the complex conjugation. (5.1.2) means that $L(\rho, s) = L(\rho^\tau, s)$ up to maybe bad factors.

It is known that (5.1.3), (5.1.4) below are true[2]:

(5.1.3). E is isogenous to E^τ.

We denote an isogeny $E\to E^\tau$ by ϕ.

(5.1.4) $\phi^\tau \circ \phi = id$, i.e. ϕ defines a $\mathbb{Q}$-structure on E.

Further, we assume

[2] I am grateful to D.Blasius who confirmed me the truth of these propositions.

(5.1.5) $\phi(y) = \tau(y)$, i.e. $y \in H^1(YK, E)^+$ with respect to the $\mathbb{Q}$-structure on E defined by ϕ, τ.

Remark 5.1.6. Assumption (5.1.5) is not essential: if $\phi(y) \neq \pm\tau(y)$ then we can replace y by $y+\phi^{-1}\circ\tau(y)$; if $\phi(y) = -\tau(y)$ then we replace ϕ by $-\phi$, i.e. we replace a $\mathbb{Q}$-structure on E.

So, we fix a $\mathbb{Q}$-structure on E defined by ϕ, and we extend ρ_l on Gal ($\mathbb{Q}$), i.e. $\rho_l = \rho_{l,\mathbb{Q}}$ is a map from Gal ($\mathbb{Q}$) to $GSp(E)$.

5.2. Analog of the end of [K1].

5.2.1. We assume for simplicity that ρ_l : Gal $(K) \to GSp(E)$ is an epimorphism. According (1.5.2), this is true for almost all l; for remaining l the proof will be slightly more difficult, like in [K1].

5.2.2. Remember that $M = l^n$ is fixed. Let $\mathcal{V}_{\mathbb{Q},a}$ be a Galois extension of $\mathbb{Q}$ such that the corresponding Galois group Gal$(\mathcal{V}_{\mathbb{Q},a})$ is the maximal subgroup of Gal($\mathbb{Q}$) that acts trivially on E/l^a, and $\mathcal{V}_a$ the composite field $\mathcal{V}_{\mathbb{Q},a}K$. We need only cases $a = n$ and $a = 2n$; we shall omit subscript a if $a = n$. (5.2.1) implies that $\mathcal{V}_{\mathbb{Q}}$ and K are disjoint, and Gal $(\mathcal{V}_{\mathbb{Q}}/\mathbb{Q})$ = Gal $(\mathcal{V}/K) = GSp(E/M)$.

We choose a basis e_1, e_2, e_3, e_4 of E/M such that the matrix of Weil pairing in it is J_4 (we assume for simplicity that there is no polarization), and we identify $GSp(E/M)$ with $GSp_4(\mathbb{Z}/M)$ using this basis.

5.2.2.1. We denote by σ the non-trivial element of Gal $(K/\mathbb{Q})$ = Gal (YK/Y) = Gal $(\mathcal{V}/\mathcal{V}_{\mathbb{Q}})$ and by α an element diag$(1, 1, -1, -1) \in GSp_4(\mathbb{Z}/M) = GSp(E/M)$ = Gal $(\mathcal{V}_{\mathbb{Q}}/\mathbb{Q})$ = Gal $(\mathcal{V}/K)$.

We have (like in Remark 5.1.6 above) either $\sigma(y) = -y$ (case of rank 0), or $\sigma(y) = y$ (case of rank 1), or $\sigma(y) \neq \pm y$. We assume in the present paper that $\sigma(y) = -y$. A condition $\sigma(y) \neq \pm y$ leads to a contradiction: we replace y by $y - \sigma(y)$ so we have case of rank 0; this means that $y + \sigma(y)$ must be 0.

Remark 5.2.3. It is interesting to find a relation between $\varepsilon = \frac{\sigma(y)}{y}$ and the eigenvalue of Fricke involution on E, as well as to prove that the sign of the functional equation of $L(E, K, s)$ is $-\varepsilon$.

We assume for simplicity that all “unpleasant multipliers” that appear in [K1] (like C in (5.3.11) below) are 1, i.e. we shall prove that SH = 1.

Now we fix an element $y_1 \in S_M(\mathbb{Q}, E)$ for which we shall prove that it is 0, and we denote $y = y_2$, $y_i \in H^1(K, E/M)$. We consider restrictions of y_i $(i = 1, 2)$ on $H^1(\mathcal{V}, E/M)$ = Hom (Gal $(\mathcal{V}), E/M)$, these restrictions will be denoted by y_i as well, so y_i can be considered as a map Gal $(\mathcal{V}) \to E/M$. The restriction map $H^1(K, E/M) \to H^1(\mathcal{V}, E/M)$ is an isomorphism (it is proved like in [Gr], (9.1)), hence we shall prove that $y_1 \in H^1(\mathcal{V}, E/M)$ is 0.

Let $W_i \supset \mathcal{V}$ be an extension that corresponds to Ker y_i, and $W = W(y_1, y_2) \supset \mathcal{V}$ be the composite field of W_1, W_2, i.e. an extension that corresponds to $\bigcap_{i=1}^{2}$ Ker y_i. We can consider y_i as homomorphisms from Gal $(W_i/\mathcal{V})$ to E/M, they are injective by definition of W_i.

Lemma 5.2.4. Both W_i/Y (and hence W/Y) are Galois extensions. ■

The group Gal $(\mathcal{V}/Y)$ acts on both Gal $(W_i/\mathcal{V})$. Particularly, we have an action of σ and $GSp_4(\mathbb{Z}/M)$ on Gal $(W_i/\mathcal{V})$.

Lemma 5.2.5.
(a) Both y_i : Gal $(W_i/\mathcal{V}) \to E/M$ are $GSp_4(\mathbb{Z}/M)$-homomorphisms.
(b) $\sigma(h) = h$ for $h \in$ Gal $(W_1/\mathcal{V})$, $\sigma(h) = h^{-1}$ for $h \in$ Gal $(W_2/\mathcal{V})$.

Proof. (a) Because $y_i \in H^1(K, E/M)$. (b) By definition of the action of σ we have $(\sigma(y_i))(h) = \sigma(y_i(\sigma h \sigma^{-1}))$, $h \in$ Gal $(W_i/\mathcal{V})$. σ acts trivially on E/M and hence on $y_i(\sigma h \sigma^{-1}) \in E/M$. Since $\sigma(y_1) = y_1$, $\sigma(y_2) = -y_2$ and maps y_i are inclusions we get the result immediately. ■

Lemma 5.2.6. $\exists n_i$ $(i = 1, 2)$ such that im $y_i = l^{n_i} E/M$.

Proof. Since y_i : Gal $(W_i/\mathcal{V}) \to E/M$ are $GSp_4(\mathbb{Z}/M)$-homomorphisms im y_i are $GSp_4(\mathbb{Z}/M)$-stable subgroups of E/M. But $l^n E/M$ are the only $GSp_4(\mathbb{Z}/M)$-stable subgroups in E/M. ■

Lemma 5.2.7. $n_2 = 0$.

Proof. Because y_2 is not a multiple of any element of $E(\mathbb{Q})$. ■

Lemma 5.2.8. $W_1/\mathcal{V}$, $W_2/\mathcal{V}$ are linearly disjoint extensions.

Proof. If not then $W_1 \cap W_2 \neq \mathcal{V}$. Let h be a non-trivial element of Gal $(W_1 \cap W_2/\mathcal{V})$. We have $\sigma(h) = h = -h$: a contradiction, because $l \neq 2$. ■

Corollary 5.2.9. $\exists h \in$ Gal $(W/\mathcal{V})$ such that $y_1(h) = l^{n_1} e_1$, $y_2(h) = e_3$. ■

Lemma 5.2.10. There exist commuting lifts of the second order of both σ, α on Gal $(W/\mathbb{Q})$.

Proof. It is sufficient to prove existence of these lifts on both Gal $(W_i/\mathbb{Q})$. We have an exact sequence $0 \to$ Gal $(W_i/\mathcal{V}) \to$ Gal $(W_i/\mathbb{Q}) \to$ Gal $(\mathcal{V}/\mathbb{Q}) \to 0$, and Lemma 5.6, b describes the action of Gal $(\mathcal{V}/\mathbb{Q})$ on Gal $(W_i/\mathcal{V})$. So, this lemma is reduced to a question of abstract group theory, and it is easily solved. ■

We shall keep notations σ, α for these lifts, and we shall fix an element h of Corollary 5.2.9.

Corollary 5.2.11. $y_1((\sigma\alpha h)^2) = 2l^{n_1} e_1$, $y_2((\sigma\alpha h)^2) = 2e_3$.
Proof. Follows immediately from Lemma 5.2.5 (b). ■

5.3. Construction of Euler systems.

We need the following
Lemma 5.3.1. $\mathcal{V}_{2n}$ and W are linearly disjoint over $\mathcal{V}$ ($\mathcal{V}_{2n}$ is defined in (5.2.2)).

Proof. For each finite subset $C \subset$ Hom (Gal $(\mathcal{V}), E/M)$ we consider (following [Gr]) an extension $W(C) \supset \mathcal{V}$ that corresponds to a subgroup $H(C) = \bigcap_{h \in C}$ Ker $h \subset$ Gal $(\mathcal{V})$. For example, $W = W(< y_i >)$ where $< y_i >$ is a subgroup generated by y_1, y_2. To find C_0 such that $\mathcal{V}_{2n} = W(C_0)$ we consider an isomorphism $\gamma : E/M \to ME/M^2E$ induced by multiplication by M. For each $x \in E/M$ let $\phi_x \in$ Hom (Gal $(\mathcal{V}), E/M)$ be defined as follows: $\phi_x(g) = \gamma^{-1}(g(x) - x)$. Here

$g \in \text{Gal}\ (\mathcal{V})$, hence $g(x) - x \in ME$, and we consider the projection of $g(x) - x$ in ME/M^2E. It is clear that $C_0 = \{\phi_x\}$, $x \in E/M$.

It is sufficient to show that $H(< y_i >) \times H(C_0) = \text{Gal}\ (\mathcal{V})$, or that $< y_i > \cap C_0 = 0$ in Hom (Gal $(\mathcal{V}), E/M)$. If $x \in < y_i > \cap C_0$ then we can assume that $lx = 0$. We have $\dim_{\mathbb{F}_l} GSp_4(\mathbb{Z}/M)(x) \leq 2$ because $x \in < y_i >$ and $\dim_{\mathbb{F}_l} GSp_4(\mathbb{Z}/M)(x) = 4$ because $x \in (C_0)_l$ - a contradiction. ■

5.3.2. Let p be a prime such that it splits in $Y/\mathbb{Q}$: $p = \mathfrak{p}_1\bar{\mathfrak{p}}_1$ and such that

5.3.2.1. $\text{fr}_{W/\mathbb{Q}}(p) = \sigma\alpha h$, h of Corollary 5.2.9;

5.3.2.2. $\text{fr}_{\mathcal{V}_{2n}/\mathbb{Q}}(p) = \sigma\ \text{diag}\ (\lambda_1, .., \lambda_4)$, where $\lambda_1 = \lambda_2 = 1 + (a+b)M$, $\lambda_3 = \lambda_4 = -1 + bM$, $a, b \in \mathbb{Z}/M$ are arbitrary numbers satisfying $a, b \not\equiv 0 \mod l$.

5.3.2.3. $\exists q$ such that p, q satisfy (3.7.1), (3.7.2).

The meaning of (5.3.2.2) is suggested by (5.3.18), (5.3.22). Lemma 5.3.1 shows that it is possible to choose p satisfying (5.3.2.1), (5.3.2.2). Since for almost all l $\mathcal{V}_{2n}W$ and $\mathbb{Q}(\mu_{d+1})$ are linearly disjoint (μ_{d+1} is a root of unity) then (3.7.1) also can be satisfied. Unfortunately (Remark 3.7.3)) we can only conjecture that (3.7.2) also can be satisfied. We assume it.

Corollary 5.3.3. p is inert in $K/\mathbb{Q}$, $\mathfrak{p}_1$ is inert in YK/Y and splits completely in $\mathcal{V}/YK$. ■

Proposition 5.3.4 (congruence relations).

1) $p \equiv -1 \pmod{M}$;

2)$a_p \equiv 2 \pmod{M}$ and moreover

3) $p \equiv -1 + aM$, $a_p \equiv 2 - 4aM$, $a_p - (p^2+1) \equiv -2aM \pmod{M^2}$

Proof. (5.3.2.2) implies that the characteristic polynomial of fr_p given in (4.2.3.5) is equal to $\prod_{i=1}^4 (Z - \lambda_i) \pmod{M^2}$, λ_i of 5.3.2.2. This gives us immediately the desired.

Really, let s_i be the i-th symmetric polynomial, $\lambda = \lambda_1\lambda_3 = \lambda_2\lambda_4$. Then (like in (5.1)) $s_3 = \lambda s_1$, hence $\lambda = p^{-1}$ and $p \equiv -1 + aM$. Further, $s_2 = 2\lambda + (\lambda_1 + \lambda_3)(\lambda_2 + \lambda_4) \equiv 2\lambda$ and $a_p = p^3 s_2 \equiv 2p^2 \equiv 2 - 4aM$, all congruences modulo M^2. ■

Now we need to show that Hecke correspondences commute with Abel-Jacobi map.

Lemma 5.3.5. Let $\phi : Y \to X$ be a surjective map of algebraic varieties of the same dimension, $W \in CH^r(Y)_0$, $V \in CH^r(X)_0$ be cycles (we consider representatives of the corresponding elements of Chow groups) such that for all irreducible components W_i of W $\deg(\phi|_{W_i})$ is the same. Then

$$H(\phi)^{-1}(\text{ cl }'_X(V)) = \text{ cl }'_Y(\phi^{-1}(V))$$
$$H(\phi)(\text{ cl }'_Y(W)) = \deg(\phi|_{W_i})\text{ cl }'_X(\phi(W))$$

where $H(\phi)$ is a map in Galois cohomology groups induced by ϕ. ■

Let now T be a correspondence on X, Y be a graph of T and $\alpha : Y \to X$, $\beta : Y \to X$ projections such that $T = \beta \times \alpha^{-1}$. Let $V \in CH^r(X)_0$ and $W = \alpha^{-1}(V)$, $W \in CH^r(Y)_0$, $W = \cup_i W_i$ be as in 5.3.5 above. Then 5.3.5 implies

$$H(T)(\text{ cl }'_X(V)) = \deg(\beta|_{W_i})\text{ cl }'_X(T(V)) \tag{5.3.6}$$

To formulate the property that the Abel-Jacobi map commutes with reductions, we need the following objects. Let X be an algebraic variety over a local field K whose residue field is k, $\tilde{X}$ its good reduction, $V \in CH^r(X)_0(K)$ a cycle (i.e. a representative of an element of $CH^r(X)_0(K)$), $V = \sum \alpha_i V_i$ where V_i are irreducible subvarieties. Let the type of (bad) reduction of all V_i be the same; we denote the cycle $\sum \alpha_i \operatorname{Supp} \tilde{V}_i$ by $\tilde{V}$. We have an isomorphism $H^1(K^{nr}/K, H^{2r-1}(X, Z_l(r))) \to H^1(k, H^{2r-1}(\tilde{X}, Z_l(r)))$ that we denote by tilde as well. Since $\mathrm{cl}\,'(V) \in H^1(K^{nr}/K, H^{2r-1}(X, Z_l(r)))$ an element $\widetilde{\mathrm{cl}\,'(V)} \in H^1(k, H^{2r-1}(\tilde{X}, Z_l(r)))$ is meaningful.

Lemma 5.3.7. In notations and assumptions above $\tilde{V} \in CH^r(\tilde{X})_0(k)$, and

$$c\,\mathrm{cl}\,'(\tilde{V}) = \widetilde{\mathrm{cl}\,'(V)}$$

where c depends only on the type of reduction of V_i. ■

Proposition 5.3.8.

1) $a_q y_2 = (q^2+1)y_2 + C_q \sum_{j \in I_q} y_{q,j}$;
2) $\forall j \in I_q$ $a_p y_{q,j} = (p^2+1)y_{q,j} + C_p \mathrm{Tr}_{\,K^{p,q}/K}(y_{p,q,j})$;
3) $\forall j \in I_q$ $\tilde{y}_{p,q,j} = c_p \tilde{y}_{q,j}$

Here c_p is defined by the type of reduction of $V_{p,i}$, $C_p = C_{p,i} = 1$, $C_q = C_{q,i} = 1$ are defined in 4.3.5, a_p, a_q are Hecke eigenvalues on E.

Proof. Follows immediately from (4.3.6), (4.4.11), definition of $y_\bullet$ in (4.5) and (5.3.6), (5.3.7). ■

5.3.9. As it was mentioned in (1.2), Step 7, the below proof is given under a non-real assumption (1.2.3). This means that we shall deal with elements $y_\bullet \in H^1(K^\bullet, E/M)$ as with elements of (a non-existing) abelian variety E, namely we assume that $y_2 \in E(K)$, $y_{q,j} \in E(K)$, $y_{p,q,j} \in E(K^{p,q})$. In (5.6) there are 2 lemmas that show how to translate propositions below to the right language.

(5.3.10) Firstly, we define $c_1 \in H^1(K, E/M)$ as an image of y_2 in the inclusion $E(K)/M \to H^1(K, E/M)$ (hence c_1 is the *real* y_2, because *only* this $c_1 = y_2$ exists)!

To define $c_{p,q}$ we use a method of [Gr], Section 4. Let g be a fixed generator of $\mathrm{Gal}(K^{p,q}/K)$,

$$D_{p,q} = C_p C_q \sum_{j \in I_q} \sum_{\gamma=1}^{p} \gamma g^\gamma y_{p,q,j}$$

(in [Gr] a notation P_n is used instead of $D_{p,q}$). We have $D_{p,q} \in E(K^{p,q})$ and (taking into consideration (5.3.8), (1), (2))

$$g(D_{p,q}) - D_{p,q} = C_p C_q (p+1) \sum_{j \in I_q} y_{p,q,j} - C_p C_q \sum_{j \in I_q} \sum_{\gamma=1}^{p} g^\gamma y_{p,q,j}$$

$$= C_p C_q (p+1) \sum_{j \in I_q} y_{p,q,j} - [a_p - (p^2+1)][a_q - (q^2+1)]y_2,$$

i.e. $g(D_{p,q}) - D_{p,q} \in ME(K^{pq})$, because of (5.3.4). (5.2.1) implies that $E(K^{pq})/M = 0$ (analogously to [Gr], Lemma 4.3). This means that we can define (like in [Gr], Section 4) an element $c_{p,q} \in H^1(K, E/M)$ using $D_{p,q}$.

Like in [K1] we can prove that $\exists C \neq 0$ such that

$$C\mathrm{loc}_r(c_{p,q}) \in H^1_f(K_r, E/M) \tag{5.3.11}$$

for all places r but p, q. Here $C = \prod_r C_r$, where $C_r \neq 1$ only for $r|N$. Further we assume that $C = 1$, this is not essential.

The Weil pairing (5.1.1) induces the Tate pairing

$$< .,. >: H^1(K, E/M) \otimes H^1(K, E/M) \to \mathrm{Br}(K)_M$$

and (5.3.11) implies (like in [K1]) that

$$< \mathrm{loc}_p(y_1), \mathrm{loc}_p(c_{p,q}) > + < \mathrm{loc}_q(y_1), \mathrm{loc}_q(c_{p,q}) >= 0 \tag{5.3.12}$$

Propositions 5.3.13, 5.3.14 below show us that it is possible always to choose such q that the corresponding member is 0.

Proposition 5.3.13. Let q be an arbitrary prime satisfying the following conditions:

5.3.13.1) q is inert in $K/\mathbb{Q}$ and splits in $Y/\mathbb{Q}$;
5.3.13.2) $(\dim\ (\mathcal{V}_q/K_q), l) = 1$;
5.3.13.3) $\mathcal{V}_q = (W_1)_q$.
Then $\mathrm{loc}\ _q(y_1) = 0$.

Proof. There is an exact sequence

$$0 \to H^1((\mathcal{V}_q/K_q), E/M) \to H^1(K_q, E/M) \to H^1(\mathcal{V}_q, E/M)$$

Since $(\dim\ (\mathcal{V}_q/K_q), l) = 1$ we have that $H^1((\mathcal{V}_q/K_q), E/M) = 0$. Since $\mathcal{V}_q = (W_1)_q$ we have that $\mathrm{Res}\ ^{\mathcal{V}_q}_{\mathbb{Q}}(y_1) = 0$ and hence $\mathrm{Res}\ ^{K_q}_{\mathbb{Q}}(y_1) = 0$. ∎

Proposition 5.3.14. For a given p there exists infinitely many q satisfying the following conditions:

5.3.14.1) $q \equiv -1 \pmod{p+1}$ (i.e. p, q satisfy 3.7);
5.3.14.2) $(a_q - 2, l) = 1$;
5.3.14.3) q satisfies conditions of Proposition 5.3.13.
5.3.14.4) p, q satisfy (3.7.1), (3.7.2).

Proof. As usual, we construct a Galois extension of $\mathbb{Q}$ and we apply the Chebotarev density theorem to an element g of this Galois group. Namely, we have field extensions ($\mu_\bullet$ are roots of unity):

$$\begin{array}{ccccccccc} & & & & K(\mu_{M}) & \subset & K(\mu_{p+1}) & & \\ & & & & \| & & & & \\ \mathbb{Q} & \subset & K & \subset & K(\mu_{M}) & \subset & \mathcal{V} & \subset & W_1 \end{array}$$

It is possible to show that W_1 and $K(\mu_{p+1})$ are linearly disjoint over $K(\mu_{M})$.

Let $g \in$ Gal $(W_1K(\mu_{p+1})/\mathbb{Q})$, g belongs to the conjugacy class fr (q), q of the statement of the Proposition. Conditions of propositions 5.3.13, 5.3.14 (1 - 3) are reformulated in terms of g as follows (we neglect (5.3.14.4), see end of (5.3.2) and (3.7.3)):

5.3.13.1') $g = \sigma g_K$, where $g_K \in$ Gal $(W_1K(\mu_{p+1})/K)$.

We denote $g_K|_{\text{Gal }(\mathcal{V}/K)}$ by g_1.

5.3.13.2') (ord $(g_1), l) = 1$.

5.3.13.3') ord $(g_K) =$ ord (g_1)

5.3.14.1') $g|_{\text{Gal }(K(\mu_{p+1})/K)} = \tau$, where τ is the complex conjugation;

5.3.14.2') Let $\sum_{i=0}^{4} b_i Z^i$ be the characteristic polynomial of g_1, we identify here Gal $(\mathcal{V}/K)$ with $GSp_4(\mathbb{Z}/M)$, Z is an independent variable. Then $(b_2+2, l) = 1$.

Really, (5.3.14.2') is equivalent to (5.3.14.2) because $b_2 = q^{-3}a_q$ and (5.3.14.1) implies that $q \equiv -1 \pmod M$.

Considering g_1 as an element of $GSp_4(\mathbb{Z}/M)$ we see that properties (5.3.13.2'), a restriction of (5.3.14.1') on $K(\mu_{_M})$ and (5.3.14.2') are formulated in terms of $g_1 \in GSp_4(\mathbb{Z}/M)$, and it is easy to find g_1 satisfying them. For example, we can take $g_1 =$ diag $(\lambda_1, .., \lambda_4)$, where $\lambda_i \in \mathbb{Z}/M$, ord $(\lambda_i) = l-1$, $\lambda_1\lambda_3 = \lambda_2\lambda_4 = -1$, $((\lambda_1+\lambda_3), l) = ((\lambda_2+\lambda_4), l) = 1$; ord $(g_1) = l-1$. (5.3.14.2') is satisfied because $b_2 = \lambda_1\lambda_3 + \lambda_2\lambda_4 + (\lambda_1+\lambda_3)(\lambda_2+\lambda_4)$.

Further, we have an exact sequence

$$0 \to \text{Gal }(W_1/\mathcal{V}) \to \text{Gal }(W_1/K) \to \text{Gal }(\mathcal{V}/K) \to 0$$

Since Gal $(W_1/\mathcal{V})$ is an l-group there exists a lift of g_1 in Gal (W_1/K) of order $l-1$ (we can take any lift of g_1 and replace it by its appropriate power if necessary). At last, linear disjointness of W_1 and $K(\mu_{p+1})$ immediately implies the existence of g_K. ■

This means that (5.3.12) can be replaced by

$$< \text{loc}_p(y_1), \text{loc}_p(c_{p,q}) >= 0 \tag{5.3.15}$$

Since $\text{Gal}(K_p)$ acts trivially on E/M then $H^1(K_p, E/M) = \text{Hom}(\text{Gal}^{\text{ab}}(K_p), E/M)$ and we have the following formula for the Tate pairing (we consider elements of $H^1(K_p, E/M)$ as group homomorphisms):

(5.3.16) If $a \in H^1_f(K_p, E/M), b \in H^1(K_p, E/M)$ then

$$< a, b >= [a(\text{fr }_{K_p}), b(g)]$$

(via an isomorphism $\mu_M \to \text{Br}(K_p)_M$ depending on g).

We apply this formula to the case $a = \text{loc }_p(y_1)$, $b = \text{loc }_p(c_{p,q})$, hence we have to find loc $_p(c_{p,q})(g)$, tilde will mean here the reduction at p.

5.3.17.We denote $B = \frac{1}{M}(g(D_{p,q}) - D_{p,q}) \in E(K^{p,q})$ (the only value, because of $E(K^{pq})/M = 0$). We have loc $_p(c_{p,q})(g) = g(\frac{D_{p,q}}{M}) - \frac{D_{p,q}}{M} - B$ ([Gr], (4.6)). Since g is identical on reduction we have loc $_p(c_{p,q})(g) = -\tilde{B}$.

5.3.17. Using (5.3.8) we have the following calculation (here c_p of (5.3.8), (3)):

$$B = C_pC_q\frac{p+1}{M}\sum_{j\in I_q} y_{p,q,j} - \frac{a_p-(p^2+1)}{M}[a_q-(q^2+1)]y_2\ ;$$

$$\tilde{B} = C_p C_q \frac{p+1}{M} \sum_{j \in I_q} \tilde{y}_{p,q,j} - \frac{a_p - (p^2+1)}{M}[a_q - (q^2+1)]\tilde{y}_2$$

$$= C_p C_q c_p \frac{p+1}{M} \sum_{j \in I_q} \tilde{y}_{q,j} - \frac{a_p - (p^2+1)}{M}[a_q - (q^2+1)]\tilde{y}_2$$

$$= C_p c_p \frac{p+1}{M}[a_q - (q^2+1)]\tilde{y} - \frac{a_p - (p^2+1)}{M}[a_q - (q^2+1)]\tilde{y}_2$$

$$= [a_q - (q^2+1)] \frac{C_p c_p (p+1) - (a_p - (p^2+1))}{M} \tilde{y}_2)$$

So, we get an analog of the main property of Euler systems for our case:

$$\text{loc}_{\,p}(c_{p,q})(g) = C\tilde{y}_2 \tag{5.3.18}$$

where $C = [a_q - (q^2+1)]\frac{C_p c_p (p+1) - (a_p - (p^2+1))}{M}$.

Congruences (5.3.4.3) imply that $C_p c_p (p+1) - (a_p - (p^2+1)) \equiv C_p c_p + 2 \pmod{M^2}$, hence we must check that

$$C_p c_p \not\equiv -2 \pmod{l} \tag{5.3.19}$$

this will imply that $(C, l) = 1$.

I think that c_p is either 2 or $2(p^3+p)$ hence (because $C_p = 1$) (5.3.19) is true. If (5.3.19) is not true then see (5.4).

Remark 5.3.20. Let us remember that in K-case the main property of Euler systems (of order 1) is the following:

$$\text{loc}_{\,p}(c_p)(g) = -\text{fr}^{\,-1}(\text{loc}_{\,p}(c_1)(\text{fr}\,)) \tag{5.3.21}$$

To show that (5.3.18) is equivalent to (5.3.21) we use the following elementary

Lemma 5.3.22. Let E be an abelian variety of dimension 2 over a finite field $\mathbb{F}_m$ such that the matrix of fr mod M^2 is diag $(1+aM, 1+aM, -1+bM, -1+bM)$. Let $z \in E_M(\mathbb{F}_{m^2})^-$ and $z' \in H^1(\mathbb{F}_{m^2}, E_M)$ its image under the Kummer map. Then $z'(\text{fr}_{\,\mathbb{F}_{m^2}}) = -2bz$. ■

(5.3.18), (5.3.22) and a condition (5.3.2.2) on p imply that

$$\text{loc}_{\,p}(c_{p,q})(g) = C'\text{loc}_{\,p}(y)(\text{fr}_{\,K_p}) \tag{5.3.23}$$

where $C' \not\equiv 0 \mod l$ (the exact value of C' is not essential). Further, (5.3.15), (5.3.16) and (5.3.23) imply that

$$[\text{loc}_p(y_1)(\text{fr}_{\,K_p}), \text{loc}_p(y_2)(\text{fr}_{\,K_p})] = 1 \tag{5.3.24}$$

At last, we need the following

Lemma 5.3.25. $\forall a \in H^1(K, E/M)$ we have

$$\text{loc}_p(a)(\text{fr}_{\,K_p}) = \text{Res}\,{}^{\mathcal{V}}_{K}(a)((\text{fr}_{\,W(a)/\mathbb{Q}}(p))^2)$$

where $W(a)$ is defined in the proof of (5.3.1).

The proof follows immediately from definitions; it is contained in a non-explicit form in [K1], [Gr]. ∎

At last, combining 5.3.25 for $a = y_i$, 5.3.24, 5.3.2.1 and 5.2.11 we get immediately that $n_1 = n$ and hence the Theorem.

5.3$'$. Here we consider the case when the restriction of the pairing $P : H^3(\bar{X} \otimes \bar{\mathbb{Q}}, \mathbb{Z}_l(2)) \otimes H^3(\bar{X} \otimes \bar{\mathbb{Q}}, \mathbb{Z}_l(2)) \to \mathbb{Z}_l(1)$ on E is 0.

There exists a subspace $E' \subset H^3(\bar{X} \otimes \bar{\mathbb{Q}}, \mathbb{Z}_l(2))$ which is orthogonal to E with respect to P. We denote $E^I = E \oplus E'$, so the restriction of P on E^I is skew-symmetric and non-degenerate; E^I will play in this case the role of E above. We choose dual basises $e_1, \dots, e_4$ of E and $e'_1, \dots, e'_4$ of E', they form a basis of E^I, the matrix of P in this basis is (we can assume to be) J_8. Let ρ'_l, ρ^I_l be l-adic Galois representations of E', E^I respectively.

Lemma 5.3$'$.1. The image of $\rho^I_l : \mathrm{Gal}\ (Y) \to GL_8(\mathbb{Z}_l)$ in the basis $e_1, \dots, e'_4$ is contained in the group of matrices $\begin{pmatrix} A & 0 \\ 0 & c(A^t)^{-1} \end{pmatrix}$ where $A \in GL_4(\mathbb{Z}_l)$, and

$$c^2 = \det\ A \tag{5.3$'$.2}$$

Proof. Only (5.3$'$.2) must be proved. Let $g \in \mathrm{Gal}\ (Y)$, $g = \mathrm{fr}\ (\mathfrak{p})$ for a place $\mathfrak{p}$, and $\lambda = (\lambda_1, \dots, \lambda_4)$, $\lambda' = (\lambda'_1, \dots, \lambda'_4)$ be eigenvalues of $\rho_l(\mathrm{fr}\ (\mathfrak{p}))$, $\rho'_l(\mathrm{fr}\ (\mathfrak{p}))$ respectively. We have

$$\lambda_i \lambda'_i = p^{-1} \tag{5.3$'$.3}$$

because of existence of P. Since the characteristic polynomial of $\rho_l(\mathrm{fr}\ (\mathfrak{p}))$ (resp. $\rho'_l(\mathrm{fr}\ (\mathfrak{p}))$) is $Z^4 - p^{-2}a_{\mathfrak{p},1}Z^3 + p^{-3}a_{\mathfrak{p},2}Z^2 - p^{-3}a_{\mathfrak{p},3}Z + p^{-2}$ (resp. $Z^4 - p^{-2}a'_{\mathfrak{p},1}Z^3 + p^{-3}a'_{\mathfrak{p},2}Z^2 - p^{-3}a'_{\mathfrak{p},3}Z + p^{-2}$ where $a'_{p,k}$ are eigenvalues of $T_{\mathfrak{p},k}$ on E') we have $\prod_{i=1}^4 \lambda_i = \prod_{i=1}^4 \lambda'_i = p^{-2}$ that implies (5.3$'$.2) ∎

5.3$'$.4. We denote by G a subgroup of $GL_8(\mathbb{Z}_l)$ of all matrices $\begin{pmatrix} A & 0 \\ 0 & c(A^t)^{-1} \end{pmatrix}$ satisfying (5.3$'$.2), and we assume the truth of Serre's conjecture for this case. For simplicity we consider only the case when im $\rho^I_l = G$.

We have relations $\sigma_i(\lambda) = p^{\frac{i(i-5)}{2}} a_{\mathfrak{p},i}$ and hence (because of (5.3$'$.3)) $a_{\mathfrak{p},i} = a'_{\bar{\mathfrak{p}},i}$, i.e. E' and E^τ have the same local L-factors. Analogs of (5.1.3), (5.1.4) are true for this situation, i.e. there exists a map $\alpha : E' \to E^\tau$ that defines a $\mathbb{Q}$-structure on E^I. We assume the truth of an analog of (5.1.5), i.e. that $\sigma(y_2) = -y_2$, where $y_2 = (y, y') = \mathrm{cl}\ '_{E^I,M}(\phi_m(V)) \in H^1(YK, E^I/M)$. We can consider the l-adic representation map $\rho^I_l : \mathrm{Gal}\ (\mathbb{Q}) \to GL_8(\mathbb{Z}_l)$, we have $\rho^I_l(\tau) = \begin{pmatrix} 0 & A \\ A' & 0 \end{pmatrix}$ where both $A, A' \in GL_4(\mathbb{Z}_l)$.

Almost the whole contents of Sections 5.2, 5.3 remain valid for the present situation if we replace E by E^I. Namely, we consider an arbitrary element $y_1 \in S_M(\mathbb{Q}, E^I)$ for which we shall prove that it is 0, we define W_1, W_2 like in 5.2, and we consider inclusions $y_i : \mathrm{Gal}\ (W_i/\mathcal{V}) \to E^I/M$. An analog of an important lemma 5.2.6 remains valid by the same reason:

Lemma 5.3$'$.5. $\exists n_i$ $(i = 1, 2)$ such that im $y_i = l^{n_i} E^I/M$.

Proof. It is easy to check that the only G-invariant subspaces in E^I/M are $l^nE/M \oplus l^{n'}E'/M$ for some n, n'. Since im y_i is stable with respect to $\rho_l^I(\tau)$ we get immediately that $n = n'$. ■

Like in lemma 5.2.7 we have $n_2 = 0$. An analog of Corollary 5.2.9 is the following:

Corollary 5.3′.6. $\exists h \in$ Gal $(W/\mathcal{V})$ such that $y_1(h) = l^{n_1}e_1$, $y_2(h) = e_1'$. ■

We fix this h.

Now we define a matrix $\alpha \in GL_8(\mathbb{Z}/M^2)$ as follows:

$$\alpha = \text{ diag } (\lambda_1, \dots, \lambda_4, c\lambda_1^{-1}, \dots, c\lambda_4^{-1})$$

where $\lambda_i = \epsilon_i + a_iM$, $\epsilon_1 = \epsilon_2 = 1$, $\epsilon_3 = \epsilon_4 = -1$, $a_1, \dots, a_4 \in \mathbb{Z}/M$, $c = -1 - aM$ where $a = \frac{a_1+a_2-a_3-a_4}{2}$, and a_i satisfy $a_1 \neq 0$, $a \neq 0$ in $\mathbb{Z}/l$. We denote the image of α in $GL_8(\mathbb{Z}/M)$ $(=$ diag $(1, 1, -1, -1, -1, -1, 1, 1)$ $)$ by α as well; we have $\alpha \in G$.

Corollary 5.2.11 remains valid for this choice of α. Further, we choose p like in (5.3.2), more exactly, (5.3.2.1) remains unchanged and (5.3.2.2) is formulated as follows: fr $_{\mathcal{V}_{2n}/\mathbb{Q}}(p) = \sigma\alpha$ for α defined above.

An analog of Proposition 5.3.4 remains valid (for a defined above) as well as the whole contents of 5.3 below. Since $[e_1, e_1'] = \mu_M$ (5.3′.6) implies that $n_1 = n$ and hence the Theorem.

5.4. Case $C_pc_p \equiv -2 \pmod l$.

Here we show how to prove the theorem if (5.3.19) is not true. We consider firstly the case when the restriction of P on E is non-degenerate. In this case we replace the choice of α in (5.2.2.1) by the following choice:

$$\alpha = \text{ diag } (1, r, -1, -r^{-1}) \tag{5.4.1}$$

where $r \in (\mathbb{Z}/M)^*$ is an element of degree $l-1$, hence $r \neq \pm 1$ (here $l \neq 3$). We have the following analog of (5.2.10):

Lemma 5.4.2. There exist commuting lifts of σ, α on Gal $(W/\mathbb{Q})$ of orders 2, $l-1$ respectively. ■

and of (5.2.11):

Lemma 5.4.3. $y_1((\sigma\alpha h)^{l-1}) = (l-1)l^{n_1}e_1$, $y_2((\sigma\alpha h)^{l-1}) = (l-1)e_3$.

Proof. We have $(\sigma\alpha)^j(y_1) = y_1$, $(\sigma\alpha)^j(y_2) = (-1)^jy_2$, $(\sigma\alpha)^j(e_1) = e_1$, $(\sigma\alpha)^j(e_3) = (-1)^je_3$, hence $\forall j$ $y_1((\sigma\alpha)^j(h)) = l^{n_1}e_1$, $y_2((\sigma\alpha)^j(h)) = e_3$. Since $y_i((\sigma\alpha h)^{l-1}) = \sum_{j=0}^{l-2} y_j((\sigma\alpha)^j(h))$ we get immediately the desired. ■

Further, we replace (5.3.2.2) by the following condition

(5.4.4). $\text{fr}_{\mathcal{V}_{2n}/\mathbb{Q}}(p) = \sigma\alpha_{2n} \in GSp_4(\mathbb{Z}/M^2)$, where $\alpha_{2n} = \alpha + AM$, $A =$ diag $(a_1, .., a_4)$, $a_i \in \mathbb{Z}/M$, here $r \in \mathbb{Z}/M^2$ is a lift of r of (5.4.1). Condition $\alpha_{2n} \in GSp_4(\mathbb{Z}/M^2)$ is equivalent to a condition $a_3 - a_1 = ra_4 - r^{-1}a_2$; we claim also $a_1 + a_3 \not\equiv 0 \pmod l$, $a_3 \not\equiv 0 \pmod l$.

We fix p satisfying (5.3.2.1), (5.4.4). Congruence relations (5.3.4), (1), (2) remain valid and (5.3.4), (3) for the present case is the following:

$p \equiv -1 + (a_1 - a_3)M$, $a_p \equiv 2 + [-4(a_1 - a_3) - (a_1 + a_3)(r - r^{-1})]M$,
$a_p - (p^2 + 1) \equiv [-2(a_1 - a_3) - (a_1 + a_3)(r - r^{-1})]M \pmod{M^2}$,

hence in (5.3.18) $C \equiv (a_q - (q^2+1))(a_1+a_3)(r-r^{-1}) \pmod M$, i.e. $C \not\equiv 0 \pmod l$ because of the choice of a_1, a_3, r.

For the present case $K_p \ne \mathcal{V}_p$, i.e. Gal (K_p) does not act trivially on E/M, hence (5.3.16) must be replaced by the following

Lemma 5.4.5. Let L_2/L_1 be a non-ramified extension of local fields of degree δ, E/M a Gal (L_1)-module such that Gal (L_2) acts trivially on E/M. Let $a, b \in H^1(L_1, E/M)$ and $a_2, b_2 \in H^1(L_2, E/M)$ be their restrictions. Then

$$\delta < a, b >= [a_2(\text{fr }_{L_2}), b_2(g)] \tag{5.4.6}$$

again via an isomorphism $\mu_M \to \mathrm{Br}(L_2)_M$ depending on a generator g of a ramified extension of L_2. ■

We apply this lemma to the case $L_2 = \mathcal{V}_p$, $L_1 = K_p$, $a = \text{loc }_p(y_1)$, $b = \text{loc }_p(c_{p,q})$ like in (5.3), here $\delta = \frac{l-1}{2}$. Calculation (5.3.17) remains the same, lemma 5.3.25 is replaced by

$$\mathrm{loc}_p(a)(\text{fr }_{\mathcal{V}_p}) = \text{Res }^{\mathcal{V}}_K(a)((\text{fr }_{W(a)/\mathbb{Q}}(p))^{l-1}) \tag{5.4.7}$$

(5.4.7) for $a = y_2$ and (5.4.3) imply

$$\mathrm{loc}_p(y_2)(\text{fr }_{\mathcal{V}_p}) = (l-1)e_3 \tag{5.4.8}$$

Now we need the following analog of lemma 5.3.22:

Lemma 5.4.9. Let E be an abelian variety of dimension 2 over a finite field $\mathbb{F}_m$ such that the matrix of fr mod M^2 is $\alpha + AM$. Let $z \in E_M(\mathbb{F}_{m^{l-1}})$ and $z' \in H^1(\mathbb{F}_{m^{l-1}}, E_M)$ its image under the Kummer map. Then $z'(\text{fr }_{\mathbb{F}_{m^{l-1}}}) = (l-1)A(z)$. ■

Applying (5.4.9) for $z = \tilde{y}_2$ we see (because of (5.4.8), a condition $a_3 \not\equiv 0 \pmod l$, (5.3.18) and (5.4.6)) that

$$[\mathrm{loc}_p(y_1)(\text{fr }_{\mathcal{V}_p}), \mathrm{loc}_p(y_2)(\text{fr }_{\mathcal{V}_p})] = 1 \tag{5.4.10}$$

Applying (5.4.7) to (5.4.10) we get

$$[y_1((\sigma\alpha h)^{l-1}), y_2((\sigma\alpha h)^{l-1})] = 1$$

This formula together with (5.4.3) and (5.2.9) implies the theorem.

5.4$'$. Here we consider the case when the restriction of P on E is 0. We prove the theorem in this case like in 5.3$'$, but we choose here $\alpha =$ diag $(\lambda_1, \dots, \lambda_4, c\lambda_1^{-1}, \dots, c\lambda_4^{-1})$ where $\lambda_i = \epsilon_i + a_i M$, $\epsilon_1 = 1$, $\epsilon_2 = r$, $\epsilon_3 = -1$, $\epsilon_4 = -r^{-1}$, $a_1, \dots, a_4 \in \mathbb{Z}/M$, $c = -1 - aM$ where $a = \frac{a_1 + r^{-1}a_2 - a_3 - ra_4}{2}$, and these numbers satisfy $a_1 \ne 0$, $a_1 + a_3 \ne 0$, $r - r^{-1} \ne 0$ in $\mathbb{Z}/l$. The union of contents of 5.3$'$ and 5.4 proves the theorem.

5.5. Euler systems of order 2.

Here we shall give a sketch of the definition of Euler systems of order 2 which is a union of ideas of [K2] (according [Gr]) and constuctions above. Throughout this section i will be 1 and 2.

Let primes p_i satisfy 5.3.2.1 for some $h \in \text{Gal } \mathcal{V}$, primes q_i satisfy conditions of Propositions 5.3.13, 5.3.14, here 5.3.14.1 is the following: $q_i \equiv -1 \pmod{p_i + 1}$, and let $((q_1+1),(q_2+1)) = 2$. We have Gal $(K^{p_1q_1p_2q_2}/K) = (\mathbb{Z}/(p_1+1)) \oplus (\mathbb{Z}/(p_2+1))$ up to a group of order 2 coming from a condition $((q_1+1),(q_2+1)) = 2$; we shall neglect this group below. Let g_i be generators of Gal $(K^{p_iq_i}/K) \hookrightarrow$ Gal $(K^{p_1q_1p_2q_2}/K)$. Further, $\forall (j_1, j_2) \in I_{q_1} \times I_{q_2}$ there are curves $V_{p_1,q_1,p_2,q_2,j_1,j_2}$ defined over $K^{p_1q_1p_2q_2}$ such that norm relations for 2 pairs of Hecke operators are the following:

$$T_{p_1}T_{q_1}T_{p_2}T_{q_2}(V) = \bigcup_{(j_1,j_2)\in I_{q_1}\times I_{q_2}} \bigcup_{\gamma_i\in[0,..,p_i]} g_1^{\gamma_1} g_2^{\gamma_2} V_{p_1,q_1,p_2,q_2,j_1,j_2}$$

modulo some non-essential components coming from components V (resp. $V_{q,j}$) in (4.3.4) (resp. (4.3.6)). Calculation 5.3.17 shows that these components are really non-essential, we shall neglect them below.

We define $y_{p_1,q_1,p_2,q_2,j_1,j_2} = \text{cl}\,'_{E,M}(\phi_m(V_{p_1,q_1,p_2,q_2,j_1,j_2})) \in H^1(K^{p_1q_1p_2q_2}, E/M)$ like in (4.5),

$$D_{p_1,q_1,p_2,q_2} = \bigcup_{(j_1,j_2)\in I_{q_1}\times I_{q_2}} \bigcup_{\gamma_i\in[0,..,p_i]} \gamma_1\gamma_2 g_1^{\gamma_1} g_2^{\gamma_2} y_{p_1,q_1,p_2,q_2,j_1,j_2}$$

(up to multipliers $C_{p,i}$ of (4.3.5)) and $c_{p_1,q_1,p_2,q_2} \in H^1(K, E/M)$ using the same construction like in [Gr], (4).

An analog of calculation (5.3.17) shows us that if p_1, p_2 satisfy 5.3.2.2 as well then the main property of these Euler systems is the following:

$$\text{loc}_{\,p_i}(c_{p_1,q_1,p_2,q_2})(g_i) = C_i' \,\text{loc}_{\,p_i}(c_{p_{i'},q_{i'}})(\text{fr}_{\,K_{p_i}})$$

where $i' \in \{1,2\}$, $i' \neq i$, $(C_i', l) = 1$.

This construction can be used for a proof of an analog of Kolyvagin's rank one case. Euler systems of higher order are constructed analogously.

5.6. Here there are (without proofs) 2 lemmas that show how to rewrite the above proofs in the language of elements of $H^1(K, E)$ but not of non-existing $E(K)$. We need to consider not only the Abel-Jacobi images of $\phi_m(V_\bullet)$ in $H^1(K, E/M)$ but in $H^1(K, E)$.

Lemma 5.6.1. Let F be a finite field, W a $\text{Gal}(F) - \mathbb{Z}_l-$module such that $\text{Gal}(F)$ acts trivially on W/M. Let $\alpha = \{\alpha_k\}$, $\alpha_k \in H^1(F, W/l^k)$ be a projective system of elements of order M. Then there is an only element $\beta \in W/M$ such that if $\bar\beta \in W$ is a lift of β then (considering α as a cocycle) $\forall \gamma \in \text{Gal}(F)$ $M\alpha_k(\gamma) = \gamma(\bar\beta) - \bar\beta$, where $M : W/l^k \hookrightarrow W/Ml^k$ is the multiplication by M. ■

We denote $\beta = \phi(\alpha)$.

Lemma 5.6.2. Let L/K be a cyclic extension of number fields totally ramified at a place $\mathfrak{p}$ of K, W a $\text{Gal}(K) - \mathbb{Z}_l-$module such that $\text{Gal}(K_\mathfrak{p})$ acts trivially on W/M. Let $D=\{D_k\}$, $D_k\in H^1_f(L,W/l^k)$, $Y=\{Y_k\}$, $Y_k\in H^1_f(L,W/l^k)$ be projective systems of elements such that $g(D)-D=MY$, where $g\in \mathrm{Gal}(L/K)$ is a generator. Then $D_n\in (H^1_f(L,W/M))^{\mathrm{Gal}(L/K)}$, and $\omega^{-1}(D_n)\in H^1(K,W/M)$ is defined. Further, let us consider $\mathrm{loc}_{\mathfrak p}(y_k)\in H^1_f(L_{\mathfrak p},W/l^k)=H^1(F,W/l^k)$ where F is the residue field of L and K. Then $\mathrm{loc}_{\mathfrak p}(y_k)$ is of order M, and $\omega^{-1}(D_n)(g)=\phi(\mathrm{loc}_{\mathfrak p}(y_k))$. ■

We apply Lemma 5.6.2 to the case $L/K=(K^{p,q})_{\mathfrak p}/K_{\mathfrak p}$, $W=E$, $Y_k=\mathrm{cl}'_{E,l^k}(\phi_m(V))$, $D_k=C_pC_q\,\mathrm{cl}'_{E,l^k}(\sum_{j\in I_q}\sum_{\gamma=1}^p\gamma g^\gamma(\phi_m(V_{p,q,j}))$. This lemma shows us that all below 5.3.10 can be rewritten in the right way.

Section 6. Calculations.

6.0. Here we prove Proposition 4.3.1. Let $t,t'\in V$, $(t,t')\in T_{p,V}$, $A_t=\mathbb{C}^4/D$, $\{x_1,x_2\}$ be an $O(YK)$-basis of D,

$$\{y_1,y_2,y_3,y_4\}=\{x_1,\sqrt{f}x_1,\frac{1}{d}x_2,\sqrt{f}x_2\} \tag{6.0.1}$$

an $O(Y)$-basis of D (see 4.1). The same objects D', x_i', y_i' will be for t'. By definition of $T_{p,V}$, we have (here $a\in O(YK)/\mathfrak p$, $a=a_1+\sqrt{f}a_2$, $a_1,a_2\in O(Y)/\mathfrak p$ depends on t').

$$x_1'=x_1+ax_2;\quad x_2'=\mathfrak p x_2 \tag{6.0.2}$$

for all but one point of $T_{p,V}(t)$; for the remaining point (6.0.2) is $x_1'=\mathfrak p x_1$, $x_2'=x_2$. Using (6.0.1) for t, t' and (6.0.2) we get

$$\begin{aligned} y_1'&=y_1+da_1y_3+a_2y_4\\ y_2'&=y_2+dfa_2y_3+a_1y_4\\ y_3'&=\mathfrak p y_3\\ y_4'&=\mathfrak p y_4\end{aligned}$$

This means that $v_{t'}$ corresponds to the matrix $\begin{pmatrix}1&0&da_1&a_2\\0&1&dfa_2&a_1\end{pmatrix}$ and the corresponding element in $\lambda^2(B)$ is $(x_1,..,x_6)=(1,dfa_2,a_1,-da_1,-a_2,da_1^2-dfa_2^2)$ (the set of 2×2-minors of the above matrix). For different a the vectors are in $P^3\cap G(2,B)$; the equations of P^3 are $x_2+dfx_5=dx_3+x_4=0$. ■

Lemma 6.1. $B_1(d)\subset B_3$ is given by the following equations: $(kz,-kz,l)$ where $z\in B_1$ is a parameter, $k=\frac{\sqrt{2d}\sqrt[4]{f}}{1+d\sqrt{f}}$, $l=\frac{1-d\sqrt{f}}{1+d\sqrt{f}}$ $(2k^2+l^2=1)$, here $B_1(d)$ and ι are defined in 4.1.5, $B_3\subset\mathbb{C}^3$ is the natural inclusion.

Proof. Let $z\in B_1(d)$, $t=\iota(z)\in V_d$, $x=(x_1,x_2)$, $x_1,x_2\in\mathbb{C}^4$ are (for this t) the same as in 4.1. Firstly, we find explicitly coordinates of x_1,x_2 using formulas of [Sh1]. For our case $g=2$, $\nu=1,2$,

$Y_1=\begin{pmatrix}1&0\\0&1\end{pmatrix}$, $Y_2=\begin{pmatrix}1&z\\\bar z&1\end{pmatrix}$ ([Sh1], p.162, (35), Type IV)

$T_\nu = \chi_\nu(T_d)$ ([Sh1], p.159, 2.4), i.e. (see 4.1.1 for T_d) $T_1 = \begin{pmatrix} i\sqrt{\Delta} & 0 \\ 0 & id\sqrt{f\Delta} \end{pmatrix}$, $T_2 = \begin{pmatrix} i\sqrt{\Delta} & 0 \\ 0 & -id\sqrt{f\Delta} \end{pmatrix}$,

$W_1 = W_2 = \begin{pmatrix} \sqrt[4]{\Delta} & 0 \\ 0 & \sqrt{d}\sqrt[4]{f\Delta} \end{pmatrix}$, $X_\nu = Y_\nu \bar W_\nu$ ([Sh1], p.161, Type IV), i.e.

$X_1 = \begin{pmatrix} \sqrt[4]{\Delta} & 0 \\ 0 & \sqrt{d}\sqrt[4]{f\Delta} \end{pmatrix}$, $X_2 = \begin{pmatrix} \sqrt[4]{\Delta} & \sqrt{d}\sqrt[4]{f\Delta}z \\ \sqrt[4]{\Delta}\bar z & \sqrt{d}\sqrt[4]{f\Delta} \end{pmatrix}$

Formulas of [Sh1], p.159, (Type IV), (20) for the present objects mean that if $x_i = (x_{ij})$ $(i = 1,2;\ j = 1,..,4)$ then $X_1 = (x_{ij})$ $(i,j = 1,2)$ and $X_2 = \begin{pmatrix} x_{13} & x_{23} \\ \bar x_{14} & \bar x_{24} \end{pmatrix}$ hence we have:

$$x_1 = (\ \sqrt[4]{\Delta} \quad 0 \quad \sqrt[4]{\Delta} \quad \sqrt[4]{\Delta}z\ )$$

$$x_2 = (\ 0 \quad \sqrt{d}\sqrt[4]{f\Delta} \quad \sqrt{d}\sqrt[4]{f\Delta}z \quad \sqrt{d}\sqrt[4]{f\Delta}\ )$$

Hence the sequence $y = (y_1,..,y_4)$ of 4.1.2 has the following coordinates of its vectors:

$$y_1 = x_1 = (\ \sqrt[4]{\Delta} \quad 0 \quad \sqrt[4]{\Delta} \quad \sqrt[4]{\Delta}z\ )$$

$$y_2 = \sqrt{f}x_1 = (\ \sqrt{f}\sqrt[4]{\Delta} \quad 0 \quad -\sqrt{f}\sqrt[4]{\Delta} \quad -\sqrt{f}\sqrt[4]{\Delta}z\ )$$

$$y_3 = \frac{1}{d}x_2 = (\ 0 \quad \sqrt{d^{-1}}\sqrt[4]{f\Delta} \quad \sqrt{d^{-1}}\sqrt[4]{f\Delta}z \quad \sqrt{d^{-1}}\sqrt[4]{f\Delta}\ )$$

$$y_4 = \sqrt{f}x_2 = (\ 0 \quad \sqrt{d}\sqrt[4]{f^3\Delta} \quad -\sqrt{d}\sqrt[4]{f^3\Delta}z \quad -\sqrt{d}\sqrt[4]{f^3\Delta}\ )$$

Now we consider t as a point of X, i.e. $g = 1$, and we have only one X_1, W_1. Again by [Sh1], p.159, (Type IV), (20) we get

$X_1 = \begin{pmatrix} \sqrt[4]{\Delta} & \sqrt{f}\sqrt[4]{\Delta} & 0 & 0 \\ 0 & 0 & \sqrt{d^{-1}}\sqrt[4]{f\Delta} & \sqrt{d}\sqrt[4]{f^3\Delta} \\ \sqrt[4]{\Delta} & -\sqrt{f}\sqrt[4]{\Delta} & \sqrt{d^{-1}}\sqrt[4]{f\Delta}z & -\sqrt{d}\sqrt[4]{f^3\Delta}z \\ \sqrt[4]{\Delta}\bar z & -\sqrt{f}\sqrt[4]{\Delta}\bar z & \sqrt{d^{-1}}\sqrt[4]{f\Delta} & -\sqrt{d}\sqrt[4]{f^3\Delta} \end{pmatrix}$. Further, W_1 is defined by (3.3.6), $W_1 = \sqrt[4]{\Delta}\begin{pmatrix} \sqrt{2} & 0 & 0 & 0 \\ 0 & \sqrt{2f} & 0 & 0 \\ 0 & 0 & \sqrt{f} & \sqrt{f} \\ 0 & 0 & \sqrt{f} & -\sqrt{f} \end{pmatrix}$,

hence $X_1\bar W_1^{-1} = \begin{pmatrix} \frac{1}{\sqrt2} & \frac{1}{\sqrt2} & 0 & 0 \\ 0 & 0 & \frac{1+d\sqrt f}{2\sqrt d\sqrt[4]{f}} & \frac{1-d\sqrt f}{2\sqrt d\sqrt[4]{f}} \\ \frac{1}{\sqrt2} & -\frac{1}{\sqrt2} & \frac{1-d\sqrt f}{2\sqrt d\sqrt[4]{f}}z & \frac{1+d\sqrt f}{2\sqrt d\sqrt[4]{f}}z \\ \frac{\bar z}{\sqrt2} & -\frac{\bar z}{\sqrt2} & \frac{1-d\sqrt f}{2\sqrt d\sqrt[4]{f}} & \frac{1+d\sqrt f}{2\sqrt d\sqrt[4]{f}} \end{pmatrix}$. At last, $t = (\mathfrak{U}_1^{-1}\mathfrak{V}_1)^t$, where $\mathfrak{U}_1, \mathfrak{V}_1$ are defined in (3.3.7), $r_1 = 3$, $s_1 = 1$, $\nu = 1$. Multiplying matrices we get the desired result. ■

6.2. Now we shall find explicitly the stabilizer of $B_1(d)$ in $G(\mathbb{R})$ denoted by $G_{T,B_1(d)}$ (subscript T means the polarization form defined in (4.1.1)). For a convenience of further calculations let us consider the following subset A_0 of B_3 which is isomorphic to B_1:

$$A_0 = \{t \in B_3 | t = (0,0,z), z \in B_1\}$$

Let $\gamma_E = \begin{pmatrix} k & 0 & k & 0 \\ k & 0 & -k & 0 \\ 0 & 1 & 0 & l \\ 0 & l & 0 & 1 \end{pmatrix}$. We have $\gamma_E(A_0) = B_1(d)$.

Let $G_E = G_E(\mathbb{R}) = \{g \in GL_4(\mathbb{C}) | \bar{g}^t E_{3,1} g = \lambda E_{3,1}\}$. G_E acts on B_3 by the ordinary way, and we consider groups

$$H_{E,A_0} = \{g \in G_E | g|_{A_0} = id\}$$

$$G_{E,A_0} = \{g \in G_E | g(A_0) = A_0\}$$

We have $H_{E,A_0} = \left\{ \begin{pmatrix} \gamma & 0 \\ 0 & aE_2 \end{pmatrix} \right\}$, $G_{E,A_0} = \left\{ \begin{pmatrix} \gamma & 0 \\ 0 & \delta \end{pmatrix} \right\}$ where entries are 2×2-matrices:

$$\gamma = (\gamma_{ij}) \in GU(2,0), \delta = (\delta_{ij}) \in GU(1,1), \lambda(\gamma) = \lambda(\delta) = a \tag{6.2.1}$$

We need to consider 2×2-matrices β, μ whose entries β_{ij}, μ_{ij} $(i,j = 1,2)$ are the following linear combinations of γ_{ij}, δ_{ij}:

$$\begin{array}{rr} \gamma_{11} = \beta_{11} + \sqrt{f}\mu_{11} & \gamma_{12} = \frac{\sqrt{d}}{\sqrt[4]{f}}(\sqrt{f}\beta_{12} + \mu_{12}) \\ \delta_{11} = \beta_{11} - \sqrt{f}\mu_{11} & \delta_{12} = \frac{\sqrt{d}}{\sqrt[4]{f}}(\sqrt{f}\beta_{12} - \mu_{12}) \\ \gamma_{21} = \sqrt{d}\sqrt[4]{f}(\sqrt{f}\beta_{21} + \mu_{21}) & \gamma_{22} = \beta_{22} + d\sqrt{f}\mu_{22} \\ \delta_{21} = \sqrt{d}\sqrt[4]{f}(\sqrt{f}\beta_{21} - \mu_{21}) & \delta_{22} = \beta_{22} - d\sqrt{f}\mu_{22} \end{array} \tag{6.2.2}$$

We denote

$$g(\beta,\mu) = \begin{pmatrix} \beta_{11} & f\mu_{11} & fd\beta_{12} & \mu_{12} \\ \mu_{11} & \beta_{11} & d\mu_{12} & \beta_{12} \\ \beta_{21} & \mu_{21} & \beta_{22} & \mu_{22} \\ d\mu_{21} & fd\beta_{21} & d^2 f\mu_{22} & \beta_{22} \end{pmatrix}$$

Now we define analogously subgroups $H_{T,B_1(d)}$, $G_{T,B_1(d)}$ (replacing $E_{3,1}$ by T and A_0 by $B_1(d)$). We have $H_{T,B_1(d)} = W_1^{-1}\gamma_E H_{E,A_0}\gamma_E^{-1}W_1$, $G_{T,B_1(d)} = W_1^{-1}\gamma_E G_{E,A_0}\gamma_E^{-1}W_1$. A calculation gives

$$G_{T,B_1(d)} = \{g(\beta,\mu)\}$$

for all β, μ satisfying (6.2.2).

6.3. Proof of the proposition 4.3.2.

We need an explicit set S of representatives of cosets in the double coset decomposition: $\Gamma T_p \Gamma = \cup_{s_i \in S} \Gamma s_i$, a map $j : S \to G(2,B)$ and a map $\chi : G(2,B) \to$

$P^1(\mathbb{F}_p)\cup\{i_0\}$ which are defined in the statement of (4.3.2). According ([L], Proposition 3) to prove (4.3.2) we must show that $\forall s_1,s_2\in S$

$$\{\exists g\in\Gamma_{B_1(d)}H_{T,B_1(d)} \text{ such that } s_1gs_2^{-1}\in\Gamma\} \iff \chi\circ j(s_1)=\chi\circ j(s_2) \quad (6.3.1)$$

where $\Gamma_{B_1(d)}=\Gamma\cap G_{T,B_1(d)}$.

We shall check (6.3.1) only for a case when both matrices s_1,s_2 are matrices of a set $s(a,b)$ where

$$s(a,b)=\begin{pmatrix} \bar{\mathfrak{p}} & 0 & 0 & \bar{\mathfrak{p}}fa\\ 0 & \mathfrak{p} & 0 & 0\\ -a & 0 & 1 & c\\ 0 & 0 & 0 & p\end{pmatrix} \quad (6.3.2)$$

where $c=\frac{-fa^2}{2}+b\sqrt{-\Delta}\in Y$, a,b run over a set of representatives of residues of $\mathbb{Z}$ modulo p; these matrices form a part of S. We replace also a condition $g\in\Gamma_{B_1(d)}H_{T,B_1(d)}$ of (6.3.1) by a weaker condition $g\in G_{T,B_1(d)}$; by analogy with [L], section 7, we can expect that there is no difference. We denote $s_i=s(a_i,b_i)$ $(i=1,2)$ and $A=(A_{ij})=s_1gs_2^{-1}$.

To write down a formula for some A_{ij} in a convenient form we introduce the following notations:

1) $(A'_1,..A'_4):=(A_{12},A_{14},A_{32},A_{34})$;

2) $(v_1,..,v_8):=(\beta_{11},..\beta_{22},\mu_{11},..,\mu_{22})$;

3) $Z=(z_{ij})$ is the following matrix:

$$\begin{pmatrix} 0 & 0 & fda_1 & 0 & 1 & 0 & 0 & 0\\ -fa_2 & fd\bar{c}_2 & 0 & fa_1 & 0 & 1 & -f^2da_1a_2 & f^2d^2a_1\bar{c}_2\\ 0 & 0 & fdc_1 & 0 & -fa_1 & 0 & 1 & 0\\ fa_1a_2 & -fda_1\bar{c}_2 & -fa_2 & c_1+\bar{c}_2 & 0 & -a_1 & -fda_2c_1 & 1+fd^2c_1\bar{c}_2\end{pmatrix}$$

A direct calculation shows that

$$pA'_k=\sum_{i=1}^{8} z_{ki}v_i \mod \mathfrak{p} \quad (6.3.3)$$

where $k=1,..,4$.

An element of $G(2,B)$ that corresponds to $s(a,b)$ is an affine plane in B generated by vectors $(\bar{\mathfrak{p}}\ \ 0\ \ 0\ \ \bar{\mathfrak{p}}fa)$, $(-a\ \ 0\ \ 1\ \ c)$ (lines of (6.3.2) mod $\mathfrak{p}$) hence its homogeneous coordinates in $P(\lambda^2(B))$ are $(0:\bar{\mathfrak{p}}:-\bar{\mathfrak{p}}\bar{c}:0:0:-\bar{\mathfrak{p}}fa)$ and hence $\chi\circ j(s(a,b))=\bar{c}$ mod $\mathfrak{p}$. This means that we must prove:

1) If for given s_i we have $\bar{c}_1\equiv\bar{c}_2$ mod $\mathfrak{p}$ then $\exists g(\mu,\beta)$ such that all A_{ij} are integer;

2) If for given s_i we have $\bar{c}_1\not\equiv\bar{c}_2$ mod $\mathfrak{p}$ then $\forall g(\mu,\beta)$ some A_{ij} are not integer.

We consider the case (2). If all A_{ij} are integer then (6.3.3) implies that $\sum_{i=1}^8 z_{ki}v_i=0$ mod $\mathfrak{p}$. The solution of this system of linear equations is the following:

$$B_k=\sum_{i=1}^{4} y_{ki}C_i \mod \mathfrak{p} \quad (6.3.4)$$

where $k = 1, .., 4$, $(B_1, .., B_4) = (\beta_{22}, \mu_{11}, \mu_{12}, \mu_{21})$, $(C_1, .., C_4) = (\beta_{11}, \beta_{12}, \beta_{21}, \mu_{22})$ and $Y = (y_{ki})$ is the following matrix:

$$Y = \begin{pmatrix} 0 & 0 & \frac{-fa_2(1-fd^2\bar{c}_1^2)}{\bar{c}_1-\bar{c}_2} & \frac{1-fd^2\bar{c}_1\bar{c}_2}{\bar{c}_1-\bar{c}_2} \\ 0 & 0 & -fda_1 & 0 \\ fa_2 & -fd\bar{c}_2 & \frac{f^2a_1a_2(1-fd^2\bar{c}_1\bar{c}_2)}{\bar{c}_1-\bar{c}_2} & \frac{-fa_1(1-fd^2\bar{c}_2^2)}{\bar{c}_1-\bar{c}_2} \\ 0 & 0 & fd\bar{c}_1 & 0 \end{pmatrix}$$

At last, a condition $\lambda = 1$ of (6.2.1) in terms of β_{ij}, μ_{ij} is the following: $\lambda = A + B\sqrt{f}$ where

$$A = \beta_{11}\beta_{22} + fd\mu_{11}\mu_{22} - fd\beta_{12}\beta_{21} - d\mu_{12}\mu_{21} = 1 \qquad (6.3.5)$$

$$B = d\beta_{11}\mu_{22} + \beta_{22}\mu_{11} - d\beta_{12}\mu_{21} - d\beta_{21}\mu_{12} = 0 \qquad (6.3.6)$$

Substituting (6.3.4) to (6.3.5), (6.3.6) we get $A = \frac{-1+fd^2\bar{c}_1\bar{c}_2}{\bar{c}_1-\bar{c}_2}C$, $B = -dC$ where $C = fa_2\beta_{11}\beta_{21} + fd(\bar{c}_1 - \bar{c}_2)\beta_{12}\beta_{21} - \beta_{11}\mu_{22} + f^3d^2a_1a_2\bar{c}_1\beta_{21}^2 - d^2f^2a_1\bar{c}_2\beta_{21}\mu_{22}$. This means that a condition $B = 0$, $A = 1$ leads to a contradiction.

Similar considerations of other cases will give us a proof of Proposition 4.3.2.

References

[B] Bloch S., Algebraic cycles and values of L-functions. II. Duke Math. J., 1985, v. 52, No. 2, p. 379 - 397.

[BK] Bloch S., Kato L., L-functions and Tamagava numbers of motives. In: The Grothendieck Festschrift, v.1, p. 333 - 400. Boston Basel Stuttgart: Birkhauser, 1990

[BlR] Blasius D., Rogawski J.D., Zeta functions of Shimura varieties. In: Motives. Proc. of Symp. in Pure Math., 1994, v. 55, part 2, p. 525 - 571.

[D] Deligne P. Travaux de Shimura. Lect. Notes in Math., 1971, v.244, p. 123 - 165.

[FCh] Faltings G., Chai Ching-Li, Degeneration of abelian varieties. Springer, 1990

[Fl] Flach M., A finiteness theorem for the symmetric square of an elliptic curve. Invent. Math., 1992, v.109, p. 307 - 327.

[GSh] Gelbart S., Shahidi F., Analytic properties of automorphic L-functions. Perspectives in Math., vol. 6. 1988.

[Gr] Gross B.H., Kolyvagin's work on modular elliptic curves. In: L-functions and Arithmetic. Proceedings of the Durham Symposium, July, 1989. Cambridge Univ. Press, 1991. p. 235 - 256.

[GrZ] Gross B.H., Zagier D.B., Heegner points and derivatives of L- series. Invent. Math., 1986, v.84, No.2, p. 225 - 320.

[J] Jannsen U., Mixed motives and algebraic K-theory. Lecture Notes in Math., 1400. Berlin Heidelberg New York: Springer 1990

[K1] Kolyvagin V.A., Finiteness of $E(\mathbb{Q})$ and $\mathrm{Sh}(E, \mathbb{Q})$ for a subclass of Weil curves. Math. USSR Izvestiya, 1989, v. 32, No. 3, p. 523 - 541

[K2] Kolyvagin V.A. Euler systems. In: The Grothendieck Festschrift, v.2. Boston Basel Stuttgart: Birkhauser 1990, p. 435 - 483

[KL] Kolyvagin V.A., Logachev D.Yu. Finiteness of Sh over totally real fields. Math. USSR Izvestiya, 1992, v. 39, No. 1, p. 829 - 853

[Ko] Kohnen W., Special quadratic forms, Siegel modular groups and Siegel modular varieties. Intern. J. Math., 1990, v.1, N.4, p. 397 - 429.

[La] Langlands R.P. On the zeta-functions of some simple Shimura varieties. Can. J. Math., 1979, v. 31, p. 1121 - 1216.

[L] Logachev D. Yu. Geometric description of Hecke action on Heegner curves on a Siegel modular threefold. Preprint. Institut of Experimental Math. (Essen), 1993, No. 21, 23 p.

[N] Nekovář J. Kolyvagin's method for Chow groups of Kuga-Sato varieties. Inv. Math. 1992, v. 107, p. 99 - 125.

[Sh1] Shimura G., On analytic families of polarized abelian varieties and automorphic functions. Annals of Math., 1963, v. 78, No. 1, p. 149 - 192

[Sh2] Shimura G., On modular correspondences for $Sp(N,\mathbb{Z})$ and their congruence relations. Proc. Nat. Acad. Sci. USA, 1963, v. 49, p. 824 - 828

[W] Weissauer R., a series of preprints:

[W1] Weissauer R., CAP-localisation. Preprint. Mannheim University, 1993.

[W2] Weissauer R., The Ramanujan conjecture for genus two Siegel modular forms (An application of the trace formula). Preprint. Mannheim University, 1994.

[W3] Weissauer R., Character identities and Galois representations related to the group $GSp(4)$, Part 1. Preprint. Mannheim University, 1994.

Institute for Applied Mathematics (Khabarovsk branch) of the Far-Eastern branch of Russian Academy of Sciences

E-mail: logachev@srdlan.npi.msu.su