GDZ
Göttinger Digitalisierungszentrum

Galois Properties of Torsion Points on Abelian Varieties.

Katz, Nicholas M.

in: Inventiones mathematicae | Inventiones Mathematicae | Periodical Issue | Article

481 - 502

Terms and Conditions

The Göttingen State and University Library provides access to digitized documents strictly for noncommercial educational, research and private purposes and makes no warranty with regard to their use for other purposes. Some of our collections are protected by copyright. Publication and/or broadcast in any form (including electronic) requires prior written permission from the Goettingen State- and University Library.
Each copy of any part of this document must contain there Terms and Conditions. With the usage of the library's online system to access or download a digitized document you accept there Terms and Conditions.
Reproductions of material on the web site may not be made for or donated to other repositories, nor may be further reproduced without written permission from the Goettingen State- and University Library
For reproduction requests and permissions, please contact us. If citing materials, please give proper attribution of the source.

Contact:

Niedersächsische Staats- und Universitätsbibliothek
Digitalisierungszentrum
37070 Goettingen
Germany
Email: gdz@www.sub.uni-goettingen.de

Purchase a CD-ROM

The Goettingen State and University Library offers CD-ROMs containing whole volumes / monographs in PDF for Adobe Acrobat. The PDF-version contains the table of contents as bookmarks, which allows easy navigation in the document. For availability and pricing, please contact:
Niedersaechisische Staats- und Universitaetsbibliothek Goettingen - Digitalisierungszentrum
37070 Goettingen, Germany, Email: gdz@www.sub.uni-goettingen.de

Invent. math. 62, 481 – 502 (1981)

Inventiones mathematicae
© Springer-Verlag 1981

Galois Properties of Torsion Points on Abelian Varieties

Nicholas M. Katz

Institut des Hautes Etudes Scientifiques, 35, route de Chartres, F-91440 Bures-sur-Yvette, France

Contents

Introduction

Consider an abelian variety A over a number field K. While it is a deep and non-effective theorem that the group $A(K)$ of all K-rational points on A is finitely generated, it is an elementary and effective fact that the torsion subgroup $\mathrm{Tors}\, A(K)$ is finite, and that its order remains uniformly bounded as we replace A by any A' which is K-isogenous to A. One shows that for *any* prime $\mathfrak{p}$ of K at which A has good reduction and whose absolute ramification $e_{\mathfrak{p}}$ satisfies $e_{\mathfrak{p}} < p-1$, the group $\mathrm{Tors}\, A(K)$ maps isomorphically, by "reduction mod $\mathfrak{p}$", to a subgroup of the finite group of all $\mathbb{F}_{\mathfrak{p}}$-rational points on $A \bmod \mathfrak{p}$ (c.f. the appendix). Thus if we denote by $N(\mathfrak{p})$ the number of $\mathbb{F}_{\mathfrak{p}}$-rational points on $A \bmod \mathfrak{p}$, we have the divisibility estimate

$$\#\,\mathrm{Tors}\, A(K) \text{ divides } N(\mathfrak{p})$$

for *any* $\mathfrak{p}$ as above. Because A and any K-isogenous A' have the *same* primes of good reduction, and the *same* $N(\mathfrak{p})$'s, this last divisibility remains valid if we replace A by any K-isogenous A'.

Serge Lang asked if *all* divisibilities of almost all the $N(\mathfrak{p})$ arise in this way:

Problem I. *Let A be an abelian variety over a number field K, and let $m \geqq 2$ be an integer. Suppose that the congruence*

$$N(\mathfrak{p}) \equiv 0 \bmod m$$

0020-9910/81/0062/0481/$04.40

holds for a set of primes $\mathfrak{p}$ *of* K *of (Dirichlet) density one. Does there exist a* K*-isogenous* A' *for which*

$$\#\operatorname{Tors} A'(K) \equiv 0 \bmod m?$$

By factoring an isogeny into isogenies of relatively prime prime-power-degree, one sees easily that this problem is equivalent to

Problem I (bis). *Let* A *be an abelian variety over a number field* K*, and let* l^n*,* $n \geqq 1$*, be a power of a prime number* l*. Suppose that*

$$N(\mathfrak{p}) \equiv 0 \bmod l^n$$

for a set of $\mathfrak{p}$ *of density one. Does there exist an* A' *over* K *which is* K*-isogenous to* A *by an* l*-power-degree isogeny, for which*

$$\#\operatorname{Tors} A'(K) \equiv 0 \bmod l^n?$$

In terms of the Tate module $T_l(A) = \operatorname{Hom}(\mathbb{Q}_l/\mathbb{Z}_l, A(\bar{K}))$, and the corresponding l-adic representation

$$\rho_l \colon \operatorname{Gal}(\bar{K}/K) \to \operatorname{Aut}_{\mathbb{Z}_l}(T_l(A)),$$

we can reformulate this problem. Recall that ρ_l is unramified at every prime $\mathfrak{p}$ of K of residue characteristic different from l at which A has good reduction, and that for each such $\mathfrak{p}$, the arithmetic Frobenius $F_{\mathfrak{p}}$ conjugacy class acting via ρ_l satisfies

$$\det(1 - \rho_l(F_{\mathfrak{p}})) = N(\mathfrak{p}).$$

If we combine the Chebataroff density theorem with the dictionary between A''s which are l-power-isogenous to A over K and $\operatorname{Gal}(\bar{K}/K)$-stable *lattices* in $T_l(A) \otimes \mathbb{Q}$, we see that Problem I (bis) is equivalent to

Problem I (ter). *Let* A *be an abelian variety over a number field* K*,* l *a prime number, and* $\rho_l \colon \operatorname{Gal}(\bar{K}/K) \to \operatorname{Aut}(T_l(A))$ *its* l*-adic representation. Suppose that for an integer* $n \geqq 1$*, we have*

$$\det(1 - \rho_l(\gamma)) \equiv 0 \bmod l^n \quad \text{for all } \gamma \in \operatorname{Gal}(\bar{K}/K).$$

Do there exist $\operatorname{Gal}(\bar{K}/K)$*-stable lattices* $\mathscr{L} \supset \mathscr{L}'$ *in* $T_l(A) \otimes \mathbb{Q}_l$ *such that the quotient* $\mathscr{L}/\mathscr{L}'$ *has order* l^n*, and such that* $\operatorname{Gal}(\bar{K}/K)$ *acts trivially on* $\mathscr{L}/\mathscr{L}'$*? (For then* $\mathscr{L}'$ *will be* $T_l(A')$ *for some* A' *which is* K*-isogenous to* A*, and* $\mathscr{L}/\mathscr{L}'$ *will be a group of* l^n K*-rational torsion points on* A'*.)*

In the special case $n = 1$, this amounts to asking for a $\operatorname{Gal}(\bar{K}/K)$-stable $\mathscr{L}'$ whose reduction modulo l, $\mathscr{L}' \otimes \mathbb{F}_l$, contains the trivial representation. By the Brauer-Nesbitt theorem ([1], p. 215), the *semisimplification* of $\mathscr{L}' \otimes \mathbb{F}_l$ as an $\mathbb{F}_l$-representation of $\operatorname{Gal}(\bar{K}/K)$ is independent of the particular choice of $\mathscr{L}'$, so in particular the semisimplification of $T_l(A) \otimes \mathbb{F}_l$ contains the trivial representation. Conversely, if the trivial representation occurs in the semisimplification of $T_l \otimes \mathbb{F}_l$, then there exists a $\operatorname{Gal}(\bar{K}/K)$-stable lattice $\mathscr{L}'$ such that $\mathscr{L}' \otimes \mathbb{F}_l$ contains the trivial representation. (Take a Jordan-Holder series for $T_l(A) \otimes \mathbb{F}_l$, say

$$T_l(A) = \mathscr{L}_0 \supset \mathscr{L}_1 \supset \ldots \supset \mathscr{L}_r = lT_l(A);$$

if, for some i, the quotient $\mathscr{L}_i/\mathscr{L}_{i+1}$ is the trivial representation of $\mathrm{Gal}(\bar{K}/K)$, then $\left(\frac{1}{l}\cdot\mathscr{L}_{i+1}\right)\otimes\mathbb{F}_l$ contains the trivial representation $\mathscr{L}_i/\mathscr{L}_{i+1}$.) Therefore the $n=1$ case of Problem I (ter), i.e., the $m=l$ case of Problem I, is equivalent to

Problem II. *Let A be an abelian variety over a number field K, l a prime number, and $\bar{\rho}_l\colon \mathrm{Gal}(\bar{K}/K)\to \mathrm{Aut}(T_l\otimes\mathbb{F}_l)$ the mod l representation on the $\bar{K}$-valued points of order l on A. If for every $\gamma\in\mathrm{Gal}(\bar{K}/K)$ we have*

$$\det(1-\bar{\rho}_l(\gamma))=0 \text{ in } \mathbb{F}_l,$$

is it true that the semisimplification of $T_l\otimes\mathbb{F}_l$ contains the trivial representation?

We will show that Problem I has an affirmative answer when A is an elliptic curve, that Problem II has an affirmative answer when A is two dimensional, and that in every dimension $\geqq 3$ there are a plethora of situations for which Problem II (and a fortiori Problem I) has a *negative* answer. We do not know whether or not Problem I has an affirmative solution for two-dimensional abelian varieties.

Note Added in Proof

In an letter (August, 1980) to the author, Serre has shown that Problem I (bis) can have a negative solution for two-dimensional abelian varieties and the prime $l=2$. The situation for odd l remains unclear.

This paper owes its existence to Serge Lang, who formulated the problems we deal with, and to Barry Mazur, who had the basic insight that they "just" amounted to "problems in group theory". I also owe to Mazur countless hours of discussion in which we jointly worked out a prototype of Theorem 1. The proof of Theorem 1 presented here was profoundly influenced by Swinnerton-Dyer's paper [5]. It also benefitted from clarifying discussions with Ribet. The "counter-examples" section owes it present from to Deligne. After this paper was written, Serre kindly ponted out to me that Problem II for elliptic curves is an exercise in his book [4], cf. p. I-2, exc. 1 and 2 and p. IV-6, exc.

My thanks to all of them.

The Case of Elliptic Curves; Reduction to "Group Theory"

In this section, we will prove that Problem I always has an affirmative answer for elliptic curves. We will reat the problem in the form I (ter). Taking for V the 2-dimensional $\mathbb{Q}_l$-vector space $T_l(A)\otimes\mathbb{Q}_l$, and for $G\subset \mathrm{Aut}_{\mathbb{Q}_l}(V)$ the image $\rho_l(\mathrm{Gal}(\bar{K}/K))$ of the l-adic representation, it suffices to prove the following

Theorem 1. *Let l be a prime number, V a two-dimensional $\mathbb{Q}_l$-vector space, $G\subset \mathrm{Aut}_{\mathbb{Q}_l}(V)$ a compact subgroup, and $n\geqq 1$ an integer.*

Suppose that we have the congruence

$$\det(1-g)\equiv 0 \bmod l^n$$

for every $g\in G$.

Then there exist G-stable lattices $\mathscr{L}\supset\mathscr{L}'$ such that the quotient $\mathscr{L}/\mathscr{L}'$ has order l^n, and such that G operates trivially on $\mathscr{L}/\mathscr{L}'$, or equivalently (elementary divisors!) there exists a $\mathbb{Q}_l$-basis v_1, v_2 of V and integers, $a, b\geqq 0$, $a+b=n$, such that the matrices of the elements of G, expressed in this basis, all lie in the subgroup of $\mathrm{GL}(2,\mathbb{Z}_l)$ consisting of all matrices of the form

$$\begin{pmatrix} 1+l^a\mathbb{Z}_l & l^a\mathbb{Z}_l \\ l^b\mathbb{Z}_l & 1+l^b\mathbb{Z}_l \end{pmatrix},$$

with the convention that when a or b is zero, we interpret "$1+l^0\mathbb{Z}_l$" to mean the group $\mathbb{Z}_l^\times$ of all l-adic units. [Given such a basis v_1, v_2, we take $\mathscr{L}=\mathbb{Z}_l v_1+\mathbb{Z}_l v_2$, $\mathscr{L}'=\mathbb{Z}_l\cdot l^a v_1+\mathbb{Z}_l\cdot l^b v_2$.]

We will prove the theorem by induction on the integer n.

Lemma 1. *The theorem is true for $n=1$.*

Proof. Because G is compact, it stabilizes some lattice $\mathscr{L}\subset V$. The universal identity for 2×2 matrices

$$\det(1-g)=1-\mathrm{tr}(g)+\det(g)$$

together with the hypothesis

$$\det(1-g)\equiv 0 \bmod l \quad \text{for } g\in G,$$

shows that the $\mathbb{F}_l$-representations of G

$$\mathscr{L}\otimes\mathbb{F}_l \quad \text{and} \quad \mathbb{1}+\det(\mathscr{L}\otimes\mathbb{F}_l)$$

have the same trace; as they visibly have the same determinant, their characteristic polynomials coincide. By the Brauer-Nesbitt theorem, their semisimplifications are isomorphic. Therefore if we take a Jordan-Holder series for $\mathscr{L}\otimes\mathbb{F}_l$

$$\mathscr{L}\supsetneqq\mathscr{L}_1\supsetneqq l\mathscr{L},$$

then either $\mathscr{L}/\mathscr{L}_1$ or $\mathscr{L}_1/l\mathscr{L}$ has trivial G-action. The required $\mathscr{L}\supset\mathscr{L}'$ are provided either by $\mathscr{L}\supset\mathscr{L}_1$ or by $\mathscr{L}_1\supset l\mathscr{L}$.

(Key) Lemma 2. *Let V be a two dimensional $\mathbb{Q}_l$-space, $G\subset \mathrm{Aut}_{\mathbb{Q}_l}(V)$ a subgroup, $G_1\subset G$ a normal subgroup of G, and $n\geqq 2$ an integer. Suppose that*

(1) *There exist G-stable lattices $\mathscr{L}\supset\mathscr{L}'$ such that $\mathscr{L}/\mathscr{L}'$ has order l, and such that G_1 operates trivially on $\mathscr{L}/\mathscr{L}'$.*

(2) *For every $g_1\in G_1$, we have $\det(g_1)\equiv 1 \bmod l$.*

(3) *Every element $g_1\in G_1$ satisfies the congruences*

$$\det(1-g_1)\equiv 0 \bmod l^n.$$

Then there exist G-stable lattices $\mathscr{L}''\supset\mathscr{L}'''$ such that

(1) *$\mathscr{L}''\supset l\mathscr{L}''\supset\mathscr{L}'''$.*

(2) *$\mathscr{L}''/\mathscr{L}'''$ has order either l^n or l^{n+1}.*

(3) *G_1 acts trivially on $\mathscr{L}''/\mathscr{L}'''$.*

Proof. We will first treat the case $n=2$, and then use an induction argument to reach any $n\geqq 3$.

For $n=2$, we will see that the required $\mathscr{L}''\supset\mathscr{L}'''$ is either provided by $\mathscr{L}\supset l\mathscr{L}$ or is provided by $\mathscr{L}'\supset l\mathscr{L}'$.

In terms of a $\mathbb{Z}_l$-basis $\{e_1 e_2\}$ of $\mathscr{L}$ such that $\{le_1, e_2\}$ is a $\mathbb{Z}_l$-basis of $\mathscr{L}'$, hypotheses (1) and (2) guarantee that every element of G_1 has a matrix of the form

$$\begin{pmatrix} 1+lX & lZ \\ Y & 1+lT \end{pmatrix} \quad \text{with } X, Y, Z, T\in\mathbb{Z}_l.$$

The two maps

$$G_1 \rightrightarrows \mathbb{F}_l$$

defined by "$Y \bmod l$" and "$Z \bmod l$" are easily verified to be group homomorphisms. But the hypothesis (3), namely

$$\det(1-g_1) \equiv 0 \bmod l^2$$

means precisely that

$$YZ \equiv 0 \bmod l,$$

whence G_1 is the union of the kernels of the two homomorphisms "$Y \bmod l$", "$Z \bmod l$". Since a group is never the union of two *proper* subgroups, one of these homomorphisms must *vanish*. If it be "$Y \bmod l$", then $\mathscr{L} \supset l\mathscr{L}$ "works" as an $\mathscr{L}'' \supset \mathscr{L}'''$; if it be "$Z \bmod l$", then $\mathscr{L}' \supset l\mathscr{L}'$ "works". Recall that $\mathscr{L}$ and $\mathscr{L}'$, hence also $l\mathscr{L}$, $l\mathscr{L}'$ are already G-stable.

Let us now prove the theorem, by induction, for an integer $n+1 \geqq 3$. Inductively, we may suppose that there exist G-stable lattices $\mathscr{L}_n \supset \mathscr{L}'_n$ such that

(1) $\mathscr{L}_n \supset l\mathscr{L}_n \supset \mathscr{L}'_n$,

(2) $\mathscr{L}_n/\mathscr{L}'_n$ has order l^n or l^{n+1},

(3) G_1 acts trivially on $\mathscr{L}_n/\mathscr{L}'_n$.

If $\mathscr{L}_n/\mathscr{L}'_n$ has order l^{n+1}, there is nothing to prove: $\mathscr{L}_n \supset \mathscr{L}'_n$ "works" for $n+1$! Therefore we will henceforth assume that $\mathscr{L}_n/\mathscr{L}'_n$ has order l^n.

By (3), for each element $g_1 \in G_1$, the element $X = g_1 - 1$ in $\mathrm{End}_{\mathbb{Q}_l}(V)$ carries $\mathscr{L}_n$ to $\mathscr{L}'_n$, and so induces an $\mathbb{F}_l$-linear map $\mathscr{L}_n \otimes \mathbb{F}_l \to \mathscr{L}'_n \otimes \mathbb{F}_l$. This construction defines a map

$$G_1 \mapsto \mathrm{Hom}_{\mathbb{F}_l}(\mathscr{L}_n \otimes \mathbb{F}_l, \mathscr{L}'_n \otimes \mathbb{F}_l).$$
$$g_1 = 1 + X \mapsto \text{"}X \bmod l\text{"}.$$

This map is a group homomorphism [for if X and X' are two elements of $\mathrm{End}(V)$ which both carry $\mathscr{L}_n$ to $\mathscr{L}'_n$, then their composition $X' \circ X$ maps $\mathscr{L}_n$ to $\mathscr{L}'_n$

$$\mathscr{L}_n \xrightarrow{X} \mathscr{L}'_n \subset l\mathscr{L}_n \xrightarrow{X'} l\mathscr{L}'_n$$

and so $X'X$ induces zero in $\mathrm{Hom}(\mathscr{L}_n \otimes \mathbb{F}_l, \mathscr{L}'_n \otimes \mathbb{F}_l)$].

The *hypothesis*

$$\det(1-g_1) \equiv 0 \bmod l^{n+1}$$

means precisely that, writing $g_1 = 1 + X$, we have

$$\det X \equiv 0 \bmod l^{n+1}$$

This in turn means that the index of $X(\mathscr{L}_n)$ in $\mathscr{L}_n$ is either infinite, or is finite and divisible by l^{n+1}. In either case, the inclusions

$$\underbrace{\mathscr{L}_n \supset \mathscr{L}'_n}_{\text{index } l^n} \supset X(\mathscr{L}_n)$$

show that

$$\mathscr{L}'_n \supsetneqq X(\mathscr{L}_n).$$

Therefore the induced element "$X \bmod l$" in $\mathrm{Hom}_{\mathbb{F}_l}(\mathscr{L}_n \otimes \mathbb{F}_l, \mathscr{L}'_n \otimes \mathbb{F}_l)$ is *not* an isomorphism.

Therefore the image S of G_1 in $\mathrm{Hom}_{\mathbb{F}_l}(\mathscr{L}_n \otimes \mathbb{F}_l, \mathscr{L}'_n \otimes \mathbb{F}_l)$, is an additive subgroup which consists entirely of non-isomorphisms. We apply to it the following lemma, whose proof is left to the reader.

Auxiliary Lemma. *Let k be a field, W and W' two-dimensional k-vector spaces, and $S \subset \mathrm{Hom}_k(W, W')$ an additive subgroup consisting entirely of non-isomorphisms. Then one of the following three possibilities holds:*

(a) $S = 0$.

(b) *The intersection, over all $s \in S$, of* $\mathrm{Ker}(s)$ *is a line $L \subset W$.*

(c) *The sum, over all $s \in S$, of* $\mathrm{Image}(s)$ *is a line $L' \subset W'$.*

We can now conclude the proof of the Key Lemma. In case (a), i.e. $S = 0$, we have G_1 acting trivially on $\mathscr{L}_n / l\mathscr{L}'_n$, so in this case $\mathscr{L}_n \supset l\mathscr{L}'_n$ "works" as the required $\mathscr{L}'' \supset \mathscr{L}'''$. In case (b), we obtain a unique line $L \subset \mathscr{L}_n \otimes \mathbb{F}_l$ which is annihilated by every $s \in S$. By its *unicity*, this line must be stable by the entire group G. Therefore

$$L + l\mathscr{L}_n \supset l\mathscr{L}'_n$$

"works" as the required $\mathscr{L}'' \supset \mathscr{L}'''$. In case (c), the unique line $L' \subset \mathscr{L}'_n \otimes \mathbb{F}_l$ which contains the image of all $s \in S$ must be G-stable. Therefore

$$\mathscr{L}_n \supset L' + l\mathscr{L}'_n$$

"works" in this case. Q.E.D.

It remains to deduce Theorem 1 for general n from Lemmas 1 and 2. The case $n = 1$ of the theorem is precisely Lemma 1. It remains to prove Theorem 1 for $n \geqq 2$. Let G_1 denote the subgroup of G consisting of all $g \in G$ with $\det(g) \equiv 1 \bmod l$. Applying the case $n = 1$ of the theorem to G, we produce an $\mathscr{L} \supset \mathscr{L}'$ which together with $G_1 \subset G$ serves as initial data for applying Lemma 2; this in turn produces G-stable lattices

$$\mathscr{L}'' \supset l\mathscr{L}'' \supset \mathscr{L}'''$$

with $\mathscr{L}''/\mathscr{L}'''$ of order l^n or l^{n+1}, such that G_1 acts trivially on $\mathscr{L}''/\mathscr{L}'''$.

If $G_1 = G$, there is nothing more to prove. If not, let $\Gamma \subset \mathbb{F}_l^\times$ denote the image of G under the composite homomorphism

$$G \xrightarrow{\det} \mathbb{Z}_l^\times \longrightarrow\!\!\!\!\!\rightarrow \mathbb{F}_l^\times.$$

Thus we have a tautological short exact sequence

$$0 \to G_1 \to G \to \Gamma \to 0,$$

which we can non-canonically *split*, as follows.

The subgroup $\Gamma \subset \mathbb{F}_l^\times$ is necessarily cyclic (because $\mathbb{F}_l^\times$ is cyclic), and non-trivial (lest $G_1 = G$). Let $\gamma \in \Gamma \subset \mathbb{F}_l^\times$ be a *generator* of Γ, and denote by $\zeta \in \boldsymbol{\mu}_{l-1}(\mathbb{Z}_l)$ the Teichmuller representative of $\gamma \in \mathbb{F}_l^\times$. Let $g \in G$ be any element such that

$$\det(g) \equiv \gamma \bmod l.$$

The *hypothesis*

$$\det(1-g) \equiv 0 \bmod l^n$$

i.e.

$$\operatorname{trace}(g) \equiv 1 + \det(g) \bmod l^n,$$

shows that the characteristic polynomial $\det(T \cdot 1 - g)$ is congruent mod l to $(T-1)(T-\det(g)) = (T-1)(T-\gamma)$. Because $\gamma \not\equiv 1 \bmod l$, Hensel's lemma shows that g has eigenvalues in $\mathbb{Z}_l^\times$ which are congruent mod l to 1 and ζ respectively. Because G is compact, the limit

$$\lim_{N \to \infty} g^{l^N} \overset{\text{dfn}}{=\!=} h$$

(which obviously exists in $\operatorname{Aut}(V)$, because g has eigenvalues in $\mathbb{Z}_l^\times$) actually lies in G, and has eigenvalues 1 and ζ. The map $\gamma \mapsto h$ then defines a splitting of the exact sequence

$$0 \to G_1 \to G \underset{h \leftarrow \gamma}{\rightleftarrows} \Gamma \to 0$$

By the Cayley-Hamilton theorem, h is diagonizable on *any* h-stable lattice in V, for the orthogonal projections onto its two eigenspaces lie in $\mathbb{Z}_l[h]$:

$$\operatorname{Proj}_1 = \frac{h-\zeta}{1-\zeta}, \qquad \operatorname{Proj}_\zeta = \frac{h-1}{\zeta-1}.$$

Applying these to $\mathscr{L}''$, $\mathscr{L}'''$, we obtain

$$\begin{array}{ccccc} \mathscr{L}'' & = & \operatorname{Proj}_1(\mathscr{L}'') & \oplus & \operatorname{Proj}_\zeta(\mathscr{L}'') \\ \cup & & \cup & & \cup \\ \mathscr{L}''' & & \operatorname{Proj}_1(\mathscr{L}''') & \oplus & \operatorname{Proj}_\zeta(\mathscr{L}'''). \end{array}$$

Let $\{v_1, v_\zeta\}$ be a $\mathbb{Z}_l$-basis of $\mathscr{L}''$ adapted to this decomposition. If we denote by l^a, l^b the respective orders of the quotients

$$\operatorname{Proj}_1(\mathscr{L}'')/\operatorname{Proj}_1(\mathscr{L}'''), \qquad \operatorname{Proj}_\zeta(\mathscr{L}'')/\operatorname{Proj}_\zeta(\mathscr{L}''').$$

then $\{l^a v_1, l^b v_\zeta\}$ is a $\mathbb{Z}_l$-basis of $\mathscr{L}'''$, and both a and b are $\geqq 1$, with $a+b \geqq n$. Because G acts trivially on $\mathscr{L}''/\mathscr{L}'''$, every element $g_1 \in G_1$ has a matrix of the form

$$g_1 \sim \begin{pmatrix} 1+l^a X & l^a Y \\ l^b Z & 1+l^b T \end{pmatrix}$$

while h has the matrix

$$\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}.$$

If we apply the *hypothesis*

$$\det(1-g)\equiv 0 \bmod l^n \quad \text{for all } g\in G$$

to an element of the form $g=g_1 h$, we find

$$l^a X(1-\zeta(1+l^b T))\equiv 0 \bmod l^n.$$

Because $b\geqq 1$ *and* $\zeta\not\equiv 1 \bmod l$, this shows that

$$l^a X\equiv 0 \bmod l^n$$

for every element $g_1\in G_1$. Therefore every $g_1\in G_1$ has matrix, with respect to the base $\{v_1, v_\zeta\}$, of the form

$$\begin{pmatrix} 1+l^n W & l^a Y \\ l^b Z & 1+l^b T \end{pmatrix} \quad W, Y, Z, T\in \mathbb{Z}_l$$

In the base $\{v_1, l^b v_\zeta\}$ of V, every $g_1\in G_1$ has matrix of the form

$$\begin{pmatrix} 1+l^n W & l^{a+b} Y \\ Z & 1+l^b T \end{pmatrix},$$

while h remains diagonal:

$$\begin{pmatrix} 1 & 0 \\ 0 & \zeta \end{pmatrix}$$

Because G is generated by G_1 and h, and $a+b\geqq n$, we find that every element of G has a matrix, w.r.t. the base $\{v_1, l^b v_\zeta\}$, of the required form

$$\begin{pmatrix} 1+l^n W & l^n Y \\ Z & T \end{pmatrix} \quad \text{with } W, Y, Z\in\mathbb{Z}_l,\ T\in\mathbb{Z}_l^\times.$$

[Intrinsically, the lattices

$$\mathrm{Proj}_1(\mathscr{L}'')+\mathrm{Proj}_\zeta(\mathscr{L}''')\supset l^n\,\mathrm{Proj}_1(\mathscr{L}'')+\mathrm{Proj}_\zeta(\mathscr{L}''')$$

"work" as the $\mathscr{L}\supset\mathscr{L}'$ required by theorem 1]. Q.E.D.

As explained above, theorem 1 implies

Theorem 2. *Let E be an elliptic curve over number field K, and $m\geqq 2$ an integer. For each prime $\mathfrak{p}$ of K at which E has good reduction let $N(\mathfrak{p})$ denote the number of $\mathbb{F}_\mathfrak{p}$-rational points on E mod $\mathfrak{p}$. If we have*

$$N(\mathfrak{p})\equiv 0 \bmod m$$

for a set of primes $\mathfrak{p}$ of density one in K, then there exists a K-isogenous elliptic curve E' over K for which

$$\#(\mathrm{Tors}\,E'(K))\equiv 0 \bmod m.$$

Remark. If the field K contains no non-trivial m'th root of unity e.g. if $K=\mathbb{Q}$ and m is *odd*), an elementary consideration of the e_m pairing shows that *any* subgroup of $E'(K)$ of order m is necessarily *cyclic*, i.e. E' has a *rational point* of exact order m. {For m a prime power l^n, the condition "K contains no non-trivial l-power root of unity" corresponds to the case "$G_1 \neq G$" in the final part of the proof of theorem 1.}

To end this section, we record a "numerical" reformulation of Theorem 2.

Theorem 2(bis). *Let E be an elliptic curve over a number field K. Let Σ be any set of primes of K of density one which consists entirely of primes $\mathfrak{p}$ at which E has good reduction and whose absolute ramification indices $e_\mathfrak{p}$ satisfy $e_\mathfrak{p} < p-1$ (e.g. Σ = all odd unramified primes of good reduction for E). Then we have*

$$\operatorname{Sup}_{E'_{K\text{-isog}}\widetilde{\ }E} \{\#\operatorname{Tors} E'(K)\} = \text{g.c.d.}_{\mathfrak{p}\in\Sigma} \{N(\mathfrak{p})\}.$$

A Mild Generalization

I am indebted to Serge Lang for remarking that the proof of Theorem 1 applies, mutatis mutandis, to prove the following analogous result for GL(2) of any local field with finite residue field.

Theorem 1 (bis). *Let K be a field which is complete under a discrete valuation, and whose residue field is finite. Let $\mathcal{O}_K$ denote the ring of integers in K, and let π denote a uniformizing parameter. Let V be a two-dimensional K-vector space, $G \subset \operatorname{Aut}_K(V)$ a compact subgroup, and $n \geqq 1$ an integer. Suppose that we have the congruence*

$$\det(1-g) \equiv 0 \bmod \pi^n$$

for every $g \in G$.

Then there exist a K-basis v_1, v_2 of V, and integers $a, b \geqq 0$, $a+b=n$, with the property that the matrices of the elements of G, expressed in this basis, all lie in the subgroup of $\mathrm{GL}(2, \mathcal{O}_K)$ consisting of all matrices of the form

$$\begin{pmatrix} 1+\pi^a\mathcal{O}_K & \pi^a\mathcal{O}_K \\ \pi^b\mathcal{O}_K & 1+\pi^b\mathcal{O}_K \end{pmatrix},$$

with the convention that when a or b is zero, we interpret $1+\pi^0\mathcal{O}_K$ to mean the group $(\mathcal{O}_K)^\times$ of all units in $\mathcal{O}_K$.

The Case of Two Dimensional Abelian Varieties

In this section, we will show that Problem II has an affirmative answer for two-dimensional abelian varieties. Let us fix a prime number l, and consider a two-dimensional abelian variety A over a number field K.

We begin by analysing the l-adic homology ring of A. Recall that the Tate module $T_l(A)$ is a free $\mathbb{Z}_l$-module of rank four on which $\mathrm{Gal}(\bar{K}/K)$ acts continuously. We denote by V the corresponding four-dimensional $\mathbb{Q}_l$-vector-space

$$V = T_l(A) \underset{\mathbb{Z}_l}{\otimes} \mathbb{Q}_l.$$

We denote by $\mathbb{Z}_l(1)$ the free $\mathbb{Z}_l$-module of rank one

$$\mathbb{Z}_l(1) = \varprojlim_n \boldsymbol{\mu}_{l^n}(\bar{K}),$$

and by $\mathbb{Z}_l(i)$, for $i \in \mathbb{Z}$, its i'th tensor power. For any $\mathbb{Z}_l$-module W on which $\mathrm{Gal}(\bar{K}/K)$ acts, we write $W(i)$ for $W \underset{\mathbb{Z}_l}{\otimes} \mathbb{Z}_l(i)$.

Choose a K-rational polarization of A, attached to a very ample symmetric K-rational divisor $D \subset A$ (since such D's are known to exist over the algebraic closure of K, hence over some finite galois extension of K, we have only to take the union of the distinct $\mathrm{Gal}(\bar{K}/K)$-conjugates of such a D defined over $\bar{K}$ to produce one over K). As is well-known (cf. [2]), such a polarization gives rise to an alternating, $\mathbb{Q}_l$-linear $\mathrm{Gal}(\bar{K}/K)$-equivariant pairing

$$\langle\ ,\ \rangle : V \times V \to \mathbb{Q}_l(1),$$

which is non-degenerate in the sense that it defines an isomorphism

$$V \xrightarrow{\sim} \mathrm{Hom}_{\mathbb{Q}_l}(V, \mathbb{Q}_l(1)) = V^\vee(1).$$

Because V is four-dimensional, we may interpret the alternating form $\langle\ ,\ \rangle$ as being a $\mathrm{Gal}(\bar{K}/K)$-invariant element ξ in

$$\Lambda^2(V) \otimes \mathbb{Q}_l(1) \otimes \det(V)^{-1}$$

which gives rise to $\langle\ ,\ \rangle$ by the formula

$$\langle v_1, v_2 \rangle = v_1 \wedge v_2 \wedge \xi.$$

The non-degeneracy of the pairing $\langle\ ,\ \rangle$ means that $\xi \wedge \xi$ is a non-zero $\mathrm{Gal}(\bar{K}/K)$-invariant element in the one-dimensional space $\Lambda^4(V) \otimes \mathbb{Q}_l(2) \otimes \det(V)^{-2} = \mathbb{Q}_l(2) \otimes \det(V)^{-1}$, i.e., $\xi \wedge \xi$ "is" a $\mathrm{Gal}(\bar{K}/K)$-isomorphism

$$\det(V) \xrightarrow{\sim} \mathbb{Q}_l(2).$$

By this identification, ξ becomes a $\mathrm{Gal}(\bar{K}/K)$-invariant element ξ in

$$\Lambda^2(V) \otimes \mathbb{Q}_l(-1).$$

Because V is four-dimensional, exterior multiplication

$$V \times \Lambda^3(V) \to \Lambda^4(V) = \det(V) \simeq \mathbb{Q}_l(2)$$

defines a $\mathbb{Q}_l$-Gal-isomorphism

$$\Lambda^3(V) \xrightarrow{\sim} \mathrm{Hom}(V, \det(V)) = V^\vee(2) \simeq V(1),$$

whose inverse is "multiplication by ξ",

$$\Lambda\xi\colon V(1) \xrightarrow{\sim} \Lambda^3(V).$$

Again because V is four-dimensional, exterior multiplication

$$\Lambda^2(V) \times \Lambda^2(V) \to \Lambda^4(V) = \det(V) \simeq \mathbb{Q}_l(2)$$

provides a $\mathbb{Q}_l$-Gal-isomorphism of $\Lambda^2(V) \otimes \mathbb{Q}_l(-1)$ with its own dual:

$$(\Lambda^2(V))(-1) \xrightarrow{\sim} ((\Lambda^2(V))(-1))^\vee.$$

Let us denote by $\mathrm{Prim} \subset \Lambda^2(V)$ the subspace ("primitive homology") defined by

$$\mathrm{Prim} = \{\lambda \in \Lambda^2(V) \mid \lambda \wedge \xi = 0\}.$$

Because $\xi \wedge \xi$ is non-zero, we have an *orthogonal* direct-sum $\mathbb{Q}_l$-Gal-decomposition

$$\Lambda^2(V)(-1) \xleftarrow{\sim} \mathbb{Q}_l \oplus \mathrm{Prim}(-1)$$

via the map (ξ, inclusion).

In summary, then, we have the following $\mathbb{Q}_l$-Gal-isomorphisms

$$V \xrightarrow{\sim} V^\vee(1).$$
$$\Lambda^3(V) \xrightarrow{\sim} V(1).$$
$$\Lambda^2(V)(-1) \xrightarrow{\sim} \mathbb{Q}_l \oplus \mathrm{Prim}(-1).$$
$$\mathrm{Prim}(-1) \xrightarrow{\sim} (\mathrm{Prim}(-1))^\vee.$$
$$\det(V) \xrightarrow{\sim} \mathbb{Q}_l(2).$$

In order to "reduce mod l", we may use the Gal-stable lattices $T_l(A) \subset V$ and $(\mathrm{Prim}) \cap (\Lambda^2 T_l(A)) \subset \mathrm{Prim}$. Let us denote by W and P respectively their reductions mod l:

$$W = T_l(A) \otimes \mathbb{F}_l$$
$$P = ((\mathrm{Prim}) \cap (\Lambda^2 T_l(A))) \otimes \mathbb{F}_l.$$

Let us denote by $\overset{s.s.}{\sim}$ the equivalence relation "having isomorphic semi-simplifications as $\mathbb{F}_l[\mathrm{Gal}]$-modules". By the Brauer-Nesbitt theorem, we obtain the following $\overset{s.s.}{\sim}$ equivalences:

$$W \overset{s.s.}{\sim} W^\vee(1)$$
$$\Lambda^3(W) \overset{s.s.}{\sim} W(1)$$
$$\Lambda^2(W)(-1) \overset{s.s.}{\sim} \mathbb{F}_l \oplus P(-1)$$
$$P(-1) \overset{s.s.}{\sim} P(-1)^\vee$$
$$\det(W) \overset{s.s.}{\sim} \mathbb{F}_l(2)$$

Therefore an affirmative solution to Problem II for two-dimensional abelian varieties results from the following theorem, applied to $G=\mathrm{Gal}(\bar{K}/K)$, $k=\mathbb{F}_l$, χ the mod l cyclotomic character, and $W=T_l(A)\otimes\mathbb{F}_l$.

Theorem 3. *Let G be a group, k a perfect field, $\chi: G\to k^\times$ a character of G, and W a four-dimensional k-representation of G. Suppose that*

$W \overset{\text{s.s.}}{\simeq} W^\vee\otimes\chi$

$\Lambda^3 W \overset{\sim}{\simeq} W\otimes\chi$

$\Lambda^2(W)\otimes\chi^{-1}$ *contains the trivial representation* $\mathbb{1}$ *in its semisimplification*

$\det(W)=\chi^2$

If k has characteristic two, suppose further that χ is trivial. In order that the semisimplification of W contain the trivial representation, it is (necessary and) sufficient that we have

$$\det(1-g|W)=0 \quad \text{for all } g\in G.$$

Proof. The necessity is obvious. For sufficiency, we use the universal identity

$$\det(1-g|W)=\Sigma(-1)^i\,\mathrm{trace}(g|\Lambda^i(W))$$

to interpret the vanishing of $\det(1-g|W)$ as saying the representations

$$\mathbb{1}+\Lambda^2(W)+\det(W), \qquad W+\Lambda^3(W)$$

have the *same trace*. As these are both *eight-dimensional* representations it follows that they have the *same characteristic polynomials*, provided the field k has characteristic $\neq 2,3,5,7$ (because the elementary symmetric functions in eight variables are universal polynomials, with coefficients in $\mathbb{Z}[1/8!]$, in the Newton symmetric functions).

Suppose first that k is of characteristic $\neq 2,3,5,7$. Then by the Brauer-Nesbitt theorem we will have

$$\mathbb{1}+\Lambda^2(W)+\det(W)\overset{\sim}{\simeq} W+\Lambda^3(W).$$

Tensoring this equivalence with χ^{-1}, we obtain

$$\chi^{-1}+\Lambda^2(W)\otimes\chi^{-1}+\det(W)\otimes\chi^{-1}\overset{\sim}{\simeq} W\otimes\chi^{-1}+\Lambda^3(W)\otimes\chi^{-1};$$

in view of the hypotheses made on W, we may rewrite this

$$\chi^{-1}+\Lambda^2(W)\otimes\chi^{-1}+\det(W)\otimes\chi^{-1}\overset{\sim}{\simeq} W^\vee+W.$$

By hypothesis, the trivial representation $\mathbb{1}$ occurs in the semisimplification of $\Lambda^2(W)\otimes\chi^{-1}$. Therefore $\mathbb{1}$ must occur in the semisimplification of either W or $W^\vee$, and therefore (autoduality of $\mathbb{1}$!) it occurs in both.

To deal with the "exceptional" cases, when k has characteristic $2,3,5$ or 7, we must resort to more drastic remedies. Let us begin by remarking that we may assume the field k to be algebraically closed (for if we denote by $W^{\text{s.s.}}$ the $k[G]$-

semisimplification of W, then $(W^{ss})\otimes_k \bar{k}$ is still semisimple (because k is perfect), and therefore it is equal to $(W\otimes\bar{k})^{ss}$, the $\bar{k}[G]$-semisimplification of $W\otimes k$. Because the action of G on W^{ss} is k-linear, the subspace $(W^{ss})^G$ of G-invariants in W^{ss} is defined by k-linear equations. Therefore by linear algebra we have

$$(W^{ss})^G\otimes_k \bar{k} \xrightarrow{\sim} (W^{ss}\otimes_k \bar{k})^G = ((W\otimes_k \bar{k})^{ss})^G;$$

in particular $\mathbb{1}$ occurs in W^{ss} exactly as often as $\mathbb{1}$ occurs in $(W\otimes_k \bar{k})^{ss}$).

The point of working over an algebraically closed field k is that the traces of the various inequivalent irreducible finite dimensional k-representations of any group G are known ([1], p. 213) to be *linearly independent* over k. How do we exploit this? Of course, any finite dimensional k-representation M of G can written uniquely, up to semisimplification, in the form

$$M \overset{ss}{\sim} n_1 M_1 + \ldots + n_r M_r$$

with *irreducible* k-representations M_i and integers $n_i \geqq 1$. If k has characteristic $l>0$, write each n_i as

$$n_i = a_i + l r_i, \qquad 0 \leqq a_i \leqq l-1;$$

the we have

$$M \overset{ss}{\sim} \Sigma\, a_i M_i + l(\Sigma\, r_i M_i).$$

The k-linear independence of the *traces* of the M_i means that the representation

$$\Sigma\, a_i M_i$$

is the *unique* semisimple representation with the following two properties:

1) its irreducible components M_i have multiplicities $0 \leqq a_i \leqq l-1$.
2) its trace is *equal* to the trace of M.

Therefore if M and M' are *two* representations with the *same* trace, the above unicity shows that there exist *unique* semisimple representations A, B, C such that

$$M \overset{ss}{\sim} A + lB$$

$$M' \overset{ss}{\sim} A + lC$$

the irreducible components of A all occur with multiplicity $\leqq l-1$.

We now apply this theory to the situation at hand. As explained above, our *hypotheses* on W imply that the two representations

$$W + W^\vee, \qquad \chi^{-1} + \quad \chi^{-1}\otimes \Lambda^2 W \quad + \chi$$

have the *same trace*. Therefore there exist unique semisimple A, B, C, such that

$$W + W^\vee \overset{ss}{\sim} A + lB$$

$$\chi^{-1} + \chi^{-1}\otimes \Lambda^2 W + \chi \overset{ss}{\sim} A + lC$$

the irreducible components of A all occur with multiplicity $\leqq l-1$.

The representation $W+W^\vee$ is visibly self-dual, hence by unicity we have

$$A \simeq A^\vee, \quad B \simeq B^\vee.$$

The representation $\chi^{-1}+\chi^{-1}\otimes \Lambda^2 \mathrm{W}+\chi$ is also self-dual - this is clear for $\chi+\chi^{-1}$, and exterior product pairs $\chi^{-1}\otimes\Lambda^2 W$ perfectly with itself into $\chi^{-2}\otimes\det(W)\simeq\mathbb{1}$. So again by unicity we find

$$A \simeq A^\vee, \quad C \simeq C^\vee.$$

Finally we note that, equating dimensions, we have

$$8=\dim(A)+l\dim(B)=\dim(A)+l\dim(C).$$
$$\dim(B)=\dim(C)$$

We may suppose that neither A nor B contains the trivial representation $\mathbb{1}$ (for $W+W^\vee \overset{\text{s.s.}}{\simeq} A+lB$). As $\mathbb{1}$ lies in the semisimplification of $\chi^{-1}\otimes\Lambda^2 W$ by hypothesis, this forces C to contain $\mathbb{1}$. For $l=5$ or $l=7$, dimension considerations force C to be at most one-dimensional, while for $l=3$ C is at most two-dimensional. Therefore for $l=3,5,7$ we must examine the cases

$$C=\mathbb{1} \quad \text{for } l=3,5,7$$
$$C=\mathbb{1}+D,\ D \text{ 1-dim}'l \quad \text{for } l=3.$$

(The case $l=2$ will require a completely separate discussion.)

We begin with the case $C=\mathbb{1}$, $l=3,5$ or 7. Then B is a character ($\dim(B)=\dim(C)$) of square 1 ($B=B^\vee$). From the equation

$$W+W^\vee=A+lB, \quad l\geqq 3$$

we infer that *either* W or $W^\vee$ must contain at least $2B$'s, and as $B=B^\vee$, *both* W *and* $W^\vee$ contain at least $2B$'s. Thereofre we may write

$$W \overset{\text{s.s.}}{\simeq} 2B+E$$

for some two-dimensional E. Computing determinants, we find

$$\chi^2=\det(W)=B^2\cdot\det E=\det E.$$

Computing $\Lambda^2 W$, we find

$$\Lambda^2 W \overset{\text{s.s.}}{\simeq} B^2+\det E+2B\otimes E$$
$$\overset{\text{s.s.}}{\simeq} \mathbb{1}+\chi^2+2B\otimes E,$$

whence we find

$$\chi^{-1}+\chi^{-1}\otimes\Lambda^2 W+\chi \overset{\text{s.s.}}{\simeq} 2\chi^{-1}+2\chi+2B\otimes E.$$

But

$$\chi^{-1}+\chi^{-1}\otimes\Lambda^2 W+\chi \overset{\text{s.s.}}{\simeq} A+l\mathbb{1}.$$

Therefore $A+l\mathbb{1}$ is *twice* some representation, and in particular $A+l\mathbb{1}$ must contain $\mathbb{1}$ an *even* number of times. As l is *odd* (3, 5, or 7), we we deduce that A contains $\mathbb{1}$. Contradiction.

To conclude the discussion of $l=3$, 5 or 7, we must treat the case $l=3$, $C=\mathbb{1}+D$ with D a character. Then B is two-dimensional ($\dim B=\dim(C)$), and $B=B^\vee$. Consider our equation

$$W+W^\vee=A+3B, \qquad A=A^\vee,\ B=B^\vee.$$

Suppose first that B is *irreducible*. Then either W or $W^\vee$ contains at least two B's, and as $B=B^\vee$ *both* W and $W^\vee$ do. Therefore $W \overset{s.s.}{\sim} 2B \overset{s.s.}{\sim} W^\vee$, hence also $A=B$. From the hypothesis $W \overset{s.s.}{\sim} W^\vee \otimes \chi$ we infer $B=B\chi$, so all in all

$$W \overset{s.s.}{\sim} 2B, \qquad B=B^\vee=B\chi.$$

Taking determinants of $B=B^\vee=B\chi$, we find

$$(\det B)^2=1, \qquad \chi^2=1.$$

Computing $\Lambda^2 W$, we find

$$\begin{aligned}\Lambda^2 W &\overset{s.s.}{\sim} 2\det B+B\otimes B\\ &\overset{s.s.}{\sim} 2\det B+\det B+\mathrm{Sym}^2(B).\\ &\overset{s.s.}{\sim} 3\det B+\mathrm{Sym}^2(B).\end{aligned}$$

From the equation

$$\chi^{-1}+\chi^{-1}\otimes\Lambda^2 W+\chi \overset{s.s.}{\sim} A+3C=A+3\mathbb{1}+3D,$$

and the equality $A=B, B$ supposed irreducible, we infer that $A(=B)$ must be contained in $\chi^{-1}\otimes\Lambda^2 W$, i.e. $\Lambda^2 W$ contains $B\chi$. As $B=B\chi$, we find B contained in $\Lambda^2 W \overset{s.s.}{\sim} 3\det B+\mathrm{Sym}^2(B)$. Again the irreducibility of B forces B to be contained in $\mathrm{Sym}^2(B)$, up to semisimplification. Therefore

$$\mathrm{Sym}^2(B) \overset{s.s.}{\sim} B+?$$

for some *character*? Comparing determinants, we find $?=(\det B)^2=1$ i.e.

$$\mathrm{Sym}^2(B) \overset{s.s.}{\sim} B+\mathbb{1}.$$

As the following sub-lemma shows, this last equation, in characteristic three, is incompatible with the supposed irreducibility of B (though in *any* other characteristic, the standard two-dimensional irreducible representation of the symmetric group on three letters $\mathfrak{S}_3$ satisfies precisely this equation!).

Sub-lemma. *Over a perfect field of characteristic three, any two-dimensional representation B of any group G which satisfies*

$$\mathrm{Sym}^2(B) \overset{s.s.}{\sim} B+\mathbb{1}$$

is the form

$$B \overset{s.s.}{\sim} \mathbb{1} + \det B.$$

Proof. Let $\{a, b\}$ be the two eigenvalues of the action on B of an element $g \in G$. By hypothesis, we have

$$\{a^2, b^2, ab\} = \{a, b, 1\}.$$

Therefore $(ab)^3 = ab$, i.e. $ab = \pm 1$. If $ab = 1$, then

$$\{a^2, b^2\} = \{a, b\},$$

and then either $a^2 = a$, $b^2 = b$ (whence $a = 1$, $b = 1$) or $a^2 = b$, $b^2 = a$ (whence $a^4 = a$, $b^4 = b$, whence $a^3 = b^3 = 1$, whence $a = b = 1$ because we're in characteristic three). If $ab = -1$, then

$$\{a^2, b^2, -1\} = \{a, b, 1\}.$$

Seeking which of $\{a, b, 1\}$ could be -1, we find either $a = -1$ or $b = -1$, and $ab = -1$, so $\{a, b\} = \{1, -1\} = \{1, ab\}$. Therefore the characteristic polynomials of B and of $\mathbb{1} + \det B$ agree. Q.E.D.

We now return to the remaining case in characteristic three, B two-dimensional reducible. Because $B = B^\vee$, we must have

$$B + E + E^\vee, \quad E \text{ one-dimensional.}$$

From the equation

$$W + W^\vee = A + 3B = A + 3E + 3E^\vee$$

we see that the two-dimensional A must be *reducible* (for which of W or $W^\vee$ would possess it?); as $A = A^\vee$ we have

$$A = F + F^\vee \quad F \text{ one-dimensional.}$$

Thus

$$W + W^\vee = 3E + 3E^\vee + F + F^\vee.$$

By symmetry, either W or $W^\vee$ contains at least two E's; interchanging E and $E^\vee$ if necessary, we may suppose W contains at least two E's.

If W contains exactly two E's, then $W^\vee$ contains exactly two $E^\vee$'s, leaving an $E^\vee$ for W. Then $W \overset{s.s.}{\sim} 2E + E^\vee + ?$, $W^\vee \overset{s.s.}{\sim} 2E^\vee + E + ?^\vee$. Interchanging F and $F^\vee$ if necessary, we find

$$W \overset{s.s.}{\sim} 2E + E^\vee + F$$

$$W^\vee \overset{s.s.}{\sim} 2E^\vee + E + F^\vee.$$

Computing determinants, we find

$$\chi^2 = \det W = EF.$$

From the hypothesis $W \overset{s.s.}{\sim} W^v \otimes \chi$, we infer that either we have

$$E = E^\vee \chi, \quad \text{i.e. } E^2 = \chi,$$

or that we have

$$F = E^{\vee} \quad \text{and} \quad E = E\chi.$$

In the first case, we have

$$F = \chi^2 E^{-1} = E^3.$$

Computing $\Lambda^2 W$, we find

$$\Lambda^2 W \overset{S\cdot S\cdot}{\sim} 2\mathbb{1} + 2EF + E^2 + E^{\vee}F$$

$$\overset{S\cdot S\cdot}{\sim} 2\mathbb{1} + 2\chi^2 + 2\chi,$$

whence

$$\chi^{-1} + \chi^{-1} \otimes \Lambda^2 W + \chi \overset{S\cdot S\cdot}{\sim} 3\chi^{-1} + 2\mathbb{1} + 3\chi.$$

Therefore by unicity in the $A + lC$ representation, we find $A = 2\mathbb{1}$, contradiction.

In the second case, we have

$$W \overset{S\cdot S\cdot}{\sim} 2E + 2E^{\vee}$$

$$\chi = \mathbb{1}.$$

Therefore we readily compute

$$\chi^{-1} + \chi^{-1} \otimes \Lambda^2 W + \chi \overset{S\cdot S\cdot}{\sim} 6\mathbb{1} + E^2 + (E^2)^{\vee},$$

and hence we have

$$A + 3C \overset{S\cdot S\cdot}{\sim} E^2 + (E^2)^{\vee} + 6\mathbb{1}.$$

By unicity of the $A + lC$ representation, we have

$$A \overset{S\cdot S\cdot}{\sim} E^2 + (E^2)^{\vee}.$$

But $A = F + F^v$, and by hypothesis $F = E^{\vee}$, so that

$$A = E + E^{\vee} = E^2 + (E^2)^{\vee}.$$

Therefore we have either $E = E^2$, where $E = \mathbb{1}$, or we have $E = (E^2)^{\vee}$, whence $E^3 = \mathbb{1}$ and hence $(l = 3)$ also $E = \mathbb{1}$. So once again $A = 2\mathbb{1}$, contradiction.

The final possibility is that W contains at least $3E$'s. Then $W^{\vee}$ contains at least $3E^{\vee}$'s, wo we must have $W = 3E + ?$, $W^{\vee} = 3E^{\vee}$; again interchanging F and $F^{\vee}$ if necessary, we get

$$W \overset{S\cdot S\cdot}{\sim} 3E + F$$

$$W^{\vee} \overset{S\cdot S\cdot}{\sim} 3E^{\vee} + F^{\vee}.$$

From the hypothesis $W \overset{S\cdot S\cdot}{\sim} W^v \otimes \chi$, we deduce

$$E = E^{\vee}\chi, \quad F = F^{\vee}\chi, \quad \text{i.r.} \quad E^2 = F^2 = \chi.$$

Computing determinants, we find

$$\chi^2 = \det W = E^3 F = E^2(EF) = \chi EF,$$

whence

$$EF = F^2 = E^2 = \chi, \quad \text{and} \quad E = F.$$

Therefore

$$W \overset{\text{s.s.}}{\sim} 4E,$$

whence

$$\Lambda^2 W \overset{\text{s.s.}}{\sim} 6E^2 = 6\chi.$$

Then

$$\chi^{-1} + \chi^{-1} \otimes \Lambda^2 W + \chi = \chi^{-1} + 6\mathbb{1} + \chi.$$

By unicity of the $A + lC$ representation, we have

$$A = \chi^{-1} + \chi = F + F^\vee,$$

ie $F = \chi$ or $F = \chi^{-1}$. But $F^2 = \chi$, so either $\chi^2 = \chi$ or $\chi^{-2} = \chi$. In the first case $\chi = 1$, and in the second case $\chi^3 = 1$, whence $\chi = 1$ because we're in characteristic three. Therefore $\chi = \mathbb{1}$, whence $A = \chi + \chi^{-1} = 2\mathbb{1}$, again a contradiction. This finishes the case $l = 3$.

We now turns to the case $l = 2$, in which case we have, by hypothesis, that χ is *trivial*, i.e.

$$W \overset{\text{s.s.}}{\sim} W^\vee \overset{\text{s.s.}}{\sim} \Lambda^3 W,$$

$\Lambda^2 W$ contains $\mathbb{1}$ in its semisimplification

$$\det(W) = \mathbb{1}.$$

That the two representations in characteristic two

$$2W = W + W^\vee, \qquad \chi^{-1} + \chi^{-1} \otimes \Lambda^2 W + \chi = 2\mathbb{1} + \Lambda^2 W$$

have the same trace tells us precisely that $\Lambda^2 W$ has trace zero; therefore $\Lambda^2 W$ is, up to semisimplification, *twice* some other representation. Because $\Lambda^2 W$ contains $\mathbb{1}$ in its semisimplification, we must have

$$\Lambda^2 W \overset{\text{s.s.}}{\sim} 2(B + \mathbb{1})$$

for some two-dimensional representation B. Computing determinants, we find

$$\mathbb{1} = \det(W)^3 = \det(\Lambda^2 W) = (\det B)^2, \qquad \text{hence } \det B = \mathbb{1}$$

because we are in characteristic two.

Now we make use of the following universal identity on four-dimensional representations W,

$$\Lambda^2(\Lambda^2 W) + \det(W) \overset{\text{s.s.}}{\sim} W \otimes \Lambda^3(W),$$

whose proof, left to the reader, consists in verifying that both sides have the same characteristic polynomial. With our hypothesis, this identity becomes

$$\Lambda^2(2B + 2\mathbb{1}) + \mathbb{1} \overset{\text{s.s.}}{\sim} W \otimes W.$$

For *any* representation W, we have the universal identity

$$W \otimes W \overset{\text{s.s.}}{\sim} \operatorname{Sym}^2(W) + \Lambda^2(W).$$

In characteristic two, if we denote by $W^{(2)}$ the representations obtained from W by applying the absolute Frobenius, squaring, to matrix coefficients, we have the identity

$$\mathrm{Sym}^2(W) \overset{s.s.}{\sim} W^{(2)} + \Lambda^2 W,$$

valid for any representation W in characteristic two. Combining all this, we find

$$\Lambda^2(2B+2\mathbb{1})+\mathbb{1} \overset{s.s.}{\sim} W^{(2)}+2\Lambda^2 W$$

i.e.

$$\Lambda^2(2B+2\mathbb{1})+\mathbb{1} \overset{s.s.}{\sim} W^{(2)}+4(B+\mathbb{1})$$

But we readily compute, for a two-dimensional representation B in characteristic two,

$$\begin{aligned}\Lambda^2(2B+2\mathbb{1}) &\overset{s.s.}{\sim} \Lambda^2(2B)+2B\otimes(2\mathbb{1})+\Lambda^2(2\mathbb{1})\\ &\overset{s.s.}{\sim} 2\det(B)+B\otimes B+4B+\mathbb{1}\\ &\overset{s.s.}{\sim} 2\mathbb{1}+B^{(2)}+2\det(B)+4B+\mathbb{1}\\ &\overset{s.s.}{\sim} 5\mathbb{1}+B^{(2)}+4B.\end{aligned}$$

Comparing this with the previous formula, we find

$$W^{(2)} \overset{s.s.}{\sim} B^{(2)}+2\mathbb{1},$$

whence

$$W \overset{s.s.}{\sim} B+2\mathbb{1}.$$

In particular, the semisimplification of W contains $\mathbb{1}$ (twice!), as required. Q.E.D.

As explained above, Theorem 3 implies

Theorem 4. *Let A be a two-dimensional abelian variety over a number field K. Let Σ be any set of primes of K of density one which consists entirely of primes $\mathfrak{p}$ at which A has good reduction, and whose absolute ramefication indices $e_{\mathfrak{p}}$ satisfy $e_{\mathfrak{p}} < p-1$. For each $\mathfrak{p}\in\Sigma$, let $N(\mathfrak{p})$ denote the numbers of $\mathbb{F}_{\mathfrak{p}}$-rational points on A mod $\mathfrak{p}$. Then the two integers*

$$\sup_{\substack{A'\sim A\\ K\text{-isog}}} \{\#\mathrm{Tors}\, A'(K)\}, \qquad \text{g.c.d.}_{\mathfrak{p}\in\Sigma}\ \{N(\mathfrak{p})\}$$

are divisible by exactly the same primes.

Counter-Examples in Dimension $\geqq 3$

Fix an integer $d\geqq 3$, and an odd integer $N\geqq 3$. We will construct a d-dimensional abelian variety A over a number field K with the following properties:

For almost all primes $\mathfrak{p}$ of K, the number $N(\mathfrak{p})$ of $\mathbb{F}_{\mathfrak{p}}$-rational points on A mod $\mathfrak{p}$ satisfies

$$N(\mathfrak{p})\equiv 0 \bmod N^2;$$

For any abelian variety A' which is K-isogenous to A, the order of $\mathrm{Tors}\, A'(K)$ is *prime* to N.

The construction is based on the observation that the subgroup H of GL(3)

$$H=\left\{\begin{pmatrix}\varepsilon_1 & 0 & 0\\ 0 & \varepsilon_2 & 0\\ 0 & 0 & \varepsilon_3\end{pmatrix}\middle|\ \varepsilon_1=\pm 1,\ \varepsilon_2=\pm 1,\ \varepsilon_3=\pm 1,\ \varepsilon_1\varepsilon_2\varepsilon_3=1\right\}$$

has the following two properties

For every element $h\in H$, we have $\det(1-h)=0$, i.e. at least one of $\varepsilon_1, \varepsilon_2, \varepsilon_3$ is equal to 1.

Over any field of odd characteristic, the given 3-dimensional representation of H is semisimple, and it does not contain the trivial representation; i.e. the ε_i, viewed as characters of H, are all nontrivial, even when reduced modulo an odd prime.

Now pick three abelian varieties A_1, A_2, A_3, the sum of whose dimensions is d, all defined over some number field K_0, and take this number field K_0 large enough that *all* the N-division points of A_1, A_2, and A_3 are K_0-rational.

The group H acts as a group of automorphisms of the product $A_1\times A_2\times A_3$ via

$$\begin{pmatrix}\varepsilon_1 & & \\ & \varepsilon_2 & \\ & & \varepsilon_3\end{pmatrix}: (a_1,a_2,a_3)\mapsto(\varepsilon_1 a_1,\varepsilon_2 a_2,\varepsilon_3 a_3).$$

Pick three distinct odd primes p_1, p_2, p_3 which are unramified in K_0. The Galois group of the extension

$$\begin{array}{ccc} L & \overset{\text{dfn}}{=\!=} & K_0(\sqrt{p_1},\sqrt{p_2},\sqrt{p_3}) \\ & & | \\ K & \overset{\text{dfn}}{=\!=} & K_0(\sqrt{p_1p_2p_3}) \end{array}$$

is isomorphic to H, via

$$\mathrm{Gal}(L/K)\ni\sigma\leftrightarrow h(\sigma)=\begin{pmatrix}\varepsilon_1 & & \\ & \varepsilon_2 & \\ & & \varepsilon_3\end{pmatrix}$$
$$\sigma(\sqrt{p_i})=\varepsilon_i\sqrt{p_i}.$$

Because H acts as automorphisms of $A_1\times A_2\times A_3$, it makes sense first to extend scalars and view $A_1\times A_2\times A_3$ as an abelian variety over K, and then to *twist* it by the above homomorphism

$$\mathrm{Gal}(L/K)\xrightarrow{\sim} H\hookrightarrow \mathrm{Aut}_K(A_1\times A_2\times A_3).$$

The resulting abelian variety will be the required A/K.

To see that this A/K "works", recall that the underlying abelian group $A(\bar{K})$ of $\bar{K}$-valued points of A "is" the group $A_1(\bar{K})\times A_2(\bar{K})\times A_3(\bar{K})$, but that the action of $\mathrm{Gal}(\bar{K}/K)$ on $A(\bar{K})$ becomes, via this identification, the action on $A_1(\bar{K})\times A_2(\bar{K})\times A_3(\bar{K})$ defined by

$$\begin{array}{c}\sigma\colon (a_1,a_2,a_3)\mapsto h(\sigma)(\sigma(a_1),\sigma(a_2),\sigma(a_3))\\ \Vert \\ (\varepsilon_1\sigma(a_1),\varepsilon_2\sigma(a_2),\varepsilon_3\sigma(a_3)).\end{array}$$

Because all the N-division points on $A_1\times A_2\times A_3$ were assumed K_0-rational and therefore K-rational, the representation of $\mathrm{Gal}(\bar{K}/K)$ on $A(\bar{K})_N$ is simply

$$\bigoplus_i A_i(K)_N\otimes\varepsilon_i.$$

By construction, for any $\sigma\in\mathrm{Gal}(\bar{K}/K)$, at least one of the $\varepsilon_i(\sigma)$ has the value 1, and therefore one of the subgroups $A_i(K)_N\subset A(\bar{K})_N$ is fixed by σ. Taking σ to be a Frobenius element $F_{\mathfrak{p}}$ for a prime $\mathfrak{p}$ of K which is prime to $2p_1p_2p_3N$ at which A has good reduction, and remembering that the order of $A_i(K)_N$ is $N^{2\dim(A_i)}$, so certainly divisible by N^2, we find $N(\mathfrak{p})\equiv 0 \bmod N^2$ for such a $\mathfrak{p}$.

But for any prime l dividing N, the above description shows that the mod l representation of $\mathrm{Gal}(\bar{K}/K)$ on $A(\bar{K})_l\sim T_l(A)\otimes\mathbb{F}$ is the direct sum of the characters $\varepsilon_i \bmod l$ with multiplicities $2\dim(A_i)$. Because the $\varepsilon_i \bmod l$ are each *non-trivial*, the semisimplification of $T_l(A)\otimes\mathbb{F}_l$ (i.e. $T_l(A)\otimes\mathbb{F}_l$ itself!) does not contain the trivial representation. As we have already pointed out in the introduction, this means that for any K-isogenous abelian variety A', the order of $\mathrm{Tors}\,A'(K)$ is prime to l. Therefore the order of $\mathrm{Tors}\,A'(K)$ is prime to N for any K-isogenous A'.

Appendix: Injectivity of Reduction mod $\mathfrak{p}$ on Torsion Points

This appendix consists entirely of well-known material; it is included only for the sake of completeness.

Let K be a number field with integer ring $\mathcal{O}$, and let A/K be an abelian variety, with Neron model $\mathbb{A}/\mathcal{O}$. By a fundamental property of Neron models, we have an isomorphism of groups

$$\mathbb{A}(\mathcal{O})\xrightarrow{\sim} A(K).$$

This isomorphism allows us to define, for every prime $\mathfrak{p}$ of K, a "reduction mod $\mathfrak{p}$" homomorphism

$$A(K)\to\mathbb{A}(\mathbb{F}_{\mathfrak{p}})$$

simply by requiring the commutativity of the diagram

$$\begin{array}{ccc} A(K) & \longrightarrow & \mathbb{A}(\mathbb{F}_{\mathfrak{p}})\\ \uparrow\wr & \nearrow_{\mathcal{O}\twoheadrightarrow\mathbb{F}_{\mathfrak{p}}} & \\ \mathbb{A}(\mathcal{O}) & & \end{array}$$

Lemma. *If $e_{\mathfrak{p}} < p-1$, then "reduction* mod $\mathfrak{p}$" *defines an injective map*

$$\mathrm{Tors}\, A(K) \hookrightarrow \mathbb{A}(\mathbb{F}_{\mathfrak{p}}).$$

We will deduce this from a stronger local statement. Denote by $K_{\mathfrak{p}}$ and $\mathcal{O}_{\mathfrak{p}}$ the $\mathfrak{p}$-adic completions of K and $\mathcal{O}$. Because $\mathbb{A} \underset{\mathcal{O}}{\otimes} \mathcal{O}_{\mathfrak{p}}$ is the Neron model of $A \underset{K}{\otimes} K_{\mathfrak{p}}$, we have an isomorphism

$$\mathbb{A}(\mathcal{O}_{\mathfrak{p}}) \xrightarrow{\sim} A(K_{\mathfrak{p}}),$$

and just as above this isomorphism allows us to define a "reduction mod $\mathfrak{p}$" homomorphism

$$A(K_{\mathfrak{p}}) \to \mathbb{A}(\mathbb{F}_{\mathfrak{p}})$$

We have a commutative diagram

$$\begin{array}{ccc} \mathbb{A}(\mathcal{O}) & \xrightarrow{\sim} & A(K) \\ \cap & & \cap \\ \mathbb{A}(\mathcal{O}_{\mathfrak{p}}) & \xrightarrow{\sim} & A(K_{\mathfrak{p}}) \end{array} \searrow \mathbb{A}(\mathbb{F}_{\mathfrak{p}}).$$

Thus our lemma follows from

Lemma'. *If $e_{\mathfrak{p}} < p-1$, then "reduction* mod $\mathfrak{p}$" *defines an injective map*

$$\mathrm{Tors}\, A(K_{\mathfrak{p}}) \hookrightarrow \mathbb{A}(\mathbb{F}_{\mathfrak{p}}).$$

Proof. We must show that the kernel of the map

$$\mathbb{A}(\mathcal{O}_{\mathfrak{p}}) \to \mathbb{A}(\mathbb{F}_{\mathfrak{p}})$$

is torsion-free. This kernel is the group $\hat{\mathbb{A}}(\mathcal{O}_{\mathfrak{p}})$ of $\mathcal{O}_{\mathfrak{p}}$-valued points of the formal group $\hat{\mathbb{A}}$ of $\mathbb{A}$ over $\mathcal{O}$. Because $\mathbb{A}$ is a smooth commutative $\mathcal{O}$-group. $\hat{\mathbb{A}}$ is a commutative formal Lie group over $\mathcal{O}$. Because $e_{\mathfrak{p}} < p-1$, the maximal ideal $\mathfrak{p}\mathcal{O}_{\mathfrak{p}}$ of $\mathcal{O}_{\mathfrak{p}}$ has topologically nilpotent divided powers, and therefore the logarithm and exponential of $\hat{\mathbb{A}}/\mathcal{O}$ define inverse isomorphism of groups

$$\hat{\mathbb{A}}(\mathcal{O}_{\mathfrak{p}}) \underset{\exp}{\overset{\log}{\rightleftarrows}} \mathrm{Lie}(\mathbb{A}/\mathcal{O}) \underset{\mathcal{O}}{\otimes} (\mathfrak{p}\mathcal{O}_{\mathfrak{p}}).$$

In particular, the group $\hat{\mathbb{A}}(\mathcal{O}_{\mathfrak{p}})$ is torsion-free. Q.E.D.

References

1. Curtis, C., Reiner, I.: Representation Theory of Finite Groups and Associative Algebras. New York: Interscience 1962
2. Mumford, D.: Abelian Varieties. Bombay: Oxford University Press 1970
3. Serre, J-P., Tate, J.T.: Good Reduction of Abelian Varieties. Annals Math **88**, 492–517 (1968)
4. Serre, J-P.: Abelian l-adic Representations And Elliptic Curves. New York and Amsterdam: W.A. Benjamin, Inc. 1968
5. Swinnerton-Dyer, H.P.F.: On l-adic represenттions and congruences for coefficients of modular forms (II). In: Modular Functions of One Variable V - Bonn 1976. Lecture Notes 601, pp. 63–91, Berlin Heidelberg New York: Springer 1977

Received June 9, 1980