Abelian varieties having very bad reduction

H.W. Lenstra jr. and F. Oort

Let E be an elliptic curve over a field K with a discrete valuation v with residue class field k. Suppose E has "very bad reduction" at v, i.e. the connected component A_0^0 of the special fibre A_0 of the Néron minimal model is isomorphic to $\mathbb{G}_a$. Then the order of $A_0(k)/A_0^0(k)$ is at most 4 as can be seen by inspection of the usual tables, cf.[9], pp. 124/125, cf. [5], p.46. Thus it follows that if the order of the torsion subgroup Tors(E(K)) is at least 5 and prime to p = char(k), the reduction cannot be very bad. This note arose from an attempt to see whether an explicit classification really is necessary to achieve this result.

We prove a generalization for abelian varieties. The proof does not use any specific classification, but it relies on monodromy arguments. It explains the special role of prime numbers l with $l \leqslant 2g + 1$ in relation with abelian varieties of dimension g.

We give the theorem and its proof in §1. Further we show that the bound in the theorem is sharp (§2), and we give examples in §3 which show that the restriction $l \neq$ char(k) in the theorem is necessary. In §4 we indicate what can happen under the reduction map $E(K) \to E_0(k)$ with points of order p in case of very bad reduction.

§1. Torsion points on an abelian variety having very bad reduction.

Let K be a field and v a discrete valuation of K. We denote the residue class field v by k; we assume k is perfect. Let K_s be a separable closure of K and $\overline{v}$ an extension of v to K_s. We denote the inertia group and first ramification group of $\overline{v}$ by I and J, respectively. These are closed subgroups of the Galois group $\mathrm{Gal}(K_s/K)$. If the residue characteristic char(k) = p is positive, then J is a pro-p-group; if char(k) = 0 then J is trivial. The group J is normal in I, and the group I/J is pro-cyclic:

$$I/J \cong \Pi_{l \text{ prime}, \, l \neq \mathrm{char}(k)} \mathbb{Z}_l.$$

Let A be an abelian variety of dimension g over K, and $\mathcal{A}$ the Néron minimal model of A at v, cf. [9]. We write A_0 for the special fibre : $A_0 = \mathcal{A} \otimes_R k$, where R is the valuation ring of v. We denote by A_0^0 the connected component of A_0. Let

$$0 \to L_s \to L_u \to A_0^0 \to B \to 0$$

be the"Chevalley decomposition" of the k-group variety A_0^0, i.e., B is an abelian variety, L_s is a torus, and L_u is a unipotent linear group. We write

$$\alpha = \dim B, \quad \mu = \dim L_s.$$

We say that A has <u>very bad reduction</u> at v if $L_u = A_0^0$, so if $\alpha = \mu = 0$.

Throughout this paper, l will stand for a prime number different from char(k). If G is a commutative group scheme over K, and $n \in \mathbb{Z}$, we write G[n] for the group scheme $\mathrm{Ker}(n.1_G : G \to G)$, and

$$T_l G = \varprojlim G[l^i](K_s).$$

This is a module over the ring $\mathbb{Z}_l$ of l-adic integers, and it has a continuous action of $\mathrm{Gal}(K_s/K)$. For $G = \mathbb{G}_m$, the multiplicative group, $T_l G$ is free of rank 1 over $\mathbb{Z}_l$, and the supgroup $I \subset \mathrm{Gal}(K_s/K)$ acts trivially on $T_l\mathbb{G}_m$. We write

$$U_l = T_l A.$$

This is a free module of rank 2g over $\mathbb{Z}_l$.

Let M be a finitely generated $\mathbb{Z}_l$-module. By the eigenvalues of an endomorphism of M we mean the eigenvalues of the induced endomorphism of the vector space $M \otimes_{\mathbb{Z}_l} \mathbb{Q}_l$ over the field $\mathbb{Q}_l$ of l-adic numbers. Suppose now that M has a continuous action of I. If $I' \subset I$ is a subgroup, we write

$$M^{I'} = \{x \in M : \tau x = x \text{ for all } \tau \in I'\}.$$

We claim that the image J_0 of J in Aut(M) is finite. If char(k) = 0 this is trivial, so suppose that char(k) = p > 0. Then J_0 is a pro-p-group, and the kernel of the natural map $\mathrm{Aut}(M) \to \mathrm{Aut}(M/lM)$ is a pro-l-group. From $p \neq l$ it follows that J_0 has trivial intersection with this kernel, so J_0 is isomorphic to a subgroup of Aut(M/lM) and therefore finite. This proves our claim.

We define, in the above situation, the averaging map N_J: $M \to M^J$ by $N_J(x) = (\# J_0)^{-1} \cdot \Sigma_{\sigma \in J_0} \sigma x$. This map is the identity on M^J, so gives rise to a splitting

$$(1.1) \qquad M = M^J \oplus \ker N_J.$$

It follows that the function $(\ )^J$ is exact:

$$(1.2) \qquad (M_1/M_2)^J = M_1^J/M_2^J.$$

Notice that M^J has a continuous action of the pro-cyclic group I/J. This is in particular the case for

$$X_l = U_l^J.$$

We denote by σ a topological generator of I/J.

(1.3) Proposition. The multiplicity of 1 as an eigenvalue of the action of σ on $X_l = U_l^J$ is equal to $2\mu + 2\alpha$. In particular, it does not depend on the choice of the prime number $l \neq \mathrm{char}(k)$.

Proof. We begin by recalling the results from [SGA], 7I, exp. IX that we need; see also [11]. Let a polarization of A over K be fixed. Then we obtain a skew-symmetric pairing

$$\langle\ ,\ \rangle : U_l \times U_l \to T_l\,\mathbb{G}_m \cong \mathbb{Z}_l,$$

which is separating in the sense that the induced map $U_l \to \mathrm{Hom}_{\mathbb{Z}_l}(U_l, T_l\mathbb{G}_m)$ becomes an isomorphism when tensored with $\mathbb{Q}_l$. The pairing is Galois-invariant in the sense that

$$\begin{aligned}\langle \tau u, \tau v\rangle &= \tau\langle u,v\rangle \text{ for } \tau \in \mathrm{Gal}(K^s/K),\ u,v \in U_l,\\ &= \langle u,v\rangle \text{ if } \tau \in I.\end{aligned}$$

We write

$$V = U_l^I,\ W = V \cap V^\perp,$$

where $\perp$ denotes the orthogonal complement in U_l with respect to $\langle\ ,\ \rangle$. We have

(1.4) $$\mathrm{rank}_{\mathbb{Z}_l} W = \mu, \quad \mathrm{rank}_{\mathbb{Z}_l} V/W = 2\alpha.$$

Since A has potentially stable reduction, there is an open normal subgroup $I' \subset I$ such that the module

$$V' = U_l^{I'}$$

satisfies

(1.5) $$V'^\perp \subset V'.$$

Notice that $V \subset V'$.

We now take J-invariants. The Galois-invariance of $\langle\ ,\ \rangle$ implies that $X_1 = U_1^J$ is orthogonal to the complement of U_1^J in U_1 defined in (1.1). Therefore $\langle\ ,\ \rangle$ gives rise to a separating Galois-invariant pairing

$$X_1 \times X_1 \to T_1\, \mathbb{G}_m$$

which will again be denoted by $\langle\ ,\ \rangle$. We let § denote the orthogonal complement in X_1 with respect to $\langle\ ,\ \rangle$.

There is a diagram of inclusions

$$\begin{tikzcd}
 & & V \arrow[dr, hook] & & \\
0 \arrow[r, hook, "\mu"] & W \arrow[ur, hook, "2\alpha"] \arrow[dr, hook] & & W^{\S} \arrow[r, hook, "\mu"] & X_1 \\
 & & V^{\S} \arrow[ur, hook, "2\alpha"'] & &
\end{tikzcd}$$

where μ and 2α indicate the $\mathbb{Z}_1$-ranks of the quotients of two successive modules in the diagram; here we use (1.4) and the equalities

$$\operatorname{rank}_{\mathbb{Z}_1}(X_1/W^{\S}) = \operatorname{rank}_{\mathbb{Z}_1}(W),\ \operatorname{rank}_{\mathbb{Z}_1}(W^{\S}/V^{\S}) = \operatorname{rank}_{\mathbb{Z}_1}(V/W),$$

which follows by duality.

All eigenvalues of σ on V are 1, and by duality the same is true for $X_1/V^{\S}$, hence for $X_1/W^{\S}$. We have

$$\operatorname{rank}_{\mathbb{Z}_1} V + \operatorname{rank}_{\mathbb{Z}_1} X_1/W^{\S} = 2\mu + 2\alpha,$$

so in order to prove the proposition it suffices to show that

(1.6) no eigenvalue of σ on $W^{\S}/V$ equals 1.

Let $Y = V'^J$. We first prove that

(1.7) no eigenvalue of σ on Y/V equals 1.

Suppose in fact, that $y \in Y$ satisfies $\sigma y = y + v$ for some $v \in V$.

Then $\sigma^n y = y + nv$ for all positive integers n. Choosing n such that $\sigma^n \in I'$ we also have $\sigma^n y = y$, since $y \in V'$, so we find that $v = 0$ and $y \in V$. This proves (1.7).

We have $Y^\S \subset Y$, by (1.5), so (1.7) implies that

(1.8) no eigenvalue of σ on $(Y^\S + V)/V$ equals 1.

By duality, (1.7) implies that no eigenvalue of σ on $V^\S/Y^\S$ equals 1, and therefore

(1.9) no eigenvalue of σ on $(V^\S+V)/(Y^\S+V)$ equals 1.

From $W = V \cap V^\S$ it follows that $V^\S + V$ is of finite index in $W^\S$, so (1.8) and (1.9) imply the desired conclusion (1.6). This proves Proposition (1.3).

<u>(1.10) Corollary</u>. The abelian variety A has very bad reduction at v if and only if σ has no eigenvalue equal to 1 on X_1.

<u>Proof.</u> Clear from Proposition (1.3). It is easy to prove the corollary directly, using that $\mathrm{rank}_{\mathbb{Z}_1} V = \mu + 2\alpha$.

Let $I' \subset I$ and $Y = (U_1^{I'})^J \subset X_1$ be as in the proof of Propositio (1.3), and n a positive integer for which $\sigma^n \in I'$. Then σ^n acts as the identity on Y, and by duality also on $X_1/Y^\S$. By $Y^\S \subset Y$ this implies that all eigenvalues of σ^n on X_1 are 1. Thus we find that all eigenvalues of σ on X_1 are <u>roots of unity</u>. These roots of unity are of order not divisible by char(k) = p, since the pro-p-part of the group I/J is trivial. Let $a_1(m)$ denote the number of eigenvalues of σ on X_1 that are m-th roots of unity, counted with multiplicities.

(1.11). Proposition. For any two prime numbers l, l' different from char(k) and any positive integer m we have $a_l(m) = a_{l'}(m)$.

Proof. We may assume that m is not divisible by char(k). Let L be a totally and tamely ramified extension of K of degree m. Replacing K by L has no effect on J, but σ should be replacedby σ^m. Since $a_l(m)$ is the multiplicity of 1 as an eigenvalue of σ^m on X_l, the proposition now follows by applying Proposition (1.3) with base field L.

(1.12) Corollary. The number $\operatorname{rank}_{\mathbb{Z}_l} X_l$ does not depend on l.

Proof. This follows from Proposition (1.11), since $\operatorname{rank}_{\mathbb{Z}_l} X_l = \sup_m a_l(m)$.

Remark. Proposition (1.11) and Corollary (1.12) can also easily be deduced from the fact, for each $\tau \in I$, the coefficients of the characteristic polynomial of the action of τ on U_l are rational integers independent of l, see [SGA], 7 I, exp. IX, Théorème 4.3.

(1.13). Theorem. Suppose that A has very bad reduction at v. then for every prime number $l \neq \text{char}(k)$ the number $b(l) \in \{0,1,2,\ldots,\infty\}$ defined by

$$\sup_{N\geq 0} \# A[l^N](K) = l^{b(l)}$$

is finite, and

$$\Sigma_{l \text{ prime}, l \neq \text{char}(k)} (l-1)b(l) \leqslant 2g.$$

Proof. First let l be a fixed prime, $l \neq \text{char}(k)$, and let N be a positive integer. We have

$$\begin{aligned}\#A[l^N](K) &\leqslant \#A[l^N](K_s)^I\\ &= \#(\text{kernel of } \sigma-1 \text{ on } A[l^N](K_s)^J)\\ &= \#(\text{cokernel of } \sigma-1 \text{ on } A[l^N](K_s)^J),\end{aligned}$$

the last equality because $A[l^N](K_s)$ is finite. By (1.2) the natural map

$$X_l = U_l^J \longrightarrow (\dot{U}_l/l^N U_l)^J = A[l^N](K_s)^J$$

is surjective, so the above number is

$$\leqslant \# \text{ (cokernel of } \sigma-1 \text{ on } X_l).$$

Let us write $|\ |_l$ for the normalized absolute value on an algebraic closure $\overline{\mathbb{Q}}_l$ of $\mathbb{Q}_l$ for which $|l|_l = l^{-1}$. Then by a well-known and easily proved formula we have

$$\begin{aligned}&\#(\text{cokernel of } \sigma-1 \text{ on } X_l)\\ &= |\det(\sigma-1 \text{ on } X_l)|_l^{-1}\\ &= \Pi|\zeta-1|_l^{-1},\end{aligned}$$

where ζ ranges over the eigenvalues of σ on X_l.

Letting N tend to infinity we see that we have proved

$$(1.14) \qquad l^{b(l)} \leqslant \Pi|\zeta-1|_l^{-1}.$$

By Corollary (1.10) the right hand side of (1.14) is finite. This proves the claim that $b(l)$ is finite.

Next we exploit the fact that the eigenvalues ζ of σ are roots of unity. It is well-known that for a root of unity $\zeta \neq 1$ we have

$$\begin{aligned}|\zeta-1|_l &\geqslant l^{-1/(l-1)} && \text{if } \zeta \text{ has } l\text{-power order,}\\ |\zeta-1|_l &= 1 && \text{otherwise.}\end{aligned}$$

Write $a_l(l^\infty) = \max\limits_N a_l(l^N)$. Then (1.14) implies that

$$b(l) \leqslant a_l(l^{\infty})/(l-1)$$

so there is a number d(l) such that

$$(l-1)b(l) \leqslant a_l(l^{d(l)}).$$

Now let q be an arbitrary prime number different from char(k). Using proposition (1.11) we deduce

$$\begin{aligned}\Sigma_{l \text{ prime}, l \neq \text{char}(k)} & (l-1).b(l) \\ & \leqslant \Sigma_l\ a_l(l^{d(l)}) \\ & = \Sigma_l\ a_q(l^{d(l)}) \\ & \leqslant \text{rank}_{\mathbb{Z}_q}(X_q) \qquad (\text{since } a_q(1) = 0) \\ & \leqslant \text{rank}_{\mathbb{Z}_q}(U_q) = 2g.\end{aligned}$$

This completes the proof of Theorem (1.13).

(1.15) Corollary. Suppose that A has very bad reduction at v. Denote by m the number of geometric components of the special fibre A_0 of the Néron minimal model of A at v. Then

$$\Sigma_{l \text{ prime}, l \neq \text{char}(k)}(l-1)\ \text{ord}_l(m) \leqslant 2g$$

where $\text{ord}_l(m)$ denotes the number of factors l in m.

Proof. Analogous to the proof of [11], 2.6.

We shall see in Section 3 that the restriction l ≠ char(k) is essential in Theorem (1.13). We do not know whether this is also the case for Corollary (1.15).

§2. An example which shows the bound in theorem (1.13) to be sharp.

(2.1) Example. Let l be an odd prime number, and $g = (l-1)/2$. We construct an abelian variety A of dimension g over a field K with a point of order l rational over K such that A has very bad restriction at a given place of K.

Let $\zeta = \zeta_l$ be a primitive l-th root of unity (in $\mathbb{C}$), and $F := \mathbb{Q}(\zeta)$. We write

$$D = \mathbb{Z}[\zeta]$$

for the ring of integers of F. The field

$$F_0 := \mathbb{Q}(\zeta+\overline{\zeta})$$

is totally real of degree g over $\mathbb{Q}$ and F is a totally imaginary quadratic extension of F_0, i.e. F is a CM field. We choose

$$\phi_j : F \to \mathbb{C},\ \phi_j(\zeta) = e^{j2\pi i/l},\ 1 \leqslant j \leqslant g;$$

in this way, cf.[14], 6.2 and 8.4(1), we obtain an abelian variety

$$B = \mathbb{C}^g/\Gamma,\ \Gamma = (\phi_1,\ldots,\phi_g)(D),$$

with

$$\mathrm{End}(B) = D,$$

with a polarization

$$\lambda : B \to B^t$$

(defined by a Riemann form, cf.[14], page 48) :

$$\mathrm{Aut}(B,\lambda) = \langle\zeta\rangle \times \{\underline{+}1\} \cong \mathbb{Z}/2l;$$

in fact by a theorem of Matsusaka, cf.[3], VII.2, Prop. 8, we know that $\mathrm{Aut}(B,\lambda)$ is a finite group, hence only the torsion elements of the group of units of $\mathbb{Z}[\zeta]$ can be automorphisms of (B,λ), moreover complex multiplicication by ζ leaves the Riemann form invariant (use [14], page 48, line 8), and the result follows. Let $P \in B$ be the point

$$P = \{\phi_j(\frac{1}{1-\zeta}) : 1 \leqslant j \leqslant g\} \bmod \Gamma \in \mathbb{C}^g/\Gamma;$$

note that $1-\zeta$ divides $l \in \mathbb{Z}[\zeta]$, hence P is an l-torsion point; moreover

$$\zeta . \frac{1}{1-\zeta} = -1 + \frac{1}{1-\zeta},$$

hence complex multiplicication by ζ leaves P invariant; thus

$$\mathrm{Aut}(B,\lambda,P) = \langle \zeta \rangle \cong \mathbb{Z}/l.$$

We choose for k an algebraically closed field over which (B,λ,P) is defined (we can choose $k = \mathbb{C}$, but we could also take for k an algebraic closure of $\mathbb{Q}$, cf.[14], p.109, Prop. 26). We recall the notation

$$B[l] := \mathrm{Ker}(l.1_B : B \to B) ;$$

we choose an isomorphism

$$\beta : (\mathbb{Z}/l)^{2g} \xrightarrow{\sim} B[l]$$

such that $\beta(1,0,\ldots,0) = P$. We denote by $A_{g,d,l}$ the fine moduli scheme (over $\mathbb{C}$) of abelian varieties of dimension g, with a polarization of degree d^2, and a level-l-structure (cf.[7], p.129 and page 139, Theorem 7.9). Let d^2 be the degree of the polarization λ defined above, and write:

$(B,\lambda,\beta)=y \in A_{g,d,1}(k)$.

Consider triples (C,μ,γ), where C is an abelian variety (of dimension g), μ a polarization on C (of degree d^2), and

$$\gamma : \mathbb{Z}/1 \hookrightarrow C[1].$$

These objects define a moduli functor, and it is easy to see (using results of [7]), that a coarse moduli scheme exists; we denote it by $A_{1,g,d,1}$; moreover there exists a morphism

$$f : Y = A_{g,d,1} \to A_{1,g,d,1} = X$$

by sending $\mathbb{Z}/1$ into $(\mathbb{Z}/1)^{2g}$ say via the first coordinate. We write

$$(B,\lambda,\gamma) = x \in A_{1,g,d,1}(k) = X(k),$$
$$f(y) = x.$$

The morphism $f : Y \to X$ is a Galois covering (same methods as in [7], 7.3), and the inertia group S_y of the point $y \in Y(k)$ is precisely

$$S = S_y = \mathrm{Aut}(B,\lambda,\gamma)/\mathrm{Aut}(B,\lambda,\beta) =$$
$$= \mathrm{Aut}(B,\lambda,\gamma) \cong \langle\zeta\rangle \cong \mathbb{Z}/1 .$$

Note that $1 \geqslant 3$, thus $Y = A_{g,d,1}$ is a fine moduli scheme (cf. [7], p.139); moreover we work in characteristic zero, hence λ is separable; thus the Grothendieck deformation theory (cf.[10], Theorem (2.4.1)) implies that Y is smooth; thus the completion $\mathcal{O}$ of the local ring of y on Y is a regular local ring. Note that

$$g : \mathbb{Z}/1 = S = \langle\zeta\rangle \hookrightarrow \mathrm{Aut}(\mathcal{O}),$$

and $\mathcal{O}^S = \hat{\mathcal{O}}_{X,x}$.

Futhermore remark that the residue characteristic of $\mathcal{O}$ equals char(k) = 0, hence it is different from l; thus it follows that there exists a local ring homomorphism

$$\mathcal{O} \twoheadrightarrow k[[T]]$$

compatible with the action

$$g : \mathbb{Z}/l \to \mathrm{Aut}(k[[T]]), (g(\bar{1}))(T) = \zeta T$$

for a suitable choice of ζ.

Proof. Let M be the maximal ideal of $\mathcal{O}$, and $y_1,\dots,y_N$ a basis of eigenvectors for the action of $\mathbb{Z}/l$ on M/M^2; these eigenvectors lift to eigenvectors $x_1,\dots,x_N$ in M, and $\mathcal{O} = k[[x_1,\dots,x_N]]$; the action is non-trivial, so $(g(T))(x_i) = \zeta x_i \neq x_i$, for some i; now map this x_i to T and the others to 0.)

Let (A',μ',α') be the abelian variety , etc., define over

$$L = k((T))$$

derived from the universal family over Y; this is the generic fibre of a family over Spec (k[[T]]), whose special fibre is B, thus A' has good reduction at T ↦ 0. We write

$$K := L^S = k((T^l)).$$

Let $\delta' : \mathbb{Z}/l \to A'[l]$ be given by the restriction of α' to the first coordinate, i.e. $\delta'(1) = \alpha'(1,0,\dots,0)$.

Note that

$$u = (A',\mu',\alpha') \in Y(L),$$

$$v = f(A',\mu',\alpha') = (A',\mu',\delta') \in X(\bar{K}).$$

The morphism f is unramified at u (because S_y acts faithfully on L), hence

$$\mathrm{Aut}(A',\mu',\delta') = \{1\}.$$

Moreover L/K is Galois, and for any

$$\sigma \in \mathrm{Gal}(L/K) \cong S,$$

the universal property of $Y = A_{g,d,1}$ induces an isomorphism between (A',μ',δ') and $(A',\mu',\delta')^{\sigma}$. Thus by the usual methods (e.g. see [15], pp. 168/169)we conclude that it is defined over K, i.e.

there exists (A,μ,δ)

defined over K such that

$$(A,\mu,\delta) \otimes_K L \cong (A',\mu',\delta').$$

Let $Q \in A(K)$ be the generator of

$$\langle Q \rangle = \delta(\mathbb{Z}/1\,) \subset A[1],$$

and let v be the valuation on K belonging to the ring

$$R_v := k[[T^{-1}]] \subset k((T^{-1})) = K.$$

We conclude the example by showing :

A has very bad reduction at v

(and note that $Q \in A(K)$ has order $1 = 2g+1$). We know that $A \otimes L = A'$ has good reduction, and the reduction of A' at $T \mapsto 0$ is B. Note that B is of CM-type, hence B is a simple abelian variety. Let $\mathcal{A}$ be the Néron minimal model of A over $k[[T^{-1}]]$, and let $\mathcal{A}'$ be the Néron minimal model of A' over $k[[T]]$; let A_0^0 be the ccnnected component of the special fibre of A, and let

$$0 \to L_s \oplus L_u \to A_0^0 \to C \to 0$$

be the "Chevalley decomposition" as before.

By the minimality property of A' the L-isomorphism

$$A' \otimes L \xrightarrow{\sim} A$$

extends to a $k[[T]]$-homomorphism

$$A' \otimes k[[T]] \to A,$$

hence it defines a k-homomorphism

$$\phi : A_0^0 \to A \otimes k = B.$$

(i) Suppose $C \neq 0$. Note that for any prime number q,

$$T_q(L_u) = 0,$$
$$0 \to T_q(L_s) \to T_q(A_0^0) \to T_q(C),$$

moreover the image of $T_q(A_0^0)$ is of finite index in $T_q(C)$. From this, and from $C \neq 0$ we easily conclude that

$$\begin{tikzcd} A_0^0 \arrow[r, "\phi"] \arrow[d] & B \\ C \arrow[ur, "\psi"'] & \end{tikzcd} \quad ,\psi \neq 0$$

($T_qB = T_q(A')$, and $T_qA_0 = (T_qA)^I$, cf. [13], page 495, Lemma 2, etc.). However, B is simple, thus $\psi(C) = B$, thus $\dim(C) \geqslant \dim(B) = g$; in this way we see that $C \neq 0$ implies that A has good reduction at v; in that case A is an abelian scheme and $\underline{A}[l]$ is étale over $\mathrm{Spec}(k[[T^l]])$. Note that $K = k((T^l))$ is a local field with algebraically closed residue class field k. Thus $\underline{A}[l]$ is constant over K. We define

$$A[l] = A[l](K) \xrightarrow{\sim} A_0[l](k) = B[l](k) \xleftarrow{\sim} A'[l] \underset{\alpha'}{\xleftarrow{\sim}} (\mathbb{Z}/l)^{2g}$$

which is a level-l-structure α on A (over K). The triple (A,μ,α)

induces a K-homorphism $L \to K$, thus $L \cong K$ as K-algebras, a contradictio and we conclude $C = 0$.

(ii). Suppose $L_s \neq 0$. On the one hand

$$\phi(L_s) = 0,$$

(cf. [3],; page 25, Corollary). On the other hand

$$\begin{tikzcd} T_qB \arrow[r, phantom, "="] & T_qA' \arrow[d, equal] \\ 0 = T_qL_s = (T_qA)^I \arrow[u, "\phi_q"] \arrow[r, hook] & T_qA \end{tikzcd}$$

for any prime number q the group T_qL_s would be non zero, and $\phi | T_qL_s = \phi_q$ would be injective, a contradiction with $\phi = 0$. Thus we conclude $C = 0 = L_s$, hence $A_0^0 = L_u$, i.e. A has very bad reduction at v, and the example is established.

(2.2) Remark. The last step of the proof can be deduced from the more general fact:

let K be a field with a discrete valuation v, and $K \subset L$, $w|L = v$ an extension. Let A be an abelian variety over K which has semi-simple rank μ at v (i.e. $\dim L_s = \mu$); then $A \otimes L$ has semi-simple rank $\geqslant \mu$ at w. In case of elliptic curves this is well-known: $\mathbb{G}_m$-reduction implies j(E) is not integral at v, hence E has bad reduction at w, it does not have $\mathbb{G}_a$-reduction, hence it has $\mathbb{G}_m$-reduction.

2.3. Remark. There exists elliptic curves with $\# E[2](K) = 4$ which have $\mathbb{G}_a$-reduction (i.e. very bad reduction: take $Y^2 = X(X-t)(X+t)$ in characteristic $\neq 2$, $\Delta = 64.t^6$, type C_4). Combination with the previou example shows the bound in the theorem to be sharp, i.e. suppose given prime numbers l_i and primitive integers b_i, g, such that

$$\Sigma_i (l_i - 1).b_i \leqslant 2g$$

then there exists an abelian variety A over a local field K such that

$$(\mathbb{Z}/l_i)^{b_i} \subset A(K),\ \dim A = g,$$

and such that A has very bad reduction at v.

§3. Points of order p on elliptic curves having very bad reduction

Let K, v, and k be as in Section 1, and suppose $\mathrm{char}(k) = p > 0$. Let A be an abelian variety over K having very bad reduction at v; we have seen in (1.13) that the prime-to-p torsion in A(K) is very limited in this case. What about the p-power torsion in this case? With the help of some examples we show this torsion can be arbitrarily large.

First we give equal-characteristic examples.

(3.1) Example. Let $p \equiv 5 \pmod 6$ and suppose given an integer $i \geqslant 1$. We construct K, v, k, E such that $\mathrm{char}(K) = p = \mathrm{char}(k)$, E has very bad reduction at v and

$$p^i \text{ divides } \#(E[p^i](K)).$$

Consider $k = \mathbb{F}_p$ and $L = k(t)$, define an elliptic curve C over L by the equation

$$Y^2 = X^3 + aX + a, \qquad a = \frac{27}{4} \cdot \frac{t}{1728 - t};$$

note that

$$j(C) = 1728 \cdot \frac{4a^3}{4a^3 + 27a^2} = t,$$

and that its discriminant equals

$$\Delta = -16(4a^3 + 27a^2) = \alpha t^2;$$

here w is the valuation on L with $w(t) = 1$, with valuation ring $R = k[t]_{(t)}$ and $\alpha \in R^*$ (note that 2 and 3 are invertible in k); thus C has potentially good reduction at w (its j-invariant being integral), and it has bad reduction at w, because its discriminant satisfies

$$0 < w(\Delta) = 2 < 12;$$

note further that for any extension $K \supset L$ of degree not divisible by 6 and for any extension v of w to K the reduction at v is very bad (note that C is of type $II = C_1$ at w, cf. [5], p. 46). Let ϕ be the i-th iterate of the Frobenius homomorphism, and let M be its kernel:

$$0 \longrightarrow M \longrightarrow C \xrightarrow{\phi} E := C^{(p^i)} \longrightarrow 0,$$

thus E is given by the equation

$$Y^2 = X^3 + a^q X + a^q, \quad q = p^i,$$

and M is a local group scheme of rank q. Note that C is not a super-singular elliptic curve (because its j-invariant is not algebraic over k), thus

$$M \otimes_L L_s \cong \mu_q .$$

By duality we obtain

$$M^D = N \subset E, \ N \otimes_L L_s \cong \mathbb{Z}/q.$$

We take for $K \supset L$ the smallest field of rationality for the points in N, and we extend w to a discrete valuation v on K. Note that $K \supset L$ is a Galois extension and the degree

$$[K : L] \text{ divides } \#(\mathrm{Aut}(\mathbb{Z}/q)) = (p-1)p^{i-1};$$

thus 3 does not divide $[K : L]$, we conclude $E \otimes_L K$ has very bad reduction at v; moreover

$$\mathbb{Z}/p^i \subset E(K)$$

by construction, and the Example (3.1) is established.

<u>(3.2) Example</u>. Take $p = 2$, the other data as in (3.1), and we construct E so that

$$2^i \text{ divides } \#(E[2^i](K)).$$

Define C over $L = k(t)$, $k = \mathbb{F}_2$, by the equation

$$Y^2 + tXY = X^3 + t^5;$$

well-known formulas (cf. [5], p. 36) yield:

$$\Delta = t^{11}, \quad j = t;$$

note that 3 does not divide

$$\#(\mathrm{Aut}(\mathbb{Z}/2^i)) = 2^{i-1}, \ i \geqslant 1,$$

and the methods of the previous example carry over.

Now we construct some examples in which $\mathrm{char}(K) = 0 < p = \mathrm{char}(k)$.

<u>(3.3) Example</u>. Take $p = 2$, let $i \geqslant 1$ be an integer. We construct K, v, k, E as before, such that E has very bad reduction at v, and such that $\mathrm{char}(K) = 0$, $\mathrm{char}(k) = 2$, and

$$E[2^i] \subset E(K).$$

Let $m \geqslant 1$ be an integer, define

$$L = \mathbb{Q}(\pi),\ \pi^{m+1} = 2,\ w(\pi) = 1,$$

choose $a \in L$, and let E be given over L by the equation

$$Y^2 + \pi^m XY = X^3 + \pi^2 aX^2 + aX;$$

the point

$$P = (\frac{-1}{\pi^2}, \frac{1}{\pi^3}) \in E(L)$$

is a point of order 2, because it is on the line

$$2Y + \pi^m X = 0,$$

and the same holds for $(0,0) \in E(L)$; thus

$$E[2] \subset E(L).$$

Suppose $w(a) \geqslant 1$; because

$$\Delta = (\pi^{2m} + 4\pi^2 a)^2 a^2 - 64a^3$$

we conclude

$$w(\Delta) = 4m + 2w(a);$$

suppose

$$m = 1 \text{ and } w(a) = 2, \text{ thus } w(\Delta) = 8 \text{ and } w(j) = 0,$$

or

$$m = 2 \text{ and } w(a) = 1, \text{ thus } w(\Delta) = 10 \text{ and } w(j) > 0;$$

then the equation in minimal, the curve E has very bad reduction at w and the reduction is potentially good. Let

$K \supset L$ be the smallest field of rationality for the points of $E[2^i]$; note that

$$\mathrm{Gal}(K/L) \subset \mathrm{Aut}((\mathbb{Z}/2^i)^2) = \mathrm{GL}(2,\mathbb{Z}/2^i)$$

is in the kernel of

$$\mathrm{GL}(2,\mathbb{Z}/2^i) \to \mathrm{GL}(2,\mathbb{Z}/2)$$

(because $E[2] \subset E(K)$ by construction), thus the degree $[K : L]$ is a power of 2, hence it is not divisible by 3. This implies that $v(\Delta)$ is not divisible by 12 (where v is some extension of w to K), thus the reduction of $E \otimes_L K$ at v is very bad (because of $w(j) \geqslant 0$ it cannot become $\mathbb{G}_m$-type). Hence over K we have

$E[2^i] \subset E(K)$, and

E has very bad reduction at v.

<u>(3.4) Example</u>. Let $p \equiv 5 \pmod 6$, and let $i \geqslant 1$ be an integer. We construct K, v, k, E as above with $\mathrm{char}(K) = 0 < \mathrm{char}(k) = p$, with E having very bad reduction at v, and

$$E[p^i] \subset E(K).$$

Consider over $\mathbb{Q}$ the modular curve $X_0(p)_{\mathbb{Q}}$; this is a coarse moduli scheme of pairs $N \subset E$ where E is an elliptic curve and N a subgroup scheme over a field K such that $N(K_s) \cong \mathbb{Z}/p$; consider the scheme $M_0(p)$ over $\mathrm{Spec}(\mathbb{Z})$ (cf. [4], p. DeRa-94, Th. 1.6; cf. [6], p. 63), and consider the point $x_0 \in M_0(p)(\mathbb{F}_p)$

given by $j = 0$. Note that $p \equiv 2 \pmod 3$ implies that the curve E_0 with $j = 0$ is supersingular in characteristic p, hence it has a unique subgroup scheme $\alpha_p \cong N_0 \subset E_0$, the kernel of Frobenius on E_0. Let $\mathcal{O}$ be the local ring of $M_0(p)\otimes_{\mathbb{Z}}W$ at x_0, where $W = W_\infty(\mathbb{F}_{p^2})$ (i.e. W is the unique unramified quadratic extension of $\mathbb{Z}_p$). We know: the local deformation space of $\alpha_p = N_0 \subset E_0$ is isomorphic to the formal spectrum of

$$\mathbb{Z}_p[[X,Y]]/(XY - p),$$

the automorphism group $\mathrm{Aut}(E\otimes\mathbb{F}_{p^2}) = A'$ acts via

$$A'/\pm 1 = \mathbb{Z}/3$$

on $W[[X,Y]]/(XY - p)$, and the completion of $\mathcal{O}$ is canonically isomorphic with the ring of invariants

$$\hat{\mathcal{O}} \cong W[[S,T]]/(ST - p^3),\ S = X^3,\ T = Y^3.$$

(cf. [6], p. 63, cf. [4], VI. 6). Let L be the field of fractions of W (i.e. L is the unramified quadratic extension of $\mathbb{Q}_p$), and construct

$$\mathcal{O} \to \hat{\mathcal{O}} \to L \text{ by } S \mapsto p^2,\ T \mapsto p;$$

this is a point $x \in X_0(p)(L)$; by results by Serre and Milne (cf. [4], p. DeRa-132, Prop. 3.2) we know there exists a pair

$$N \subset E \text{ defined over } L,\ N \otimes L_s \cong \mathbb{Z}/p,$$

with moduli-point x. Let K be the smallest field containing

L such that all points of $E[p^i]$ are rational over K. Note that the degree $[K : L]$ divides $(p-1)^2p^?$, thus it is not divisible by 3; hence

$$\begin{tikzcd}
\mathcal{O} \arrow[r] \arrow[d, hook] & L \arrow[d, hook] \\
W[[X,Y]]/(XY-p) \arrow[r, dotted, "\nexists"] & K
\end{tikzcd}$$

the pair $(N \subset E)\otimes K$ does not extend to a deformation of $\alpha_p \subset E_0$; it follows that E does not have good reduction at the discrete valuation v of K (if so, N would extend flatly, reduce to a subgroup scheme of rank p of E_0, hence to $\alpha_p = N_0 \subset E_0$). Thus E has very bad reduction at v, and by construction

$$E[p^i] \subset E(K).$$

<u>(3.4 bis) Example</u>. Consider p = 11, take 121.H of [5], p. 97. This is a curve E over $L = \mathbb{Q}$ with very bad reduction at $w = v_{11}$, with $w(\Delta) = 2$, with $w(j) \geqslant 0$ and which has a subgroup scheme of order 11. Now proceed as before: $K = L(E[11^i])$, etc., and we obtain a curve E over K with very bad reduction at v (a valuation lying over w), and with $E[11^i] \subset E(K)$.

<u>(3.5) Remark</u>. We have not been able to produce examples analogous to (3.4) in case $p \equiv 1 \pmod 3$. Hence for these primes the situation is not clear; we did not get beyond an example of the following type: -

(3.6) Example. Take $p = 7$, consider a curve with conductor 49 over $\mathbb{Q}$, cf. [5], p. 86. Then $w(\Delta) = 3$ or $w(\Delta) = 9$ (with $w = v_{11}$), and the curve has potentially good reduction (because of CM); furthermore it has a subgroup scheme $N \subset E$ over $\mathbb{Q}$ of rank 7. Thus $K := \mathbb{Q}(N)$ has degree dividing 6, we see that $v(\Delta)$ is not divisible by 12 (where v lies over w) thus E has very bad reduction at v and

$$\mathbb{Z}/7 \subset E(K).$$

(3.7) Example. Consider $p = 3$, and let $i \geqslant 1$ be an integer. We construct K, v, k, E as before with $\mathrm{char}(K) = 0$, $\mathrm{char}(k) = 3$ and $E[3^i] \subset E(K)$. We start with $L = \mathbb{Q}$, $w = v_3$, and we choose an elliptic curve E over $\mathbb{Q}$ with minimal equation f such that:

E has very bad reduction at w,
$w(j) \geqslant 0$,
$w(\Delta_f) \equiv 1 \pmod 2$, and
$(\mathbb{Z}/3) \subset E(\mathbb{Q})$;

such examples exist, e.g. see [5], p. 87, the curve 54.A has $w(\Delta) = 3$, $w(j) \geqslant 0$, and $\mathbb{Z}/3 \cong E(\mathbb{Q})$. Let $K = \mathbb{Q}(E[3^i])$; then $[K : \mathbb{Q}]$ divides $2.3^{?}$, thus $v(\Delta) \not\equiv 0 \pmod 4$ for any v lying over $w = v_3$; thus:

E has very bad reduction at v, and
$E[3^i] \subset E(K)$.

§4. The image of a point of order p under the reduction map.

Let A be an abelian variety over a field K, let $R \subset K$ be the ring defined by a discrete valuation v on K, and let $\mathcal{A}$ be the Néron minimal model of A over Spec(R). At first suppose $n \geqslant 1$ is an integer such that char(k) dos not divide n (here k is the residue class field of v, i.e. $k = R/\mathfrak{m}$). Let $\mathcal{A}[n]$ denote the kernel of multiplication by n on $\mathcal{A}$. Note that

$$\mathcal{A}[n] \rightarrow \mathrm{Spec}(R)$$

is étale and quasi-finite. Thus we see that A(K)[n] injects in $A_0(k)$ (here $A_0 = \mathcal{A} \otimes_R k$ is the special fibre), and all torsion points of $A_0(\overline{k})$ lift to torsion points of A defined over an extension of K which is unramified at v. In short: for n-torsion the relation between A(K) and $A_0(\overline{k})$ is clear (as long as char(k) does not divide n).

We give some examples what happens if we consider points whose order is divisible by char(k) = p > 0. Also in case of stable reduction it is not so difficult to describe the situation ($\mathcal{A}[p] \rightarrow \mathrm{Spec}(R)$ is quasi-finite in that case). Thus we suppose the reduction is <u>very bad</u>; in that case all points on the connected component A_0^0 of the special fibre A_0 are p-power torsion, and $\mathcal{A}[p] \rightarrow \mathrm{Spec}(R)$ is <u>not</u> quasi-finite. We use the filtration on E(K) as introduced in [5], Section 4.

$$E(K) \supset E(K)_0 \supset E(K)_1$$

where

$$E(K)_m = \{(x,y) \in E(K) \mid v(x) \leqslant -2m,\ v(y) \leqslant -3m\}$$

after having chosen a minimal equation for E.

(4.1.1) Remark. We take $p > 3$. If $P \in E(K)$ (and $\mathrm{ord}(P) = p = \mathrm{char}(k)$, and E has very bad reduction at v) then $P \in E(K)_0$ (because $p > 3$ does not divide the number of connected components of E_0, and $E(K)_0 \to E_0^0(k)$, use p. 46, table of [5]). We show that both cases $P \notin E(K)_1$ and $P \in E(K)_1$ indeed occur:

(4.1.2) Example. Take $p > 3$, we construct $P \in E(K)$, $\mathrm{ord}(P) = p$ and $P \notin E(K)_1$. Let E be the curve 150.C (cf. [5], p. 103), thus the curve given by the minimal equation

$$Y^2 + XY = X^3 - 28X + 272;$$

it has very bad reduction at $v = v_5$ (because 5^2 divides its conductor 150), and it has a point of order 5 (indeed $\#E(\mathbb{Q}) = 10$). We claim

$$P \in E(\mathbb{Q})_0, \ P \notin E(\mathbb{Q})_1$$

(relative the valuation v_5). This we can prove as follows: by (4.1.1) we know $P \in E(\mathbb{Q})_0$, thus the group $<P> = N \subset E$ extends flatly to a finite group scheme

$$\mathcal{N} \subset \mathcal{E}$$

over $\mathrm{Spec}(\mathbb{Z}_{(5)})$ (one can work with the Néron minimal model $\mathcal{E}$, but also with the (plane) Weierstrass minimal model, and then $\mathcal{N} \otimes \mathbb{F}_5$ is not the singular point because of $P \in E(\mathbb{Q})_0$). If we would have $P \in E(\mathbb{Q})_1$ then it would follow

$$\alpha_5 \cong \mathcal{N} \otimes \mathbb{F}_5$$

(because of very bad reduction), but α_5 over $\mathbb{F}_5$ does not lift to the unramified situation $\mathbb{Z}_{(5)} \to \mathbb{F}_5$ (cf. [16], Section 5), thus

$$P \notin E(\mathbb{Q})_1.$$

One can avoid the abstract proof by an explicit computation:

$$P = (-4,20) \in E(\mathbb{Q}),\ P \notin E(\mathbb{Q})_1,$$

the tangent line at P is $y = 20$, so

$$-2P = (8,20),$$

the tangent line at $-2P$ is $3X - Y - 4 = 0$, so

$$4P = (-4,-16) = -P,$$

thus $\langle P\rangle \cong \mathbb{Z}/5$; the singular point on E mod 5 is $(x = 2, y = -1) \bmod 5$, thus $P \in E(\mathbb{Q})_0$, and the example is established.

<u>(4.1.3) Remark</u>. Take $p > 3$, and construct $Q \in E(K)_1$ with $\operatorname{ord}(Q) = p$. Indeed, take $i > 1$, and use Example (3.4); then $\operatorname{ord}(P) = p^i$, and $P \in E(K)_0$ (because of 4.1.1), thus $p.P \in E(K)_1$ (because E has very bad reduction), thus $Q := p^{i-1}P \in E(K)_1$ and $\operatorname{ord}(Q) = p$.

Next we choose $p = 3$, and we show various possibilities indeed occur:

<u>(4.2.1) Example</u>. We construct $P \in E(\mathbb{Q})$, with $\operatorname{ord}(P) = 3$, $P \notin E(\mathbb{Q})_0$. Let E be given by the equation

$$Y^2 + 3aXY + 3bY = X^3;$$

by well-known formulas (cf. [5], p. 36) one computes

$$\Delta = 3^6 b^3 (a^3 - 3b).$$

If 3^6 does not divide $b^3(a^3 - 3b)$ this equation is minimal (e.g. take $a = 1 = b$). Furthermore $P = (0,0)$ is a flex on E (hence $\mathrm{ord}(P) = 3$), and E mod 3 has a cusp at $(0,0)$. Thus $P \notin E(\mathbb{Q})_0$.

<u>(4.2.2) Example</u>. It is very easy to give $P \in E(K)$ with $\mathrm{ord}(P) = 3$, $P \in E(K)_0$ and $P \notin E(K)_1$. E.g.

$$P = (0,2) \text{ on } Y^2 = X^3 + 4$$

(cf. 108.A, [5], p. 95) has this property, because $(x = -1, y = 0)$ mod 3 is the singular point on E mod 3, thus P reduces to a point on E_0^0 but not to the identity. Another example:

$$P = (0,0) \text{ on } Y^2 + Y = X^3$$

(cf. 27.A, [5], p. 83) is a flex, which does not reduce to the cusp $(x = 1, y = 1)$ mod 3 on E mod 3.

<u>(4.2.3) Example</u>. We construct $P \in E(K)$ with $\mathrm{ord}(P) = 9$, $P \notin E(K)_0$ and $3P \notin E(K)_1$. Indeed consider $K = \mathbb{Q}$, $v = v_3$, and take 54.B (cf. [5]. p. 87), a curve which has very bad reduction at 3 such that $\# E(\mathbb{Q}) = 9$. Note that $\mathbb{Q}$ does not contain a primitive cube root of unity, thus $E(\mathbb{Q})$ does not contain $(\mathbb{Z}/3)\mathrm{x}(\mathbb{Z}/3)$, hence

$$E(\mathbb{Q}) \cong \mathbb{Z}/9;$$

let P be a generator for this group. Note that α_3 over $\mathbb{F}_3$ does not lift to $\mathbb{Z}_{(3)}$, thus P and 3P do not reduce to the identity under reduction modulo 3, hence

$$E(\mathbb{Q}) \to E(\mathbb{Q})/E(\mathbb{Q})_1$$

is injective, thus

$$\mathrm{ord}(P) = 9,\ 3P \notin E(\mathbb{Q})_1,\ P \notin E(\mathbb{Q})_0,$$

and note that the extension

$$0 \to E(\mathbb{Q})_0 \to E(\mathbb{Q}) \to \mathbb{Z}/3 \to 0$$

is non-split.

(4.2.4) Remark. Take i = 3 in (3.7), then

$$p = 3,\ P \in E(K),\ \mathrm{ord}(P) = 3^3$$

and E has very bad reduction at v. Then

$$3P \in E(K)_0,\ 0 \neq 9P \in E(K)_1,$$

thus Q := 9P has the property

$$\mathrm{ord}(Q) = 3,\ Q \in E(K)_1.$$

(4.3) Example. We conclude by an example with p = 2. Consider 48.E (cf. [5], p. 86), i.e.

$$Y^2 = X^3 + X^2 + 16X + 180;$$

the right hand side factors over $\mathbb{Q}$ in the irreducible factors

$$(X + 5)(X^2 - 4X + 36),$$

hence $E[2](\mathbb{Q}) = \mathbb{Z}/2$. Because $\#E(\mathbb{Q}) = 8$ we conclude

$$E(\mathbb{Q}) \cong \mathbb{Z}/8$$

(of course it is well-known that such examples exist, e.g. cf. [6], p. 35, Th. 8). Thus

$$E(\mathbb{Q})_1 = 0, \ E(\mathbb{Q})_0 = \mathbb{Z}/2 \ = <Q = (5,0)>$$

and

$$E(\mathbb{Q})/E(\mathbb{Q})_0 \cong \mathbb{Z}/4$$

(because $(0,0)$ mod 2 is the cusp on E mod 2, and Q mod 2 is smooth on E mod 2).

References

[1] A. Fröhlich - Local fields. In: Algebraic number theory, Ed. J.W.S. Cassels & A. Fröhlich. Academic Press, 1967.

[2] A. Grothendieck, M. Raynaud & D.S. Rim - Séminaire de géométrie algébrique, SGA 7 I, 1967-1969. Lect. Notes Math. 288, Springer-Verlag, 1972.

[3] S. Lang - Abelian varieties. Intersc. Publ. 1959.

[4] Modular functions of one variable II (Antwerp, 1972). Lect. Notes Math. 349, Springer-Verlag 1973. Expecially: P. Deligne & M. Rapoport - Les schémas de modules de courbes elliptiques, pp. 143-316.

[5] Modular functions of one variable IV (Antwerp, 1972). Lect. Notes Math. 476, Springer-Verlag 1975. Expecially: J. Tate - Algorithm for determining the type of a singular fibre in an elliptic pencil, pp. 33-52; Table 1, pp. 81-113.

[6] B. Mazur - Modular curves and the Eisenstein ideal. Publ. Math. No. 47, IHES 1978.

[7] D. Mumford - Geometric invariant theory. Ergebnisse, Vol. 34, Springer-Verlag 1965.

[8] M. Nagata - Complete reducibility of rational representations of a matric group. J. Math. Kyoto Univ. 1 (1961), 87-99.

[9] A. Néron - Modèles minimaux des variétés abéliennes sur les corps locaux et globaux. Publ. Math. No. 21, IHES 1964.

[10] F. Oort - Finite group schemes, local moduli for abelian varieties and lifting problems. Compos. Math. 23 (1971), 265-296 (also in: Algebraic geometry, Oslo 1970, Wolters-Noordhoff Publ. Cy., 1972).

[11] F. Oort - Good and stable reduction of abelian varieties. Manuscr. Math. 11 (1974), 171-197.

[12] J.-P. Serre - Corps locaux. Act. Sc. Ind. 1296; Hermann, Paris 1962.

[13] J.-P. Serre & J. Tate - Good reduction of abelian varieties. Ann. Math. 88 (1968), 492-517.

[14] G. Shimura & Y. Taniyama - Complex multiplication of abelian varieties and its applications to number theory. The Math. Soc. Japan, 1961.

[15] G. Shimura - On the field of rationality for an abelian variety. Nagoya Math. Journ. 45 (1972), 167-178.

[16] J. Tate & F. Oort - Group schemes of prime order. Ann. Sc. École Norm. Sup. 4me série, 3 (1970), 1-21.

H.W. Lenstra jr.
Mathematisch Instituut
Roetersstraat 15
1018 WB AMSTERDAM

F. Oort
Mathematisch Instituut
Budapestlaan 6
3508 TA UTRECHT