



Semistable abelian varieties with good reduction outside 15.

René Schoof

Dipartimento di Matematica
2^a Università di Roma “Tor Vergata”
I-00133 Roma ITALY
Email: schoof@science.uva.nl

Abstract. We show that there are no non-zero semi-stable abelian varieties over $\mathbf{Q}(\sqrt{5})$ with good reduction outside 3 and we show that the only semi-stable abelian varieties over \mathbf{Q} with good reduction outside 15 are, up to isogeny over \mathbf{Q} , powers of the Jacobian of the modular curve $X_0(15)$.

1. Introduction.

In his paper [3], Luis Dieulefait gives a proof of Serre’s modularity conjecture for the case of odd level and arbitrary weight. By means of an intricate inductive procedure he reduces the issue to the case of Galois representations of level 3 and weight 2, 4 or 6. As explained in [3], these cases are taken care of by the following three theorems respectively.

Theorem 1.1. *There are no non-zero semi-stable abelian varieties over \mathbf{Q} with good reduction outside 3.*

Theorem 1.2. *There are no non-zero semi-stable abelian varieties over $\mathbf{Q}(\sqrt{5})$ with good reduction outside 3.*

Theorem 1.3. *Every semi-stable abelian variety over \mathbf{Q} with good reduction outside 15 is isogenous, over \mathbf{Q} , to a power of the Jacobian of the modular curve $X_0(15)$.*

Theorem 1.1 is due to Brumer and Kramer [2]. In this paper we prove Theorems 1.2 and 1.3, each of which imply Theorem 1.1.

In section 2 we discuss extensions of μ_p and $\mathbf{Z}/p\mathbf{Z}$ by one another. These play an important role in this paper. In section 3 we prove Theorem 1.2 and in section 4 we prove Theorem 1.3.

2. Extensions of μ_p and $\mathbf{Z}/p\mathbf{Z}$ by one another.

This section contains preliminary material used in the proofs of Theorems 1.2 and 1.3 given in the next two sections. Let F be a number field and set $\Gamma = \text{Gal}(\overline{F}/F)$. Let S be a finite set of primes of F and let R denote the ring of S -integers.

Lemma 2.1. *Let p be a prime and let G, H be finite flat group schemes over R that are killed by p . Let $\text{Ext}_{R,[p]}^1(G, H)$ denote the subgroup of $\text{Ext}_R^1(G, H)$ consisting of the extensions of G by H that are killed by p . Then there is a natural exact sequence*

$$0 \longrightarrow \text{Ext}_{R,[p]}^1(G, H) \longrightarrow \text{Ext}_R^1(G, H) \longrightarrow (\text{Hom}_{\text{ab}}(H(\overline{F}), G(\overline{F}))_{\Gamma})^{\vee}.$$

Proof. First we consider extensions of G by H over the quotient field F . Clearly $\text{Ext}_{F,[p]}^1(G, H)$ is the kernel of the natural map $\text{Ext}_F^1(G, H) \longrightarrow \text{Ext}_{\text{ab}}^1(G(\overline{F}), H(\overline{F}))$. Moreover, Γ acts on $\text{Ext}_{\text{ab}}^1(G(\overline{F}), H(\overline{F}))$ and the image of the map is contained in the subgroup of the Γ -invariant extensions. Since $\text{Ext}_{\text{ab}}^1(G(\overline{F}), H(\overline{F}))$ is naturally isomorphic to the \mathbf{Q}/\mathbf{Z} -dual of $\text{Hom}_{\text{ab}}(H(\overline{F}), G(\overline{F}))$, the lemma follows, but with the ring R replaced by its quotient field F .

To get the sequence over R , we observe that the following diagram is Cartesian

$$\begin{array}{ccc} \text{Ext}_{R,[p]}^1(G, H) & \xrightarrow{\subset} & \text{Ext}_R^1(G, H) \\ \downarrow & & \downarrow \\ \text{Ext}_{F,[p]}^1(G, H) & \xrightarrow{\subset} & \text{Ext}_F^1(G, H) \end{array}$$

Indeed, if the generic fiber of a finite flat group scheme over R is killed by p , then so is the group scheme itself. Therefore the induced map between the cokernels of the two horizontal homomorphisms is injective. This implies the lemma.

We turn next to extensions of $\mathbf{Z}/p\mathbf{Z}$ by μ_p . First we construct one such extension over the ring $\mathbf{Z}[\zeta_p]$. Applying the functor $\text{Hom}(\mathbf{Z}/p\mathbf{Z}, -)$ to the exact sequence $0 \rightarrow \mu_p \rightarrow \mu_{p^2} \rightarrow \mu_p \rightarrow 0$, we obtain an injective homomorphism $\text{Hom}(\mathbf{Z}/p\mathbf{Z}, \mu_p) \longrightarrow \text{Ext}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$. The image of any non-zero morphism $\mathbf{Z}/p\mathbf{Z} \rightarrow \mu_p$ is a non-split extension

$$0 \longrightarrow \mu_p \longrightarrow C \longrightarrow \mathbf{Z}/p\mathbf{Z} \longrightarrow 0$$

with group of points $C(\overline{F})$ cyclic of order p^2 and trivial action by $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q}(\zeta_p))$.

For every S -unit $\varepsilon \in R^*$ we let G_{ε} denote the group scheme over R as defined in [8, p.418]. It is an extension of $\mathbf{Z}/p\mathbf{Z}$ by μ_p . Its group of points is killed by p and the Galois group $\Gamma = \text{Gal}(\overline{F}/F)$ acts through matrices of the form

$$\begin{pmatrix} \omega & \psi \\ 0 & 1 \end{pmatrix}$$

where, for a suitable choice of a p -th root of unity ζ_p in \overline{F} , the character ψ is given by the formula $\zeta_p^{\psi(\sigma)} = \sigma(\sqrt[p]{\varepsilon})/\sqrt[p]{\varepsilon}$ for every $\sigma \in \Gamma$. Two group schemes G_{ε} and $G_{\varepsilon'}$ are isomorphic if and only if ε/ε' is a p -th power.

Proposition 2.2. *Let p be a prime and let w_p denote the number of p -th roots of unity in R . Then*

- (i) *The index of $\text{Ext}_{R,[p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ inside $\text{Ext}_R^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ is equal to w_p ;*
- (ii) *If the class number of R is not divisible by p , then $\text{Ext}_{R,[p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ consists of the extensions provided by the group schemes G_ε with $\varepsilon \in R^*$. The group $\text{Ext}_{R,[p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ is naturally isomorphic to R^*/R^{*p} .*

Proof. (i) A non-trivial homomorphism $\mu_p(\overline{F}) \rightarrow \mathbf{Z}/p\mathbf{Z}$ is Γ -equivariant if and only if the field F contains the p -th roots of unity. Therefore Lemma 2.1 implies that the index is at most w_p . When $w_p = 1$ we have equality. If $w_p = p$ we observe that the group scheme C constructed above is *not* killed by p and we again have equality. This proves (i).

(ii) By the long exact sequence of flat cohomology groups associated to the exact sequence $0 \rightarrow \mathbf{Z} \rightarrow \mathbf{Z} \rightarrow \mathbf{Z}/p\mathbf{Z} \rightarrow 0$, we get an exact sequence

$$0 \longrightarrow \mu_p(R) \longrightarrow \text{Ext}_R^1(\mathbf{Z}/p\mathbf{Z}, \mu_p) \longrightarrow H_{\text{flat}}^1(\text{Spec}(R), \mu_p) \longrightarrow 0.$$

The non-trivial classes in $\text{Ext}_R^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ that come from $\mu_p(R)$ are all isomorphic to the group scheme C constructed above. By part (i), the group $\text{Ext}_{R,[p]}^1(\mathbf{Z}/p\mathbf{Z}, \mu_p)$ is therefore isomorphic to $H_{\text{flat}}^1(\text{Spec}(R), \mu_p)$. The latter group sits in the exact Kummer sequence

$$0 \longrightarrow R^*/R^{*p} \longrightarrow H_{\text{flat}}^1(\text{Spec}(R), \mu_p) \longrightarrow \text{Cl}(R)[p] \longrightarrow 0.$$

Since p does not divide the class number of R , part (ii) follows.

The rest of this section is devoted to extensions by μ_p by $\mathbf{Z}/p\mathbf{Z}$. For simplicity we restrict ourselves to the case $p = 2$. This is all we need in the applications.

Proposition 2.3. *Suppose that $2 \notin S$. Then every extension of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 over R is killed by 2. If in addition the class number of R is odd and 2 is prime in R , then there is a natural isomorphism*

$$\text{Ext}_R^1(\mu_2, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{\cong} \{\varepsilon \in R^* : \varepsilon \text{ is a 2-adic square}\} / R^{*2}.$$

It maps an extension to the unit $\varepsilon \in R^$ that has the property that the Galois group acts on the points through matrices of the form*

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

where χ is given by the formula $(-1)^{\chi(\sigma)} = \sigma(\sqrt{\varepsilon})/\sqrt{\varepsilon}$ for every $\sigma \in \Gamma$.

Proof. Every extension of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 over the ring of S -integers R is killed by 2 over $R \otimes \mathbf{Z}_2$ and hence, since $2 \notin S$, also over R . Moreover, we also have that $\text{Hom}_R(\mu_2, \mathbf{Z}/2\mathbf{Z}) = \text{Ext}_R^1(\mu_2, \mathbf{Z}/2\mathbf{Z}) = 0$. Since 2 is prime in R , the group $\mu_2(F \otimes \mathbf{Q}_2)$ has order 2. Therefore the Mayer-Vietoris sequence in [8, Cor.2.4] gives rise to the sequence

$$0 \longrightarrow \text{Ext}_R^1(\mu_2, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \text{Ext}_{R[\frac{1}{2}]}^1(\mu_2, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \text{Ext}_{R \otimes \mathbf{Q}_2}^1(\mu_2, \mathbf{Z}/2\mathbf{Z})$$

Since the group schemes μ_2 and $\mathbf{Z}/2\mathbf{Z}$ are isomorphic over the rings $R[\frac{1}{2}]$ and $R \otimes \mathbf{Q}_2$ we may switch their roles. A short computation, using the fact that 2 does not divide the class number of R , leads to the following commutative diagram with exact rows

$$\begin{array}{ccccccc} 0 & \rightarrow & \mu_2(R[\frac{1}{2}]) & \longrightarrow & \text{Ext}_{R[\frac{1}{2}]}^1(\mu_2, \mathbf{Z}/2\mathbf{Z}) & \longrightarrow & R[\frac{1}{2}]^*/R[\frac{1}{2}]^{*2} \longrightarrow 0, \\ & & \parallel & & \downarrow & & \downarrow \\ 0 & \rightarrow & \mu_2(F \otimes \mathbf{Q}_2) & \longrightarrow & \text{Ext}_{F \otimes \mathbf{Q}_2}^1(\mu_2, \mathbf{Z}/2\mathbf{Z}) & \longrightarrow & (F \otimes \mathbf{Q}_2)^*/(F \otimes \mathbf{Q}_2)^{*2} \longrightarrow 0. \end{array}$$

We deduce that $\text{Ext}_{R[\frac{1}{2}]}^1(\mu_2, \mathbf{Z}/2\mathbf{Z})$ is isomorphic to the kernel of the rightmost vertical map. Since the prime 2 is principal the proposition follows.

We apply Proposition 2.3 to $F = \mathbf{Q}$ and the ring $R = \mathbf{Z}[\frac{1}{15}]$. The unit group R^* is generated by $-1, 3$ and 5 . The kernel of the map $R^*/R^{*2} \rightarrow \mathbf{Q}_2^*/\mathbf{Q}_2^{*2}$ is the cyclic group generated by -15 . Therefore $\text{Ext}_R^1(\mu_2, \mathbf{Z}/2\mathbf{Z})$ has order 2.

Definition. Let Φ denote the *unique* non-split extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$ over $\mathbf{Z}[\frac{1}{15}]$:

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow \Phi \longrightarrow \mu_2 \longrightarrow 0.$$

Since Φ is unique, it is self-dual. The Galois group $\text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ acts on $\Phi(\overline{\mathbf{Q}})$ through the unique quadratic character χ of conductor 15. The group scheme Φ is isomorphic to the group scheme of 2-torsion points of the semi-stable elliptic curve [1, p.82] of conductor 15 given by the minimal Weierstrass equation $Y^2 + XY + Y = X^3 + X^2$. The coordinates of the points of order 2 are $x = -1$ and $x = \frac{-1 \pm \sqrt{-15}}{8}$. The Zariski closure of the point $(-1, 0)$ is isomorphic to the closed subgroup scheme $\mathbf{Z}/2\mathbf{Z}$.

Remark 2.4. In section 3, we consider Φ over the extension ring $\mathbf{Z}[\eta, \frac{1}{15}]$. Here $\eta = \frac{1}{2}(1 + \sqrt{5})$. Let $F = \mathbf{Q}(\sqrt{5})$ and $F_2 = F \otimes \mathbf{Q}_2$. Let ω_3 denote the unique Dirichlet character of conductor 3. Since $-15 = -3$ times a square in F , the restrictions of the characters χ and ω_3 to $\text{Gal}(\overline{F}/F)$ are equal. Therefore χ is unramified at 5 and Φ can be extended to a finite flat group scheme over the ring $\mathbf{Z}[\eta, \frac{1}{3}]$. Since the kernel of the natural map

$$\mathbf{Z}[\eta, \frac{1}{3}]^* \longrightarrow F_2^*/F_2^{*2}$$

is the *cyclic* group generated by -3 , we see that over $\mathbf{Z}[\eta, \frac{1}{3}]$ the group scheme Φ is also the *unique* non-split extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$.

Here is an explicit equation for Φ over $\mathbf{Z}[\eta, \frac{1}{3}]$. It is given by

$$(W^2 - W)(W^2 + \sqrt{5}W + 2) = 0$$

with addition formula given by

$$u + v + \frac{uv}{3}(2\eta - 1 + (\eta - 3)(u + v) + (5 - 3\eta)uv - 2(u^2 + v^2) + (1 - \eta)(u^2v + v^2u) + (\eta - 2)u^2v^2).$$

Remark 2.5. In section 4 we consider Φ over the ring $\mathbf{Z}[\zeta_3, \frac{1}{15}]$. Let $E = \mathbf{Q}(\zeta_3)$ and $E_2 = F \otimes \mathbf{Q}_2$. Since the kernel of the natural map

$$\mathbf{Z}[\zeta_3, \frac{1}{15}]^* \longrightarrow E_2^*/E_2^{*2}.$$

is the cyclic group generated by $-15 = 5$ times a square in E , we see that over $\mathbf{Z}[\zeta_3, \frac{1}{15}]$ the group scheme Φ is once again the *unique* non-split extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$. Note that $\chi : \text{Gal}(\overline{E}/E) \longrightarrow \mathbf{F}_2$ is unramified outside 5. The corresponding field extension is $E(\sqrt{5})$.

An explicit equation for the group scheme Φ over $\mathbf{Z}[\frac{1}{5}, \zeta_3]$ is given by

$$(Z^2 - Z)(Z^2 - \sqrt{-3}Z - 2) = 0.$$

We leave the linear algebra computation required to compute the group law to the reader.

3. Proof of Theorem 1.2.

Put $\eta = \frac{1+\sqrt{5}}{2}$ and $F = \mathbf{Q}(\sqrt{5})$. Let \underline{C} be the category of finite flat commutative 2-power order group schemes G over the ring $\mathbf{Z}[\eta, \frac{1}{3}]$ for which $(\sigma - \text{id})^2 = 0$ on $G(\overline{\mathbf{Q}})$ for all $\sigma \in \text{Gal}(\overline{F}/F)$ in the inertia group of any of the primes lying over 3.

The category \underline{C} has good stability properties. Duals and subquotients of objects in \underline{C} are again objects of \underline{C} . An object G is simple if and only if the Galois action on its group of points $G(\overline{F})$ is irreducible. For two objects G, G' in \underline{C} , the group $\text{Ext}^1(G, G')$ classifies extensions of G by G' in the category of group schemes over $\mathbf{Z}[\eta, \frac{1}{3}]$. The subset $\text{Ext}_{\underline{C}}^1(G, G')$ of such extensions that are themselves objects in \underline{C} , is a subgroup. To any exact sequence $0 \longrightarrow G \longrightarrow G' \longrightarrow G'' \longrightarrow 0$ of group schemes in \underline{C} and any H in \underline{C} there is associated a long exact sequence of the form

$$\begin{aligned} 0 \longrightarrow \text{Hom}_{\underline{C}}(H, G) \longrightarrow \text{Hom}_{\underline{C}}(H, G') \longrightarrow \text{Hom}_{\underline{C}}(H, G'') \longrightarrow \\ \longrightarrow \text{Ext}_{\underline{C}}^1(H, G) \longrightarrow \text{Ext}_{\underline{C}}^1(H, G') \longrightarrow \text{Ext}_{\underline{C}}^1(H, G''). \end{aligned}$$

There is an analogous contravariant exact sequence.

The group schemes Φ and G_ε for $\varepsilon \in \mathbf{Z}[\eta, \frac{1}{3}]^*$ are objects of \underline{C} .

Proposition 3.1. *The only simple objects in the category \underline{C} are $\mathbf{Z}/2\mathbf{Z}$ and μ_2 .*

Proof. Let G be a simple object. Then G is killed by 2. We multiply G by the group schemes G_ε that were discussed in section 2. The result is still an object of \underline{C} that is killed by 2. The field K generated by the points of G is a Galois extension of \mathbf{Q} . The square roots of the generators $-1, \eta$ and 3 of the group $\mathbf{Z}[\eta, \frac{1}{3}]^*$ are in K . Since $(\sigma - \text{id})^2 = 0$ on $G(\overline{\mathbf{Q}})$ for all σ in the inertia subgroup in $\text{Gal}(\overline{F}/F)$ of any of the primes lying over 3, the field K is tamely ramified at 3 with ramification index 2. By Fontaine [5, Cor.3.3.2] the root discriminant of K is therefore at most $4\sqrt{15} = 15.49\dots$. Odlyzko's discriminant bounds [7] imply $[K : \mathbf{Q}] < 76$. We have the inclusions

$$\mathbf{Q} \stackrel{2}{\subset} F \stackrel{8}{\subset} k \stackrel{\leq 4}{\subset} K,$$

where k denotes the field $F(\sqrt{-3}, i, \sqrt{\eta})$. We show that the index of the rightmost inclusion cannot be 3. Since η^3 is congruent to 1 modulo $(1+i)^2$, the relative discriminant of k over $F(\sqrt{-3}, i)$ divides 2. Therefore the root discriminant of k is at most $\sqrt{2} \cdot \sqrt{60} = 10.95\dots$. Odlyzko's bounds imply that any unramified extension of the latter field has degree $< 26/16$ and hence is trivial. There are 2 primes in k lying over 3. Their product is equal to $(\sqrt{-3})$ and $(O_k/(\sqrt{-3}))^* \cong \mathbf{F}_4^* \times \mathbf{F}_4^*$ is generated by the global units $\zeta_3 = \frac{1}{2}(1 + \sqrt{-3})$ and η . Therefore by class field theory the field k does not admit any odd degree non-trivial extension inside K . In particular $[K : k]$ cannot be 3.

It follows that $\text{Gal}(K/F)$ is a 2-group. Therefore it fixes some non-zero point P of the group scheme G we started with. Since G is simple, $G(\bar{F})$ must be generated by P . Therefore G has order 2. Since 2 is prime in the ring $\mathbf{Z}[\eta, \frac{1}{3}]$, the theorem by Oort-Tate [10] implies that G is isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or μ_2 , as required.

Proposition 3.2. *The ring $\mathbf{Z}[\eta, \zeta_3, \frac{1}{3}]$ is an unramified quadratic extension of $\mathbf{Z}[\eta, \frac{1}{3}]$. It does itself not admit any non-trivial 2-power degree unramified Galois extension.*

Proof. Clearly the ring $\mathbf{Z}[\eta, \zeta_3, \frac{1}{3}]$ is an unramified quadratic extension of $\mathbf{Z}[\eta, \frac{1}{3}]$. Let π_1 denote the Galois group of the maximal 2-power degree unramified Galois extension of $\mathbf{Z}[\eta, \frac{1}{3}]$. By class field theory, the maximal *abelian* quotient of π_1 is isomorphic to the multiplicative group $\mathbf{F}_9^* \times \mathbf{R}^*/\mathbf{R}_{>0}^* \times \mathbf{R}^*/\mathbf{R}_{>0}^*$ modulo the image of the global units of $\mathbf{Z}[\eta]$. It is easy to see that the units -1 and η of $\mathbf{Z}[\eta]$ generate a subgroup of index 2. Group theory implies then that π_1 is cyclic of order 2. This proves the proposition.

Let $\omega_3 : \text{Gal}(\bar{F}/F) \rightarrow \mathbf{F}_2$ denote the restriction of the unique Dirichlet character of \mathbf{Q} of conductor 3.

Corollary 3.3. *The \mathbf{F}_2 -vector space $\text{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ of extensions of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$ over $\mathbf{Z}[\eta, \frac{1}{3}]$ has dimension 2. It is generated by the class of $\mathbf{Z}/4\mathbf{Z}$ and by an extension killed by 2 on which the Galois group acts via matrices of the form*

$$\begin{pmatrix} 1 & \omega_3 \\ 0 & 1 \end{pmatrix}.$$

Proof. It suffices to observe that étale group schemes are characterized by the action of the Galois group on their points and that the maximal unramified 2-power degree Galois extension of $\mathbf{Z}[\eta, \frac{1}{3}]$ is the ring $\mathbf{Z}[\eta, \frac{1}{3}, \zeta_3]$.

Corollary 3.4. *Any extension of group schemes $\mathbf{Z}/2\mathbf{Z}$ over $\mathbf{Z}[\eta, \frac{1}{3}]$ becomes constant over $\mathbf{Z}[\eta, \zeta_3, \frac{1}{3}]$. Any extension of group schemes μ_2 over $\mathbf{Z}[\eta, \frac{1}{3}]$ becomes diagonalizable over $\mathbf{Z}[\eta, \zeta_3, \frac{1}{3}]$.*

Proof. This follows from Prop. 3.2 and Cartier duality.

The group of upper triangular 3×3 -matrices over \mathbf{F}_2 is isomorphic to the dihedral group D_4 . Consider a subgroup

$$\Gamma \subset \left\{ \begin{pmatrix} 1 & a & c \\ 0 & 1 & b \\ 0 & 0 & 1 \end{pmatrix} : a, b, c \in \mathbf{F}_2 \right\}.$$

The maps $\Gamma \rightarrow \mathbf{F}_2$ given by $g \mapsto a$ and $g \mapsto b$ are group homomorphisms. The following elementary lemma is repeatedly used in the sequel.

Lemma 3.5. *Let Γ be as above and let $N \subset \Gamma$ be a normal subgroup of order at most 2. Then either $a(N) = b(N) = 0$ or one of a, b vanishes on Γ .*

Proof. Since $g^2 = 1$ we have $a(g)b(g) = 0$ for all $g \in N$. If the homomorphisms $a, b : \Gamma \rightarrow \mathbf{F}_2$ are equal, we have $a(g) = b(g) = a(g)b(g) = 0$ for every $g \in N$ and we are done. Suppose now $a \neq b$. If neither a nor b vanish on Γ , we must have that Γ is *equal* to the order 8 group of upper triangular matrices. Thus N is contained in its unique normal subgroup of order 2, which is given by $a = b = 0$.

This proves the lemma.

Let Φ denote the group scheme over $\mathbf{Z}[\eta, \frac{1}{3}]$ that was introduced in section 2. It is an object of the category $\underline{\mathcal{C}}$.

Proposition 3.6. *We have*

$$\mathrm{Ext}_{\underline{\mathcal{C}}}^1(\Phi, \mathbf{Z}/2\mathbf{Z}) = \mathrm{Ext}_{\underline{\mathcal{C}}}^1(\mu_2, \Phi) = 0.$$

Proof. By Cartier duality it suffices to show that $\mathrm{Ext}_{\underline{\mathcal{C}}}^1(\Phi, \mathbf{Z}/2\mathbf{Z})$ vanishes. Consider an extension in the category $\underline{\mathcal{C}}$

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow G \longrightarrow \Phi \longrightarrow 0.$$

This leads to an extension of the form

$$0 \longrightarrow C \longrightarrow G \longrightarrow \mu_2 \longrightarrow 0.$$

where C is an extension of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$. Since the Galois action on $\Phi(\overline{F})$ is non-trivial, the group $C(\overline{F})$ cannot be cyclic. Therefore C is killed by 2. It follows that G is killed by 2 over the completion at the prime 2. This implies that G itself is also killed by 2. By Remark 2.4 the Galois group acts on $G(\overline{F})$ through matrices of the form

$$\begin{pmatrix} 1 & \chi & a \\ 0 & 1 & \omega_3 \\ 0 & 0 & 1 \end{pmatrix}$$

where the character $\chi : \mathrm{Gal}(\overline{F}/F) \rightarrow \mathbf{F}_2$ is unramified outside 2 and 3. Since C is étale, χ is unramified at 2. Since G is an object of $\underline{\mathcal{C}}$, any prime over 3 is tamely ramified with inertia group of order ≤ 2 . Therefore Lemma 3.5 applies with Γ equal to the decomposition group of a prime over 3 and N its inertia subgroup: since $\omega_3(N) \neq 0$, we have $\chi(\Gamma) = 0$. It follows that χ is unramified at all finite primes. Since the narrow class number of F is 1, class field theory implies $\chi = 0$.

To finish the proof, we consider the exact sequence

$$\mathrm{Hom}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{g} \mathrm{Ext}^1(\mu_2, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}^1(\Phi, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{h} \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}).$$

By Remark 2.4 the map g is an isomorphism of two groups of order 2. It follows that the map h is injective. It maps the class of G to the class of the extension determined by χ . This implies the proposition.

Proposition 3.7. *The natural maps*

$$\begin{aligned}\mathrm{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi) &\longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2), \\ \mathrm{Ext}_{\underline{C}}^1(\Phi, \mu_2) &\longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)\end{aligned}$$

are both zero.

Proof. By Cartier duality it suffices to deal with the first map. First we show that extensions

$$0 \longrightarrow \Phi \longrightarrow G \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0.$$

in \underline{C} that are *killed by 2* map to zero in $\mathrm{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$.

The Galois group acts on the points of \overline{G} via matrices of the form

$$\begin{pmatrix} 1 & \omega_3 & a \\ 0 & 1 & \chi \\ 0 & 0 & 1 \end{pmatrix}$$

The quotient of G by the subgroup scheme $\mathbf{Z}/2\mathbf{Z}$ of Φ is an extension of $\mathbf{Z}/2\mathbf{Z}$ by μ_2 . By Proposition 2.2 it is a group scheme of the form G_ε for some ε in $\mathbf{Z}[\eta, \frac{1}{3}]^*$. We want to show that the corresponding character χ vanishes.

Let K denote the field generated by the points of G and let $\Gamma \subset \mathrm{Gal}(K/F)$ denote a decomposition group of a prime over 3. Since G is an object of \underline{C} , Lemma 3.5 applies to Γ with N equal to its inertia subgroup: since ω_3 is ramified at 3, the character χ is split at 3. We conclude that ε is a square modulo 3.

Since $\varepsilon = \pm\eta$ are not squares in the residue field \mathbf{F}_9 , we have therefore $\varepsilon = \pm 1$. If $\varepsilon = -1$, then the field K is a quadratic extension of $F(i, \sqrt{-3})$. Locally at 2 the extension of $\mathbf{Z}/2\mathbf{Z}$ by Φ looks like

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \times \mu_2 \longrightarrow G \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0.$$

Therefore the ramification index of the prime 2 in $F \subset K$ is equal to 2. It follows that K is everywhere unramified over $F(i, \sqrt{-3})$. A standard computation shows that the latter field does not admit any non-trivial everywhere unramified extension. Contradiction. It follows that $\varepsilon = 1$ and hence $\chi = 0$ as required.

To show that *every* extension in $\mathrm{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$ maps to zero in $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$, we first consider the exact sequence

$$\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{g} \mathrm{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi) \longrightarrow \mathrm{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2).$$

The image under g of the class of $\mathbf{Z}/4\mathbf{Z}$ is a group scheme that is *not* killed by 2. By exactness it maps to zero in $\mathrm{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$. To prove the proposition, we apply Lemma 2.1: since the Γ -covariants of the group $\mathrm{Hom}(\Phi(\overline{F}), \mathbf{Z}/2\mathbf{Z})$ have order 2, the subgroup of $\mathrm{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$ of extensions that are killed by 2 has index 2.

This proves the proposition.

As a consequence of Propositions 3.6 and 3.7 we obtain the following commutative diagram with exact rows and columns

$$\begin{array}{ccccccc}
& & & & & & 0 \\
& & & & & & \downarrow \\
& & & & & & \mathbf{F}_2 \\
& & & 0 & \longrightarrow & & \downarrow \\
& & & \downarrow & & & \text{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi) \\
& & 0 & \longrightarrow & \text{Ext}_{\underline{C}}^1(\Phi, \Phi) & \longrightarrow & \text{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi) \\
& & \downarrow & & \downarrow & & \downarrow \\
& & 0 & \longrightarrow & \mathbf{F}_2 & \longrightarrow & \text{Ext}_{\underline{C}}^1(\Phi, \mu_2) & \longrightarrow & 0
\end{array}$$

Here the “ \mathbf{F}_2 ” in the upper right corner denotes the extension of $\mathbf{Z}/2\mathbf{Z}$ by Φ that is the image of the class of $\mathbf{Z}/4\mathbf{Z}$ in $\text{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$. It is also an extension of μ_2 by $\mathbf{Z}/4\mathbf{Z}$. Similarly, the “ \mathbf{F}_2 ” in the lower left corner denotes the extension of Φ by μ_2 that is the image of the class of μ_4 in $\text{Ext}^1(\mu_2, \mu_2)$. It is also an extension of μ_4 by $\mathbf{Z}/2\mathbf{Z}$. It follows at once that in the category \underline{C} there is at most one non-trivial extension of Φ by itself. We prove the following stronger statement.

Proposition 3.8. *We have*

$$\text{Ext}_{\underline{C}}^1(\Phi, \Phi) = 0.$$

Proof. If a non-trivial extension exists, it maps to the image of the class of $\mathbf{Z}/4\mathbf{Z}$ in $\text{Ext}_{\underline{C}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$ and to the image of μ_4 in $\text{Ext}_{\underline{C}}^1(\Phi, \mu_2)$. This means that the group $G(\overline{F})$ of a non-trivial extension

$$0 \longrightarrow \Phi \longrightarrow G \longrightarrow \Phi \longrightarrow 0,$$

is of type 4×4 . The Galois group acts on the points of G via matrices of the form

$$\begin{pmatrix} 1 & a \\ 0 & \omega_4 \end{pmatrix}$$

where ω_4 is the character that gives the action on the group μ_4 of 4th roots of unity and $a : \text{Gal}(\overline{F}/F) \rightarrow \mathbf{Z}/4\mathbf{Z}$ is a 1-cocycle with the property that the restriction of a to the absolute Galois group of $F(i)$ is a character of order 4 satisfying $2a = \omega_3$. In particular, the field K generated by the points of G contains $F(i)$ and has degree 8 over F .

Since the extension $0 \rightarrow \Phi \rightarrow G \rightarrow \Phi \rightarrow 0$ is split locally at 2, the prime of $F(i)$ lying over 2 is split in K . As a consequence the extension $F(i) \subset K$ is unramified outside 3. Since $F(i)$ admits no non-trivial everywhere unramified extensions, class field theory implies that $\text{Gal}(K/F(i))$ is a quotient of the multiplicative group $(\mathcal{O}_{F(i)}/3\mathcal{O}_{F(i)})^* \cong \mathbf{F}_9^* \times \mathbf{F}_9^*$ by the subgroup generated by the global units i, η and by the generator $1 + i$ of the prime lying over 2. However, this quotient group has order 2 rather than 4.

It follows that $\text{Ext}_{\underline{C}}^1(\Phi, \Phi)$ is trivial, as required.

Proof of Theorem 1.2. Let A be a semistable abelian variety over $F = \mathbf{Q}(\sqrt{5})$ with good reduction outside 3. A result by Grothendieck [6, Cor.3.5.2] implies that $(\sigma - \text{id})^2$ acts as zero on the 2^n -torsion subgroup schemes $A[2^n]$ for $n \geq 1$. Therefore the latter are objects of the category $\underline{\mathcal{C}}$. Proposition 3.6 implies that each $A[2^n]$ admits a filtration of the form

$$0 \underbrace{\subset}_{\mu_2\text{'s}} M_n \underbrace{\subset}_{\Phi\text{'s}} N_n \underbrace{\subset}_{\mathbf{Z}/2\mathbf{Z}\text{'s}} A[2^n]$$

where M_n is filtered by copies of μ_2 , the quotient N_n/M_n is filtered by copies of Φ and $A[2^n]/N_n$ is filtered by copies of $\mathbf{Z}/2\mathbf{Z}$.

By Corollary 3.4 the étale group schemes M_n^\vee and $A[2^n]/N_n$ become *constant* over the ring $\mathbf{Z}[\eta, \zeta_3, \frac{1}{3}]$. Therefore, for every residue field \mathbf{F}_q of this ring, the groups of points of $A[2^n]/N_n$ and M_n^\vee map injectively to the group of \mathbf{F}_q -rational points of the abelian varieties A/N_n and A^{dual}/N_n' respectively. Here $N_n' = \ker(A[2^n]^\vee \rightarrow M_n^\vee)$.

The abelian varieties A/N_n and A^{dual}/N_n' are all isogenous to A . Therefore they have the same number of points as A over \mathbf{F}_q . It follows that $\#M_n$ and $\#(A[2^n]/N_n)$ are at most $\#A(\mathbf{F}_q)$. In particular, they remain bounded as n grows. By Proposition 3.8 the exponent of N_n/M_n is 2. Therefore $A[2^n]$ is killed by some positive integer that does not depend on n . This is only possible when $A = 0$.

This proves Theorem 1.2.

4. Proof of Theorem 1.3.

Let $\underline{\mathcal{B}}$ be the category of finite flat 2-power order group schemes over $\mathbf{Z}[\frac{1}{15}]$ on which $(\sigma - \text{id})^2 = 0$ for all $\sigma \in \text{Gal}(\overline{\mathbf{Q}}/\mathbf{Q})$ in the inertia group of any of the primes lying over 3 or 5. We write S for the set of primes $\{3, 5\}$. The category $\underline{\mathcal{B}}$ enjoys the same stability properties as the category $\underline{\mathcal{C}}$ of the previous section.

Proposition 4.1. *The only simple objects in $\underline{\mathcal{B}}$ are $\mathbf{Z}/2\mathbf{Z}$ and μ_2 .*

Proof. Let G be a simple object. As in the proof of Prop. 3.1, we multiply G by the group schemes G_ε of section 2, where ε runs through the group $\mathbf{Z}[\frac{1}{15}]^*$ modulo squares. Let K be the field generated by the points of G . Then K is a Galois extension of \mathbf{Q} . The square roots of -1 , 3 and 5 are contained in K . The field K is tamely ramified at 3 and 5 with ramification index 2. By Fontaine's theorem [5, Cor.3.3.2] the root discriminant of K is therefore at most $4\sqrt{15} = 15.49\dots$. Odlyzko's discriminant bounds [7] imply $[K : \mathbf{Q}] < 76$. We have the inclusions

$$\mathbf{Q} \overset{8}{\subset} k \overset{\leq 9}{\subset} K.$$

where $k = \mathbf{Q}(\sqrt{5}, \sqrt{-3}, i)$. Put $\Gamma = \text{Gal}(K/\mathbf{Q})$. By the Kronecker-Weber Theorem we have $\Gamma' = \text{Gal}(K/\mathbf{Q}(\sqrt{5}, \sqrt{-3}, i))$. The group Γ' is solvable. The extension $k \subset K$ is unramified outside 2. A standard computation shows that k admits no non-trivial unramified extensions. There are two primes over 2. Their product is $(1 + i)$. Since the global units η and ζ_3 generate the group $(O_k/(1 + i)O_k)^* \cong \mathbf{F}_4^* \times \mathbf{F}_4^*$, it follows from class field theory that $[\Gamma' : \Gamma'']$ is a power of 2.

If $[\Gamma' : \Gamma''] = 1$ or ≥ 4 , it is immediate that Γ is a 2-group. If $[\Gamma' : \Gamma''] = 2$, we have $\#\Gamma'' \leq 4$. If $\#\Gamma'' = 3$, the group Γ' is isomorphic to the symmetric group S_3 . Since

S_3 is not the commutator subgroup of any group, this is impossible. Therefore $\#\Gamma''$ is necessarily a power of 2 and Γ is a 2-group. Since Γ has fixed points in the simple group scheme G we started with, G must have order 2. By the Oort-Tate Theorem [10] the group scheme G is isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or μ_2 as required.

The maximal 2-power degree unramified Galois extension of $\mathbf{Z}[\frac{1}{15}]$ is *not cyclic*. As a consequence the group $\text{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ is relatively large. It has order 8. This affects the size of other extension groups, in particular the ones involving the group scheme Φ of section 2. A computation similar to the one performed in the proof of Prop. 3.7 shows that $\text{Ext}_{\underline{B}}^1(\Phi, \Phi)$ has dimension 2 over \mathbf{F}_2 . It is generated by the 4-torsion of the Jacobian of the modular curve $X_0(15)$ and an unramified quadratic twist of $\Phi \times \Phi$.

Since it is essential for our method that $\text{Ext}_{\underline{B}}^1(\Phi, \Phi)$ be one dimensional we make a base change. We move over to the ring $\mathbf{Z}[\zeta_3, \frac{1}{15}]$ and modify the category \underline{B} accordingly. Put $E = \mathbf{Q}(\zeta_3)$ and let S denote the set of $\mathbf{Z}[\zeta_3]$ -primes $\{\sqrt{-3}, 5\}$. Let R denote the ring of integers of the ray class field of conductor $5\sqrt{-3}$ of E .

Definition. Let \underline{D} be the category of commutative finite flat 2-power order group schemes over $\mathbf{Z}[\zeta_3, \frac{1}{15}]$ that admit a filtration with subquotients isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or μ_2 and on which $(\sigma - \text{id})^2 = 0$ on $G(\overline{\mathbf{Q}})$ for all $\sigma \in \text{Gal}(\overline{E}/E)$ contained in the inertia group of any of the primes lying over S .

The category \underline{D} has the same stability properties as the category \underline{C} of the previous section. The group schemes Φ and G_ε for $\varepsilon \in \mathbf{Z}[\zeta_3, \frac{1}{15}]^*$ of section 2 are objects of \underline{D} .

Proposition 4.2. *The ring $R[\frac{1}{15}]$ is an unramified cyclic degree 8 extension of $\mathbf{Z}[\zeta_3, \frac{1}{15}]$. It does itself not admit any non-trivial 2-power degree unramified Galois extension.*

Proof. The ray class group of E of conductor $5\sqrt{-3}$ is equal to $\mathbf{F}_3^* \times \mathbf{F}_{25}^*$ modulo the global unit -1 . This proves that $R[\frac{1}{15}]$ is the maximal unramified *abelian* 2-power degree extension of $\mathbf{Z}[\zeta_3, \frac{1}{15}]$. Since the Galois group is actually *cyclic*, group theory implies that $R[\frac{1}{15}]$ does not admit any non-trivial 2-power degree unramified Galois extension, as required.

Corollary 4.3. *The \mathbf{F}_2 -vector space $\text{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$ of extensions of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$ over $\mathbf{Z}[\zeta_3, \frac{1}{15}]$ has dimension 2. It is generated by $\mathbf{Z}/4\mathbf{Z}$ and an extension killed by 2 on which the Galois group acts via matrices of the form*

$$\begin{pmatrix} 1 & \chi_5 \\ 0 & 1 \end{pmatrix}.$$

Here $\chi_5 : \text{Gal}(\overline{E}/E) \rightarrow \mathbf{F}_2$ is the restriction of the unique quadratic Dirichlet character of conductor 5. It corresponds to the extension $E \subset E(\sqrt{5})$.

Proof. It suffices to observe that $E(\sqrt{5})$ is the unique quadratic extension of E that is unramified outside S . Now apply Prop.4.2.

Corollary 4.4. *Any extension of group schemes $\mathbf{Z}/2\mathbf{Z}$ over $\mathbf{Z}[\zeta_3, \frac{1}{15}]$ is constant over $R[\frac{1}{15}]$. Similarly, any extension of group schemes μ_2 over $\mathbf{Z}[\zeta_3, \frac{1}{15}]$ is diagonalizable over $R[\frac{1}{15}]$.*

Proof. This follows from Proposition 4.2 and Cartier duality.

Proposition 4.5. *We have*

$$\mathrm{Ext}_{\underline{D}}^1(\Phi, \mathbf{Z}/2\mathbf{Z}) = \mathrm{Ext}_{\underline{D}}^1(\mu_2, \Phi) = 0.$$

Proof. By Cartier duality it suffices to show that the left hand side group vanishes. Consider an extension in the category \underline{D}

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow G \longrightarrow \Phi \longrightarrow 0.$$

It gives rise to an extension

$$0 \longrightarrow C \longrightarrow G \longrightarrow \mu_2 \longrightarrow 0.$$

where C is an extension of $\mathbf{Z}/2\mathbf{Z}$ by $\mathbf{Z}/2\mathbf{Z}$. Since the Galois action on $\Phi(\overline{E})$ is not trivial, the group $C(\overline{E})$ cannot be cyclic. Therefore C and hence G itself are killed by 2. So the Galois group acts through matrices of the form

$$\begin{pmatrix} 1 & \psi & a \\ 0 & 1 & \chi_5 \\ 0 & 0 & 1 \end{pmatrix}$$

Here ψ is a character of $\mathrm{Gal}(\overline{E}/E)$ that is unramified outside 2, $\sqrt{-3}$ and 5. Since C is étale, it is unramified at 2. Since G is an object of \underline{D} , Lemma 3.5 applies. We apply it first with Γ equal to a decomposition group of a prime over 5 and N its inertia subgroup. We see that ψ is split at 5. Then we apply Lemma 3.5 to the decomposition group of a prime over $\sqrt{-3}$ and its inertia subgroup and we see that ψ is unramified at $\sqrt{-3}$.

So, ψ is everywhere unramified. Therefore it is zero. Consider the exact sequence

$$\mathrm{Hom}(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{g} \mathrm{Ext}^1(\mu_2, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}^1(\Phi, \mathbf{Z}/2\mathbf{Z}) \xrightarrow{h} \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$$

By Proposition 4.4 and Remark 2.3 the map g is an isomorphism of two groups of order 2. It follows that the map h is injective. It maps the class of G to the class of the extension determined by ψ . Now the proposition follows.

The following proposition is analogous to Proposition 3.7.

Proposition 4.6. *The images of both natural maps*

$$\begin{aligned} \mathrm{Ext}_{\underline{D}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi) &\longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2), \\ \mathrm{Ext}_{\underline{D}}^1(\Phi, \mu_2) &\longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2) \end{aligned}$$

are contained in the subgroup generated by the class $[G_{-1}]$.

Proof. By Cartier duality it suffices to give a proof for the first map. Since the Galois covariants of $\mathrm{Hom}_{\mathrm{ab}}(\Phi(\overline{E}), \mathbf{Z}/2\mathbf{Z})$ have order 2, Prop. 2.1 implies that $\mathrm{Ext}_{\underline{D}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$ is

generated by the extensions that are killed by 2 and by the image of the class of $\mathbf{Z}/4\mathbf{Z}$. The latter is mapped to zero because the sequence

$$\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \mathrm{Ext}_{\underline{D}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi) \longrightarrow \mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2).$$

is exact. Therefore it suffices to show that any extension in \underline{D} of the form

$$0 \longrightarrow \Phi \longrightarrow G \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow 0,$$

that is *killed by 2*, maps to the subgroup generated by $[G_{-1}]$ in $\mathrm{Ext}_{\underline{D}}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$.

The Galois group acts on the points of G via matrices of the form

$$\begin{pmatrix} 1 & \chi_5 & a \\ 0 & 1 & \psi \\ 0 & 0 & 1 \end{pmatrix}.$$

The character ψ corresponds to an extension of the form G_ε in $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ for some S -unit ε . Since G is an object of \underline{D} , Lemma 3.5 applies to the decomposition group of any prime lying over $\sqrt{5}$ and we see that, as χ_5 is ramified, the prime $\sqrt{5}$ splits in the field cut out by ψ . Since $\varepsilon = \pm\sqrt{-3}$ are not squares in the residue field \mathbf{F}_{25} , we have $\varepsilon = \pm 1$. The class in $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$ associated to the S -unit $\varepsilon = -1$ is precisely $[G_{-1}]$.

This proves the proposition.

We do not need this for the proof of Theorem 1.3, but there actually does exist a group scheme H in the category \underline{D} that is killed by 2 and is a non-split extension of $\mathbf{Z}/2\mathbf{Z}$ by Φ mapping to the class $[G_{-1}]$ in $\mathrm{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$. It is unique. The Galois group acts on its points through matrices of the form

$$\begin{pmatrix} 1 & \chi_5 & a \\ 0 & 1 & \omega_2 \\ 0 & 0 & 1 \end{pmatrix}, \quad (*)$$

where $\omega_2 : \mathrm{Gal}(\overline{E}/E) \longrightarrow \mathbf{F}_2$ is the character corresponding to the field $E(i)$. It follows from the proof of Proposition 4.6 that the field K generated by the points of H is a quadratic extension of $E(i, \sqrt{5})$, unramified outside the primes lying over 3. There is only one such field. It happens to be the ray class field of conductor $\sqrt{-3}$ of the field $E(\sqrt{-5}) = \mathbf{Q}(\sqrt{-5}, \zeta_3)$.

As a consequence of the previous propositions, we have the following commutative diagram

$$\begin{array}{ccccccc} & & & & & & 0 \\ & & & & & & \downarrow \\ & & & & & & \mathbf{F}_2 \\ & & & 0 & \longrightarrow & & \downarrow \\ & & & \downarrow & & & \mathrm{Ext}_{\underline{D}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi) \\ & & 0 & \longrightarrow & \mathrm{Ext}_{\underline{D}}^1(\Phi, \Phi) & \longrightarrow & \downarrow \\ & & \downarrow & & \downarrow & & \mathbf{F}_2 \\ 0 & \longrightarrow & \mathbf{F}_2 & \longrightarrow & \mathrm{Ext}_{\underline{D}}^1(\Phi, \mu_2) & \longrightarrow & \mathbf{F}_2 \end{array}$$

Here the “ \mathbf{F}_2 ” in the upper right corner denotes the extension of $\mathbf{Z}/2\mathbf{Z}$ by Φ that is the image of the class of $\mathbf{Z}/4\mathbf{Z}$ in $\text{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z})$. It is also an extension of $\mathbf{Z}/4\mathbf{Z}$ by μ_2 . Similarly, the “ \mathbf{F}_2 ” in the lower left corner denotes the extension of Φ by μ_2 that is the image of the class of μ_4 in $\text{Ext}^1(\mu_2, \mu_2)$. It is also an extension of $\mathbf{Z}/2\mathbf{Z}$ by μ_4 . The “ \mathbf{F}_2 ” in the lower right corner is the extension $[G_{-1}]$ in $\text{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mu_2)$.

It follows that the dimension of $\text{Ext}_{\underline{D}}^1(\Phi, \Phi)$ is at most 2. On the other hand the dimension is at least 1, because the 4-torsion of the elliptic curve $Y^2 + XY + Y = X^3 + X^2$ of section 2, is a non-trivial extension of Φ by Φ in \underline{D} .

Lemma 4.7. *Let G be an extension of Φ by Φ . Then the underlying group structure of $G(\overline{E})$ is not of type $4 \times 2 \times 2$.*

Proof. Suppose it is. Let $e_1 \in G(\overline{E})$ be a point of order 4. Choose e_2 of order 2 so that $2e_1$ and e_2 are a basis for the group of points of the closed subgroup scheme Φ of G . Finally, choose $e_3 \in G(\overline{E})$ of order 2 so that e_1, e_3 are a basis for the group $G(\overline{E})/\Phi(\overline{E})$. Every point in the coset of e_3 modulo $\Phi(\overline{E})$ has order 2, while the points in the cosets of e_1 and $e_1 + e_3$ all have order 4. This implies that $\text{Gal}(\overline{E}/E)$ fixes e_3 and switches e_1 to $e_1 + e_3$ modulo the group generated by $2e_1$ and e_2 . It follows that $\text{Gal}(\overline{E}/E)$ fixes $2e_1$ and hence switches e_2 and $e_1 + e_2$.

Over \mathbf{Z}_2 the group scheme Φ is a split extension of μ_2 by $\mathbf{Z}/2\mathbf{Z}$. Being isomorphic to Φ , the group scheme G/Φ admits a unique morphism onto $\mathbf{Z}/2\mathbf{Z}$. Let N denote the quotient of the kernel of the composition $G \rightarrow G/\Phi \rightarrow \mathbf{Z}/2\mathbf{Z}$ by the connected component of the subgroup scheme Φ of G . Let E_2 be the completion of E at 2. For any embedding $\overline{E} \hookrightarrow \overline{E}_2$, either e_1 or $e_1 + e_3$ is contained in $N(\overline{E}_2)$. In the first case the natural map $\langle e_1 \rangle \rightarrow N(\overline{E}_2)$ is an isomorphism. In the second case the map $\langle e_1 + e_3 \rangle \rightarrow N(\overline{E}_2)$ is an isomorphism. This shows that the group $N(\overline{E}_2)$ is cyclic of order 4. On the other hand, there is an exact sequence

$$0 \longrightarrow \mathbf{Z}/2\mathbf{Z} \longrightarrow N \longrightarrow \mu_2 \longrightarrow 0.$$

Since this sequence is split over \mathbf{Z}_2 , the group scheme N is killed by 2. Contradiction.

This proves the lemma.

Corollary 4.8. *The group $\text{Ext}_{\underline{D}}^1(\Phi, \Phi)$ is generated by the subgroup of extensions that are killed by 2 and by the extension of Φ by Φ realized by the 4-torsion of the elliptic curve with Weierstrass equation $Y^2 + XY + Y = X^3 + X^2$.*

Proof. The underlying group of the extension provided by the 4-torsion of the elliptic curve is of type 4×4 . Suppose that every non-trivial extension has this underlying group. The natural homomorphism $\text{Ext}_{\underline{D}}^1(\Phi, \Phi) \hookrightarrow \text{Ext}_{\underline{D}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$ maps such extensions to extensions of $\mathbf{Z}/2\mathbf{Z}$ by Φ that are *not* killed by 2. By Prop. 4.6 there are at most two such extensions. Therefore the dimension of $\text{Ext}_{\underline{D}}^1(\Phi, \Phi)$ is at most 1 and we are done.

On the other hand, if not every non-trivial extension has underlying group of type 4×4 , then we are done by Lemma 4.7 and the fact that $\text{Ext}_{\underline{D}}^1(\Phi, \Phi)$ has \mathbf{F}_2 -dimension ≤ 2 .

Proposition 4.9. *We have*

$$\dim_{\mathbf{F}_2} \text{Ext}_{\underline{D}}^1(\Phi, \Phi) = 1.$$

Proof. By Lemma 4.7 and Corollary 4.8 it suffices to show that extensions in \underline{D} of the form

$$0 \longrightarrow \Phi \longrightarrow G \longrightarrow \Phi \longrightarrow 0,$$

that are *killed by 2* are necessarily split.

Suppose G is a non-split extension. The 2-dimensional \mathbf{F}_2 -vector space $\text{Ext}_{\underline{D}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$ is generated by the class of the group scheme H constructed above and by the image of $\mathbf{Z}/4\mathbf{Z}$ under the natural map $\text{Ext}^1(\mathbf{Z}/2\mathbf{Z}, \mathbf{Z}/2\mathbf{Z}) \longrightarrow \text{Ext}_{\underline{D}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$. The only non-trivial extension class $\text{Ext}_{\underline{D}}^1(\mathbf{Z}/2\mathbf{Z}, \Phi)$ that is killed by 2, is the one represented by H . It follows that the class of G in $\text{Ext}_{\underline{D}}^1(\Phi, \Phi)$ maps to the class of H . Similarly, the class of G maps to the class of the Cartier dual H^\vee in $\text{Ext}_{\underline{D}}^1(\Phi, \mu_2)$.

A short computation shows that (*) above implies that, with respect to the dual basis, the Galois group acts on $H^\vee(\overline{E})$ through matrices of the form

$$\begin{pmatrix} 1 & \omega_2 & a + \chi\omega_2 \\ 0 & 1 & \chi_5 \\ 0 & 0 & 1 \end{pmatrix}.$$

With respect to any other basis that is compatible with the ‘flag’ induced by the exact sequence $0 \rightarrow \mu_2 \rightarrow G \rightarrow \Phi \rightarrow 0$, the Galois group acts through matrices of the form

$$\begin{pmatrix} 1 & \omega_2 & a + \mu\omega_2 + \lambda\chi + \chi\omega_2 \\ 0 & 1 & \chi \\ 0 & 0 & 1 \end{pmatrix}, \quad \text{for certain } \lambda, \mu \in \mathbf{F}_2.$$

It follows that the Galois group acts on $G(\overline{E})$ through matrices of the form

$$\begin{pmatrix} 1 & \chi & a & b \\ 0 & 1 & \omega_2 & a + \mu\omega_2 + \lambda\chi + \chi\omega_2 \\ 0 & 0 & 1 & \chi \\ 0 & 0 & 0 & 1 \end{pmatrix}, \quad \text{for certain } \lambda, \mu \in \mathbf{F}_2.$$

The field L generated by the points of G contains the field K generated by the points of H (or equivalently H^\vee). The index $[L : K]$ is either 1 or 2. We have the following diagram of fields

$$\begin{array}{ccccc} & & L & & \\ & & | & & \\ & & K & & \\ & & | & & \\ & & E(i, \sqrt{5}) & & \\ & \nearrow & | & \nwarrow & \\ E(\sqrt{5}) & & E(\sqrt{-5}) & & E(i) \\ & \nwarrow & | & \nearrow & \\ & & E & & \end{array}$$

Let $\rho, \tau \in \text{Gal}(L/E)$ be automorphisms that act as

$$\begin{pmatrix} 1 & 0 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad \begin{pmatrix} 1 & 1 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{pmatrix}$$

respectively on the subgroup $H(\overline{E})$ of $G(\overline{E})$. This means that $\omega_4(\rho) = 1$ and $\chi(\rho) = a(\rho) = 0$ while $\chi(\tau) = 1$ and $\omega_4(\tau) = a(\tau) = 0$. Then there are $\beta, \beta' \in \mathbf{F}_2$ such that ρ and τ act on the group $G(\overline{E})$ through matrices of the form

$$A = \begin{pmatrix} 1 & 0 & 0 & \beta \\ 0 & 1 & 1 & \mu \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad A' = \begin{pmatrix} 1 & 1 & 0 & \beta' \\ 0 & 1 & 0 & \lambda \\ 0 & 0 & 1 & 1 \\ 0 & 0 & 0 & 1 \end{pmatrix}$$

respectively. The square of A is the identity. We have

$$A'^2 = \begin{pmatrix} 1 & 0 & 0 & \lambda \\ 0 & 1 & 0 & 0 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix} \quad \text{and} \quad (AA')^2 = \begin{pmatrix} 1 & 0 & 1 & \mu + \lambda + 1 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Claim. We have $\lambda = 0$ and $L = K$.

Indeed, if $\lambda \neq 0$, then τ^2 is a non-trivial automorphism in $\text{Gal}(L/K)$. Therefore ρ and τ generate the image of $\Gamma = \text{Gal}(L/E)$. By class field theory the fixed field of Γ' is contained in the ray class field of E of conductor $5\sqrt{-3} \cdot 2^a$ for some $a \geq 0$. Since G is an object in \underline{D} , the ramification indices of the primes in S are at most 2. By Fontaine we can take $a = 2$. Writing O for the completion of $\mathbf{Z}[\zeta_3]$ at 2, the group Γ/Γ' is therefore a quotient of

$$\mathbf{F}_3^* \times \mathbf{F}_{25}^*/\mathbf{F}_{25}^{*2} \times O^*/\{u \in O^* : u \equiv 1 \pmod{4}\}$$

Since the 2-part of this group is killed by 2 and Γ is generated by two elements, the group Γ/Γ' is isomorphic to the Klein 4-group. By Tausky's theorem $\Gamma' = \text{Gal}(L/E(i, \sqrt{5}))$ is therefore cyclic [11]. Since $(AA')^2$ has order 2 and A'^2 has order dividing 2, we see that A'^2 must be trivial so that $\lambda = 0$ and hence $L = K$ as required.

The group $\text{Gal}(L/E(\sqrt{5}))$ has order 4 and consists of the matrices

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

with

$$M = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & \mu + 1 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 0 & \beta \\ 1 & \mu \end{pmatrix}, \quad \begin{pmatrix} 1 & \beta + \mu + 1 \\ 1 & \mu + 1 \end{pmatrix}.$$

Since the rightmost two matrices have the same determinants, we see that the number of automorphisms $\sigma \in \text{Gal}(L/E(\sqrt{5}))$ for which the rank of $\sigma - \text{id}$ is equal to 2, is *odd*.

Claim. *The decomposition subgroup $\Gamma_2 \subset \Gamma$ of any prime lying over 2 has order 2.*

Proof of the claim. Consider the extension G of Φ by Φ over \mathbf{Z}_2 . Over \mathbf{Z}_2 we have $\Phi \cong \mathbf{Z}/2\mathbf{Z} \times \mu_2$. Therefore the local Galois group $\text{Gal}(\overline{E}_2/E_2)$ acts on the points of G through matrices of the form

$$\begin{pmatrix} 1 & 0 & \gamma & 0 \\ 0 & 1 & \omega_2 & \gamma' \\ 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 \end{pmatrix}.$$

Here γ and γ' are unramified characters. Since ω_2 is ramified at 2, the order of Γ_2 is *at least* 2. Suppose that Γ_2 has order 4. Then it is necessarily equal to $\text{Gal}(L/E(\sqrt{5}))$. If one of the characters γ, γ' is trivial, then all $\sigma \in \text{Gal}(L/E(\sqrt{5}))$ have the property that the rank of $\sigma - \text{id}$ is at most 1. This is a contradiction. Therefore both γ and γ' are equal to the unique unramified character of E_2 . This implies that the local Galois group acts through matrices of the form

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

with

$$M = \begin{pmatrix} 0 & 0 \\ 0 & 0 \end{pmatrix}, \quad \begin{pmatrix} 0 & 0 \\ 1 & 0 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 0 & 1 \end{pmatrix}, \quad \begin{pmatrix} 1 & 0 \\ 1 & 1 \end{pmatrix}.$$

Since two of these matrices are invertible, precisely two $\sigma \in \text{Gal}(L/E(\sqrt{5}))$ have the property that the rank of the 4×4 -matrix corresponding to $\sigma - \text{id}$ is equal to 2. Contradiction. It follows that the decomposition group of any of the the primes over 2 has order 2, as required.

This means that the two primes over 2 in $E(i, \sqrt{5})$ split in the extension K . But they don't. Indeed, consider the element $\sqrt{-3} + \sqrt{-5}$ of the field $E(\sqrt{-5})$. Since its norm to E is -2 , it generates one of the prime ideals over 2. The other is generated by $\sqrt{-3} - \sqrt{-5}$. Since both primes are principal ideals, they split in the Hilbert class field $E(\sqrt{5}, i)$ of $E(\sqrt{-5})$. If they were to split in K , then they could be generated by elements that are congruent to 1 (mod $\sqrt{-3}$). This means that $u(\sqrt{-3} + \sqrt{-5}) \equiv 1 \pmod{\sqrt{-3}}$ for some unit u in $E(i)$. Since the unit group of $E(\sqrt{-5})$ is generated by $\pm(4 + \sqrt{-3}\sqrt{-5})$, this means that

$$\pm(4 + \sqrt{-3}\sqrt{-5})^a(\sqrt{-3} + \sqrt{-5}) \equiv 1 \pmod{\sqrt{-3}}, \quad \text{for some } a \in \mathbf{Z}.$$

However, the left hand side is congruent to $\pm\sqrt{-5}$, so that this is impossible for any $a \in \mathbf{Z}$.

This proves the proposition.

Proof of Theorem 1.3. Let A be a semistable abelian variety over \mathbf{Q} with good reduction outside 15. By Grothendieck [6, Cor.3.5.2], for every $n \geq 1$ the 2^n -torsion subgroup schemes $A[2^n]$ are objects of the category \underline{B} over the ring $\mathbf{Z}[\frac{1}{15}]$. Proposition 4.1 implies then that

for every $n \geq 1$, the subgroup scheme $A[2^n]$ admits a filtration with simple subquotients isomorphic to $\mathbf{Z}/2\mathbf{Z}$ or μ_2 . We now make a base change to the ring $\mathbf{Z}[\zeta_3, \frac{1}{15}]$. The group schemes $A[2^n]$ are objects of the category \underline{D} . By Propositions 4.5 and 4.6 we obtain for any $n \geq 1$ over $\mathbf{Z}[\zeta_3, \frac{1}{15}]$ a filtration of $A[2^n]$ as follows.

$$0 \underbrace{\subset}_{\mu_2\text{'s}} M_n \underbrace{\subset}_{\Phi\text{'s}} N_n \underbrace{\subset}_{\mathbf{Z}/2\mathbf{Z}\text{'s}} A[2^n]$$

where M_n is filtered by copies of μ_2 , the quotient N_n/M_n is filtered by copies of the group scheme Φ and $A[2^n]/N_n$ is filtered by copies of $\mathbf{Z}/2\mathbf{Z}$.

By Corollary 4.4 the étale group schemes M_n^\vee and $A[2^n]/N_n$ become *constant* over the ring $R[\frac{1}{15}]$. Therefore, for every residue field \mathbf{F}_q of this ring, the groups of points of M_n^\vee and $A[2^n]/N_n$ map injectively to the group of \mathbf{F}_q -rational points of the abelian varieties A/N_n and A^{dual}/N_n' . Here $N_n' = \ker(A[2^n]^\vee \rightarrow M_n^\vee)$. As in the proof of Theorem 1.2 it follows that $\#M_n$ and $\#(A[2^n]/N_n)$ remain bounded as n grows.

Let J denote the elliptic curve given by the Weierstrass equation $Y^2 + XY + Y = X^3 + X^2$. Then $J[2] \cong \Phi$ and $J[4]$ is a non-trivial extension in \underline{D} of Φ by Φ . It is unique by Proposition 4.9. Since $\text{End}(\Phi)$ is isomorphic to the finite field \mathbf{F}_2 , one proves by induction [9, section 8] that any object in \underline{D} that is an extension of group schemes isomorphic to Φ is isomorphic to

$$\bigoplus_{i=1}^t J[2^{m_i}],$$

for certain integers $m_i > 0$. We apply this to the subquotients N_n/M_n of $A[2^n]$. For every $n \geq 0$ the underlying group of $A[2^n]$ is isomorphic to $(\mathbf{Z}/2^n\mathbf{Z})^{2g}$ where $g = \dim A$. This implies that for all $n \geq 0$ there are morphisms of group schemes

$$A[2^n] \xrightarrow{f_n} J[2^n]^g$$

whose kernels and cokernels are bounded as n grows. The morphisms f_n are not necessarily compatible, but there is a *cofinal* compatible system. Taking the limit we obtain an exact sequence of 2-divisible groups

$$0 \longrightarrow H \longrightarrow A_{\text{div}} \longrightarrow J_{\text{div}}^g \longrightarrow 0.$$

where H is a finite subgroup scheme of A . By Faltings' theorem [4] the abelian varieties A and J^g are isogenous over E . The following two propositions imply that A and J^g are also isogenous over \mathbf{Q} . Since J is isogenous to the Jacobian of the modular curve $X_0(15)$, Theorem 1.3 follows.

Lemma 4.9. *Let Γ be a group and let M and N be \mathbf{Z} -torsionfree $\mathbf{Z}[\Gamma]$ -modules. Let H be a subgroup of Γ of finite index and let $I \subset \Gamma$ be a subset for which any $\sigma \in I$ has the properties that $(\sigma - 1)^2$ annihilates M and N with the property that H and I generate Γ . Then every H -linear morphism $f : M \rightarrow N$ is actually Γ -linear.*

Proof. Let $f : M \rightarrow N$ be H -linear. Let $\sigma \in I$ and consider the left H -coset σH . We have $\sigma^k \in H$ for some positive integer k . Writing $T = \sigma - 1$, we have $\sigma^k = (1 + T)^k =$

$1 + kT = 1 + k(\sigma - 1)$ plus a multiple of T^2 in the ring $\mathbf{Z}[\Gamma]$. Since $\sigma \in I$, it follows that $\sigma^k - 1 - k - k\sigma$ kills the modules M and N . Let $m \in M$. Then f maps $(\sigma^k - 1 - k - k\sigma)m$ to $(\sigma^k - 1 - k - k\sigma)f(m)$. Indeed, both sides are zero. Since f is H -linear, it maps $(\sigma^k - 1 - k)m$ to $(\sigma^k - 1 - k)f(m)$. It follows that $f(-k\sigma m) = -k\sigma f(m)$. Since N and M are torsion-free, we find that $f(\sigma m) = \sigma f(m)$. This implies that f is Γ -linear, as required.

Proposition 4.10. *Let F be a number field and let A, B be two semi-stable abelian varieties. Let K be a finite extension of F that does not contain any proper subextension that is unramified outside the set S of primes of bad reduction of A and B . Then A and B are isogenous over K if and only if they are isogenous over F .*

Proof. Pick a prime l . Any K -isogeny $A \rightarrow B$ induces a Galois isomorphism between the Tate modules. More precisely, it gives rise to an isomorphism $f : V_l(A) \rightarrow V_l(B)$ of $\mathbf{Q}_l[H]$ -modules. Here H denotes $\text{Gal}(\overline{F}/K)$. By assumption, the union I of the inertia groups in $G = \text{Gal}(\overline{F}/F)$ of any of the primes lying over S has the property that I and H generate G . Since A and B are semi-stable abelian varieties, the conditions of Lemma 4.9 are satisfied. Therefore $f : V_l(A) \rightarrow V_l(B)$ is G -linear. Faltings' theorem implies then that A and B are isogenous over F .

Bibliography

- [1] Birch, B. and Kuyk, W. Eds.: *Modular functions in one variable IV*. Lecture Notes in Math. **476**, Springer-Verlag, New York 1975.
- [2] Brumer, A. and Kramer, K.: Non-existence of certain semistable abelian varieties, *Manuscripta Math.* **106** (2001) 291–304.
- [3] Dieulefait, L.: Remarks on Serre's modularity conjecture, <http://arxiv.org/abs/math/0603439>.
- [4] Faltings, G.: Endlichkeitssätze für abelsche Varietäten über Zahlkörpern, *Invent. Math.* **73** (1983) 349–366.
- [5] Fontaine, J.-M.: Il n'y a pas de variété abélienne sur \mathbf{Z} , *Invent. Math.* **81**, (1985) 515–538.
- [6] Grothendieck, A.: Modèles de Néron et monodromie, Exp IX in *Groupes de monodromie en géométrie algébrique*, SGA 7, Part I, Lecture Notes in Mathematics **288** (1971) Springer-Verlag, New York.
- [7] Odlyzko, A.M.: Unconditional bounds for discriminants, 1976. <http://www.dtc.umn.edu/~odlyzko/unpublished/discr.bound.table2>
- [8] Schoof, R.: Abelian varieties over cyclotomic fields with good reduction everywhere, *Math. Annalen* **325** (2003), 413–448.
- [9] Schoof, R.: Abelian varieties over \mathbf{Q} with bad reduction in one prime only, *Compositio Math.* **141** (2005), 847–868.
- [10] Tate, J.T. and Oort, F.: Group schemes of prime order, *Ann. Scient. École Norm. Sup.* **3** (1970) 1–21.
- [11] Taussky, O.: A remark on the class field tower, *J. London Math. Soc.* **12** (1937), 82–85.