

# SEMISTABLE ABELIAN VARIETIES OVER $\mathbf{Q}$ . II

ASTRA 6.0, FABLE 5.1

ABSTRACT. We prove that for  $N = 6$  and  $N = 10$ , there do not exist any non-zero semistable abelian varieties over  $\mathbf{Q}$  with good reduction outside primes dividing  $N$ . Combined with results of Brumer–Kramer and of Schoof, this result is best possible: if  $N$  is squarefree, there exists a non-zero semistable abelian variety over  $\mathbf{Q}$  with good reduction outside primes dividing  $N$  if and only if  $N \notin \{1, 2, 3, 5, 6, 7, 10, 13\}$ .

## CONTENTS

|                                                           |   |
|-----------------------------------------------------------|---|
| 1. Introduction                                           | 1 |
| 2. Acknowledgments: Human disclosure                      | 3 |
| 3. Raynaud uniformization and the integral torsion groups | 3 |
| 4. Ramification and root discriminants                    | 6 |
| 5. The two-group criterion                                | 7 |
| 6. The two-division fields for $p = 3$ and $p = 5$        | 8 |
| References                                                | 9 |

## 1. INTRODUCTION

In this paper, we address the following question: for what integers  $N$  does there exist a non-zero abelian variety  $A/\mathbf{Z}[1/N]$  with semistable reduction at primes dividing  $N$ . Without loss of generality, one may assume that  $N$  is squarefree. The Jacobians  $J_0(N)$  provide examples of such  $A$  whenever  $N \notin \{1, 2, 3, 5, 6, 7, 10, 13\}$ . The main theorem of this paper is that this list is complete; namely, that there does not exist a non-zero semistable abelian variety  $A/\mathbf{Z}[1/N]$  for such  $N$ . This is a theorem of Fontaine for  $N = 1$  [Fon85] (see also [Abr87]), of Brumer and Kramer for  $N \in \{2, 3, 5, 7\}$  [BK01], and of Schoof for  $N \in \{2, 3, 5, 7, 13\}$  [Sch05]. For  $N \in \{6, 10\}$ , it was proved by Calegari [Cal04] under the assumption of the GRH discriminant bounds of Odlyzko. Hence the remaining goal in this paper is to remove that assumption.

**Theorem 1.1.** *There is no non-zero semistable abelian variety over  $\mathbf{Q}$  with good reduction outside  $\{2, 3\}$ , and none with good reduction outside  $\{2, 5\}$ .*

All the proofs mentioned above follow Fontaine’s strategy. One chooses a prime  $l \nmid N$ , bounds the ramification of the  $l$ -division field  $\mathbf{Q}(A[l])$  using Fontaine’s theorem on finite flat group schemes [Fon85], bounds its degree using Odlyzko’s lower bounds for discriminants [Odl90, Odl76], deduces that the  $l$ -power torsion is built from the group schemes  $\mathbf{Z}/l$  and  $\mu_l$ , and derives a contradiction with the Weil bounds at a prime of good reduction. For  $N = 6$ , the smallest admissible prime is  $l = 5$  and the root discriminant of  $\mathbf{Q}(A[5])$  is bounded by  $5^{5/4}6^{4/5} \approx 31.35$ ; for  $N = 10$  one takes  $l = 3$  and obtains  $3^{3/2}10^{2/3} \approx 24.12$ . Both exceed  $4\pi e^\gamma \approx 22.38$ , the limit of Odlyzko’s unconditional bounds, so no unconditional discriminant bound can bound the degree of these fields; under GRH the limit is  $8\pi e^\gamma \approx 44.76$  and the degrees are bounded. It does not seem possible to avoid the use of GRH using this method.

The new variation of this paper is to consider instead  $l = 2$  which divides  $N$ . At the odd prime  $p \mid N$ , we deduce (as in [BK01, Sch05, Cal04]) that inertia acts on  $A[2]$  through an element  $\sigma$  with

---

Date: 2 October 2026.

This work was supported in part by NSF Grant DMS-2001097.

$(\sigma - 1)^2 = 0$ , hence  $\sigma^2 = 1$ , so the ramification at  $p$  is tame of index at most 2 and contributes at most  $p^{1/2}$  to the root discriminant. But now at  $l = 2$  Fontaine's theorem does not apply, and we need a replacement to bound the action of inertia in this case; this will be the first result of this paper.

We use Serre's upper numbering [Ser68, Chap. IV]: for a finite Galois extension  $L/K$  of local fields with group  $G$ ,  $G^{-1} = G$ ,  $G^u = G^0$  is the inertia group for  $-1 < u \leq 0$ , and  $G^u$  decreases with  $u$ . Fontaine [Fon85] uses the shifted numbering  $G^{(v)} = G^{v-1}$ . If  $K/\mathbf{Q}_2$  is unramified, valuations on algebraic extensions of  $K$  are normalized by  $v(2) = 1$ .

**Theorem 1.2.** *Let  $A/\mathbf{Q}_2$  be an abelian variety with semistable reduction, let  $L = \mathbf{Q}_2(A[2])$  and  $G = \text{Gal}(L/\mathbf{Q}_2)$ . Then*

$$|G^u| \leq 2 \quad (u > 1), \quad G^u = 1 \quad (u > 2).$$

*In particular, if  $e = e(L/\mathbf{Q}_2)$ , then*

$$v_2(\mathfrak{D}_{L/\mathbf{Q}_2}) \leq \frac{5}{2} - \frac{2}{e} < \frac{5}{2}.$$

Note that the cutoff 2 is optimal; for the Tate curve with parameter 2 one has  $L = \mathbf{Q}_2(\sqrt{2})$  whose upper jump is 2.

For torsion quotients of lattices in semistable  $p$ -adic representations with Hodge–Tate weights in  $\{0, \dots, r\}$  there is a general ramification bound due to Hattori [Hat09] and Caruso–Liu [CL11]: in the shifted numbering, Hattori proves that  $G^{(v)}$  acts trivially for  $v > 1 + e(n + 1/(p - 1))$  when  $r = 1$ , where  $e$  is the absolute ramification index and  $p^n$  kills the module. Both proofs assume that  $p$  odd (Hattori's hypothesis is  $r < p - 1$ ). Both results give the same bound when  $n = r = 1$  and  $e < p - 1$ . For  $p = 2$ , and  $e = n = r = 1$ , their bound would read  $G^{(v)} = 1$  for  $v > 3$ , i.e.  $G^u = 1$  for  $u > 2$ , which is the second assertion of Theorem 1.2. It may well be possible to adapt the methods of those papers to cover the case  $p = 2$ . Our proof, however, is specific to abelian varieties: it uses the Raynaud uniformization and only Fontaine's theorem for finite flat group schemes, which holds for all primes including 2. It also gives the extra information that  $|G^u| \leq 2$  for  $u > 1$  which will be useful.

The global argument has two separate parts. One (standard) part is to use the discriminant bound of Theorem 1.2 to show that  $\text{Gal}(\mathbf{Q}(A[2])/\mathbf{Q})$  is a 2-group. The other is the following criterion, which is where the restriction to  $p \in \{3, 5\}$  is not yet needed:

**Theorem 1.3.** *Let  $p$  be an odd prime with  $p \equiv 3$  or  $5 \pmod{8}$ , and let  $A/\mathbf{Q}$  be an abelian variety with semistable reduction at 2 and good reduction outside  $\{2, p\}$ . If  $\text{Gal}(\mathbf{Q}(A[2])/\mathbf{Q})$  is a 2-group, then  $A$  has good reduction at 2. The same holds with  $\{2, p\}$  replaced by  $\{2\}$ .*

The proof is short. The hypothesis on  $p$  implies that every 2-extension of  $\mathbf{Q}$  unramified outside  $\{2, p, \infty\}$  has full decomposition group at 2. Applied to the fields  $\mathbf{Q}(A[2^n])$ , this shows that the toric part  $V_2(\mathcal{T}) \subset V_2(A)$  of the Raynaud uniformization at 2, which is a priori only stable under  $G_{\mathbf{Q}_2}$ , is stable under  $G_{\mathbf{Q}}$ , and that  $G_{\mathbf{Q}}$  acts on it through the image of  $G_{\mathbf{Q}_2}$ , an abelian group. By Kronecker–Weber, Frobenius at a prime  $q$  of good reduction then acts on  $V_2(\mathcal{T})$  with eigenvalues of absolute value  $q$ , contradicting the Weil bound unless  $\mathcal{T} = 0$ . Once  $A$  has good reduction at 2, Theorem 1.1 follows from Brumer–Kramer [BK01] or [Sch05].

The paper is organized as follows. Section 3 recalls the Raynaud uniformization of  $A$  over  $\mathbf{Q}_2$  and deduces from it the two facts we need: the description of the toric part of  $V_2(A)$  as a  $G_{\mathbf{Q}_2}$ -representation, and a finite flat group scheme  $\mathcal{H}_2$  over  $\mathcal{O}_K$  with  $K(A[2]) \subset K(\mathcal{H}_2)(\sqrt{2})$ . Section 4 proves Theorem 1.2 and the resulting root discriminant bound. Section 5 proves Theorem 1.3, and Section 6 proves Theorem 1.1.

**Remark 1.4.** When semistable abelian varieties with good reduction outside  $N$  do exist, one can ask whether they are all isogenous to powers of  $J_0(N)$ . Schoof proved this for  $N = 11$  in [Sch05], for  $N = 15$  in [Sch12b], and for  $N = 23$  in [Sch12a]; Campagna and Goodman [CG25] have recently proved it for  $N = 19$ . The case  $N = 15$  is the only other squarefree  $N$  with two prime factors for which such a classification is known.

## 2. ACKNOWLEDGMENTS: HUMAN DISCLOSURE

We acknowledge that human assistance was used in polishing the manuscript, improving the exposition, and exploring possible research directions. The authors independently developed, verified, refined, and wrote all mathematical arguments, and take full responsibility for the current manuscript. Frank Calegari (version 1.0, set to medium intelligence) was used to explore possible research directions and to provide occasional guidance. In particular, he raised the initial question and, after some initial considerations, offered Fable the following prompt:

It seems to me that we should then start at  $p=2$ , and assume that we know the "simple" objects are  $\mathbf{Z}/2\mathbf{Z}$ . I'm not sure what category we should work in to capture the semistability (log-flat??). But there is definitely something to explore here. Work out a program and push how far it goes

Fable then came up with an initial version of the argument, contingent on the assumption that [Hat09, CL11] could be adapted for  $p = 2$ . The argument was then passed to Chat GPT Astra 6.0 with the request to supply this missing ingredient:

I want you to #1 stress test this argument, and #2 supply the missing ingredient for  $\mathbf{Q}_2(A[2])$  and  $A$  a semistable abelian variety over 2 (can this also be extracted from Raynaud uniformization!?)

Astra then provided the precise statement and proof of Theorem 1.2, and a complete argument which proceeded by analyzing the connected parts of  $A[2^n]$  for all  $n$ . Calegari then observed that the resulting argument, which analysed the connected parts of  $A[2^n]$  for all  $n$ , could be replaced by the argument of Section 5:

Once we know that the action of  $G_{\mathbf{Q}}$  on  $A[2^\infty]$  is seen by  $G_{\mathbf{Q}_2}$ ; surely we can go immediately to the full 2-adic Tate module, and a soft version of Raynaud shows that there can not be any toric part, because (looking globally) the ss of the toric part is abelian and then globally abelian. So then we have good reduction at 2 and we are done by previous results???

## 3. RAYNAUD UNIFORMIZATION AND THE INTEGRAL TORSION GROUPS

Throughout this section,  $A/\mathbf{Q}_2$  is an abelian variety with semistable reduction. We need two facts about its 2-power torsion, Lemma 3.4 and Lemma 3.9 below. Both are elementary consequences of the rigid analytic uniformization of  $A$ , which we now recall. For proofs and for the comparison with the Néron model see Raynaud [Ray71], Bosch–Lütkebohmert [BL91, §1] and Faltings–Chai [FC90, Ch. II, §1, and Ch. III].

**The uniformization.** There is a semiabelian scheme  $\mathcal{G}$  over  $\mathbf{Z}_2$ , the *Raynaud extension* of  $A$ , which is an extension

$$0 \longrightarrow \mathcal{T} \longrightarrow \mathcal{G} \longrightarrow \mathcal{B} \longrightarrow 0$$

of an abelian scheme  $\mathcal{B}$  by a torus  $\mathcal{T}$  over  $\mathbf{Z}_2$ , together with a  $G_{\mathbf{Q}_2}$ -stable subgroup  $Y \subset \mathcal{G}(\overline{\mathbf{Q}_2})$ , free of rank  $t = \dim \mathcal{T}$  (the *period lattice*), such that

$$(3.1) \quad 0 \longrightarrow Y \longrightarrow \mathcal{G}(\overline{\mathbf{Q}_2}) \longrightarrow A(\overline{\mathbf{Q}_2}) \longrightarrow 0$$

is an exact sequence of  $G_{\mathbf{Q}_2}$ -modules. The exactness of (3.1) is the statement on points of the isomorphism of rigid analytic groups  $A^{\text{an}} \simeq \mathcal{G}^{\text{an}}/Y$ . (The isomorphism directly gives  $A(\mathbf{C}_2) = \mathcal{G}(\mathbf{C}_2)/Y$  rather than the statement for  $\overline{\mathbf{Q}_2}$ -points, however, the map  $\mathcal{G}^{\text{an}} \rightarrow A^{\text{an}}$  is an étale covering, so its fibre over a point of  $A$  rational over a finite extension of  $\mathbf{Q}_2$  consists of points of  $\mathcal{G}$  rational over finite extensions.) The torus  $\mathcal{T}$  is split by a finite unramified extension, as is every torus over the henselian ring  $\mathbf{Z}_2$ , and  $G_{\mathbf{Q}_2}$  acts on  $Y$  through a finite unramified quotient, since  $Y$  is the character group of the torus in the Raynaud extension of the dual abelian variety. These two unramifiedness statements are the only place where semistability (as opposed to potentially

semistable reduction) is used. The special fibre of  $\mathcal{G}$  is the identity component of the special fibre of the Néron model of  $A$  [BL91, §1], so  $t$  is the toric rank of  $A$  at 2.

**Notation.** Fix a finite unramified extension  $K/\mathbf{Q}_2$  over which  $\mathcal{T}$  is split and  $G_K$  acts trivially on  $Y$ . Put  $R = \mathcal{O}_K$ , so that  $\mathcal{T}_R \simeq \mathbf{G}_m^t$  and  $Y \simeq \mathbf{Z}^t$ , and let  $k$  be the residue field of  $R$  and  $\varpi = 2$  its uniformizer. Let  $\bar{K}$  be an algebraic closure of  $K$ ,  $\mathcal{O}_{\bar{K}}$  its valuation ring and  $\bar{k}$  its residue field. For an  $R$ -scheme  $Z$  we put  $Z(\mathcal{O}_{\bar{K}}) = \bigcup Z(\mathcal{O}_{K'})$ , the union over the finite extensions  $K'/K$  inside  $\bar{K}$ . Reduction modulo the maximal ideal gives a map  $Z(\mathcal{O}_{\bar{K}}) \rightarrow Z(\bar{k})$ ,  $z \mapsto \bar{z}$ , which is  $G_K$ -equivariant when  $G_K$  acts on  $Z(\bar{k})$  through  $\text{Gal}(\bar{k}/k)$ ; in particular the inertia group  $I_K$  acts trivially on  $Z(\bar{k})$ . If  $Z$  is finite over  $R$  then  $Z(\bar{K}) = Z(\mathcal{O}_{\bar{K}})$ . We use additive notation in  $\mathcal{G}$ , including on the torus; the notation  $\lambda(a)$ , for a cocharacter  $\lambda \in X_*(\mathcal{T}) = \text{Hom}(\mathbf{G}_m, \mathcal{T})$  and  $a \in \bar{K}^\times$ , keeps its multiplicative meaning.

Since  $G_K$  acts trivially on  $Y$ , we have  $Y \subset \mathcal{G}(K)$ ; we write  $u : Y \rightarrow \mathcal{G}(K)$  for the inclusion, the *period homomorphism*. (Here we follow the notion of Deligne [Del74, §10] and Raynaud [Ray94] for the homomorphism defining a 1-motive  $[Y \xrightarrow{u} \mathcal{G}]$ .) By (3.1), for every  $m \geq 1$ ,

$$(3.2) \quad A[m](\bar{K}) = \{g \in \mathcal{G}(\bar{K}) : mg \in u(Y)\} / u(Y)$$

as  $G_K$ -modules, where  $\sigma[g] = [\sigma g]$ . The map  $\mathcal{G}[m](\bar{K}) \rightarrow A[m](\bar{K})$ ,  $g \mapsto [g]$ , is injective because  $u(Y)$  is torsion free, and its cokernel is  $Y/mY$ , with trivial Galois action.

**The toric part of the Tate module.** Passing to the inverse limit over  $m = 2^n$  in (3.2) gives an exact sequence of  $G_{\mathbf{Q}_2}$ -modules

$$(3.3) \quad 0 \longrightarrow T_2(\mathcal{G}) \longrightarrow T_2(A) \longrightarrow Y \otimes \mathbf{Z}_2 \longrightarrow 0,$$

and  $\mathcal{T} \subset \mathcal{G}$  gives  $T_2(\mathcal{T}) \subset T_2(\mathcal{G})$ . We write  $V_2(\mathcal{T}) = T_2(\mathcal{T}) \otimes \mathbf{Q}_2$ , a  $G_{\mathbf{Q}_2}$ -stable subspace of  $V_2(A)$  of dimension  $t$ , the *toric part* of  $V_2(A)$ .

**Lemma 3.4.**

- (i) *There is a  $G_{\mathbf{Q}_2}$ -equivariant isomorphism  $T_2(\mathcal{T}) \simeq X_*(\mathcal{T}) \otimes \mathbf{Z}_2(1)$ , where  $G_{\mathbf{Q}_2}$  acts on the cocharacter group  $X_*(\mathcal{T})$  through the finite unramified quotient  $\text{Gal}(K/\mathbf{Q}_2)$ . In particular  $I_{\mathbf{Q}_2}$  acts on  $T_2(\mathcal{T})$  through the cyclotomic character  $\chi$ , by scalars, and the image of  $G_{\mathbf{Q}_2}$  in  $\text{Aut}(T_2(\mathcal{T}))$  is abelian.*
- (ii) *If  $t = 0$ , then  $A$  has good reduction at 2.*

*Proof.* For every  $m$ , the map  $X_*(\mathcal{T}) \otimes \mu_m \rightarrow \mathcal{T}[m]$ ,  $\lambda \otimes \zeta \mapsto \lambda(\zeta)$ , is a  $G_{\mathbf{Q}_2}$ -equivariant isomorphism; pass to the limit. The group  $\text{Gal}(K/\mathbf{Q}_2)$  is cyclic, so the image of  $G_{\mathbf{Q}_2}$  is generated by commuting elements: the images of  $\text{Gal}(K/\mathbf{Q}_2)$  acting on the first factor and the scalars  $\chi(G_{\mathbf{Q}_2})$  acting on the second. This proves part (i). If  $t = 0$ , then  $\mathcal{T} = 0$  and  $Y = 0$ , so  $\mathcal{G} = \mathcal{B}$  is an abelian scheme over  $\mathbf{Z}_2$  and (3.1) identifies  $A$  with its generic fibre. This proves part (ii).  $\square$

**Remark 3.5.** For  $l \neq 2$ , the analogous description of  $T_l(A)$  as a  $G_{\mathbf{Q}_2}$ -module is Grothendieck's [Gro72, Exp. IX]:  $T_l(\mathcal{G})$  is unramified, with toric part  $X_*(\mathcal{T}) \otimes \mathbf{Z}_l(1)$  and abelian part  $T_l(\mathcal{B})$ , and the quotient  $Y \otimes \mathbf{Z}_l$  is unramified. For  $l = 2$  the module  $T_2(\mathcal{B})$  is crystalline rather than unramified, and the sequence (3.3) does not split in general, but the toric part behaves exactly as for  $l \neq 2$ . This is all that is used in Section 5.

**Lemma 3.6** (Raynaud [Ray94]). *There are homomorphisms  $u_0 : Y \rightarrow \mathcal{G}(R)$  and  $\nu : Y \rightarrow X_*(\mathcal{T})$  such that*

$$u(y) = u_0(y) + \nu(y)(\varpi) \quad \text{for all } y \in Y.$$

*Proof.* It suffices to define  $u_0$  and  $\nu$  on a basis  $y_1, \dots, y_t$  of  $Y$  and to extend additively. The image of  $u(y_j)$  in  $\mathcal{B}(K)$  lies in  $\mathcal{B}(R)$ , as  $\mathcal{B}$  is proper. Its inverse image in  $\mathcal{G}$  is a torsor under the split torus  $\mathcal{T}_R \simeq \mathbf{G}_m^t$  over  $\text{Spec } R$ ; since  $H_{\text{fppf}}^1(R, \mathbf{G}_m) = \text{Pic}(R) = 0$ , this torsor has an  $R$ -point  $g_j$ . Then  $u(y_j) - g_j \in \mathcal{T}(K) = (K^\times)^t$ , and each coordinate is uniquely a unit times a power of  $\varpi$ . Moving the unit coordinates into  $g_j$  gives  $u_0(y_j) \in \mathcal{G}(R)$ , and the vector of valuations is  $\nu(y_j) \in \mathbf{Z}^t = X_*(\mathcal{T})$ .  $\square$

This is the split case of a theorem of Raynaud [Ray94, 4.5.1], which decomposes the period homomorphism of the 1-motive  $[Y \rightarrow \mathcal{G}_K]$  into an integral part and a part with values in the torus; see also [BCC04, Thm. 9] and [Gun21, Prop. 2.17]. Only the elementary statement above is used here. The homomorphisms  $u_0$  and  $\nu$  depend only on the choice of the uniformizer  $\varpi$ .

**Example 3.7.** Let  $A = E_q$  be the Tate curve over  $\mathbf{Q}_2$  with parameter  $q = 2^n \epsilon$ ,  $n \geq 1$ ,  $\epsilon \in \mathbf{Z}_2^\times$ . Then  $\mathcal{G} = \mathbf{G}_m$ ,  $Y = q^{\mathbf{Z}} \subset \mathbf{Q}_2^\times$ , and, in multiplicative notation,  $u_0(q) = \epsilon$  and  $\nu(q) = n \in \mathbf{Z} = X_*(\mathbf{G}_m)$ .

**The group scheme  $\mathcal{H}_2$ .** Fontaine's ramification bound (Theorem 4.1 below) applies to the points of a finite flat group scheme over  $R$ . The Galois module  $A[2]$  is not (necessarily) of this form when  $t > 0$ , but Lemma 3.6 allows us to compare it with one. For  $y \in Y$ , let

$$X_y = [2]^{-1}(u_0(y)) \subset \mathcal{G}$$

be the fibre of multiplication by 2 over the  $R$ -point  $u_0(y)$ ; thus  $X_0 = \mathcal{G}[2]$ .

**Lemma 3.8.**

- (i) Each  $X_y$  is a finite flat  $R$ -scheme and a torsor under  $\mathcal{G}[2]$ , and for  $z \in Y$  translation by  $u_0(z)$  is an isomorphism  $X_y \rightarrow X_{y+2z}$ .
- (ii) Choose a representative  $\tilde{a} \in Y$  for each class  $a \in Y/2Y$ . The disjoint union

$$\mathcal{H}_2 = \coprod_{a \in Y/2Y} X_{\tilde{a}}$$

is a finite flat commutative group scheme over  $R$  killed by 2, with group law  $(g, a) + (h, b) = (g + h - u_0(d), c)$  where  $\tilde{a} + \tilde{b} = \tilde{c} + 2d$ ,  $d \in Y$ . There is an exact sequence  $0 \rightarrow \mathcal{G}[2] \rightarrow \mathcal{H}_2 \rightarrow (Y/2Y)_R \rightarrow 0$ .

*Proof.* Multiplication by 2 on  $\mathcal{G}$  is flat by the fibral flatness criterion [Con, §5] and surjective on fibres, and its kernel  $\mathcal{G}[2]$  is finite flat, being an extension of  $\mathcal{B}[2]$  by  $\mathcal{T}[2] \simeq \mu_2^t$ . The map  $\mathcal{G} \times \mathcal{G}[2] \rightarrow \mathcal{G} \times_{[2], \mathcal{G}[2]} \mathcal{G}$ ,  $(g, h) \mapsto (g, g + h)$ , is an isomorphism, so after the faithfully flat base change  $[2]$  the morphism  $[2] : \mathcal{G} \rightarrow \mathcal{G}$  becomes the projection  $\mathcal{G} \times \mathcal{G}[2] \rightarrow \mathcal{G}$ , which is finite flat; by descent,  $[2]$  is finite flat. Hence so is its base change  $X_y \rightarrow \text{Spec } R$  along  $u_0(y)$ , which is a torsor under  $\mathcal{G}[2]$ . The last assertion holds because  $2u_0(z) = u_0(2z)$ . This proves part (i).

For part (ii), let  $Y_R$  be the constant group scheme and  $\hat{\mathcal{H}} = \mathcal{G} \times_{[2], \mathcal{G}, u_0} Y_R = \coprod_{y \in Y} X_y$ , a closed subgroup scheme of  $\mathcal{G} \times Y_R$  whose points are the pairs  $(g, y)$  with  $2g = u_0(y)$ . The homomorphism  $Y_R \rightarrow \hat{\mathcal{H}}$ ,  $z \mapsto (u_0(z), 2z)$ , is a closed immersion, and translation by its image maps  $X_y$  isomorphically onto  $X_{y+2z}$  by part (i). The morphism  $\hat{\mathcal{H}} \rightarrow \coprod_a X_{\tilde{a}}$  sending  $(g, y)$ ,  $y = \tilde{a} + 2d$ , to  $(g - u_0(d), \tilde{a})$  is invariant under  $Y_R$  and restricts to the identity on  $\coprod_a X_{\tilde{a}} \subset \hat{\mathcal{H}}$ ; hence it identifies  $\coprod_a X_{\tilde{a}}$  with the quotient  $\hat{\mathcal{H}}/Y_R$ , with the group law stated. Since  $2(g, y) = (u_0(y), 2y)$  lies in the image of  $Y_R$ , the quotient is killed by 2; it is finite flat by part (i). Finally  $(g, a) \mapsto a$  is a homomorphism onto  $(Y/2Y)_R$  with kernel the open and closed subgroup  $X_0 = \mathcal{G}[2]$ .  $\square$

**Lemma 3.9** (Comparison). *With  $\mathcal{H}_2$  as in Lemma 3.8, the field  $K(\mathcal{H}_2) = K(\mathcal{H}_2(\bar{K}))$  is Galois over  $K$  and*

$$K(A[2]) \subset K(\mathcal{H}_2)(\sqrt{2}).$$

*Proof.*  $K(\mathcal{H}_2)$  is Galois over  $K$  because  $\mathcal{H}_2(\bar{K})$  is  $G_K$ -stable,  $\mathcal{H}_2$  being defined over  $R$ . Let  $x = [g] \in A[2](\bar{K})$ , so that  $2g = u(y) = u_0(y) + \nu(y)(2)$  for some  $y \in Y$ , and put  $g_0 = g - \nu(y)(\sqrt{2})$ . Then  $2g_0 = u_0(y)$ , i.e.  $g_0 \in X_y(\bar{K})$ . Writing  $y = \tilde{a} + 2d$ , we have  $g_0 - u_0(d) \in X_{\tilde{a}}(\bar{K}) \subset \mathcal{H}_2(\bar{K})$  and  $u_0(d) \in \mathcal{G}(K)$ , so  $g_0 \in \mathcal{G}(K(\mathcal{H}_2))$ . Since  $\mathcal{T}$  is split over  $K$ ,  $\nu(y)(\sqrt{2}) \in \mathcal{T}(K(\sqrt{2}))$ . Hence  $g \in \mathcal{G}(K(\mathcal{H}_2)(\sqrt{2}))$ , so  $x$  is fixed by  $G_{K(\mathcal{H}_2)(\sqrt{2})}$ . As  $x$  was arbitrary,  $K(A[2]) \subset K(\mathcal{H}_2)(\sqrt{2})$ .  $\square$

**Remark 3.10.** The map  $[g] \mapsto [g - \nu(y)(\sqrt{2}), y]$  in the proof is a bijection  $A[2](\bar{K}) \rightarrow \mathcal{H}_2(\bar{K})$  which is compatible with the group structures and with the action of  $G_{K(\sqrt{2})}$ ; for general  $\sigma \in G_K$  it is equivariant only up to the  $\mathcal{T}[2]$ -valued cocycle  $\nu(y)(\sigma\sqrt{2}/\sqrt{2})$ . In the language of Deligne [Del74, §10],  $\mathcal{H}_2$  is the 2-torsion of the 1-motive  $[Y \xrightarrow{u_0} \mathcal{G}]$  over  $R$  and  $A[2]$  that of the 1-motive

$[Y \xrightarrow{u} \mathcal{G}_K]$  over  $K$ ; this is the simplest instance of Raynaud’s decomposition of the latter into an integral 1-motive and a toric one [Ray94], cf. [Gun21, §2.2]. Nothing beyond Lemmas 3.6–3.9 is used below.

**Remark 3.11.** For the Tate curve of Example 3.7,  $E_q[2] = \{\pm 1, \pm \sqrt{q}\} \subset \overline{\mathbf{Q}}_2^\times / q^{\mathbf{Z}}$  and  $\mathcal{H}_2 = \mu_2 \sqcup \text{Spec } \mathbf{Z}_2[x]/(x^2 - \epsilon)$ , the 2-torsion of the “Tate curve with unit parameter”  $[\mathbf{Z} \rightarrow \mathbf{G}_m, 1 \mapsto \epsilon]$ . The comparison lemma reads  $\mathbf{Q}_2(\sqrt{q}) \subset \mathbf{Q}_2(\sqrt{\epsilon}, \sqrt{2})$ . Here  $\mathbf{Q}_2(\sqrt{\epsilon})/\mathbf{Q}_2$  is unramified or has upper ramification jump 1, in accordance with Fontaine’s bound, whereas  $\mathbf{Q}_2(\sqrt{2})/\mathbf{Q}_2$  has upper jump 2.

#### 4. RAMIFICATION AND ROOT DISCRIMINANTS

**Theorem 4.1** (Fontaine). *Let  $K/\mathbf{Q}_2$  be a finite unramified extension and  $H/\mathcal{O}_K$  a finite flat commutative group scheme killed by 2. Put  $F = K(H(\overline{K}))$ . Then  $\text{Gal}(F/K)^u = 1$  for  $u > 1$ .*

This is [Fon85, Théorème A], which for a finite flat group scheme killed by  $l^n$  over the ring of integers of a local field of absolute ramification index  $e$  gives trivial action of  $G^{(v)}$  for  $v > e(n + 1/(l - 1))$  in the shifted numbering; here  $e = n = 1$ ,  $l = 2$ , so the cutoff is  $v = 2$ , i.e.  $u = 1$ . Fontaine’s theorem has no restriction on the residue characteristic; it is used at  $l = 2$  for instance in [Sch05].

*Proof of Theorem 1.2.* Let  $K, \mathcal{H}_2$  be as in Section 3, and put  $F = K(\mathcal{H}_2)$ ,  $L' = F(\sqrt{2})$ . Both are Galois over  $K$  and  $K(A[2]) \subset L'$  by Lemma 3.9. Upper numbering is compatible with quotients, so for  $u > 1$  Theorem 4.1 gives  $\text{Gal}(L'/K)^u \subset \text{Gal}(L'/F)$ , a group of order at most 2. The quadratic extension  $K(\sqrt{2})/K$  has discriminant exponent 3, hence upper jump 2; so for  $u > 2$  the group  $\text{Gal}(L'/K)^u$  maps trivially to both  $\text{Gal}(F/K)$  and  $\text{Gal}(K(\sqrt{2})/K)$ , and since  $L' = F \cdot K(\sqrt{2})$  it is trivial. Passing to the quotient  $\text{Gal}(K(A[2])/K)$  preserves both assertions. Finally  $K/\mathbf{Q}_2$  is unramified, so the inertia groups, their upper numbering filtrations and the normalized different of  $L/\mathbf{Q}_2$  and of  $LK/K$  coincide.

For the different, with  $e = |G^0|$ ,

$$v_2(\mathfrak{D}_{L/\mathbf{Q}_2}) = \int_{-1}^{\infty} \left(1 - \frac{1}{|G^u|}\right) du \leq 2\left(1 - \frac{1}{e}\right) + \frac{1}{2} = \frac{5}{2} - \frac{2}{e},$$

since the integrand is at most  $1 - 1/e$  on  $(-1, 1]$ , at most  $1/2$  on  $(1, 2]$ , and zero beyond. The Tate curve with parameter 2 has  $A[2] = \{\pm 1, \pm \sqrt{2}\} \subset \overline{\mathbf{Q}}_2^\times / 2^{\mathbf{Z}}$  and  $L = \mathbf{Q}_2(\sqrt{2})$ , with upper jump 2.  $\square$

**Remark 4.2.** The bound  $5/2 - 2/e$  is sharp for every  $e = 2^{f+1}$ . Let  $K/\mathbf{Q}_2$  be unramified of degree  $f$  and  $L = K(\sqrt{K^\times})$ , so that  $\text{Gal}(L/K) \simeq K^\times / K^{\times 2} \simeq (\mathbf{Z}/2)^{f+2}$  and  $e = 2^{f+1}$ . The Tate curves over  $K$  with parameters 2 and  $4u$ ,  $u \in \mathcal{O}_K^\times$ , have 2-division fields  $K(\sqrt{2})$  and  $K(\sqrt{u})$ , so  $L = K(A[2])$  for their product  $A$ , and  $L = \mathbf{Q}_2(\text{Res}_{K/\mathbf{Q}_2} A[2])$ . By local class field theory  $G^u$  is the image of  $U_K^{([u])}$  in  $K^\times / K^{\times 2}$ ; as  $U_K^{(3)} \subset K^{\times 2}$  and the squares of  $U_K^{(1)}$  have index 2 in  $U_K^{(2)}$ , one finds  $|G^u| = 2^{f+1}$  for  $u \leq 1$ ,  $|G^u| = 2$  for  $1 < u \leq 2$  and  $G^u = 1$  for  $u > 2$ , so that  $v_2(\mathfrak{D}_{L/\mathbf{Q}_2}) = 5/2 - 2/e$ .

**Proposition 4.3.** *Let  $p$  be an odd prime and  $A/\mathbf{Q}$  an abelian variety with semistable reduction at 2 and at  $p$  and good reduction outside  $\{2, p\}$ . Every subfield  $E \subset \mathbf{Q}(A[2])$  satisfies*

$$\text{rd}(E) < 2^{5/2} \sqrt{p}.$$

*For  $p = 3$  one has  $[E : \mathbf{Q}] \leq 20$ , and for  $p = 5$  one has  $[E : \mathbf{Q}] \leq 37$ .*

*Proof.* Put  $L = \mathbf{Q}(A[2])$ ; it is unramified outside  $\{2, p, \infty\}$ . By Grothendieck’s semistable reduction theorem [Gro72, Exp. IX, 3.5], inertia at  $p$  acts on  $T_2(A)$  through its tame pro-2 quotient and every inertia element  $\sigma$  satisfies  $(\sigma - 1)^2 = 0$ ; on  $A[2]$  this gives  $\sigma^2 = 1$ . So the ramification at  $p$  is tame of index at most 2 and contributes at most  $p^{1/2}$  to  $\text{rd}(L)$ , while Theorem 1.2 bounds the contribution at 2 strictly by  $2^{5/2}$ . The root discriminant of a subfield is at most that of the field.

Odlyzko’s unconditional Table 2 [Odl76] lists, in its totally complex column, lower bounds valid for all fields of degree at least  $n$  of that signature; the bounds for other signatures are larger. Its

entries at  $n = 21$  and  $n = 38$  are 10.010 and 12.737. Since  $\sqrt{96} < 9.798$  and  $\sqrt{160} < 12.650$ , the degree bounds follow.  $\square$

## 5. THE TWO-GROUP CRITERION

**Lemma 5.1.** *Let  $p \equiv 3$  or  $5 \pmod{8}$ . No quadratic field unramified outside  $\{2, p, \infty\}$  is split at 2.*

*Proof.* The fields in question are  $\mathbf{Q}(\sqrt{d})$  with  $d \in \{-1, \pm 2, \pm p, \pm 2p\}$ . An even squarefree  $d$  is not a square in  $\mathbf{Q}_2$ , and an odd  $d$  is a square in  $\mathbf{Q}_2$  if and only if  $d \equiv 1 \pmod{8}$ ; the odd entries are  $-1 \equiv 7$  and  $\pm p \equiv \pm 3, \pm 5 \pmod{8}$ .  $\square$

**Lemma 5.2** (Full decomposition group at 2). *Let  $S = \{2, p\}$  with  $p \equiv 3, 5 \pmod{8}$ , or  $S = \{2\}$ . If  $L/\mathbf{Q}$  is a finite Galois extension with 2-group Galois group, unramified outside  $S \cup \{\infty\}$ , then the decomposition group of  $L/\mathbf{Q}$  at 2 is all of  $\text{Gal}(L/\mathbf{Q})$ . Consequently, if  $M$  is a  $G_{\mathbf{Q}}$ -module on which  $G_{\mathbf{Q}}$  acts through  $\text{Gal}(L/\mathbf{Q})$ , every  $G_{\mathbf{Q}_2}$ -stable subgroup of  $M$  is  $G_{\mathbf{Q}}$ -stable.*

*Proof.* Let  $G = \text{Gal}(L/\mathbf{Q})$  and  $D \subset G$  a decomposition group at 2. If  $D \neq G$ , then  $D$  lies in a maximal subgroup  $H$  of the 2-group  $G$ , which is normal of index 2, and  $L^H$  is a quadratic field unramified outside  $S$  in which 2 splits, since  $D$  maps trivially to  $G/H$ . This contradicts Lemma 5.1.  $\square$

**Lemma 5.3** (Infinite level). *Let  $S$  be as in Lemma 5.2, and let  $A/\mathbf{Q}$  be an abelian variety with good reduction outside  $S$  such that  $\text{Gal}(\mathbf{Q}(A[2])/\mathbf{Q})$  is a 2-group. Then the image of  $G_{\mathbf{Q}_2}$  in  $\text{Aut}(T_2(A))$  equals the image of  $G_{\mathbf{Q}}$ . Consequently every  $G_{\mathbf{Q}_2}$ -stable submodule of  $T_2(A)$  is  $G_{\mathbf{Q}}$ -stable, and  $G_{\mathbf{Q}}$  acts on it through the image of  $G_{\mathbf{Q}_2}$ .*

*Proof.* Let  $L_n = \mathbf{Q}(A[2^n])$ . Each  $\text{Gal}(L_n/\mathbf{Q})$  is a 2-group, since its image in  $\text{GL}_{2g}(\mathbf{Z}/2^n)$  maps onto a 2-group in  $\text{GL}_{2g}(\mathbf{F}_2)$  with kernel a 2-group; and  $L_n$  is unramified outside  $S \cup \{\infty\}$  by good reduction. By Lemma 5.2,  $G_{\mathbf{Q}_2}$  surjects onto  $\text{Gal}(L_n/\mathbf{Q})$  for every  $n$ . Hence the image of  $G_{\mathbf{Q}_2}$  in  $\text{Gal}(L_\infty/\mathbf{Q}) = \varprojlim \text{Gal}(L_n/\mathbf{Q})$ , which is closed, is dense, so is everything.  $\square$

**Lemma 5.4** (Abelian 2-extensions). *Let  $p$  be an odd prime,  $m_p = 2^{v_2(p-1)}$ , and  $F_p$  the subfield of  $\mathbf{Q}(\zeta_p)$  of degree  $m_p$ . Every abelian pro-2 extension of  $\mathbf{Q}$  unramified outside  $\{2, p, \infty\}$  is contained in  $M_p = \mathbf{Q}(\zeta_{2^\infty})F_p$ . One has  $\text{Gal}(M_p/\mathbf{Q}) = \text{Gal}(M_p/F_p) \times \text{Gal}(M_p/\mathbf{Q}(\zeta_{2^\infty})) \simeq \mathbf{Z}_2^\times \times \mathbf{Z}/m_p$ , and  $\text{Gal}(M_p/F_p)$  is the inertia group at 2, identified with  $\mathbf{Z}_2^\times$  by the cyclotomic character. The same holds for  $\{2, \infty\}$  with  $F_p$  replaced by  $\mathbf{Q}$  and  $m_p$  by 1.*

*Proof.* By Kronecker–Weber the maximal abelian extension of  $\mathbf{Q}$  unramified outside  $\{2, p, \infty\}$  is  $\mathbf{Q}(\zeta_{2^\infty p^\infty})$ , with group  $\mathbf{Z}_2^\times \times \mathbf{Z}_p^\times$ , whose maximal pro-2 quotient is  $\mathbf{Z}_2^\times \times \mathbf{Z}/m_p$  with fixed field  $M_p$ . The field  $F_p$  is unramified at 2 and  $\mathbf{Q}(\zeta_{2^\infty})$  is totally ramified at 2, so the inertia group at 2 of  $M_p/\mathbf{Q}$  is  $\text{Gal}(M_p/F_p)$ , on which  $\chi$  is an isomorphism onto  $\mathbf{Z}_2^\times$ .  $\square$

*Proof of Theorem 1.3.* Let  $S = \{2, p\}$  or  $\{2\}$ , and let  $V_2(\mathcal{T}) \subset V_2(A)$  be the toric part of the Raynaud uniformization of  $A$  over  $\mathbf{Q}_2$  (Lemma 3.4). By Lemma 5.3 the subspace  $V_2(\mathcal{T})$  is  $G_{\mathbf{Q}}$ -stable and the representation

$$\rho_{\mathcal{T}} : G_{\mathbf{Q}} \longrightarrow \text{Aut}(V_2(\mathcal{T}))$$

has the same image as its restriction to  $G_{\mathbf{Q}_2}$ . By Lemma 3.4(i) this image is abelian, and it is pro-2, being a quotient of  $\text{Gal}(L_\infty/\mathbf{Q})$ . As  $\rho_{\mathcal{T}}$  is unramified outside  $S \cup \{\infty\}$ , Lemma 5.4 shows that it factors through  $\text{Gal}(M_p/\mathbf{Q}) \simeq \mathbf{Z}_2^\times \times \mathbf{Z}/m_p$  (with  $m_p = 1$  if  $S = \{2\}$ ).

The factor  $\mathbf{Z}_2^\times$  is the inertia group at 2, and by Lemma 3.4(i) an inertia element  $\sigma$  acts on  $V_2(\mathcal{T})$  as the scalar  $\chi(\sigma)$ ; so  $\rho_{\mathcal{T}}(a, 1) = a$  for  $a \in \mathbf{Z}_2^\times$ . Put  $M = \rho_{\mathcal{T}}(1, \gamma)$  for a generator  $\gamma$  of  $\mathbf{Z}/m_p$ ; then  $M^{m_p} = 1$ . Let  $q \notin S$  be a prime, so that  $A$  has good reduction at  $q$ , and let  $\text{Frob}_q \in \text{Gal}(M_p/\mathbf{Q})$  be the arithmetic Frobenius. Its image in  $\mathbf{Z}_2^\times$  is  $q$ , so

$$\rho_{\mathcal{T}}(\text{Frob}_q) = q \cdot M^j \quad \text{for some } j,$$

whose eigenvalues all have complex absolute value  $q$ . But  $V_2(\mathcal{T})$  is a  $\text{Frob}_q$ -stable subspace of  $V_2(A)$ , on which every eigenvalue of  $\text{Frob}_q$  has absolute value  $\sqrt{q}$  by the Weil bound. Hence  $V_2(\mathcal{T}) = 0$ , i.e.  $t = 0$ , and  $A$  has good reduction at 2 by Lemma 3.4(ii).  $\square$

**Remark 5.5.** The condition  $p \equiv 3, 5 \pmod{8}$  is necessary. For  $p \equiv \pm 1 \pmod{8}$  the field  $\mathbf{Q}(\sqrt{p^*})$  is split at 2, and indeed the elliptic curves 14a (conductor  $2 \cdot 7$ , torsion  $\mathbf{Z}/6$ ), 34a ( $2 \cdot 17$ , torsion  $\mathbf{Z}/6$ ) and 46a ( $2 \cdot 23$ , torsion  $\mathbf{Z}/2$ ) are semistable at 2 with a rational 2-torsion point [LMF26]. Conversely, for  $p \in \{3, 19, 29\}$  no elliptic curve of conductor  $2p^k$  has a point of order 2 (there are no curves of conductor 18, and those of conductors 54, 162, 486, 38, 58 have torsion of odd order), in accordance with Theorem 1.3.

**Remark 5.6.** Under the hypotheses of Theorem 1.3 one can in fact show that  $A = 0$  for every  $p \equiv 3, 5 \pmod{8}$ . Since  $A$  has good reduction at 2, each  $A[2^n]$  is a finite flat group scheme over  $\mathbf{Z}_2$  with connected-étale sequence  $0 \rightarrow C_n \rightarrow A[2^n] \rightarrow E_n \rightarrow 0$ . The connected part  $C_n$  has 2-group Galois image, so by Tate–Oort [TO70] (a connected group scheme of order 2 over  $\mathbf{Z}_2$  is  $\mu_2$ ) and induction it is filtered by copies of  $\mu_2$ , hence is of multiplicative type and  $X_n = \text{Hom}(C_n, \mu_{2^n})$  is unramified at 2. By Lemma 5.2,  $E_n$  and  $X_n$  are  $G_{\mathbf{Q}}$ -modules; they are unramified outside  $\{p, \infty\}$  with 2-group image. A Galois 2-extension of  $\mathbf{Q}$  unramified outside  $\{p, \infty\}$  has a unique quadratic subfield, namely  $\mathbf{Q}(\sqrt{p^*})$ , so its group has cyclic Frattini quotient and is cyclic; by Kronecker–Weber the extension lies in  $F_p$ . Hence  $G_{\mathbf{Q}}$  acts on  $E_n$  and  $X_n$  through  $\text{Gal}(F_p/\mathbf{Q})$ , of exponent  $m_p$ . For  $q \notin S$  this gives  $(\text{Frob}_q^{m_p} - q^{m_p})(\text{Frob}_q^{m_p} - 1) = 0$  on  $A[2^n]$  for all  $n$ , hence on  $V_2(A)$ , contradicting the Weil bound. For the main theorem this is not needed, since for  $p \in \{3, 5\}$  the vanishing of  $A$  follows from [BK01].

**Remark 5.7.** Theorem 1.3 and its proof are an  $l = p$  analogue of [BK01, Prop. 4.3], which shows that a semistable abelian variety over  $\mathbf{Q}$  with good reduction outside a single prime  $p$  and nilpotent  $\text{Gal}(\mathbf{Q}(A[2])/\mathbf{Q})$  must have  $p \equiv 1 \pmod{4}$ . Brumer and Kramer also pass from  $A[2]$  to the pro-2 extension  $\mathbf{Q}(A[2^\infty])$  and use Kronecker–Weber to show that the decomposition group at  $p$  is everything; the contradiction is then obtained from an isogeny which raises their “effective stage of inertia” at  $p$ , where we instead use the Frobenius eigenvalues on the toric part at 2. In the same spirit, [BK04, Thm. 1.1] shows that if  $A$  is semistable with bad reduction only at  $p$  and  $\text{Gal}(\mathbf{Q}(A[2])/\mathbf{Q}(i))$  is nilpotent, then the reduction of  $A$  at  $p$  is totally toric and  $p \equiv 1 \pmod{8}$ ; the second conclusion gives another proof of the vanishing of  $A$  in the previous remark.

## 6. THE TWO-DIVISION FIELDS FOR $p = 3$ AND $p = 5$

In this section  $p \in \{3, 5\}$  and  $A/\mathbf{Q}$  is a semistable abelian variety with good reduction outside  $\{2, p\}$ . Let  $\mathcal{K}$  be the set of Galois subfields of  $\mathbf{Q}(A[2])$ . Each  $K \in \mathcal{K}$  is unramified outside  $\{2, p, \infty\}$ , has tame ramification index at most 2 at  $p$ , and has 2-adic upper ramification groups trivial above 2 (Theorem 1.2, and compatibility of upper numbering with quotients). By Proposition 4.3,  $[K : \mathbf{Q}] \leq 20$  for  $p = 3$  and  $[K : \mathbf{Q}] \leq 37$  for  $p = 5$ .

**Lemma 6.1.** *For every  $K \in \mathcal{K}$  the maximal abelian subfield satisfies  $K^{\text{ab}} \subset \mathbf{Q}(\zeta_8, \sqrt{p})$ . In particular  $\text{Gal}(K/\mathbf{Q})^{\text{ab}}$  is an elementary abelian 2-group of rank at most 3.*

*Proof.* For an abelian extension, upper jumps  $\leq 2$  at 2 means conductor exponent  $\leq 3$  at 2, and tameness at  $p$  means conductor exponent  $\leq 1$  at  $p$ ; so  $K^{\text{ab}} \subset \mathbf{Q}(\zeta_{8p})$  by Kronecker–Weber. Its inertia group at  $p$ , a quotient of  $(\mathbf{Z}/p)^\times$ , has order at most 2, so  $K^{\text{ab}}$  lies in the fixed field of the subgroup of order  $(p-1)/2$  of  $(\mathbf{Z}/p)^\times$ , which is  $\mathbf{Q}(\zeta_8, \sqrt{p^*}) = \mathbf{Q}(\zeta_8, \sqrt{p})$  for  $p = 3, 5$ . This field has Galois group  $(\mathbf{Z}/2)^3$ .  $\square$

**Lemma 6.2** (Quadratic ray class groups). *Let  $p \in \{3, 5\}$  and let  $F$  be a quadratic field unramified outside  $\{2, p, \infty\}$ . Then  $F$  has no non-trivial abelian extension of odd degree unramified outside the primes above 2 and the infinite places.*

*Proof.* For the 11 possible fields  $F$  of discriminants

$$\{-3, -4, 5, 8, -8, 12, -20, 24, -24, 40, -40\},$$

one first checks that the class group in each case has order at most 2. To show that the ray class groups of conductor  $2^k \infty$  are also 2-groups, it suffices to note that  $\mathcal{O}_{F,2}^\times$  is a pro-2 group whenever 2 is ramified in  $F$ , which covers every case except for  $F = \mathbf{Q}(\sqrt{-3})$  and  $F = \mathbf{Q}(\sqrt{5})$  where

$(\mathcal{O}_F/2)^\times = \mathbf{F}_4^\times$ . In those two latter cases, the image of the global units  $\zeta_3$  and  $\phi = (1 + \sqrt{5})/2$  each have order 3 modulo 2 and so the result follows from class field theory.  $\square$

**Proposition 6.3.** *Every field in  $\mathcal{K}$  is a 2-extension of  $\mathbf{Q}$ . Hence  $\text{Gal}(\mathbf{Q}(A[2])/\mathbf{Q})$  is a 2-group.*

*Proof.* Suppose not, and let  $K \in \mathcal{K}$  be of minimal degree with  $G = \text{Gal}(K/\mathbf{Q})$  not a 2-group;  $\mathcal{K}$  is closed under passing to Galois subfields. Since  $|G| \leq 37 < 60$ ,  $G$  is solvable.

The largest normal 2-subgroup  $O_2(G)$  is trivial: otherwise  $K^{O_2(G)} \in \mathcal{K}$  has smaller degree, so  $G/O_2(G)$  and then  $G$  would be 2-groups. Let  $M$  be a minimal non-trivial normal subgroup of  $G$ ; it is elementary abelian,  $M \simeq \mathbf{F}_l^r$  with  $l$  odd by the previous sentence. By minimality of  $K$ ,  $\Gamma = G/M$  is a 2-group, and  $G = M \rtimes \Gamma$  by Schur–Zassenhaus. The action of  $\Gamma$  on  $M$  is irreducible,  $M$  being minimal normal, and faithful: the kernel of the action of a complement  $\Gamma$  centralizes  $M$  and is normal in  $\Gamma$ , hence is a normal 2-subgroup of  $G$ , hence trivial.

If  $\Gamma$  is non-abelian then  $|\Gamma| \geq 8$ , and  $r \geq 2$  because a faithful one-dimensional representation would embed  $\Gamma$  in  $\mathbf{F}_l^\times$ . Then  $|G| = l^r |\Gamma| \geq 9 \cdot 8 = 72 > 37$ , a contradiction. So  $\Gamma$  is abelian. The image of  $\mathbf{F}_l[\Gamma]$  in  $\text{End}(M)$  is a commutative algebra which is a field by irreducibility, so  $\Gamma$  embeds in the multiplicative group of a finite field and is cyclic. Being an abelian quotient of  $G$ , it has exponent at most 2 by Lemma 6.1, and it is non-trivial since otherwise  $G = M$  would be an abelian group of odd order, again contradicting Lemma 6.1. So  $\Gamma \simeq \mathbf{Z}/2$ , and since its irreducible representations over  $\mathbf{F}_l$  are one-dimensional,  $r = 1$ .

Thus  $F = K^M$  is a quadratic field unramified outside  $\{2, p\}$ , and  $K/F$  is cyclic of odd prime degree  $l$ . An inertia group of  $K/\mathbf{Q}$  at a prime over  $p$  has order at most 2 and meets  $M$  trivially, so  $K/F$  is unramified at the primes over  $p$ , hence unramified outside the primes over 2 and  $\infty$ . This contradicts Lemma 6.2.  $\square$

*Proof of Theorem 1.1.* By Proposition 6.3,  $\text{Gal}(\mathbf{Q}(A[2])/\mathbf{Q})$  is a 2-group, and Theorem 1.3 applies with  $p = 3$  or  $p = 5$  (both  $\equiv 3, 5 \pmod{8}$ ):  $A$  has good reduction at 2. Thus  $A$  is a semistable abelian variety over  $\mathbf{Q}$  with good reduction outside  $\{p\}$ , and  $A = 0$  by Brumer–Kramer [BK01].  $\square$

## REFERENCES

- [Abr87] V. A. Abrashkin, *Galois modules of group schemes of period  $p$  over the ring of Witt vectors*, Izv. Akad. Nauk SSSR Ser. Mat. **51** (1987), no. 4, 691–736, English translation: Math. USSR-Izv. **31** (1988), no. 1, 1–46. [1](#)
- [BCC04] Alessandra Bertapelle, Maurizio Candilera, and Valentino Cristante, *Monodromy of logarithmic Barsotti–Tate groups attached to 1-motives*, J. Reine Angew. Math. **573** (2004), 211–234. MR 2084588 [5](#)
- [BK01] Armand Brumer and Kenneth Kramer, *Non-existence of certain semistable abelian varieties*, Manuscripta Math. **106** (2001), no. 3, 291–304. MR 1869222 [1](#), [2](#), [8](#), [9](#)
- [BK04] ———, *Semistable abelian varieties with small division fields*, Galois theory and modular forms, Dev. Math., vol. 11, Kluwer Acad. Publ., Boston, MA, 2004, pp. 13–37. [8](#)
- [BL91] Siegfried Bosch and Werner Lütkebohmert, *Degenerating abelian varieties*, Topology **30** (1991), no. 4, 653–698. MR 1133878 [3](#), [4](#)
- [Cal04] Frank Calegari, *Semistable abelian varieties over  $\mathbf{Q}$* , Manuscripta Math. **113** (2004), no. 4, 507–529. MR 2129874 [1](#)
- [CG25] Francesco Campagna and Pip Goodman, *Semistable abelian varieties over  $\mathbf{Q}$  with bad reduction at 19 only: an overview of the Fontaine–Schoof strategy*, 2025, Preprint, [arXiv:2510.12625](#). [2](#)
- [CL11] Xavier Caruso and Tong Liu, *Some bounds for ramification of  $p^n$ -torsion semi-stable representations*, J. Algebra **325** (2011), 70–96. MR 2745530 [2](#), [3](#)
- [Con] Brian Conrad, *Semistable reduction for abelian varieties*, Notes for the Stanford Number Theory Learning Seminar on Faltings’ proof of the Mordell conjecture, 2010–11, <https://math.stanford.edu/~conrad/mordellsem/Notes/L13.pdf>. [5](#)
- [Del74] Pierre Deligne, *Théorie de Hodge. III*, Inst. Hautes Études Sci. Publ. Math. (1974), no. 44, 5–77. MR 498552 [4](#), [5](#)
- [FC90] Gerd Faltings and Ching-Li Chai, *Degeneration of abelian varieties*, Ergebnisse der Mathematik und ihrer Grenzgebiete (3), vol. 22, Springer-Verlag, Berlin, 1990, With an appendix by David Mumford. MR 1083353 [3](#)
- [Fon85] Jean-Marc Fontaine, *Il n’y a pas de variété abélienne sur  $\mathbf{Z}$* , Invent. Math. **81** (1985), no. 3, 515–538. MR 807070 [1](#), [2](#), [6](#)
- [Gro72] Alexander Grothendieck, *Modèles de Néron et monodromie*, Groupes de monodromie en géométrie algébrique. I (SGA 7 I), Lecture Notes in Mathematics, vol. 288, Springer-Verlag, Berlin-New York, 1972, Exposé IX, pp. 313–523. MR 0354656 [4](#), [6](#)

- [Gun21] Christopher Gunton, *Semistable abelian varieties and maximal torsion 1-crystalline submodules*, J. Théor. Nombres Bordeaux **33** (2021), no. 1, 39–81. MR 4292382 [5](#), [6](#)
- [Hat09] Shin Hattori, *On a ramification bound of torsion semi-stable representations over a local field*, J. Number Theory **129** (2009), no. 10, 2474–2503. MR 2541027 [2](#), [3](#)
- [LMF26] LMFDB Collaboration, *The L-functions and modular forms database*, 2026, <https://www.lmfdb.org>. [8](#)
- [Odl76] A. M. Odlyzko, *Discriminant bounds*, 1976, Unpublished tables, Table 2 (unconditional bounds) and accompanying description, <https://www-users.cse.umn.edu/~odlyzko/unpublished/>. [1](#), [6](#)
- [Odl90] ———, *Bounds for discriminants and related estimates for class numbers, regulators and zeros of zeta functions: a survey of recent results*, Sémin. Théor. Nombres Bordeaux (2) **2** (1990), no. 1, 119–141. MR 1061762 [1](#)
- [Ray71] Michel Raynaud, *Variétés abéliennes et géométrie rigide*, Actes du Congrès International des Mathématiciens (Nice, 1970), Tome 1, Gauthier-Villars Éditeur, Paris, 1971, pp. 473–477. MR 0427326 [3](#)
- [Ray94] ———, *1-motifs et monodromie géométrique*, Périodes  $p$ -adiques (Bures-sur-Yvette, 1988), Astérisque, vol. 223, Société Mathématique de France, Paris, 1994, pp. 295–319. MR 1293976 [4](#), [5](#), [6](#)
- [Sch05] René Schoof, *Abelian varieties over  $\mathbf{Q}$  with bad reduction in one prime only*, Compos. Math. **141** (2005), no. 4, 847–868. MR 2148198 [1](#), [2](#), [6](#)
- [Sch12a] ———, *On the modular curve  $X_0(23)$* , Geometry and arithmetic, EMS Ser. Congr. Rep., Eur. Math. Soc., Zürich, 2012, pp. 317–345. [2](#)
- [Sch12b] ———, *Semistable abelian varieties with good reduction outside 15*, Manuscripta Math. **139** (2012), no. 1-2, 49–70. [2](#)
- [Ser68] Jean-Pierre Serre, *Corps locaux*, Publications de l’Université de Nancago, No. VIII, Hermann, Paris, 1968. MR 0354618 [2](#)
- [TO70] John Tate and Frans Oort, *Group schemes of prime order*, Ann. Sci. École Norm. Sup. (4) **3** (1970), 1–21. MR 265368 [8](#)